SECURITY FOR VIRTUALIZATION:

SICHERHEIT UND LEISTUNG IM GLEICHGEWICHT

Kombinieren Sie Sicherheit und Leistung
in Ihrer virtualisierten Umgebung.

www.kaspersky.de/beready

KASPERSKY lab

Einleitung

> Im Endeffekt handelt es sich immer um Server, die irgendjemand von irgendwo aus knacken will.“
> John Sawyer

Laut einer Umfrage von Forrester haben 85 % der befragten Unternehmen bereits eine Server-Virtualisierung vorgenommen oder planen dies.[1]

Führende Analysten belegen in einer anderen Studie ebenfalls die zunehmende Virtualisierung in Unternehmen und schätzen, dass bis Ende 2012 50 % aller Arbeitslasten auf Servern mit x86-Architektur in einer virtualisierten Umgebung ausgeführt werden.[2]

Die Virtualisierung entwickelt sich damit zwar zu einem Standardverfahren, die Sicherheit dieser virtualisierten Umgebungen lässt aber immer mehr zu wünschen übrig.

In einer weiteren Studie wird sogar angenommen, dass „...2012 60 % aller virtualisierten Server unsicherer sind als die Server, deren Platz sie eingenommen haben.“ [3]

Dabei ist die Gefahr durch Sicherheitsbedrohungen, insbesondere Malware-Bedrohungen, so hoch wie nie zu vor.

John Sawyer von der einflussreichen Technologie-Seite Tech Center beschreibt dies so:
„Im Endeffekt handelt es sich immer um Server, die irgendjemand von irgendwo aus knacken will.“ [4]

Doch wo liegen die Gründe für die offenkundig paradoxe Entwicklung zunehmender Virtualisierung bei abnehmender Sicherheit?

Hauptsächlich in der Auffassung, dass eine virtuelle Maschine sicherer ist als eine physische:

- durch Leistungs- und Sicherheitsprobleme aufgrund herkömmlicher agentenbasierter Anti-Malware-Lösungen in virtualisierten Umgebungen
- durch unzureichenden Schutz und erhöhte Verwaltungskosten von agentenlosen Anti-Malware-Lösungen

Bislang steht fest, dass die Optionen zum Schutz virtueller Maschinen zu einem unvorteilhaften Kompromiss zwischen Sicherheit, Leistung und Verwaltung geführt haben.

1 | The CISO's Guide to Virtualization Security, Forrester Research, Inc., Januar 2012
2 & 3 | Gartner: Virtualization security will take time, SCMagazine.com, März 2012
4 | Tech Insight: Keeping Server Virtualization Secure, John Sawyer auf Darkreading.com, Mai 2009

Wahrung der Vorteile einer Virtualisierung durch ausgewogenen Schutz

1.0

Die Eindämmung des „Server-Wildwuchses“ durch eine Virtualisierung von Servern und Desktop-Computern bringt enorme geschäftliche Vorteile.

Beispiele:

- Kosteneindämmung: Durch Virtualisierung lässt sich die gesamte Hardware-Bilanz reduzieren. Die Folge: geringere Ausgaben für Hardware, weniger Platzbedarf, niedrigerer Energieverbrauch, geminderter Verwaltungsbedarf usw.
- Geschwindigkeit: Dank der Virtualisierung lässt sich die IT-Bereitstellungszeit durch neue On-Demand-Kapazität beschleunigen. Unterm Strich führt diese Flexibilität zu einer erhöhten Wettbewerbsfähigkeit des gesamten Unternehmens.
- Stabilität: Einfachere, redundante Standardsysteme führen zu erhöhter Widerstandsfähigkeit und besserer Systemverfügbarkeit, so dass Mitarbeiter zu jedem Zeitpunkt und an allen Standorten produktiver arbeiten können.
- Zentrale Verwaltung: Virtualisierte Systeme können bei Bedarf sofort zentral erstellt, verwaltet und konfiguriert werden, so dass sich die Verwaltungs- und Supportkosten senken lassen.
- BS-Migrationen: In virtualisierten Umgebungen können BS-Migrationen schneller und einfacher vorgenommen werden und erfordern einen niedrigeren Grad an laufender Instandhaltung.

Virtualisierte Systeme werden mit zunehmender Verbreitung auch immer mehr zum Ziel von Cyberkriminellen. Unzureichender Schutz kann innerhalb kürzester Zeit alle Vorteile einer virtualisierten IT-Infrastruktur zunichtemachen.

Hinzu kommt, dass die Implementierung von Antiviren-Software die gesamte virtualisierte Infrastruktur verlangsamen kann, wodurch die Konsolidierungsraten reduziert und der Return on Investment (kurz: ROI) eingeschränkt werden.

IT-Abteilungen stehen vor der Herausforderung, eine heterogene IT-Landschaft bestehend aus virtualisierten und physischen Komponenten gleichermaßen effektiv schützen und dabei die Leistungsfähigkeit des gesamten IT-Systems sicherstellen zu müssen.

In diesem Whitepaper werden drei Ansätze zum Thema Sicherheit und ihre Auswirkungen auf den ROI von Virtualisierung beschrieben.
Außerdem erhalten Sie Ratschläge dazu, wie Sie Ihre virtualisierte Umgebung sowie die physischen und mobilen Umgebungen am besten schützen können.

Die Option KEIN SCHUTZ

2.0

> In den letzten 15 Monaten hat sich die Cyberkriminalität auf Unternehmen mit wertvollen Daten verlagert, die sich gewinnbringend verkaufen lassen. Cyber-Gangs weiten ihre Aktivitäten immer mehr auf Unternehmen aus.“
> Roel Schouwenberg, Senior Researcher bei Kaspersky Lab

Eine allgemeine, aber falsche Auffassung ist, dass virtuelle Maschinen sicherer seien als Physische.

Zwar sind virtuelle Maschinen widerstandsfähiger gegenüber Angriffen durch Spyware und Ransomware, zeigen aber die gleichen Schwachstellen wie physische Maschinen gegenüber Malware in Form von bösartigen E-Mail-Anhängen, Drive-by-Downloads, Botnet-Trojanern und selbst zielgerichteten Spearfishing-Angriffen.

Diese Bedrohungen bleiben so lange bestehen, wie das virtualisierte System aktiv und in Verwendung ist. Nach Aussagen des National Institute of Standards and Technology „werden durch Virtualisierung Technologie-Ebenen hinzugefügt, was ein erhöhtes Sicherheitsmanagement und somit zusätzliche Sicherheitsüberwachung erforderlich macht. Das Zusammenfassen einer Reihe von Systemen in einem einzigen physischen Computer kann bei einer Sicherheitsgefährdung scherwiegendere Auswirkungen haben. Außerdem basieren Virtualisierungssysteme auf einer Infrastruktur mit gemeinsam genutzten Ressourcen, die eine gefährliche Angriffsmöglichkeit bietet, da sich eine einzige infizierte Maschine auf die gesamte virtualisierte Infrastruktur auswirkt.“ [5]

Weitere Risiken in der virtualisierten Umgebung:

- Durch Infizierung einer virtuellen Maschine können die Datenspeicher anderer virtueller Maschinen beschädigt und der Angriff so auf andere Systeme und Daten ausgeweitet werden.
- Eine infizierte virtuelle Maschine kann für Lauschangriffe auf den Datenverkehr einer anderen virtuellen Maschine eingesetzt werden.
- Herkömmliche Malware zielte ursprünglich nicht auf virtualisierte Systeme ab – heutige Malware-Programme allerdings enthalten Codes, die Angriffe nicht nur auf physische, sondern auch auf virtuelle Maschinen durchführen können.
- Einige Malware-Programme überleben sogar ein Abrüsten nicht-persistenter virtueller Maschinen, werden also wieder aktiv, wenn die virtuelle Maschine wieder in Betrieb genommen wird.

Zudem konzentriert sich die Cyberkriminalität nicht mehr nur auf Privatkonsumenten, sondern zunehmend auf Unternehmen.

Roel Schouwenberg, Senior Researcher bei Kaspersky Lab, sagt dazu: „In den letzten 15 Monaten hat sich die Cyberkriminalität auf Unternehmen mit wertvollen Daten verlagert, die sich gewinnbringend verkaufen lassen. Cyber-Gangs weiten ihre Aktivitäten immer mehr auf Unternehmen aus.“

Der Anstieg von Bedrohungen durch Malware ist besorgniserregend.

Anfang 2011 waren in der Hauptdatenbank von Kaspersky Lab, dem führenden Anbieter von Antiviren-Software, noch 35 Millionen Bedrohungen aufgezeichnet. Ein Jahr später hatte sich diese Datenbank mit über 67 Millionen Einträgen fast verdoppelt. Inzwischen nimmt Kaspersky Lab täglich durchschnittlich 70.000 neue Bedrohungen in die Datenbank auf. Heutzutage enthält einer von 14 Web-Downloads Malware. Die Anfälligkeit für solche Angriffe ist unter physischen und virtuellen Maschinen gleich hoch. Fazit: Der Bedarf an erstklassigen Schutzfunktionen sowohl für die physische als auch für die virtuelle Umgebung liegt so hoch wie nie zuvor.

5 | Guide to Security for Full Virtualization Technologies National Institute of Standards & Technology

Die Option
AGENTENBASIERTER SCHUTZ

3.0

Viele Unternehmen arbeiten mit der herkömmlichen, agentenbasierten Antiviren-Methode.

Dabei wird eine Vollversion der Antiviren-Software auf jede virtuelle Maschine geladen. Dieser Ansatz bietet zwar u. U. umfassenden Schutz, die Kosten für eine Bereitstellung redundanter Software über eine gemeinsam genutzte Ressource sind allerdings enorm hoch.

Beim Laden der Antiviren- und Signaturdatenbanken auf die einzelnen virtuellen Maschinen wirken sich die zugrunde liegenden redundanten Ressourcenanforderungen negativ auf Festplattenspeicher, Arbeitsspeicher und CPU-Verfügbarkeit aus. Dadurch erhöht sich die Hardware-Auslastung, was wiederum zu Leistungseinbußen führt. Präzise Symptome:

- Ressourcenkonflikte
- Scan-Storms: Wenn geplante Scan-Vorgänge auf mehreren virtuellen Maschinen gleichzeitig gestartet werden, wird die Rechenleistung des Hostcomputers möglicherweise erheblich beeinträchtigt. Dies kann zur Überlastung des Hosts und zu Leistungsproblemen (mit der Gefahr eines Host-Absturzes) führen.
- I/O-Storms: Diese treten ähnlich wie Scan-Storms auf, wenn alle virtuellen Maschinen mit lokalen Signaturdatenbanken Updates gleichzeitig herunterladen.
- Duplizierung/Redundanz: Durch Duplizierung von Signaturdatenbanken und Scannen redundanter Dateien werden wertvolle Systemressourcen unnötig belastet.

- „Instant-on“-Lücken
  Virtuelle Maschinen können schnell stillgelegt werden und über lange Zeiträume offline bleiben. Wenn sie wieder aktiviert werden, sind möglicherweise Sicherheitslücken vorhanden, z. B. fehlende Patches für Software und veraltete Viren-Signaturdatenbanken.

- Transparenz bei VM-Wildwuchs und Sicherheit
  Virtuelle Maschinen können in wenigen Minuten eingerichtet werden, oft ohne Wissen oder Genehmigung der IT-Abteilung. Die Transparenz des Systems wird somit zum Problem – virtuelle Maschinen, die nicht sichtbar sind, können auch nicht geschützt werden.

Ein agentenbasierter Antiviren-Schutz in virtualisierten Umgebungen, besonders bei virtualisierten Desktop-Computern, wirkt sich u. U. negativ auf den ROI aus, da die Leistungsfähigkeit des Gastcomputers beeinträchtigt und die Dichte des virtualisierten Clusters eingeschränkt werden.

Die Option
AGENTENLOSER SCHUTZ

4.0

Aufgrund der zunehmenden Verbreitung virtualisierter Systeme entwickeln Anbieter von Antiviren-Software jetzt Programme speziell für virtuelle Umgebungen.

Ein virtualisiertes Gerät kann somit Antiviren-Schutz für viele virtuelle Maschinen bereitstellen. Dies führt zu einer Leistungssteigerung, da die Antiviren-Prozesse nicht mehr auf jeder einzelnen virtuellen Maschine ausgeführt werden müssen.
Die allgemeine Speicherauslastung wird daher reduziert, die Fähigkeiten der physischen Hardware werden erweitert und die Konsolidierungsraten (Dichte) erhöht.

Dieser agentenlose Ansatz hat zwar einen besseren ROI zur Folge, wirft aber zwei Probleme auf, die gelöst werden müssen:

1. Eingeschränkter Schutz:

Einerseits umfasst die moderne agentenbasierte Antiviren-Software oft Schutzmodulschichten wie Anwendungssteuerung, Webfilter, Host-Angriffsschutz, eine Personal Firewall und weitere. Agentenlose Antiviren-Lösungen dagegen bieten für virtualisierte Umgebungen nur einen eingeschränkten Schutz, da sie lediglich herkömmliche Antiviren-Schutzfunktionen bereitstellen.

Sind die oben genannten robusten Tools nicht vorhanden, muss die übrige Engine zur Virenerkennung so gut wie möglich angelegt sein, um die Unzulänglichkeiten abzudecken, die andernfalls durch die zusätzlichen Schutzschichten aufgefangen würden.

Wenn die agentenlose Lösung in unabhängigen Tests nur schlechte Erkennungsraten aufweist, setzt sich das Unternehmen möglicherweise unbewusst vermeidbaren Risiken aus.

In manchen Fällen erfordern kritische Systeme zusätzlich agentenbasierte Antiviren-Lösungen. Anwendungen erforderlich. Die Folge ist eine Mischung beider Schutzmethoden, was zu erhöhten Verwaltungs- und Instandhaltungskosten führt.

2. Verwaltung des physischen und virtuellen Systems:

In allen Unternehmen mit virtualisierten Systemen ist die Verwaltung sowohl physischer als auch virtualisierter Umgebungen erforderlich.

Dazu sind mehrere Verwaltungskonsolen notwendig, da beide Umgebungen separat verwaltet und instand gehalten werden müssen. Es fallen also doppelte Verwaltungskosten an.

Agentenlose Antiviren-Lösungen stellen zweifellos einen guten Schritt in Richtung Effizienz dar, aber eine nicht geeignete agentenlose Lösung kann sich negativ auf den angestrebten ROI auswirken.

Die Option:
RICHTIGER SCHUTZ

5.0

Die überwiegende Mehrheit der IT-Experten stimmt darin überein, dass es keine Option ist, überhaupt keinen Antiviren-Schutz einzusetzen.

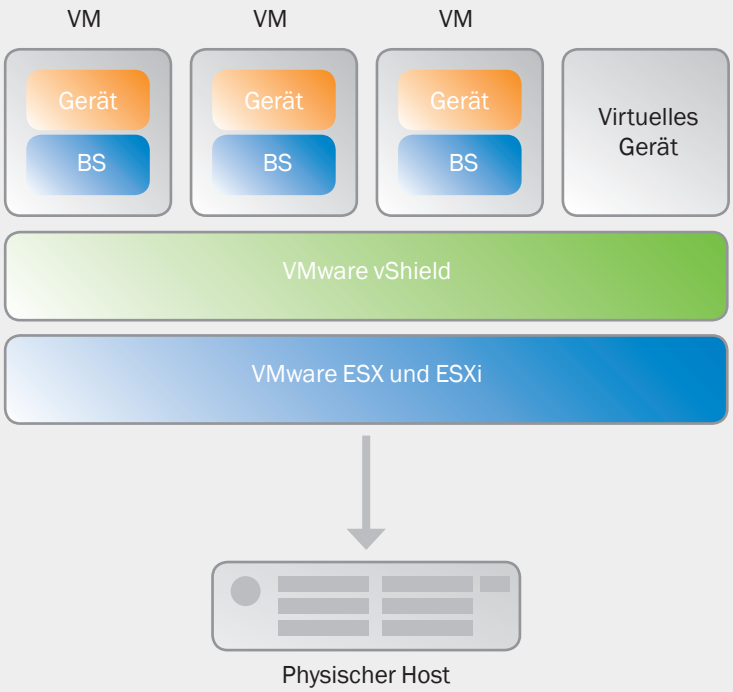
Wenn der ROI und andere durch die Servervirtualisierung ermöglichte Geschäftsziele durch einen Schutz nicht beeinträchtigt werden sollen, bleiben also die mängelbehafteten Alternativen einer agentenbasierten oder agentenlosen Antiviren-Lösung für virtuelle Systeme – oder der Mittelweg einer Kombination beider Ansätze.

Diese „richtige Schutzoption“ umfasst ein in den vShield Endpoint von VMware integriertes virtuelles Gerät, das Anti-Malware-Scanfunktionen in Echtzeit für alle Gäste auf einem physischen Host bereitstellt. Der Endpoint verwendet ein virtualisiertes Gerät auf dem Host, das über einen kleinen Treiber mit allen virtuellen Maschinen verbunden ist. Der Treiber überträgt die Scan- und Aktualisierungsvorgänge von den einzelnen virtuellen Maschinen auf das virtuelle Gerät.

Dadurch lässt sich eine Überlastung der Host-Ressourcen vermeiden. Der Volleinsatz mehrerer Antiviren-Agenten ist nicht mehr erforderlich, da das virtuelle Gerät, das als zentraler Hub agiert, die Auslastung des Hosts verringert.

Wie unten dargestellt, umfasst eine virtualisierte Sicherheitsplattform unter Verwendung eines VMware vShield Endpoint drei Komponenten:

1. vShield Manager: ein Modul, das über vShield Manager auf physischen Computern im vSphere Hypervisor installiert wird.
2. vShield Endpoint: ein automatisch auf allen virtuellen Maschinen installierter Sub-Agent zur Erfassung des Datei-Ereigniskontexts.



3. ein Sicherheitsgerät von einem Anti-Malware-Anbieter, das APIs für vShield Endpoint unterstützt.

vShield Endpoint verwendet das Netzwerk von vSphere 4.1 oder 5.0, um die Dateien dem jeweils ausgewählten Sicherheitsgerät zur Überprüfung bereitzustellen.

Auf diese Weise lassen sich die Probleme mit agentenbasierten und agentenlosen Sicherheitslösungen wie oben beschrieben überwinden:

- **Verwaltbarkeit/Transparenz/Agilität/Flexibilität:** eine einzelne Ansicht aller geschützten Maschinen (virtuelle und physische) zur einfachen Verwaltung. Der Schutzstatus, alle Sicherheitsereignisse und Berichte werden klar und auf benutzerfreundliche Weise angezeigt. Die logische und physische Struktur wird ähnlich wie bei den bekannten Verwaltungstools von VMware für Administratoren transparent dargestellt. Daher können Sicherheitsvorgänge wie Fehlerbeseitigung, Diagnosen und Forensik effektiv verwaltet und schnell ausgeführt werden.
- **Effektive Malware-Erkennung und -Beseitigung:** integrierte Anti-Malware-Technologie mit leistungsstarken Steuerungsfunktionen wie der Filterung von Web-Inhalten, Anwendungssteuerung und detaillierte Gerätesteuerung.
- **Effizienz:** Redundanz und Duplizierung der Antiviren-Engine oder -Datenbank treten nicht auf. Außerdem wird dieser Formfaktor den Anforderungen in Bezug auf Redundanz und Ressourcen verbunden mit agentenbasierten Antiviren-Programmen gerecht.
- **Automatischer Schutz, einfache Bereitstellung/Richtlinienkonformität:** Durch Kombination von vShield Endpoint Security und Anti-Malware-Technologie wird automatischer Schutz für virtualisierte VMware-Umgebungen gewährleistet. Nach Bereitstellung des virtuellen Geräts auf einem Host werden alle virtuellen Gastcomputer (ob bestehend oder neu erstellt) automatisch mit den neuesten Signaturen geschützt. (Eine zentrale Signatur-Datenbank steht für Schutz, der immer auf dem neuesten Stand ist, unabhängig davon, ob die virtuelle Maschine zuvor offline war). Dadurch lassen sich gleichzeitig viele Probleme mit der Richtlinienkonformität lösen.
- **Integration der Durchsetzung von Sicherheitsrichtlinien:** Dank der engen Integration mit der VMware-Plattform und den zugehörigen Tools wird der Schutz (und die Sicherheitseinstellungen) nahtlos an die sich zwischen verschiedenen Hosts bewegenden Arbeitslasten angepasst.
- Zudem können unterschiedliche Sicherheitseinstellungen flexibel für ausgewählte Gruppen virtueller Maschinen konfiguriert und auf sie angewendet werden. Weiterhin sind intensive Scans ausgewählter virtueller Maschinen möglich.

6.0 Schlussfolgerung

Die meisten Unternehmen sind am attraktiven Mehrwert, den Virtualisierung bietet, äußerst interessiert. Die Herausforderungen, die sich aus der Verwaltung herkömmlicher agentenbasierter und agentenloser virtualisierten Bestände ergeben, bedeuten jedoch eine erhebliche Einschränkung der potenziellen Vorteile.

Durch die richtige Schutzlösung lassen sich die Unzulänglichkeiten veralteter Schutzlösungen überwinden. Der Ansatz dazu entspricht dem der Virtualisierung selbst: Er ist flexibel, anpassbar und erweiterbar, ermöglicht einen schnellen ROI und stellt ein Gleichgewicht zwischen Sicherheit und Leistung her.

Security for Virtualization.
Bringen Sie mit Kaspersky Lab Sicherheit und Leistung ins Gleichgewicht.
www.kaspersky.de/beready
Be Ready for What's Next