PRAKTISCHER LEITFADEN

VIRTUALIZATION SECURITY

Tipps für den Schutz der Systeme und vertraulichen Daten Ihres Unternehmens

Erfolgreiches Business geht auf Nummer sicher!

kaspersky.de/business-security

#securebiz

KASPERSKY lab

INHALT

VORTEILE DER VIRTUALISIERUNG FÜR UNTERNEHMEN ALLER GRÖSSENORDNUNGEN

In der heutigen Wettbewerbslandschaft versuchen Unternehmen, ihre Effizienz zu steigern und Kosten zu senken. Virtualisierung ist nicht mehr nur ein Thema für internationale Konzerne und große Rechenzentren.
Die Aussichten sind vielversprechend:

- Ausführen von mehr Programmen und Services auf weniger Servern
- Senken der Hardwarebeschaffungskosten
- Senken der Betriebskosten bezogen auf Wartung, Platz- und Energiebedarf

… Virtualisierung ist oft ein wichtiger Bestandteil der Bemühungen von IT-Abteilungen weltweit, mit weniger Ressourcen mehr zu erreichen.

Aber unabhängig davon, ob Sie Programme auf physischen oder virtualisierten Maschinen ausführen, benötigen Sie Schutz vor der ständigen Zunahme an komplexer Malware und anderer Cyberbedrohungen, die Ihren alltäglichen Betrieb lahmlegen können, z. B. durch folgende Eingriffe:

- Unterbrechung von Geschäftsprozessen, Steigerung der Betriebskosten
- Diebstahl und Offenlegung vertraulicher Geschäftsdaten
- Verletzung der Sicherheit von Daten Ihrer Kunden und Lieferanten
- Verlust des Wettbewerbsvorteils, den Ihr Unternehmen durch geistiges Eigentum geschaffen hat

DAS IST MAX, DER FURCHTLOSE IT- UND SICHERHEITSEXPERTE

Als IT-Manager eines Unternehmens mit 150 Mitarbeitern kümmert sich Max um die physischen, virtualisierten und mobilen IT-Systeme und IT-Dienste seines Unternehmens. Zu seinem Zuständigkeitsbereich gehört auch der Betrieb aller Server, Desktops und mobilen Geräte. Darüber hinaus muss er dafür sorgen, dass die vertraulichen Daten des Unternehmens sicher bleiben.

Bei dieser Aufgabenvielfalt und den strengen Budgetvorgaben sucht Max beständig nach IT-Lösungen, die ihm dabei helfen, den Support zu vereinfachen, Routineaufgaben zu automatisieren und Kosten unter Kontrolle zu halten.

Die Vorgesetzten von Max verstehen natürlich nicht alle Einzelheiten der täglichen Schwierigkeiten, die er bewältigen muss – für sie zählt nur, dass alles funktioniert. Sie sind sich jedoch auch dessen bewusst, dass der Erfolg des Unternehmens immer mehr von der IT abhängt … und verlassen sich daher auf Max bei der Einführung neuer Technologien und IT-Dienste zur Verbesserung der Geschäftsabläufe, wobei wichtige Informationen nachhaltig geschützt bleiben müssen.

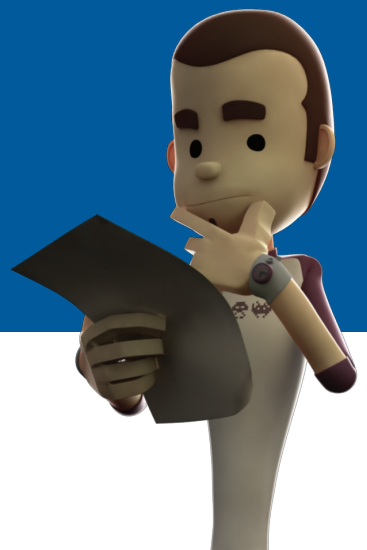
Obgleich die IT-Infrastruktur des Unternehmens geschäftskritische Abläufe ermöglicht hat, die in der Vergangenheit so nicht möglich gewesen wären, wird von Max ständig gefordert, mehr Leistung mit weniger Aufwand zu erbringen. Immer neue Sicherheitsbedrohungen und der ständige Kampf gegen Dienst- und Betriebsausfälle lassen Max in seinen tagtäglichen Aufgaben kaum Zeit, seine IT-Strategie weiter zu entwickeln.

Eine Nachricht von Max

„Für unsere ersten Virtualisierungsprojekte habe ich zunächst weniger wichtige Programme in eine virtualisierte Umgebung migriert. Zu diesem Zeitpunkt wollten wir die Migration wichtiger Programme noch hinauszögern.“

„Durch dieses Vorgehen gewannen wir wichtige Erfahrungen und Selbstvertrauen, bevor wir wichtige Geschäftsabläufe und Programme virtualisierten.“

„Mit dem, was wir in den ersten Projekten gelernt hatten, konnten wir einen reibungslosen Ablauf der späteren Projekte erzielen.“



SIND VIRTUALISIERTE UMGEBUNGEN SICHERER … ODER UNSICHERER?

Der Glaube, dass virtualisierte Umgebungen irgendwie sicherer seien als physische, ist ein Mythos. Obgleich diesem Glauben keine Wahrheit und keine Logik zugrunde liegen, kann er bei Unternehmen zu einem falschen Sicherheitsgefühl führen, wenn Sicherheitsanforderungen an ein Virtualisierungsprojekt formuliert werden.

Von den Schnittstellen und Interaktionen mit einer virtualisierten Maschine aus betrachtet, erscheint diese Maschine genau so, wie jede andere physische Maschine. Nur der Hypervisor (und das IT-Team!) wissen, dass es sich um eine virtualisierte Maschine handelt.

Tatsache ist, dass virtualisierte Umgebungen den gleichen potentiellen Sicherheitsrisiken ausgesetzt sind wie physische Umgebungen und sie diesen Risiken ebenso begegnen müssen.

FIREWALLS ALLEIN REICHEN NICHT

Nur, weil sich eine virtualisierte Maschine hinter einer Firewall befindet – innerhalb des Rechenzentrums eines Unternehmens – ist sie noch lange nicht sicher vor Angriffen, die von außerhalb gestartet werden könnten.

Haben Angreifer erst einmal den Sicherheitsperimeter eines Unternehmens durchbrochen, sind ungeschützte virtualisierte Maschinen für sie ein leichtes Ziel.

VERWENDUNG VORHANDENER SICHERHEITSRICHTLINIEN

Die Services und Programme, die Ihre IT-Abteilung dem Unternehmen bereitstellt, sind natürlich wichtig, unabhängig davon, ob diese auf physischen oder virtualisierten Maschinen ausgeführt werden.

Wenn Ihr Unternehmen erkannt hat, wie wichtig es ist, Programme und Daten auf physischen Servern zu schützen, weiß es auch, wie wichtig dieser Schutz für Programme oder Geschäftsprozesse in einer virtualisierten Umgebung ist.

Ein Großteil der Richtlinien, die Sie auf Programme und Prozesse auf physischen Servern oder Desktops angewendet haben, bleibt weiterhin gültig.

Der erste Schritt zu einer sicheren virtualisierten Umgebung ist ganz einfach: Nehmen Sie die aktuellen Sicherheits- und Betriebsrichtlinien, die Sie bereits auf physische Server und Desktops anwenden, und replizieren Sie diese auf die gesamte neue virtualisierte Umgebung. Aber Vorsicht: Die Replikation vorhandener Sicherheitsrichtlinien ist zwar sinnvoll, doch die Replikation derselben Sicherheitstechnologien kann zu Folgendem führen:

- Einführung neuer Sicherheitslücken
- Explosion der IT-Kosten
- Einführung von Systemineffizienzen

Bei der Auswahl der Sicherheitstechnologien für virtualisierte Maschinen ist Sorgfalt geboten. Es ist bekannt, dass agentenbasierte Sicherheitslösungen höchst unerwünschte Nebeneffekte haben können.

CYBERKRIMINELLE KONZENTRIEREN IHRE ANGRIFFE AUF SCHWACHSTELLEN

Cyberkriminellen ist es in ihrem Bestreben nach maximalen illegalen Gewinnen bei minimalem illegalem Aufwand nicht entgangen, dass manche Unternehmen die Sicherheitsmaßnahmen für virtualisierte Umgebungen vernachlässigen.

Diese Kriminellen haben erkannt, dass virtualisierte Komponenten innerhalb der IT-Infrastruktur vieler Unternehmen eine Schwachstelle darstellen … und damit den Zugriff auf Systeme und wertvolle Informationen von Unternehmen erleichtern können.

AGENTENBASIERTE SICHERHEITSSOFTWARE

Dies ist im Grunde die gleiche Art Paket, die Sie auf einer physischen Maschine installieren würden. In einer nicht virtualisierten Umgebung werden sowohl die vollständige Sicherheitssoftware als auch die Malware-Datenbank auf der Maschine (Server oder Desktop) installiert.

Diese agentenbasierten Produkte innerhalb einer virtualisierten Umgebung sind in der Regel eher nachteilig. Auf jeder virtualisierten Maschine müssen der vollständige Agent sowie die gesamte Malware-Signaturdatenbank installiert werden. Wenn Sie also 100 virtualisierte Maschinen auf einem virtualisierten Host ausführen, befinden sich 100 Instanzen des Sicherheitsagenten sowie 100 Instanzen der Malware-Signaturdatenbank auf diesem virtualisierten Host.

Dieses hohe Maß an Duplizierung führt unweigerlich zu einer Verschwendung von Speicherplatz durch die Virendatenbank. Darüber hinaus sinkt die Performance, wenn mehrere Instanzen des Sicherheitsprogramms ausgeführt werden, vor allem, wenn die Sicherheitssoftware speicherintensive Prozesse auf mehreren virtualisierten Maschinen auf dem Host ausführt.

Wenn eine der Motivationen für ein Virtualisierungsprojekt darin besteht, mit weniger Hardware mehr zu erreichen, wird die Fähigkeit der Lösung, einen guten ROI zu erzielen, von allen Faktoren erheblich beeinträchtigt, die sich negativ auf die Konsolidierungsrate auswirken.

Neben der Speicherplatz verschwendenden Duplizierung der Sicherheitssoftware und Datenbanken kann eine agentenbasierte Sicherheitslösung auch dazu führen, dass die Performance weiter eingeschränkt wird oder neue Sicherheitslücken eingeführt werden. Dies geschieht durch Folgendes:

- Scan-Storms
- Panikattacken
- Update-Storms
- Instant-on-Lücken

SCAN-STORMS

Da mehrere Instanzen des Sicherheitsagenten auf jedem virtualisierten Host installiert sind, werden andere Programme beeinträchtigt, wenn mehrere oder sogar alle virtualisierten Maschinen gleichzeitig gestartet werden oder einen routinemäßigen Sicherheitsscan ausführen. Bei einem Virenbefall können die gestarteten Malware-Scan-Prozesse dazu führen, dass wichtige Programme nahezu stillstehen.

Diese Scan-Storms können Sie vermeiden, indem Sie sich für eine Sicherheitslösung entscheiden, die für virtualisierte Umgebungen optimiert wurde.

PANIKATTACKEN

IT-Administratoren legen oft Richtlinien fest, welche die Sicherheitsprozesse bei einem Virenbefall stark ausweiten, d. h. auf allen virtualisierten Maschinen werden gleichzeitig Scan-Prozesse gestartet, und die heuristische Analyse wird auf „maximal“ eingestellt. Dies führt unweigerlich dazu, dass jede virtualisierte Maschine einen großen Anteil der Host-Ressourcen beansprucht, einschließlich Arbeitsspeicher und CPU. Dies kann zu deutlichen Performance-Verlusten auf der Host-Maschine führen.

UPDATE-STORMS

Da auf dem virtualisierten Host Malware-Datenbanken für mehrere Instanzen des Sicherheitsagenten gespeichert sind, werden diese Datenbanken bei jedem regelmäßigen Update mit aktualisiert. Gleichzeitige Updates der Malware-Datenbanken auf jeder virtualisierten Maschine können die Performance der anderen Programme deutlich verschlechtern.

Um dies zu vermeiden, versuchen Sie möglicherweise, die Updates der Datenbanken zu staffeln, damit nur eine bestimmte Anzahl an virtualisierten Maschinen gleichzeitig aktualisiert wird. Bei diesem Ansatz bleibt der Schutz einiger virtualisierter Maschinen auf demselben Host jedoch auf der Strecke, oder einige der virtualisierten Maschinen sind anfälliger für neue oder aufkommende Malware und Angriffe.

Einige Sicherheitsprodukte, die speziell für virtualisierte Umgebungen entwickelt wurden, führen Updates nach dem Zufallsprinzip durch, um potentielle Update-Storms zu minimieren.

INSTANT-ON-LÜCKEN

Instant-on-Lücken können ein großes Sicherheitsrisiko für agentenbasierte Produkte darstellen.

Stellen Sie sich Folgendes vor: Ein Büroangestellter meldet sich um 17:00 Uhr von seinem virtualisierten Desktop ab und am nächsten Morgen um 08:00 Uhr wieder an. In den 15 Stunden dazwischen ist seine virtualisierte Maschine vollständig inaktiv. Das bedeutet, dass die

Viren-Datenbank und das Sicherheitsprogramm in dieser Zeit keine Updates erhalten haben.

15 Stunden scheinen nicht allzu lang zu sein … doch in der schnelllebigen Welt von heute können in diesem relativ kurzen Zeitraum zahlreiche neue Malware-Programme in Umlauf gebracht werden. Beim ersten Hochfahren am nächsten Morgen ist der virtualisierte Desktop den neuesten Bedrohungen unter Umständen schutzlos ausgeliefert.

Beginnt der Benutzer den Arbeitstag mit dem Besuch einiger Webseiten, bevor die Sicherheitssoftware aktualisiert wurde, kann sein virtualisierter Computer extrem anfällig für Angriffe sein.

Ähnliches gilt, wenn Administratoren eine neue virtualisierte Maschine einrichten. Die Instant-on-Lücke führt dazu, dass die Maschine so lange anfällig ist, bis das Sicherheitsprogramm und die Datenbank aktualisiert wurden.

Eine Nachricht von Max

„Unser erstes Projekt war, gelinde gesagt, etwas überstürzt. An Sicherheit wurde praktisch erst nachher gedacht – wir haben einfach unser normales Sicherheitspaket für jede virtualisierte Maschine benutzt."

„Wir dachten wirklich, dass es von Vorteil ist, wenn wir ein Sicherheitsprodukt verwenden, mit dem wir vertraut sind. Gegen Ende des Projekts wunderten wir uns dann, warum wir die vorausgesetzten Konsolidierungsraten und die von meinem Chef erwarteten Kosteneinsparungen nicht annähernd erzielten!"

AGENTENLOSE SICHERHEITSSOFTWARE

Für virtualisierte Umgebungen mit VMware bieten Hersteller agentenlose Sicherheitsprodukte, die sich eine spezielle Funktion von VMware vSphere zunutze machen – den Zugriff auf Dateisysteme in virtualisierten Maschinen.

Während bei agentenbasierten Sicherheitsprodukten der Sicherheitsagent und dessen Datenbank – auf jeder virtualisierten Maschine auf jedem Host repliziert werden muss, benötigen agentenlose Programme lediglich eine Instanz der Malware-Datenbank und eine für die Sicherheitsfunktionen vorgesehene virtualisierte Maschine … und schützen damit jede virtualisierte Maschine auf dem Host.

Agentenlose Sicherheitsprodukte können virtualisierte Server und virtualisierte Desktops schützen, ohne sich nennenswert auf die Leistung des Hypervisors auszuwirken.

Im Vergleich zur herkömmlichen agentenbasierten Sicherheit sind die Ansprüche agentenloser Lösungen an CPU, Arbeits- und Festplattenspeicher wesentlich geringer. IT-Abteilungen können damit Folgendes erzielen:

- Höhere Dichte virtualisierter Gastmaschinen
- Bessere Performance wichtiger Programme und Geschäftsabläufe
- Einfaches Deployment und automatischer Schutz neu erstellter virtualisierter Maschinen
- Höherer ROI

Darüber hinaus sind aufgrund der einzigen virtualisierten Maschine speziell für Sicherheitszwecke Malware-Scan-Storms und Update-Storms von Datenbanken und Programm ausgeschlossen. Instant-on-Lücken kommen ebenfalls nicht vor.

AGENTEN MIT KLEINEM SPEICHERPLATZBEDARF

Für eine Citrix- oder Microsoft-basierte virtualisierte Infrastruktur ist agentenlose Sicherheit keine Option. Hersteller haben hier Sicherheitslösungen mit einer Kombination entwickelt, die aus einem virtualisierten Gerät auf einem virtualisierten Host und einem Agenten mit kleinem Speicherplatzbedarf (auch „Light Agent“) auf jeder virtualisierten Maschine besteht. Light-Agent-Lösungen bieten eine Kombination aus erweiterter Sicherheit und relativ hohen Konsolidierungsraten.

Light-Agent-Lösungen bieten oft auch Sicherheits- und Verwaltungstechnologien, die agentenlose Produkte nicht haben, u. a.:

- Die Fähigkeit, Arbeitsspeicher zu scannen und speicherresidente Malware zu finden
- Die Kontrolle über Tools, die insbesondere in virtualisierten Desktop-Umgebungen sehr nützlich sein kann
- Host-basierte Netzwerksicherheit – einschließlich Firewall und einem System zur Angriffsüberwachung auf Host-Basis (Host-Based Intrusion Prevention System, HIPS)

Obgleich sich auf jeder virtualisierten Maschine ein Light Agent befindet, kommen Update-Storms nicht vor, da es lediglich eine Instanz der Sicherheitsdatenbank gibt, die sich innerhalb des virtualisierten Geräts befindet – und Scan-Storms werden dadurch ausgeschlossen, dass das virtualisierte Gerät Dateisystem-Scans automatisch randomisiert.

FINDEN SIE HERAUS, WELCHE TECHNOLOGIE AM BESTEN ZU IHREM UNTERNEHMEN PASST

Es gibt keine allgemeingültige Lösung für eine sichere Virtualisierung. Der optimale Ansatz für Ihr Unternehmen und die einzigartige Architektur Ihrer IT hängen von einer Reihe von Faktoren ab, darunter:

- Die Schwere der möglichen Risiken
- Der Wert der gespeicherten und verarbeiteten Daten
- Die angestrebte Konsolidierungsrate
- Die virtualisierte Umgebung Ihres Unternehmens, einschließlich Server und Desktops
- Ihre gewählte Virtualisierungsplattform, einschließlich VMware, Citrix oder Microsoft

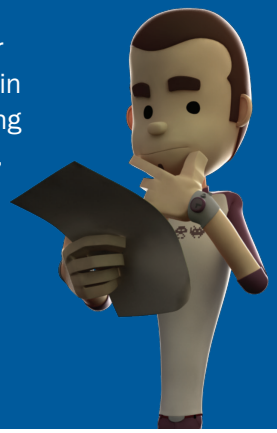
Es gibt zwar Extremfälle, in denen herkömmliche, agentenbasierte Sicherheitsprodukte erforderlich sind, in der Regel sollten Sie aber eine Lösung anstreben, die für virtualisierte Umgebungen optimiert ist, denn diese bietet Ihnen erhebliche Vorteile hinsichtlich Performance, Konsolidierung und Betriebskosten. Bei Lösungen, die für virtualisierte Umgebungen optimiert sind, geht es um die Entscheidung zwischen einer agentenlosen Lösung oder einem Sicherheitsprodukt mit kleinem Speicherplatzbedarf (Light Agent):

- Wenn Sie über eine VMware-basierte virtualisierte Umgebung verfügen, erreichen Sie mit agentenlosen Sicherheitslösungen hohe Konsolidierungsraten und deutliche ROI-Steigerungen aufgrund des einfachen Deployments und Managements.
- Light-Agent-Sicherheit kann einen erhöhten Schutz bieten. Da keine agentenlosen Lösungen für Citrix- und Microsoft-basierte virtualisierte Infrastrukturen vorhanden sind, bieten Light-Agent-Sicherheitslösungen den besten Schutz für diese Umgebungen.
- Eine virtualisierungsorientierte und umfassende Agentenlösung kann in solchen Fällen nützlich sein, in denen mehrere Gastbetriebssysteme (einschließlich Linux) zum Einsatz kommen, oder wenn Sie einen weniger gebräuchlichen Hypervisor verwenden.

Eine Nachricht von Max

„Es hat auch seine Vorteile, wenn ein einziger Mitarbeiter für IT und Sicherheit zuständig ist. Ein Freund von mir, der die IT-Sicherheit in einem sehr viel größeren Unternehmen leitet, war entsetzt, als sein Arbeitgeber sich zum ersten Mal an eine Virtualisierung wagte und diese allein von der IT-Abteilung leiten ließ, ohne das Team für IT-Sicherheit einzubeziehen.“

„Er musste dann auf den fahrenden Zug aufspringen und einige schlaflose Nächte verbringen, um die Sicherheit nachzurüsten.“



MAN KANN AUCH ALLES HABEN

Manchmal ist für ein Unternehmen eine Kombination aus agentenlosen und Light-Agent-Sicherheitsprodukten das Richtige.

So kann eine agentenlose Sicherheitslösung in einem streng kontrollierten Rechenzentrum, in dem die Server von ihren Aufgaben her keine ständige Internetverbindung benötigen, einen angemessenen Schutz bieten.

In einer virtualisierten Desktop-Umgebung hingegen, die weitaus weniger Kontrolle darüber bietet, wie die virtualisierten Desktops der Mitarbeiter genutzt werden, ist mitunter ein weiterreichender Schutz erforderlich, den eine Light-Agent-Lösung bieten kann. Dies ist insbesondere dann der Fall, wenn das Light-Agent-Produkt zusätzliche Sicherheitstechnologien z. B. zur Programm-, Geräte- und Web-Kontrolle umfasst, die einen Schutz gegen unsachgemäße oder sicherheitsgefährdende Benutzeraktivitäten bieten.

SICHERHEIT, DIE IHNEN MEHR OPTIONEN BIETET

Kaspersky Lab bietet virtualisierte Sicherheitslösungen für eine große Bandbreite Windows-basierter virtualisierter Umgebungen, einschließlich:

- VMware
- Citrix
- Microsoft

… und Umgebungen, in denen zwei oder mehr Produkte von Herstellern virtualisierter Lösungen verwendet werden.

Kaspersky Lab ermöglicht Unternehmen auch die Auswahl des für ihre spezifische virtualisierte Umgebung am besten geeigneten Sicherheitsansatzes:

- Kaspersky Security for Virtualization | Agentless
- Kaspersky Security for Virtualization | Light Agent
- Agentenbasierte Sicherheitslösungen von Kaspersky Lab

EINE LIZENZ – ZWEI SICHERHEITSTECHNOLOGIEN VON WELTRANG

Beim Erwerb von Kaspersky Security for Virtualization haben Sie Zugriff auf zwei Lösungen:

- Kaspersky Security for Virtualization | Agentless
- Kaspersky Security for Virtualization | Light Agent

… damit können Sie in verschiedenen Bereichen Ihrer IT-Infrastruktur unterschiedliche Sicherheitsprogramme einsetzen.

Sie haben gleichfalls die Auswahl zwischen Lizenzen „pro virtualisierter Maschine“ oder „pro Kern“ und können so die für Ihr Unternehmen kosteneffizienteste Lösung verwenden.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Während bei herkömmlichen Sicherheitsprodukten die Installation eines umfassenden Sicherheitsagenten auf jeder einzelnen virtualisierten Maschine erforderlich ist, ermöglicht Kaspersky Security for Virtualization | Agentless den Schutz jeder virtualisierten Maschine auf einem virtualisierten Host – und dafür muss nur ein einziges virtualisiertes Sicherheitsgerät installiert werden.

Kaspersky Security for Virtualization | Agentless ist die ideale Lösung für VMware-basierte Projekte, bei denen Sie durch ein nahtloses Deployment einen guten ROI und beständige Konsolidierungsraten erzielen wollen; hierzu gehören auch Rechenzentren und Server, die keine ständige Internetverbindung benötigen.

Kaspersky Security for Virtualization | Agentless hat folgende Merkmale:

- Malware-Schutz auf fünf Ebenen
- Schutz auf Netzwerkebene mit der Network-Attack-Blocker-Technologie von Kaspersky Lab
- Cloud-basierte Bedrohungsinformationen in Echtzeit – aus dem Kaspersky Security Network

Da für das Deployment von Kaspersky Security for Virtualization | Agentless keine einzige Maschine neu gestartet oder der Hostserver in den Wartungsmodus versetzt werden muss, ist diese Lösung ideal für Rechenzentren geeignet, die eine Leistung mit „fünf Neunen“ (99,999 %) bei der Betriebszeit erbringen müssen.

Darüber hinaus sind Scan-Storms, Update-Storms und Instant-on-Lücken ausgeschlossen.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Bei Kaspersky Security for Virtualization | Light Agent wird ein für die Sicherheitsfunktionen vorgesehenes virtualisiertes Gerät auf dem Host und ein ressourcenschonender Agent (auch „Light Agent“ genannt) auf jeder virtualisierten Maschine installiert. Dies bietet einen besseren Schutz als eine agentenlose Lösung, verbraucht dabei aber immer noch sehr viel weniger Rechenleistung und Speicherkapazität als eine herkömmliche, agentenbasierte Lösung.

Kaspersky Security for Virtualization | Light Agent hat folgende Merkmale:

- Moderner Malware-Schutz
- Erweiterter Schutz auf Netzwerkebene mit HIPS, Firewall und der Network-Attack-Blocker-Technologie von Kaspersky Lab
- Programmkontrolle, mit der Sie verwalten können, welche Programme ausführungsberechtigt sind
- Gerätekontrolle, mit der Sie die Zugriffsberechtigungen von Wechseldatenträgern auf Ihre Systeme verwalten können
- Web-Kontrolle, mit der Sie Internetnutzung verwalten und den Zugang auf bestimmte Arten von Webseiten blockieren können
- Automatic Exploit Prevention (AEP) zur Verteidigung gegen Malware, die Schwachstellen von Betriebssystem und Programmen ausnutzt
- Cloud-basierte Bedrohungsinformationen in Echtzeit – aus dem Kaspersky Security Network

Beim Deployment von Kaspersky Security for Virtualization | Light Agent ist es nicht mehr erforderlich, eine Maschine neu zu starten oder den Hostserver in den Wartungsmodus zu versetzen – dies ermöglicht es Ihnen, „fünf Neunen“ (99,999 %) Betriebszeit Wirklichkeit werden zu lassen.

Auch hier gilt: Scan-Storms, Update-Storms und Instant-on-Lücken sind ebenfalls ausgeschlossen.

EINE VERWALTUNGSKONSOLE – VIELE VORTEILE

Zu Kaspersky Security for Virtualization zählt auch das Kaspersky Security Center, die benutzerfreundliche Verwaltungsoberfläche von Kaspersky Lab, mit der Sie ein breites Spektrum an Sicherheits- und Systems-Management-Technologien von Kaspersky Lab konfigurieren und steuern können.

Egal, ob Sie Kaspersky Security for Virtualization | Agentless, Kaspersky Security for Virtualization | Light Agent oder eine Kombination beider Programme verwenden, Sie können beide mit einer einheitlichen Verwaltungskonsole steuern und haben dadurch folgende Vorteile:

- Wenn Sie von VMware zu Citrix, von Microsoft zu VMware oder von Citrix zu Microsoft migrieren, können Sie in allen Fällen die selbe Verwaltungskonsole verwenden.

- Da mit der selben Verwaltungskonsole auch die agentenbasierten Sicherheitslösungen von Kaspersky Lab gesteuert werden – einschließlich Kaspersky Endpoint Security for Business und Kaspersky Total Security for Business – können Sie einfach von einer physischen in eine virtualisierte Umgebung migrieren und dabei das Tempo frei wählen.

Kaspersky Security Center erleichtert Ihnen die Verwaltung der Sicherheits- und Systems-Management-Technologien von Kaspersky Lab auf physischen und virtualisierten Maschinen sowie auf mobilen Geräten.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

In den seltenen Fällen, in denen Sie einen vollständigen Sicherheitsagenten auf Ihren virtualisierten Maschinen benötigen, haben Sie die Auswahl aus einer der Stufen von Kaspersky Endpoint Security for Business, oder verwenden Sie unsere umfassendste Sicherheitslösung: Kaspersky Total Security for Business.

STRATEGIETIPPS VON MAX – FÜR EINE SICHERE VIRTUALISIERUNG

„Die Kosteneinsparungen und die weiteren Vorteile von Virtualisierung können sehr verlockend sein, aber Sie sollten beim Entwickeln Ihrer Projektstrategie schon ein paar Dinge beachten, damit die System- und Datensicherheit Ihres Unternehmens erhalten bleibt."

- Achten Sie darauf, dass die Sicherheit bei jedem Virtualisierungsprojekt von Beginn an eingeplant wird. Wenn Sicherheit bei der Einführung eines Virtualisierungsprojekts keine Rolle spielt, ist Ihre Strategie unvollständig und potentiell gefährlich.

- Denken Sie bei Ihren Überlegungen, welche Virtualisierungsplattform für Ihr Projekt die richtige ist, auch daran, wie sich diese Plattform auf Ihre Sicherheitsoptionen auswirkt.

- Ein guter Anfang besteht darin, Ihre aktuellen, für die physische IT-Infrastruktur geltenden Sicherheitsrichtlinien auf die neue virtualisierte Umgebung anzuwenden.

- Nehmen Sie eine Analyse des Projekts und seiner Sicherheitsanforderungen vor, bevor Sie Leistungsziele und Vorgaben für Konsolidierungsraten festlegen.

- Überprüfen Sie sorgfältig die verfügbaren Sicherheitstechnologien, einschließlich:
  – Agentenbasiert
  – Agentenlos
  – Light Agent

- Wählen Sie eine Sicherheitslösung, die sich auch flexibel an Änderungen der verwendeten Virtualisierungssoftware anpassen lässt. Wenn Sie beispielsweise jetzt VMware verwenden, später aber zu Citrix wechseln, können Sie dadurch die Kosten für den Kauf neuer Sicherheitssoftware-Lizenzen und die damit zusammenhängenden Schulungskosten sparen.

- Nehmen Sie eine Analyse des Zusammenspiels zwischen der Sicherheitssoftware für Virtualisierung und anderen Sicherheitstechnologien vor. Ein besseres Zusammenspiel bedeutet weniger Belastung für Ihre IT-Administration.

- Entlasten Sie Ihre Teams für IT-Sicherheit und IT-Administration, indem Sie eine Sicherheitslösung wählen, die Ihnen mithilfe einer einzigen Verwaltungskonsole die Kontrolle über mehrere Sicherheitstechnologien und -Funktionen gibt.

ERFAHREN SIE MEHR ÜBER VIRTUALIZATION SECURITY

Wenn Sie mehr über das Thema Virtualization Security erfahren möchten, besuchen Sie
www.kaspersky.de/business-security

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 16-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Kaspersky Lab ist derzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 300 Millionen Anwendern weltweit.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2012“ den vierten Rang. Die Rangfolge wurde im IDC-Bericht „Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares“ (IDC Nr. 242618, August 2013) veröffentlicht. In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2012 eingestuft.