KASPERSKY lab

VIRTUALIZATION SECURITY: WELCHE UNTERSCHIEDE GIBT ES?

www.kaspersky.de

VIRTUALIZATION SECURITY: WELCHE UNTERSCHIEDE GIBT ES?

Virtualisieren Sie Ihre Hardware schon? Dann ist Ihr Ziel wahrscheinlich maximale Effizienz Ihrer IT-Infrastruktur. Die Verwendung mehrerer virtualisierter Maschinen (VMs) auf einem einzelnen Computer anstelle von mehreren Servern, die alle mit Strom versorgt, gekühlt und gewartet werden wollen, ist ein überzeugendes Argument. Virtualisierte Nodes auf einem einzigen physischen Server bedeuten Kosteneinsparungen. Der wirtschaftliche Effekt der Virtualisierung kann beeindruckend sein: Nach einer 2011 durchgeführten Umfrage von Forrester brachte die Einführung einer VMware VDI Infrastruktur in einem Zeitraum von vier Jahren beeindruckende 255 % an risikobereinigtem ROI, mit einer Gewinnschwelle von 17 Monaten nach der Einführung.

Die Frage ist: Wie viele VMs passen in die Hardware, ohne dass die Performance darunter leidet? Dies wird auch als Konsolidierungsrate bezeichnet und stellt die eigentliche Herausforderung dar, bei der viele Faktoren zu berücksichtigen sind. Welche Art von Aufgaben sollen Ihre virtualisierten Maschinen übernehmen? Welche Hypervisor-Software verwenden Sie? Welche Gefahren birgt die Konzentration auf wenige Server? Und wie können Sie Ihre neue virtualisierte Infrastruktur zuverlässig schützen und deren Anfälligkeit für Angriffe minimieren, ohne die Geschäftsabläufe extrem zu verlangsamen? Bevor Sie eine Entscheidung treffen, sollten Sie sich mit den einzelnen Konzepten und ihrem gegenseitigen Zusammenwirken vertraut machen.

Virtualisierungsmodelle

Branchenüblich sind mehrere Virtualisierungsmodelle definiert. Hier werden drei Modelle erörtert:

- **Server-Virtualisierung** – diese ermöglicht die Ausführung mehrerer Instanzen eines Betriebssystems auf einem Server. Dieses Modell bietet die beste Ressourcennutzung – bis zu 80 % im Vergleich zum üblichen Auslastungsgrad von 10–20 % für herkömmliche einzeln genutzte physische Server[1].
  Hardware-Server-Virtualisierung mit lediglich einer Zwischenebene (Hypervisor) zwischen virtualisierter Maschine (VM) und Hardware bietet einen größeren Nutzwert als **Software-Server-Virtualisierung,** bei der das zugrunde liegende Betriebssystem zusätzliche Ressourcen verbraucht. Für die meisten Geschäftsanwendungen ist daher Hardware-Virtualisierung vorzuziehen.

1 Ruest D. Virtualization. A Beginner's Guide. McGraw-Hill, 2010, Seite 4

- **Desktop-Virtualisierung** – eine mögliche Alternative, bei der zahlreiche physische Desktops durch eine virtualisierte Desktop-Infrastruktur (**Virtual Desktop Infrastructure, VDI**) ersetzt werden. Die Vorteile sind: kosteneffiziente Thin Clients, rollenbasierte Remote-Desktops, Niederlassungen, für die kein spezieller IT-Service erforderlich ist und Reduzierung der Wartung von Hunderten von Desktops auf eine Handvoll physischer Server.
- **Programm-Virtualisierung** – im Unterschied zur rollenbasierten Remote-Desktop-Infrastruktur wird die virtualisierte Umgebung hier nur für ein einzelnes Programm eingerichtet. Für den immer mehr verbreiteten Ansatz des Software-as-a-Service ist dies eine naheliegende und effiziente Wahl.

Alle Virtualisierungsmodelle haben zahlreiche Einsatzmöglichkeiten, wobei jede mit bestimmten Risiken verbunden ist. Cyberbedrohungen sind dabei das größte Risiko, eine Sicherheitslösung ist deshalb unverzichtbar. Diese Herausforderung wird größer, wenn man bedenkt, dass alle drei Ansätze innerhalb eines einzigen IT-Netzwerks zur Anwendung kommen können. Zusätzlicher Ressourcenverbrauch ist natürlich ebenfalls zu berücksichtigen.

Es gibt jedoch Möglichkeiten, die Auswirkungen auf Ihre neue hocheffiziente virtualisierte Infrastruktur abzumildern.

EINE SPEZIALISIERTE SICHERHEITSLÖSUNG FÜR VIRTUALISIERTE UMGEBUNGEN IST ENTSCHEINDEND

Selbstverständlich können Sie die Ihnen vertraute Software-Lösung mit einzelnen Agenten für den Endpoint-Schutz auch auf Ihren virtualisierten Maschinen installieren. Dabei gibt es jedoch beträchtliche Nachteile, die die Vorteile einer virtualisierten Infrastruktur aushebeln können.

1. **Duplizierung:** Jede VM weist identische Sicherheitskomponenten auf, einschließlich einer eigenen Malware-Engine und einer Signaturdatenbank, die unabhängig voneinander aktualisiert werden müssen. Ein bedeutender Teil Ihrer wertvollen Ressourcen – Prozessorleistung, RAM und Speicherplatz – wird so relativ nutzlos verbraucht und senkt dadurch die Konsolidierungsrate erheblich.
2. **„Storms“:** Dieser Begriff bezieht sich auf simultane Malware-Scans oder Datenbank-Updates durch zahlreiche Computer, die zu Verbrauchsspitzen und damit zu Leistungseinbußen bis hin zu Ausfällen führen können. Teilweise kann dieses Problem durch manuelle Konfigurierung behoben werden, bei Hunderten von VMs können manuelle Eingriffe jedoch extrem zeitaufwändig sein.
3. **„Instant-on“-Lücken:** Bestimmte virtualisierte Maschinen werden erst aktiv, wenn sie gebraucht werden. Leider können auf einer inaktiven VM keine Komponenten oder Datenbanken der Sicherheitslösung aktualisiert werden. Unmittelbar nach dem Hochfahren, und bevor die Aktualisierung abgeschlossen ist, ist die VM daher anfällig für Angriffe.
4. **„Panikattacken“:** Systemadministratoren definieren das Reaktionsmuster auf den Ausbruch von Viren in der Regel als Einengung der Sicherheitsparameter, einschließlich Wechsel in einen „paranoiden“ Modus und Auslösen eines ungeplanten Scan-Vorgangs. Für physische Nodes kann eine solche Richtlinie sinnvoll sein, in einer virtualisierten Umgebung jedoch kann sie zum Stillstand führen.
5. **Inkompatibilitätsprobleme:** Virtualisierte Maschinen ähneln in vieler Hinsicht ihren physischen Gegenübern – es sind jedoch auch wesentliche Unterschiede zu beachten, u. a. die Verwendung nicht-persistenter Laufwerke und die VM-Live-Migration. Da Standard-Malwareschutzprogramme für physische Endpoints und nicht für die Feineinstellungen virtualisierter Umgebungen ausgelegt sind, können unerwartete Verzögerungen und Fehler bis hin zu vollständigen Ausfällen auftreten.

Vor diesem Hintergrund wird der Bedarf nach einer Speziallösung offensichtlich. Der Entwicklung eines solchen Produkts sind die o. g. Erwägungen zugrunde zu legen. Dabei gilt es, den bestmöglichen Schutz mit möglichst geringen Auswirkungen auf die Gesamtperformance zu erzielen. Kaspersky Lab ist dieser Aufgabe gewachsen und bietet eine Lösung für die drei meistverbreiteten Virtualisierungsplattformen: VMware, Microsoft Hyper-V und Citrix.

PLATTFORMEN UND SCHUTZMODI

Agentenloser Ansatz

VMware, eine der ältesten und nach wie vor beliebtesten Virtualisierungsplattformen, bietet eine Lösung mit dem Namen vShield, bei der die VM von der Notwendigkeit identischer Datenbanken und vielfacher Malware-Scan-Agenten befreit ist. Dieser Ansatz wird auch als „agentless" (agentenlos) bezeichnet.

Kaspersky Lab bietet mit **Kaspersky Security for Virtualization | Agentless** eine spezialisierte Sicherheitslösung für VMware-Plattformen. Die Scan-Funktionen werden hier auf eine Security Virtual Appliance (SVA) übertragen. Diese virtualisierte Spezialmaschine umfasst sowohl die Scan-Engine als auch die Sicherheitsdatenbanken und schützt alle VMs, die auf dem Hypervisor ausgeführt werden.

Die Vorteile liegen auf der Hand:

- Die Originalschnittstelle von VMware vShield bietet effizienten Zugriff auf die VMs, wodurch die Ressourcen der einzelnen Maschinen frei werden für andere Aufgaben, wobei gleichfalls die Kompatibilität mit anderen VMware-Produkten gewährleistet ist.
- Durch die Zentralisierung der Malware-Schutzfunktion und der Signaturdatenbanken in einer einzigen Virtual Appliance werden Ressourcen frei, die für zusätzliche VMs eingesetzt werden können. So steigt die Konsolidierungsrate.
- Beim Hochfahren neuer VMs besteht durch die SVA sofortiger Schutz, d. h. keine „Instant-on"-Lücke und keine Notwendigkeit, weitere Software zu installieren.
- Die SVA von Kaspersky Lab ist rund um die Uhr in Betrieb, sodass die Signaturdatenbank stets aktuell bleibt. Darüber hinaus besteht ständig eine Verbindung mit dem Kaspersky Security Network (KSN), einer weltweiten Infrastruktur, in der die Daten Millionen freiwilliger Teilnehmer verarbeitet werden. So können wir unsere Kunden auch vor neu aufkommenden Bedrohungen schützen, noch bevor ein Datenbank-Update ausgerollt wird.
- Das Problem von Scan- und Update-Storms wird durch die Verwendung einer einzelnen ständig aktualisierten SVA eliminiert. Die SVA scannt die VMs automatisch anhand eines Zufallszeitplans, wodurch die Anzahl der Scan-Durchläufe reduziert wird.

Darüber hinaus ist die Kaspersky-Lösung mithilfe der grundlegenden Netzwerk-Sicherheitsfunktionen von vCloud Networking and Security in der Lage, Angriffe auf VMs zu erkennen und mit der Network-Attack-Blocker-Technologie abzuwehren[2].

2 Das Einrichten des Netzwerkschutzes in KSV | Agentless erfordert das Deployment einer sekundären SVA

Die Möglichkeiten von vShield sind jedoch eingeschränkt und bieten Zugriff auf geschützte VMs lediglich auf Dateisystemebene. Speicherresidente Prozesse innerhalb der VMs selbst können daher durch agentenlose Malware-Schutzprogramme nicht überwacht und kontrolliert werden. Weitere Technologien für den Endpoint-Schutz, wie Programmkontrolle mit dynamischen Whitelists, die wirksame zusätzliche Schutzebenen bieten, können mit diesem Ansatz ebenfalls nicht implementiert werden.

Gleichfalls ist zu beachten, dass der agentenlose Ansatz zum Schutz virtualisierter Infrastrukturen derzeit nur auf VMware-Plattformen angewendet werden kann, da es sich bei vShield um proprietäre VMware-Technologie handelt.

Light Agent-Ansatz

Im Hinblick auf die o. g. Einschränkungen hat **Kaspersky Lab** einen weiteren Lösungsansatz entwickelt, der zwischen „agentenlos" und „Full Agent" eingeordnet werden kann: **Kaspersky Security for Virtualization | Light Agent**

Ebenso wie beim agentenlosen Ansatz befinden sich auch hier die Datenbanken und die Scan-Engine auf einer SVA. Der Unterschied besteht darin, dass auf jeder geschützten VM ein ressourcenschonendes residentes Modul bereitgestellt wird.

Kaspersky Security for Virtualization | Light Agent unterliegt nicht den durch vShield gegebenen Einschränkungen und hat direkten Zugriff auf jede VM und deren Arbeitsspeicher. Daher kann die volle Bandbreite der führenden Technologien von Kaspersky Lab zum Schutz der virtualisierten Infrastruktur eingesetzt werden.

Hauptvorteile von Kaspersky Security for Virtualization | Light Agent:

- Niedriger Verbrauch von Ressourcen im Vergleich zu einer agentenbasierten Lösung, da sich die Dateisystem-Scan-Engine und die Datenbanken auf der SVA befinden
- Unterstützung für die drei am weitesten verbreiteten Virtualisierungsplattformen: VMware, Microsoft Hyper-V und Citrix*
- Höchstmöglicher Schutz durch vollen Zugriff auf alle VM-Ressourcen einschließlich Arbeitsspeicher
- Zusätzliche Sicherheitsebenen wie HIPS mit Automatic Exploit Prevention und Programmkontrolle mit dynamischen Whitelists werden verfügbar; einfache Umsetzung selbst der strengsten Sicherheitsszenarien, einschließlich „Default Deny"
- Da die Lösung von Anfang an auf Virtualisierung ausgelegt ist, arbeitet sie nicht gegen die, sondern mit den spezifischen Merkmalen einer virtualisierten Umgebung.

Der Light Agent muss auf jeder neuen VM bereitgestellt werden, wobei sich dieser Prozess jedoch durch Einbeziehung des Light Agent in das VM-Image einfach automatisieren lässt. Durch den Light Agent hat Kaspersky Security for Virtualization | Light Agent einen etwas höheren Speicherbedarf, allerdings kann die Performance der Light-Agent-Lösung die der agentenlosen V-Shield-basierte Anwendung unter bestimmten Voraussetzungen auch übertreffen.

Eine weitere Einschränkung ist die Anzahl der unterstützten Hypervisoren, die durch die drei meistverbreiteten Plattformen gegeben ist. Zum Zeitpunkt der Erstellung dieses Dokuments sind die Betriebssysteme von Microsoft Windows die einzigen, die sowohl agentenlose als auch Light-Agent-Anwendungen unterstützen.

Das bedeutet jedoch nicht, dass Sie schutzlos dastehen, nur weil Sie keine dieser drei Plattformen verwenden. Für diesen Fall gibt es immer noch die von Kaspersky Lab entwickelte Full-Agent-Sicherheit.

Full Agent-Ansatz

Kaspersky Endpoint Security ist, obwohl es sich um eine Full Agent-Lösung handelt, auch für virtualisierte Umgebungen sehr gut geeignet. Obgleich der Ressourcenverbrauch größer ist als bei Kaspersky Security for Virtualization, kann diese Lösung an den Einsatz in virtualisierten Umgebungen angepasst werden. Wenn Sie also eine bestimmte Konfiguration wie beispielsweise eine Gruppe von Linux-Servern oder Windows-Gäste auf einem exotischen Hypervisor schützen wollen, ist dies möglich.

Vorteile von Kaspersky Endpoint Security in einer virtualisierten Infrastruktur:

- Unterstützung der modernsten Betriebssysteme
- Umfassende Nutzung der führenden Technologien von Kaspersky Lab
- Vertraute Verwaltung wie bei physischen Computern
- Anerkannte Effizienz dieser Lösung durch drei weltweit führende Consulting-Agenturen: Gartner, IDC und Forrester, mit der Auszeichnung für eine der besten verfügbaren Plattformen für den Endpoint-Schutz.

Tabelle 1: Funktionsvergleich

Funktion	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Unterstützte Virtualisierungsplattform	VMware	VMware, Microsoft Hyper-V, Citrix	Jede mit Ausnahme von Betriebssystemebene[3]
Unterstütztes Gast-Betriebssystem	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Konsolidierungsrate pro Host	* * *	* */* * *[4]	*
Zentrale Verwaltung mit dem Kaspersky Security Center	+	+	+
KSN-Funktion	+	+	+
Schutz neuer VMs ohne zusätzliche Softwareinstallation	+	+/-[5]	-
Virenschutz	* *	* * *	* * *
Firewall	-	+	+
Host-basierte Angriffsüberwachung (HIPS)	-	+	+
Network Attack Blocker	+	+	+
Programmkontrolle mit dynamischen Whitelists und Default-Deny-Unterstützung	-	+	+
Webkontrolle	-	+	+
Gerätekontrolle	-	+	+
Systems Management	-	+[6]	+[6]
Verschlüsselung	-	-	+

Zum Abschluss dieser eingehenden Überlegungen steht dann erneut die Frage: Wie schaffe ich maximale Effizienz, ohne anfällig für Cyberbedrohungen zu werden? Als Faustregel gibt es hier einen Ansatz mit der Bezeichnung **rollenbasierte Sicherheit.**

3 Bei der Virtualisierung auf Betriebssystemebene, auch zonenbasierte oder containerbasierte Virtualisierung genannt, verwenden mehrere „Container" einen gemeinsamen Betriebssystem-Kernel. Beispiele für diese Plattformen sind Parallels und Proxmox.

4 Je nach Hypervisor und Virtualisierungstyp.

5 Bei nicht-persistenten VMs ist ein sofortiger Schutz verfügbar, sobald der Light Agent im Image der VM integriert ist. Bei persistenten VMs muss der Administrator den Light Agent manuell einrichten.

6 Vulnerability Assessment/Patch Management sind zwar in Kaspersky Security for Virtualization | Light Agent verfügbar, sind jedoch äußerst ressourcenintensiv und daher für virtualisierte Umgebungen nicht zu empfehlen.

PARIEREN SIE NUR ECHTE ANGRIFFE – EIN ROLLENBASIERTER ANSATZ

Jeder Cyberkriminelle, der Ihre physischen Endpoints bedroht, kann auch Ihre virtualisierte Infrastruktur gefährden. Jeder Angreifer muss jedoch Ihren Sicherheitsperimeter überwinden, um einen Angriff starten zu können. So kann ein Cyberkrimineller einen PC beispielsweise dadurch infizieren, dass er einen Ihrer Mitarbeiter auf eine schädliche Webseite lockt, die für die Infektion eine Schwachstelle im Browser ausnutzt. Um jedoch beispielsweise einen Datenbankserver zu infizieren, der tief in der IT-Infrastruktur verborgen ist und oftmals nicht einmal über einen Internetanschluss verfügt, muss eine andere Angriffsmöglichkeit gefunden werden. Wenn Sie sich also sicher sind, dass die einzigen möglichen Angriffe auf Dateisystemebene erfolgen können, oder wenn die betroffenen Daten nur von niedrigem Wert sind, oder wenn Sie eine VDI mit strengen Richtlinien und ohne Internetanschluss verwenden, könnte Ihnen der agentenlose Ansatz die Vorteile von sofortigem Schutz ohne „Instant-on"-Lücken bieten.

Tabelle 2: Rollenbasierte Sicherheit

Position	Externer Zugriff	Daten-wert*	Service-wert**	Ext. Bedingungen	Lösung (Warum eine bestimmte Lösung vorzuziehen ist)
Backend-Datenbankserver	Nein	Niedrig bis mittel	Mittel bis hoch	Regelmäßige Backups	KSV | Agentless (kurzlebige Daten wenige Angriffsmöglichkeiten)
Frontend-Webserver	Ja	Niedrig	Hoch	Vertrauenswürdige Beziehungen durch mehrere Backends	KSV | Light Agent (Gefahr durch die Möglichkeit des öffentlichen Zugriffs, nach einem erfolgreichen Angriff ist die Ausnutzung von Vertrauensbeziehungen möglich)
VDI mit Zweckeinschränkung oder virtualisierte Programme	Nein	Mittel bis hoch	Mittel	Hohe Einschränkung, keine Programminstallation, keine Verwendung von Wechseldatenträgern	KSV | Agentless (vorausschaubare Umgebung, wenige Angriffsmöglichkeiten)
VDI als Ersatz für Desktops	Ja	Mittel	Mittel	Persönliche Wechseldatenträger im Einsatz, Benutzer mit Installationsrechten	KSV | Light Agent (Hohe Sicherheit ist wichtiger als schnelle Reaktionszeiten. Mehr Angriffsmöglichkeiten durch Internetverbindung)
Unternehmenseigene Intranet-Webserver	Ja	Niedrig bis mittel	Niedrig bis mittel	*Externer Zugriff nur durch befugte Benutzer mit Hardware-Tokens	KSV | Agentless (Geringer Geschäftswert der Daten, stark eingeschränkter Internetzugang)

Position	Externer Zugriff	Daten-wert*	Service-wert**	Ext. Bedingungen	Lösung (Warum eine bestimmte Lösung vorzuziehen ist)
Infrastruktur zur Verarbeitung von Kundendaten	Ja	Hoch	Hoch	Stabile, unveränderte Umgebung ist erforderlich; Programmkontrolle mit „Default Deny" empfohlen	KSV | Light Agent (Compliance-Bedarf macht zusätzliche Schutzebenen zu einer absoluten Notwendigkeit.)
Testinfrastruktur für Webentwickler	Ja	Niedrig bis mittel	Mittel	Linux-basierter Hypervisor und heterogene Gast-VMs	KESB für Linux, KESB für Windows (ständig aktualisierte kurzlebige Daten, verschiedene Betriebssysteme)

Die oben stehende Tabelle enthält Beispiele zur Erläuterung rollenbasierter Verteidigungsstrategien, sie ist jedoch nicht als direkte Empfehlung für die dort aufgelisteten Rollen zu verstehen. Es ist stets eine Einzelfallentscheidung erforderlich, wobei eine Vielzahl individueller Bedingungen zu berücksichtigen ist, die nicht in einer einzelnen Tabelle zusammengefasst werden können. Um jedoch das Konzept näher zu erläutern, werden hier die Klassifizierungen für Datenwert und Servicewert ausführlicher aufgeführt:

- **Daten von geringem Wert** – Diese Daten sind in der Regel nicht personenbezogen und enthalten keine persönlichen, geschäftlichen oder behördlichen Geheimnisse, möglicherweise sind sie kurzlebig und werden ständig aktualisiert. Verlust oder Aufdeckung dieser Daten bedeuten keine wesentlichen wirtschaftlichen Verluste und in keinem Falle Rufschäden. Ein gutes Beispiel hierfür ist eine Arbeitsdatenbank, in der vorübergehend Übergangsdaten gespeichert werden.
- **Daten von mittlerem Wert** – Diese Daten enthalten unter Umständen persönliche oder geschäftliche Informationen, jedoch keine Daten, die direkt mit Finanzen oder mit dem persönlichen Wohlergehen zusammenhängen. Streng vertrauliche Informationen sind dabei nicht enthalten. Ein Verlust führt unter Umständen zu gewissen finanziellen Schäden für das Unternehmen. Eine Aufdeckung kann spürbare finanzielle Folgen haben und den Ruf des Unternehmens in eingeschränktem Maße schädigen. Beispiel – Kundendaten eines Internet-Händlers.
- **Daten von hohem Wert** – Diese können vertrauliche persönliche und/oder finanzielle Informationen oder Handelsgeheimnisse enthalten, die einen erheblichen Bestandteil der Marktvorteile eines Unternehmens ausmachen. Geheiminformationen können ebenfalls beinhaltet sein. Ein Verlust kann zu erheblichen wirtschaftlichen Verlusten und Rufschäden führen. Eine Aufdeckung kann hohe Geldbußen und Gerichtsklagen nach sich ziehen und zu irreparablen Rufschäden führen. Beispiel – Entwürfe wichtiger Infrastrukturen oder vertraulicher Schriftverkehr auf Managementebene.

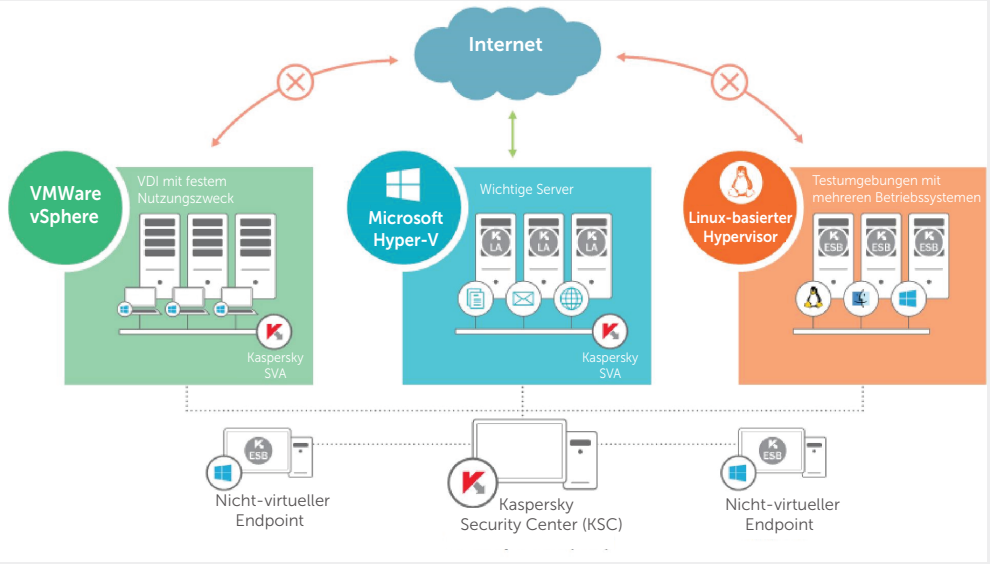
- **Geringer Servicewert** – Dritte sind nicht betroffen, die Geschwindigkeit der Dienstwiederherstellung ist eher unbedeutend. Keine oder nur geringe finanzielle Konsequenzen im Falle von Funktionsausfällen. Die Wahrscheinlichkeit von Rufschäden ist sehr gering. Beispiel – Info-Portal eines Unternehmens.
- **Mittlerer Servicewert** – Dritte können von einem Dienstausfall betroffen sein. Ein Datenverlust kann zu spürbaren finanziellen Schäden führen. Die Rufschäden sind ebenfalls spürbar und stehen in direktem Zusammenhang mit der sozialen Bedeutung des Dienstes: Je bekannter und beliebter der Dienst (bzw. das auf diesen aufbauende Produkt) ist, desto schwerer sind die Rufschäden. Die Daten können Bestandteil einer Behörden-Infrastruktur sein, wobei der Zustand der Daten sich jedoch nur wenig auf das allgemeine Wohlergehen auswirkt. Eine rasche Wiederherstellung ist von höchster Wichtigkeit. Beispiel – VDI-Infrastruktur eines Systemintegrators, der u. a. Umgebungen für den Ersatz von Computer-Desktops anbietet.
- **Hoher Servicewert** – Dritte sind höchstwahrscheinlich betroffen. Der Dienst ist ein Schlüsselelement des Unternehmens und möglicherweise auch ein wichtiges Element von Drittunternehmen. Ein Einfluss auf das allgemeine Wohlergehen ist möglich. Rufschäden sind sehr schmerzhaft und möglicherweise irreparabel. Wiederherstellung ist dringlich und muss unverzüglich erfolgen, andernfalls kann dies erhebliche Konsequenzen nach sich ziehen. Beispiel – öffentliche Infrastruktur zur Videoüberwachung.

Da Sie Ihre Infrastruktur am besten kennen, können Sie auch am besten entscheiden, wie die optimalen Sicherheitsmaßnahmen zu gestalten sind; an dieser Stelle handelt es sich lediglich um einen Leitfaden zur Entscheidungsfindung. Es ist jedoch grundsätzlich möglich, die Effizienz von Ressourcen zu steigern und damit Kosten einzusparen und gleichzeitig die virtualisierte Infrastruktur zu schützen. Denken Sie aber vor der Einführung einer speziellen Sicherheitslösung daran, dass Sie die grundlegenden Sicherheitseinstellungen Ihres IT-Netzwerks prüfen und justieren sollten. Ein einwandfrei verwaltetes Netzwerk bedeutet weniger Angriffsmöglichkeiten und geringere Konsequenzen für Sie, wenn doch einmal etwas schiefgehen sollte.

EFFIZIENZ BEDEUTET INTEGRITÄT

Ein effizienter Einsatz von Ressourcen ist schön, ohne eine effektive Kontrolle jedoch wertlos. Natürlich können Sie die agentenlose Lösung eines Herstellers für Ihre Backends verwenden, eine Light Agent-Lösung eines anderen Herstellers für Ihre VDI und zusätzlich noch die Programmkontrolle eines Drittanbieters für einen bestimmten Bereich hinzufügen. Die Folge dieses Ansatzes ist jedoch, dass Sie drei Verwaltungskonsolen haben, dreifache Richtlinien konfigurieren müssen und zusätzlichen Datenverkehr bei Aktualisierungen zu verkraften haben.
Da ist es bestimmt sehr viel besser, auf einen Hersteller zu vertrauen, so dass alle Steuer- und Kontrollelemente auf einer gemeinsamen Konsole organisiert sind. Alle Sicherheitslösungen von Kaspersky Lab können zentral mit dem Kaspersky Security Center gesteuert werden. Sie können also Ihre virtualisierten Ressourcen mit derselben Konsole verwalten, die Sie auch zum Steuern der Sicherheitslösung Ihrer physischen Endpoints verwenden.

Ein weiterer Vorteil besteht in der zentralen Aktualisierung. Sie müssen nicht wiederholt dieselben Updates für jede SVA auf jedem Hypervisor herunterladen, da Updates automatisch bereitgestellt werden, nachdem sie in den KSC-Speicher geladen wurden.



Ein weiteres Unterscheidungsmerkmal der Lösungen von Kaspersky Lab ist die Unterstützung verschiedener Virtualisierungsplattformen. Sie können daher eine Multi-Hypervisor-Umgebung verwenden und trotzdem sämtliche Kontrollfunktionen von KSC nutzen.

Abbildung 1: Eine Multi-Hypervisor-Umgebung kann zuverlässig und effizient geschützt werden

Beispiel: Ihr Active-Directory-Kern (Domain Controller, Domain-Name-Systeme usw.) können auf virtualisierten Microsoft Hyper-V-Servern gehostet werden, eine Citrix-basierte VDI verwenden und Datenbankserver mit VMware ESXi enthalten. Sie können aber auch, wie in der obigen Abbildung, kombinierte Umgebungen mit mehr als einer Hypervisor-Plattform und physischen Endpoints verwenden.

In diesem Fall gilt für ein optimales Verhältnis von Performance und Sicherheit und optimale Konsolidierungsraten Folgendes:

- Eine isolierte VDI mit einem bestimmten Nutzungszweck kann durch KSV | Agentless geschützt werden.
- Die geschäftskritische Server-Infrastruktur, die wichtige Daten enthält, sollte durch die robusten Sicherheitsebenen von KSV | Light Agent geschützt werden.
- Für die Testumgebung mit Linux-Hypervisor und einer Sammlung von Gast-Betriebssystemen und physischen Endpoints ist der Schutz mit Kaspersky Endpoint Security am besten geeignet.

In jedem Fall bieten Ihnen die Produkte von Kaspersky Lab zuverlässigen Schutz und ermöglichen Ihnen die Auswahl zwischen einfachem Deployment und ROI-Effizienz von KSV | Agentless, dem soliden Schutz von KSV | Light Agent und einer beliebigen Kombination innerhalb einer einzelnen IT-Infrastruktur.

Da Kaspersky Lab agentenlose, Light Agent und agentenbasierte Virtualisierungslösungen bietet, können wir unsere Kunden objektiv beraten. Wir brauchen keine bestimmte Technologie zu bevorzugen, sondern können die jeweils beste Option bzw. Kombination von Optionen für die spezifische Umgebung des Kunden empfehlen. Und da alle unsere Lösungen auf derselben Malware-Engine aufbauen und alle Lösungen Bestandteil einer integrierten Sicherheitsplattform sind, wissen wir, dass Sie, wofür auch immer Sie sich entscheiden, eine effiziente Lösung für den Schutz Ihrer virtualisierten Systeme haben werden.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Labs GmbH, Ingolstadt, Deutschland
www.kaspersky.de

Informationen zur Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in Ihrer Nähe finden Sie hier:
http://www.kaspersky.com/de/partner_finden

KASPERSKY lab