KASPERSKY lab

LIGHT AGENT ODER AGENTLESS

Ein Feature-Leitfaden zu Kaspersky Security for Virtualization

www.kaspersky.de

Die immer stärkere Verbreitung der Virtualisierung macht den Bedarf an geeigneten Sicherheitslösungen offensichtlich. Obwohl virtualisierte Umgebungen genauso anfällig für Cyberangriffe sind wie physische Systeme, weisen sie doch einige besondere Merkmale auf, die im Hinblick auf Sicherheitslösungen berücksichtigt werden müssen.

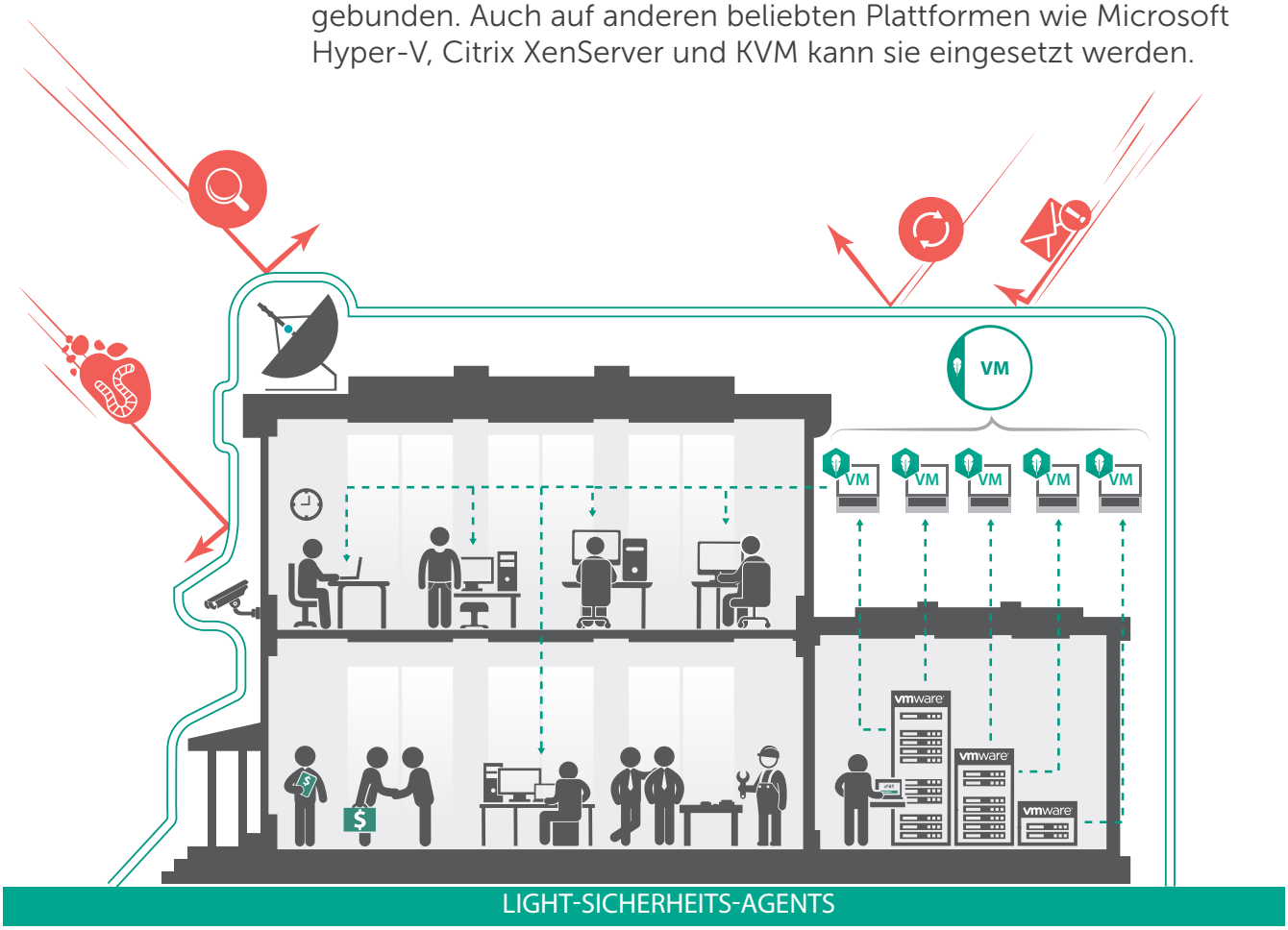
Unternehmen können dieselbe Sicherheitssoftware zum Schutz von physischen und virtuellen Maschinen einsetzen. Standardlösungen, die nicht speziell für virtualisierte Umgebungen entwickelt wurden, können zwar ein bestimmtes Maß an Schutz bieten, sie bergen jedoch häufig auch Risiken wie die folgenden:

1. **Exzessive Ressourcennutzung:** Verursacht durch die Replikation von Signaturdatenbanken und aktiven Anti-Malware-Engines auf der jeweiligen geschützten virtuellen Maschine (VM).
2. **„Storms“:** Simultane Datenbank-Updates und/oder Anti-Malware-Scans auf mehreren VMs führen zu einer lawinenartigen Zunahme der Ressourcenauslastung, die drastische Leistungseinbußen bis hin zum Denial of Service (DoS) verursachen können. Versuche, dieses Problem durch die Planung solcher Prozesse zu umgehen, führen zu „Vulnerability-Zeitfenstern“ – Zeitphasen, in denen auf einen späteren Zeitpunkt verlegte Malware-Scans die VM für Angriffe anfällig machen.
3. **„Instant-on“-Lücken:** Auf inaktiven VMs können Signaturdatenbanken nicht aktualisiert werden. Vom Start der Maschine bis zum Abschluss des Update-Vorgangs ist die VM für Angriffe anfällig.
4. **Inkompatibilitäten:** Da Standardlösungen nicht für virtualisierungsspezifische Funktionen wie die Migration von VMs oder nicht persistentem Speicher geschaffen sind, kann ihre Nutzung zu Instabilität und Systemabstürzen führen.

Um den Sicherheitsanforderungen virtualisierter Systeme und den besonderen Merkmalen der Virtualisierung gerecht zu werden, entwickelte Marktführer VMware mit vShield-Endpoint-Technologie einen speziellen Sicherheits-Layer für seine vSphere-Virtualisierungsplattform. Diese zusätzliche Ebene schafft einen integrierten sicheren Raum für Drittanbieterlösungen, die nativ über VMware-APIs, wie z. B. vShield Endpoint und NSX Guest Introspection, integriert werden können und alle virtualisierten Assets umfassen. So erhalten entsprechende Sicherheitslösungen einfachen und effizienten Zugriff auf die entsprechenden Ressourcen. Es ist nur eine Security Virtual Machine (SVM) – eine spezielle, mit Anti-Malware-Scan-Engine und Signaturdatenbanken ausgestattete virtualisierte Maschine – pro Host erforderlich, sodass die Ressourcen einzelner VMs geschont

werden und die Ressourcenauslastung erheblich reduziert wird. Der größte Vorteil dieses Ansatzes für Enterprise-Unternehmen ist die naht- und reibungslose Integration in die VMware-Umgebung.

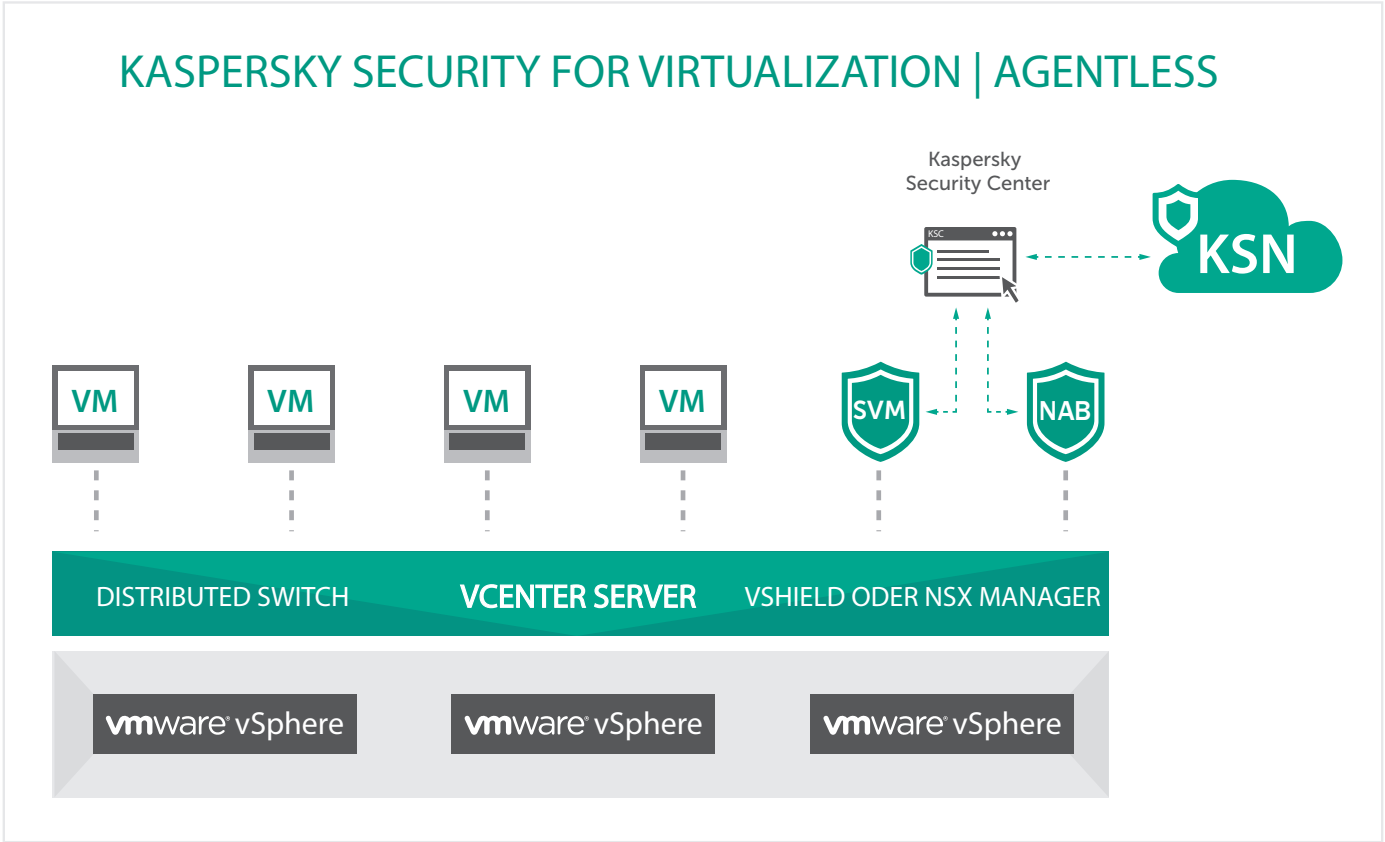
Eine Alternative stellen Lösungen dar, die von APIs bzw. Virtualisierungsplattformen unabhängig agieren und einen ressourcenschonenden Agenten nutzen, der für das Betriebssystem der jeweiligen VM optimiert ist. Da sich Scan-Engine und Datenbanken auch bei diesem Ansatz zentral auf der SVM befinden, beansprucht die Light-Agent-Technologie die Systemressourcen deutlich weniger als traditionelle Lösungen mit Full Agents. Die Lösung liegt bei der Ressourcenauslastung zwischen dem agentenlosen und dem Full-Agent-Ansatz und ist darüber hinaus nicht an VMware-Technologien gebunden. Auch auf anderen beliebten Plattformen wie Microsoft Hyper-V, Citrix XenServer und KVM kann sie eingesetzt werden.



KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless wurde speziell für die Nutzung von vShield Endpoint und der damit einhergehenden Vorteile entwickelt. Die direkt einsetzbare Security Virtual Machine (SVM) wird von der vielfach ausgezeichneten Anti-Malware-Engine von Kaspersky Lab unterstützt und bietet eine hervorragende Erkennungsrate und Performance. Die Einbindung des Cloud-basierten Kaspersky Security Network-Service gewährleistet geringstmögliche Reaktionszeiten und die Erkennung neuer Malware im Sekundenbereich. So kann Kaspersky Security for Virtualization Ihre virtualisierte Umgebung selbst vor Zero-Day-Bedrohungen schützen.

VMware NSX-Umgebungen können die Vorteile der Integration zwischen Kaspersky Security for Virtualization | Agentless und VMware NSX Guest Introspection optimal nutzen. So lässt sich Ihre Infrastruktur grenzenlos skalieren, während Ihre Sicherheitslösung nahtlos über alle Topologie- und Infrastrukturänderungen informiert ist.



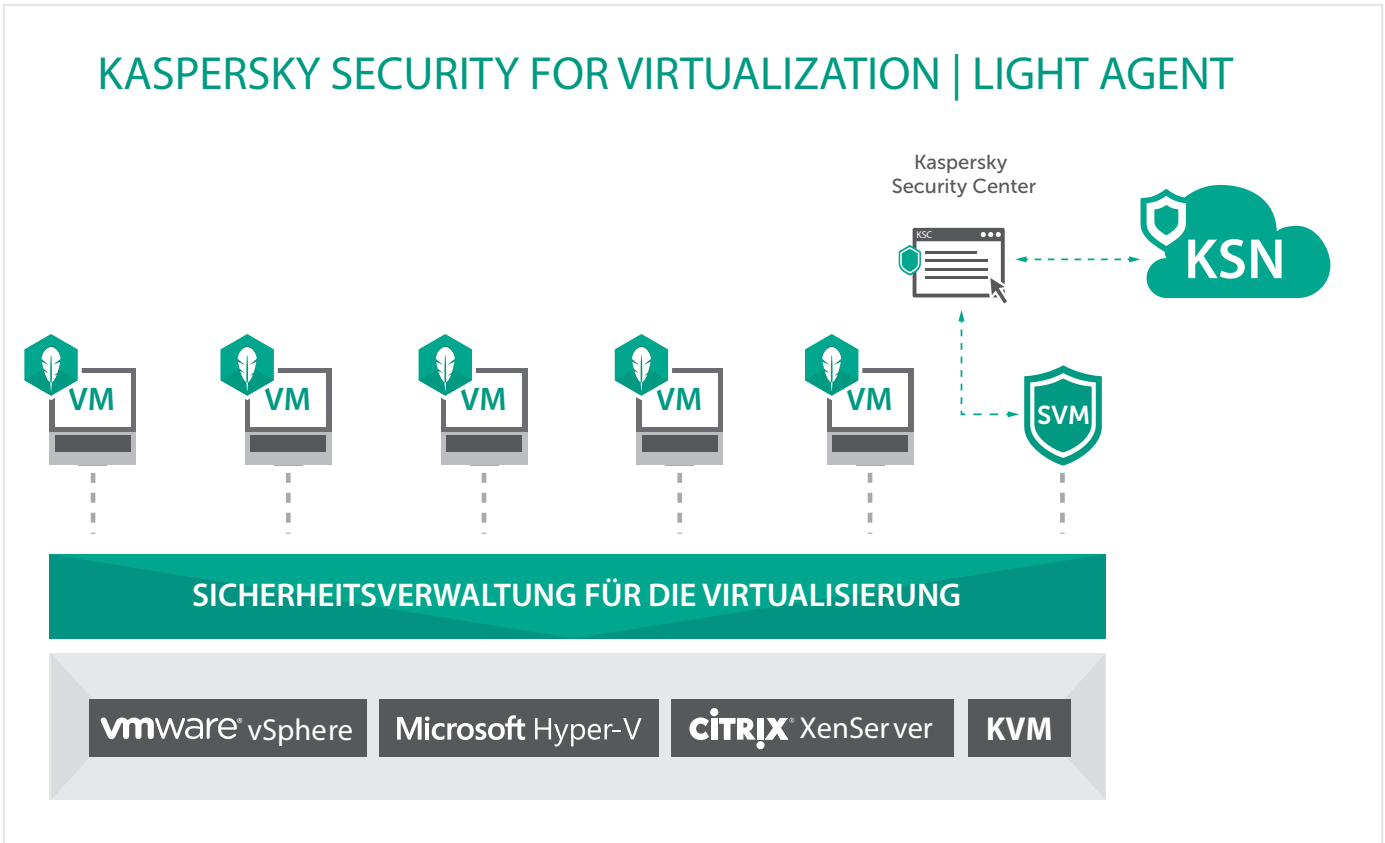
Zur Steigerung des Netzwerkschutzes kann eine zweite SVM eingesetzt werden, um die Funktionalität von Kaspersky Network Attack Blocker mit enger Integration in die VMware NSX-Plattform sowie in die Komponente vCloud Networking & Security bereitzustellen.

Bei einem agentenlosen Ansatz gibt es Defizite. Zunächst ist VMware vSphere die einzige Virtualisierungsplattform mit einer zwischengeschalteten Sicherheitsebene: NSX oder vShield Endpoint. Bei anderen Virtualisierungsplattformen muss die Sicherheitslösung in Form eines Agenten innerhalb des Gastbetriebssystems der jeweiligen VMs installiert werden, um Dateiscans auf Geräteebene durchführen zu können. Zweitens bieten native Technologien wie vShield Endpoint und NSX Guest Introspection aufgrund des VMware-Designs keinen Zugriff auf die internen Prozesse, Programme und den Web-Datenverkehr der VM sowie auf virtualisierte Geräte. Der Schutz der Infrastruktur ist auf Scans der Dateiebene beschränkt, was die Fähigkeit der Lösung, tief gehenden Schutz vor fortschrittlicher Malware auf VM-Ebene zu bieten, deutlich einschränkt.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Der Ansatz mit Light Agent umgeht all diese Einschränkungen. Da sich Scan-Engine und Datenbanken auch bei diesem Ansatz zentral auf der SVM befinden, beansprucht diese Lösung die Systemressourcen deutlich weniger als traditionelle Lösungen mit Full Agents. Die auf den VMs installierten Light Agents bieten Zugriff auf den Arbeitsspeicher, die Programme und die internen Prozesse des jeweiligen Geräts sowie zum Web-Datenverkehr und zu virtualisierten Geräten. Mithilfe dieses Zugriffs können fortschrittliche Sicherheitstechnologien direkt auf Maschinenebene installiert werden. So werden Effizienz und Systemleistung der Virtualisierungsplattform geschont.

Kaspersky Security for Virtualization | Light Agent wurde speziell für virtuelle Umgebungen entwickelt und unterstützt viele der beliebtesten Plattformen: Citrix XenServer, Microsoft Hyper-V, VMware und die neueste Version von KVM.



In virtualisierten Serverumgebungen genießen Nutzer von Kaspersky Security for Virtualization | Light Agent die Vorteile verschiedener nützlicher Technologien wie ein HIPS (Host-based Intrusion Prevention System) und unsere Firewall, die Schutz vor Netzwerkangriffen bieten. In VDI-Umgebungen wird die Sicherheit durch umfassende Funktionen zum Netzwerkschutz sowie einer Reihe von Endpoint-Kontrollen ergänzt. So können Sie Ihre Systeme nicht nur vor Malware schützen, sondern können auch die Nutzung nicht vertrauenswürdiger Programme, Geräte und Web-Ressourcen einschränken. Die Architektur der Lösung reduziert die Angriffsfläche deutlich und spart wertvolle Rechenressourcen. Der leistungsstarke mehrschichtige Verteidigungsparameter, der die Gefahr durch raffinierte Malware und sogar Zero-Day-Bedrohungen beseitigt, wird durch AEP-Technologie (Automatic Exploit Prevention) ergänzt.

Mit dem Light-Agent-Ansatz können Sie Ihre virtuelle Umgebung, einschließlich virtueller Server und VDI, schützen und hierbei die Systemressourcen des Hypervisors schonen. So schützen Sie Ihre Systeme und vertraulichen Unternehmensdaten vollständig, aber bewahren gleichzeitig die Maschinendichte und Qualität der Benutzererfahrung.

SCHUTZ VON KASPERSKY LAB VOR DEN BEDROHUNGEN IHRER VIRTUELLEN INFRASTRUKTUR

VMs sind genauso gefährdet wie ihre physischen Pendants – vielleicht sogar noch mehr. In diesen blitzschnellen virtualisierten Netzwerken kann die Ausbreitung von Infektionen verheerende Folgen haben. Daher ist es wichtig, etwaige Sicherheitslücken in Ihrer virtualisierten Infrastruktur zu kennen und eine effiziente Sicherheitslösung zu implementieren, die Schutz speziell vor fortschrittlichen Bedrohungen bietet. Im Folgenden untersuchen wir potentielle Bedrohungen für virtualisierte Systeme und die Technologien zu deren Bekämpfung.

Ausführbare Malware-Dateien

Ob es sich um einen heimtückischen E-Mail-Anhang, infizierte Unterhaltungsmedien oder eine temporäre ausführbare Malware-Datei handelt – der Malware-Schutz ist unumgänglich, um diesen grundlegenden Bedrohungen Herr zu werden. Den Kern von Kaspersky Security for Virtualization | Agentless und Light Agent bildet unsere leistungsstarke Anti-Malware-Engine, jedoch werden verschiedene Methoden eingesetzt, um auf die Dateiebene der geschützten VM zuzugreifen.

Eine andere Möglichkeit, Ihre virtualisierten Ressourcen vor Malware zu schützen, bietet die Programmkontrolle mit dynamischen Whitelists. Wenn nur vertrauenswürdige Software auf einer VM ausgeführt werden darf, hat ausführbare Malware keine Chance. Kaspersky Security for Virtualization | Light Agent bietet Endpoint-Kontrollen, einschließlich Programmkontrolle, die auf den einzelnen VMs aktiviert werden können.

Körperlose Malware

Eine raffinierte Form der Malware agiert sozusagen „körperlos“. Das heißt, im Dateisystem ist kein Hinweis darauf zu finden. Ausgelöst durch eine vorher gestartete EXE-Datei oder via Exploit eingebracht ist diese Malware mit traditionellen Malware-Schutzlösungen kaum zu entdecken. Hier sind erweiterte Techniken erforderlich, die Prozesse im Speicher überwachen und Programme sofort blockieren können, wenn diese verdächtige oder gefährliche Aktivitäten ausführen.

Kaspersky Security for Virtualization | Light Agent ist mit einer Reihe von Technologien ausgerüstet, die einen feindlichen Einfall in den Speicher der VM verhindern. Diese beinhalten:

- Aktivitätsmonitor, der das Programmverhalten überwacht und Systemereignisse anzeigt.
- Verhaltensmuster-Signaturen, die Malware-Aktivitäten anhand von Verhaltensmuster-Merkmalen erkennen.

- Steuerung von Programmberechtigungen, die Programme daran hindert, unzulässige Änderungen (z. B. Prozessinjektionen) vorzunehmen.

Diese Werkzeuge ermöglichen dem HIPS (Host-based Intrusion Prevention System) das Verfolgen und Stoppen schädlicher Prozesse im VM-Speicher.

Exploits

Die Ausnutzung von Schwachstellen, die in Systemkomponenten und häufig genutzten Programmen zu finden sind, ist jedoch weiterhin eine äußerst effektive Angriffsmethode. Es ist zwar möglich, diesen Einbrüchen mithilfe der oben genannten Technologien entgegenzuwirken, wenn das betroffene Programm jedoch auf hoher Berechtigungsebene arbeitet, ist die Kontrolle über seine Aktivitäten beschränkt.

Die effektivste Methode, solche Bedrohungen zu meistern, ist es, die Ausnutzung von Schwachstellen zu verhindern. Um der Gefahr ungepatchter Schwachstellen schnell Einhalt zu gebieten, beinhaltet Kaspersky Security for Virtualization | Light Agent eine Technologie, die wir Automatic Exploit Prevention (AEP) nennen. AEP überwacht speziell die am häufigsten angegriffenen Programme in kritischen Umgebungen wie VDI – darunter Adobe Reader, Internet Explorer, Microsoft Office und Java – und bietet somit eine zusätzliche Ebene der Sicherheitsüberwachung und des Schutzes vor unbekannten Bedrohungen.

Die Effizienz dieser Technologie wurde bereits in unabhängigen Tests des MRG Effitas Institute bestätigt, in denen die AEP-Technologie von Kaspersky Lab selbst bei Deaktivierung aller anderen Schutzkomponenten zu 100 % wirksam gegen Angriffe ist, bei denen Exploits eingesetzt werden (weitere Informationen hierzu finden Sie in Real World Enterprise Security Exploit Prevention, MRG Effitas, März 2015). Sogar unbekannte Zero-Day-Exploits werden mithilfe dieser Technologie blockiert.

Rootkits

Ausgeklügelte Malware ist häufig in der Lage, sich zu verbergen, und mithilfe sogenannter „Bootkits“ und „Rootkits“ die Erkennung durch traditionelle Anti-Malware zu verhindern. Diese Tools versuchen, die Malware so früh wie möglich zu starten und auszuführen, sodass sie innerhalb des Gastbetriebssystems hohe Berechtigungen erhält und so unerkannt bleiben kann.

Kaspersky Security for Virtualization | Light Agent agiert auf Speicher- und Dateisystemebene und nutzt die Anti-Rootkit-Technologie von Kaspersky Lab, um solche tief versteckte Malware zu finden und zu beseitigen.

Netzwerkangriffe

Netzwerkbasierte Cyberbedrohungen können es dem Angreifer ermöglichen, wichtige Informationen über das Netzwerk abzurufen, Zugang zu den Ressourcen des angegriffenen Systems zu erhalten und so wichtige Prozesse zu stören und den reibungslosen Betrieb zu unterbrechen. Diese Bedrohungen beinhalten schädliche Aktionen wie Portscans, DoS-Attacken (Denial of Service) und Buffer-Underruns. Beide Konfigurationen, Agentless und Light Agent, verfügen über integrierte Technologien für den Netzwerkschutz. Kaspersky Security for Virtualization | Light Agent erweitert den Netzwerkschutz um ein integriertes HIPS (Host-based Intrusion Prevention System) und zusätzliche Kaspersky-eigene Technologien zur Abwehr externer und interner Netzwerkangriffe – einschließlich Bedrohungen, die sich in nicht transparentem virtualisierten Datenverkehr verbergen.

Auch Kaspersky Security for Virtualization | Agentless geht dieses Problem an, indem über die VMware-Integration unser Network Attack Blocker bereitgestellt wird. Hierbei handelt es sich um eine virtuelle Appliance, die den Netzwerkdatenverkehr nach Anzeichen häufiger Angriffsaktivitäten durchsucht.

Schädliche Webseiten

Eine der häufigsten Infektionsquellen sind schädliche oder infizierte Webseiten. Zwar wirken sich diese selten auf virtualisierte Server aus, jedoch stellen sie ein ernsthaftes Risiko für VDIs dar – eine Tatsache, die von vielen Unternehmensbenutzern gerne ignoriert wird. An dieser Stelle kommen die Web-Schutztechnologien von Kaspersky Lab ins Spiel.

Der Phishing-Schutz verhindert, dass Benutzer auf Webseiten zugreifen, die als gefährlich gemeldet wurden. Hierfür werden Informationen aus dem Kaspersky Security Network (KSN) bereitgestellt, die mithilfe von Millionen freiwilliger Teilnehmer des KSN überall auf der Welt kontinuierlich aktualisiert werden. Auch bisher nicht erkannte Phishing-Webseiten werden dank einer heuristischen Engine blockiert, die den Quelltext der geladenen Seite analysiert und dabei Hinweise auf schädlichen Code erkennt. Mit der Web-Kontrolle können Sie die Internetnutzung steuern: Sie können den Zugang zu sozialen Netzwerken, Musik, Videos, externen E-Mail-Tools und anderen Webseiten mit unangemessenen oder gemäß Unternehmensrichtlinie ungeeigneten Inhalten blockieren. Darüber hinaus können Sie für unterschiedliche Benutzerrollen verschiedene Kontrollen festlegen und zwischen der vollständigen Blockierung und der Blockierung zu bestimmten Zeiten wählen.

Angriffe über Peripheriegeräte

Eine der traditionell wirksamsten Methoden der Infizierung eines IT-Netzwerks ist die Verwendung von externen Speichergeräten. Während über das Netzwerk eingeschleppte Infektionen derzeit rein zahlenmäßig die größte Bedrohung ausmachen, geht auch von externen Speichergeräten eine deutliche Gefahr aus – insbesondere, wenn sie als Teil eines sorgfältig geplanten Angriffs eingesetzt werden. Hierbei ist erwähnenswert, dass nicht nur Speichergeräte, sondern auch andere nicht regulierte Peripheriegeräte eine Gefahr darstellen können, jedoch werden am häufigsten Speicherlaufwerke eingesetzt, um vertrauliche Daten zu stehlen. Zwar ist es für eine nicht autorisierte Person nicht leicht, auf die physischen Geräte zuzugreifen, die Ihre virtuelle Infrastruktur hostet, aber es ist dennoch möglich.

Hardware, die eine Verbindung zu Ihrer virtualisierten Umgebung herstellt, stellt also einen wichtigen Sicherheitsaspekt dar. So sehen die Best Practices für VDI-Umgebungen beispielsweise den Einsatz von Thin Clients vor, und auch die einfachsten Thin Clients verfügen über USB-Ports. Die Kontrolle von Peripheriegeräten kann sich schnell zum Albtraum entwickeln – nicht aber mit der Gerätekontrolle von Kaspersky Lab. Mit dieser Technologie können Sie bestimmen, welche externen Geräte Zugriff auf die jeweilige VM erhalten, indem Sie auf einfache Weise Richtlinien festlegen, die die erlaubten Geräte einschließlich Wechseldatenträgern, Druckern und externen Netzwerkverbindungen beinhalten.

Datenlecks

Wenn Unternehmensgeheimnisse, die eigentlich sicher in der IT-Umgebung gespeichert sein sollten, das Licht der Öffentlichkeit erblicken, gefährdet dies nicht nur geschäftskritische Prozesse und Systeme, sondern das gesamte Geschäft – einschließlich Rufschädigung, die langfristige und schmerzhafte Folgen für Ihr Unternehmen haben kann. Für den Schutz Ihres Geschäfts empfiehlt es sich also, die Anzahl der Möglichkeiten einzuschränken, über die Benutzer auf die entsprechenden Informationen zugreifen können.

Sowohl die Programmkontrolle als auch die Gerätekontrolle von Kaspersky Lab sind in diesem Fall nützlich. Mit der Programmkontrolle kann die Ausführung potentiell gefährlicher Programme wie Instant Messenger und Programme für Datei-Hosting und P2P-Clients verhindert werden. Die Gerätekontrolle beschränkt die Verwendung externer Speichergeräte, die zum Diebstahl vertraulicher Daten missbraucht werden können. Beide Technologien sind in Kaspersky Security for Virtualization | Light Agent enthalten.

Agentless oder Light Agent: Was ist besser?

Die Antwort hängt davon ab, welche Virtualisierungsplattform oder anderen Plattformen und welche spezifischen Deployments Sie nutzen. Unabhängig davon, welcher Hypervisor für den Aufbau der virtualisierten Umgebung eingesetzt wurde (VMware vSphere, Citrix XenServer, Microsoft Hyper-V oder KVM), können Sie für den Schutz Ihrer kritischen virtuellen Server und Ihrer schnell wachsenden VDI Kaspersky Security for Virtualization | Light Agent nutzen. Für nicht kritische VMware-basierte Server können Sie jedoch auch Kaspersky Security for Virtualization | Agentless in Erwägung ziehen, die keine starke mehrschichtige Sicherheit benötigen.

Glücklicherweise ermöglicht es Ihnen das Lizenzmodell von Kaspersky Security for Virtualization, im Rahmen einer einzigen Lizenz den optimalen Ansatz für jeden Teil Ihrer virtualisierten Umgebung auszuwählen: Agentless, Light Agent oder eine Kombination aus beidem.

Egal, welche Kombination von Virtualisierungsplattformen wie Citrix XenServer, VMware vSphere, KVM und Microsoft Hyper-V Sie verwenden und welchen Ansatz Sie verfolgen: Sie können all Ihre virtuellen und physischen Geräte sowie die Sicherheit mobiler Geräte einfach und zentral über das Kaspersky Security Center verwalten. Darüber hinaus ermöglicht die Nutzung von Kaspersky Security Network, unseres Cloud-basierten Sicherheitsservice, die sofortige Erkennung neuester Bedrohungen.