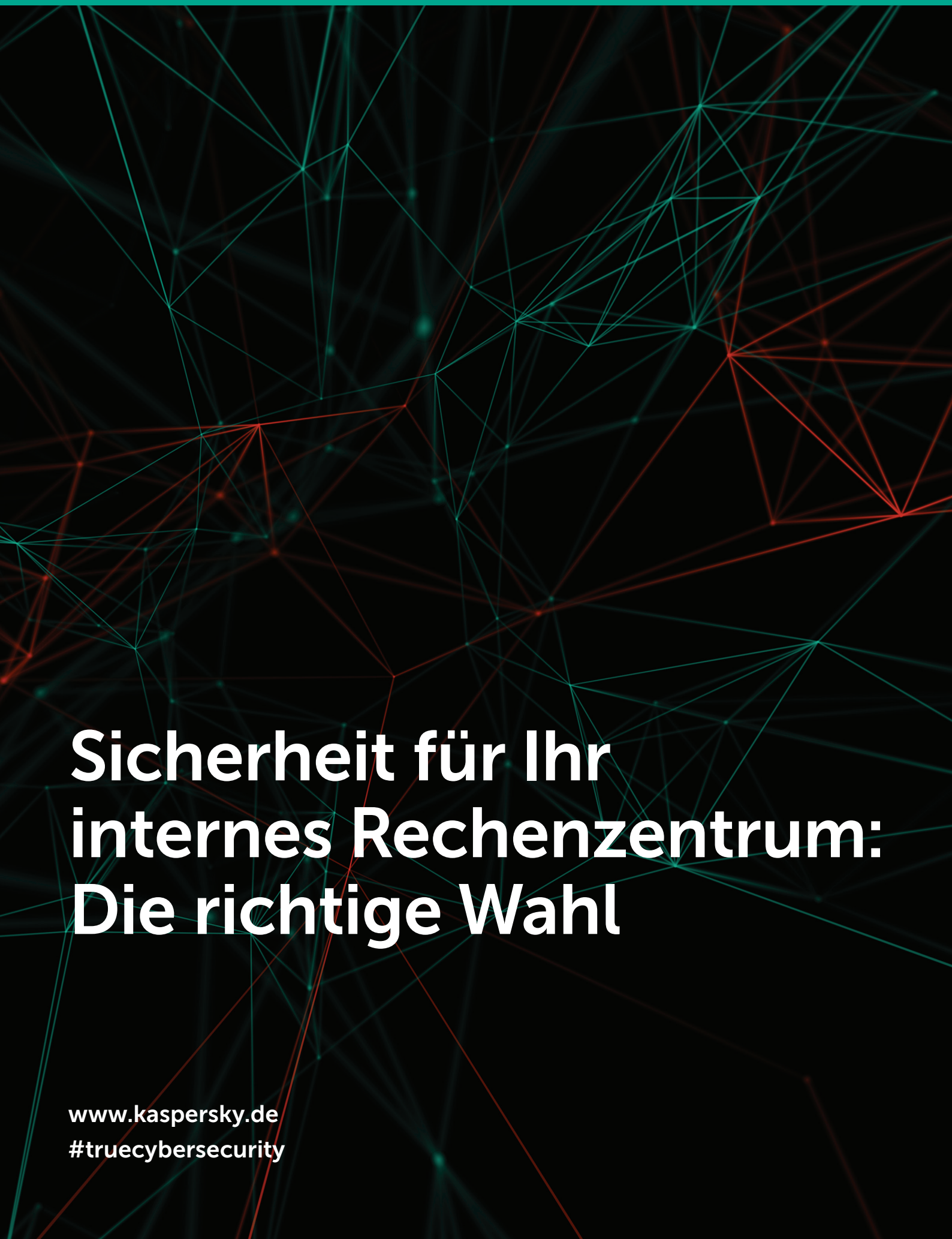
KASPERSKY lab



Sicherheit für Ihr internes Rechenzentrum: Die richtige Wahl

www.kaspersky.de
#truecybersecurity

Sicherheit für Ihr internes Rechenzentrum: Die richtige Wahl

Zweck dieses Dokuments

Das Denkmuster bei der Einrichtung von Rechenzentren unterliegt einem deutlichen Wandel und erfolgt zunehmend auf softwarezentrierter Basis. Konzepte zur Virtualisierung von Computing-Ressourcen, die seit Jahren erfolgreich im Einsatz sind, haben auch in anderen Branchen Anwendung gefunden – ein Beispiel ist die Virtualisierung der Netzwerkinfrastruktur. Virtualisierungstechnologien sind längst zum Unternehmensstandard geworden (einer Statistik von 2016 zufolge erreicht die Virtualisierungstechnologie im Unternehmenssegment eine Durchdringung von 75 %). Ziel dieses Übergangs ist es, die Verwaltung eines Unternehmens-Rechenzentrums so zu gestalten, dass sie von Geschäftsprozessen und nicht von der Infrastruktur bestimmt wird.

Alle diese Änderungen erfordern natürlich eine genaue Prüfung der Schutzrichtlinien für Unternehmensrechenzentren. Diese Richtlinien müssen bei der Aktualisierung von Rechenzentrum-Technologien aktualisiert werden. Wenn die IT-Sicherheit nicht mit den Änderungen der Infrastruktur Schritt halten oder sich schnell an diese Änderungen anpassen kann, sollten Sie sich überlegen, ob Sie stattdessen zum Schutz Ihres Rechenzentrums dedizierte Lösungen einsetzen.

Dabei ist zu berücksichtigen, dass das Rechenzentrum ursprünglich als effiziente Hochleistungsplattform zur Erreichung der Geschäftsziele dienen sollte. Sicherheitslösungen sollten daher die Leistung der im Rechenzentrum des Unternehmens eingesetzten Systeme nicht beeinträchtigen.

Kaspersky Lab bietet eine dedizierte Sicherheitslösung für Rechenzentren, die speziell entwickelt wurde, um Unternehmens-Rechenzentren vor den fortschrittlichsten Cyberbedrohungen zu schützen und gleichzeitig die Auswirkungen auf die darin enthaltenen Systeme zu minimieren.

Was ist ein Unternehmens-Rechenzentrum, und warum muss es unbedingt geschützt werden?

Eine Welt, in der Unternehmen keine Informationen verarbeiten, speichern und weitergeben müssen, ist heute unvorstellbar. All dies geschieht in den modernen Rechenzentren von Unternehmen. Ein Unternehmens-Rechenzentrum kann entweder privat oder öffentlich sein. Es kann sich auf dem oder außerhalb des Firmengeländes befinden. In den meisten Fällen ist ein Rechenzentrum jedoch eine viel kompliziertere Entität, in der oft öffentliche, private und geografisch verteilte Infrastrukturen kombiniert werden. In jedem Fall wird der Unternehmensbetrieb durch ein modernes Rechenzentrum sehr viel effizienter, da geschäftliche Veränderungen anhand der Infrastruktur schneller verfolgt und Ressourcen für neue betriebliche Aufgaben effizienter bereitgestellt werden können.

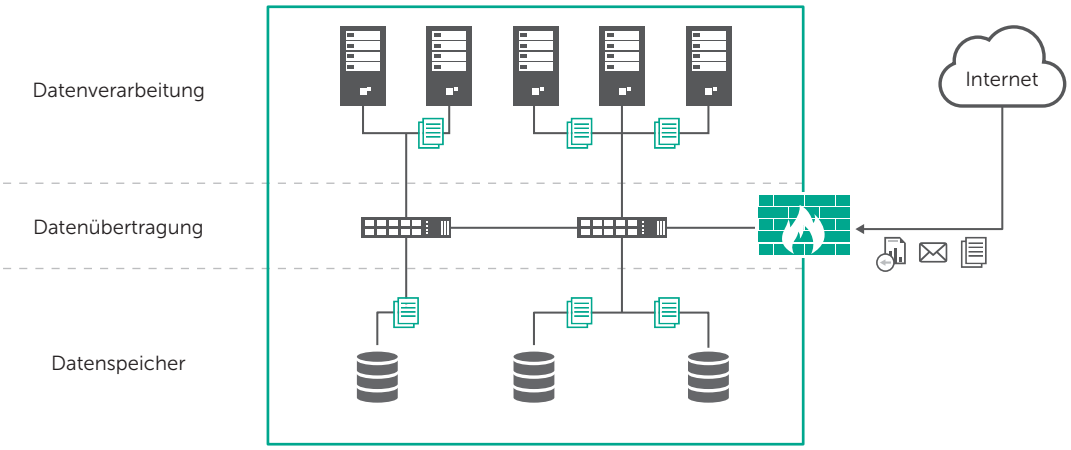


Abbildung 1: Übergeordnete Architektur eines Rechenzentrums

„Über 75 % von Unternehmen arbeiten bereits mit softwarezentrierten Rechenzentren, und die Durchdringungsrate der Virtualisierung wächst von Jahr zu Jahr weiter."

Zwar werden Rechenzentren für Unternehmen mithilfe moderner Technologien aufgebaut, aber die bei der Organisation der Infrastruktur an den Tag gelegte Ideologie ist weitgehend unverändert:

- **Datenverarbeitung**: stellt Rechenressourcen für Geschäftsanwendungen zur Verfügung
- **Datenspeicher**: ist für die Speicherung der Unternehmensdaten verantwortlich
- **Datenübertragung**: hilft, alle Kommunikations- und Datenströme problemlos zu organisieren

Alle diese Komponenten sind für den effizienten Betrieb eines Rechenzentrums unerlässlich, egal, ob es sich um ein öffentliches, privates oder hybrides Rechenzentrum handelt.

Rechenzentren gelten heute in Unternehmen als ein Werkzeug mit einer zuverlässigen Infrastruktur und flexibel skalierbaren Systemen, die stets höchste Leistung und Effizienz bieten. Unternehmen stellen weitere Anforderungen an Rechenzentren: Sie benötigen mehr Ressourcen, erhöhte Kontrolle, gesteigerte Zuverlässigkeit, maximierte betriebliche Effizienz und bessere Sicherheit.

Den neuesten Studien und Umfragen zufolge **gehört die Sicherheit der Infrastruktur zu den drei wichtigsten Aspekten des Rechenzentrums-Betriebs,** sowohl für die Eigentümer von Rechenzentren als auch für große Unternehmen.

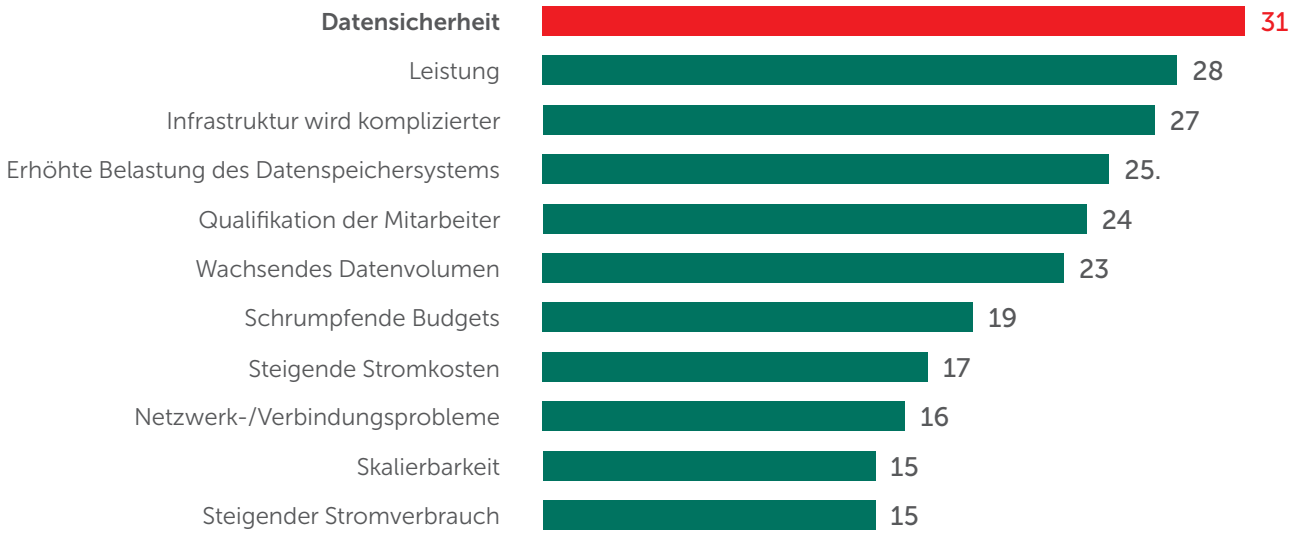


Abbildung 2: Hauptprobleme beim Rechenzentrums-Management[1]

Gleichzeitig stehen Unternehmen bei der Umstellung ihrer geschäftskritischen Systeme auf Unternehmens-Rechenzentren zunehmend vor der Herausforderung, dass ihr bestehendes IT-Sicherheitskonzept überarbeitet werden muss, da es nicht zum Schutz eines modernen Rechenzentrums geeignet ist.

Grundsätzlich besteht das Problem darin, dass die Technologien, auf denen moderne Rechenzentren beruhen, neue Arten der Benutzerinteraktion ermöglichen und zusätzliche Verbindungen zwischen Infrastrukturkomponenten schaffen.

„Bei der Sicherheit moderner Rechenzentren muss ein neuer Denkansatz verfolgt werden, um den Technologien Rechnung zu tragen, mit denen Unternehmen ihre eigenen Rechenzentren aufbauen."

Hervorzuheben ist, dass Sicherheit zwar der Hauptmotivationsfaktor für die Überarbeitung des IT-Sicherheitskonzepts moderner Rechenzentren ist, dass aber die Aufrechterhaltung der Systemleistung und eine benutzerfreundliche Steuerung der gesamten Infrastruktur für die Führungskräfte des Unternehmens nach wie vor wichtige Themen bleiben.

---

[1] http://www.seagate.com/de/de/tech-insights/data-center-management-master-ti/

Was in Ihrem Rechenzentrum den stärksten Schutz erfordert

Aus infrastruktureller Sicht ist ein modernes Rechenzentrum eine relativ einfache Kombination mehrerer Systeme.

- Eine Datenverarbeitungsinfrastruktur, die mit einer Virtualisierungsplattform wie VMware vSphere, Microsoft Hyper-V, Citrix XenServer oder KVM aufgebaut wird und Unterstützung für virtuelle Server und Workstations bietet
- Eine Unternehmensdatenspeicher-Infrastruktur, die meistens als Kombination aus direkt mit dem Unternehmensnetzwerk verbundenen Dateiservern und Datenspeichersystemen aufgebaut ist
- Eine Netzwerkinfrastruktur, die Datenströme und -Interaktion zwischen den Infrastrukturkomponenten des Rechenzentrums ermöglicht und unter anderem virtualisierte Netzwerke umfasst, etwa solche, die mit der VMware NSX-Technologie erstellt wurden

Alle diese Komponenten tragen dazu bei, den effizienten Betrieb des Rechenzentrums sicherzustellen. Selbstverständlich kann die Sicherheit jeder dieser Komponenten gefährdet werden.

„Die Werkzeuge zum Schutz eines Rechenzentrums sollten sich der Technologien ‚bewusst' sein, die sie schützen."

Kaspersky Lab hat sich zum Ziel gesetzt, für jede der oben genannten Komponenten einen auf die spezifischen Technologien von Rechenzentren abgestimmten Schutz zu bieten.

Speicherintensive Schutzmechanismen haben in einem modernen Rechenzentrum keinen Platz

Manchmal werden herkömmliche Lösungen, die üblicherweise zum Schutz physischer Server und Workstations verwendet werden, auch auf virtuellen Maschinen eingesetzt. Herkömmliche Sicherheitslösungen verbrauchen aber oft mehr Ressourcen, wodurch kritische Geschäftsanwendungen weniger Rechenleistung erhalten und langsamer ausgeführt werden. Benutzer bemerken dies zwangsläufig und sind dann irritiert, weil sie geschäftliche Aufgaben nicht mehr so schnell und bequem erledigen können.

„Die Idee der Virtualisierung in Rechenzentren ist es, Ressourcen effizient zu nutzen. IT-Sicherheitslösungen sollten dieser Idee nicht zuwiderhandeln."

- Konsequenterweise führt **jede virtuelle Maschine** Aufgaben aus, die zwar an sich nützlich, aber auf der Ebene des Virtualisierungs-Hosts redundant sind: Antiviren-Datenbanken werden lokal gespeichert und aktualisiert, Anti-Malware-Scans werden lokal durchgeführt, und jede VM schützt sich selbst vor Netzwerkangriffen.
- Man sollte meinen, dass dies zuverlässige Sicherheit für jede einzelne virtuelle Maschine bietet. Dieser Schutzansatz führt jedoch zu einer übermäßigen Belastung der einzelnen VMs, was letztendlich zu einer **erheblichen zusätzlichen Belastung des Virtualisierungs-Hosts** führt, während gleichzeitig die Effizienz der gesamten Infrastruktur für die Benutzer sinkt.
- Wenn Antiviren-Datenbanken gleichzeitig von virtuellen Maschinen heruntergeladen werden oder zeitgesteuerte Scans gleichzeitig durchgeführt werden, wird die Infrastruktur des Rechenzentrums extrem belastet, was zu **„Update-Storms"** und **„Scan-Storms"** führt.
- Das Herunterfahren einer virtuellen Maschine, auf der eine herkömmliche Antivirenlösung installiert ist, hat zur Folge, dass die Antiviren-Datenbanken nach und nach überaltern. Dadurch entsteht ein **„Angriffsfenster"** für neue Malware und somit eine erhebliche Bedrohung für die Sicherheit des gesamten Unternehmens-Rechenzentrums.
- Darüber hinaus ist der herkömmliche Ansatz auch für den Schutz von Netzwerkspeichersystemen und Dateiservern nutzlos, da er nicht die **Sicherheit aller Dateioperationen** gewährleistet: Der Schutz ist auf das Scannen von Dateien beschränkt, die von Datenspeichersystemen auf Benutzer-Workstations heruntergeladen werden, und schützt Netzwerkordner nicht vor **Verschlüsselungs-Malware (einschließlich Ransomware)**.

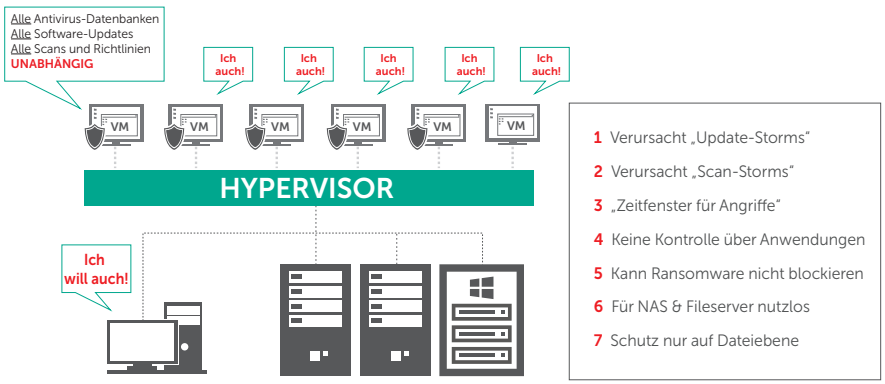


Abbildung 3: Mängel herkömmlicher Sicherheitslösungen

Die Bedrohungslage in modernen Rechenzentren

Wenn herkömmliche Lösungen zum Schutz virtueller Infrastrukturen eingesetzt werden, werden diese Infrastrukturen u. U. selbst ohne Einwirkung von Malware beschädigt. Dies drückt sich in einer deutlichen Verlangsamung aus, sodass die IT-Systeme nicht mehr ordnungsgemäß funktionieren und den Mitarbeitern des Unternehmens die Erfüllung ihrer geschäftlichen Aufgaben erschwert wird.

Untersuchungen führender IT-Sicherheitsunternehmen, darunter auch Studien von Kaspersky Lab, bestätigen, dass viele der vorhandenen Bedrohungen auch für modernste Rechenzentren gefährlich sind, wenn diese über keine oder nur unzureichend umgesetzte IT-Sicherheitsmaßnahmen verfügen.

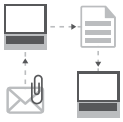
Dies liegt nicht daran, dass die in modernen Rechenzentren eingesetzten Technologien nicht ausreichen, um Bedrohungen abzuwehren. Im Gegenteil: Neue Lösungen, die in Rechenzentren implementiert werden, beruhen auf hervorragenden Ideen zum Schutz der Infrastruktur, beispielsweise auf Zero-Trust-Richtlinien für Firewalls und Mikrosegmentierungs-Methoden. Dennoch sollte der Schutz von Rechenzentren vor Cyberangriffen und Malware auf dedizierten Lösungen basieren, die speziell für virtualisierte Umgebungen und Datenspeichersysteme entwickelt wurden und mehrstufigen Schutz für das gesamte Rechenzentrum bieten.

Die gesamte Infrastruktur braucht neue Schutzmethoden

Die Infrastrukturen moderner softwarezentrierter Rechenzentren werden immer komplexer und vereinen eine Vielzahl von Systemen für unterschiedliche Geschäftsaufgaben. Je unterschiedlicher die Aufgaben, desto mehr Verbindungen gibt es zwischen Systemen und ihren Benutzern auf verschiedenen Ebenen. Die gesamte Infrastruktur muss zuverlässig geschützt werden, ohne die Performance und die in der Infrastruktur ablaufenden Geschäftsprozesse zu beeinträchtigen. Die fortschrittlichsten Technologien sollten am richtigen Ort und zur richtigen Zeit zum Tragen kommen, egal wie komplex und umfangreich die Infrastruktur des Rechenzentrums ist.

Unkontrolliertes Wachstum bei der Anzahl virtueller Maschinen

In sehr großen Infrastrukturen ist es schwierig, die Zahl der virtuellen Maschinen zu kontrollieren. Da Virtualisierung die Erstellung virtueller Maschinen mittels Vorlagen und Klonen ermöglicht, darf die Sicherheit niemals vernachlässigt werden. Einfacher ausgedrückt kann die Replikation ungeschützter oder infizierter virtueller Maschinen zu Massenausfällen und schwerwiegenden Verlusten für ein Unternehmen führen. Die Sicherheitslösung sollte jede Aktivität in Ihrem Rechenzentrum erkennen, sodass sich mit zunehmender Integration von Sicherheitsfunktionen in die IT-Umgebung die allgemeine Unternehmenssicherheit erhöht.



Netzwerkbasierte Cyberangriffe

Der Großteil der Netzwerkinteraktionen in virtualisierten Infrastrukturen erfolgt über virtualisierte Netzwerke, wobei Netzwerkverkehr und Datenströme nur selten die Hardware erreichen, die dem Schutz der Netzwerkinfrastruktur oder des Netzwerkperimeters dient. Dadurch haben weder teure Router noch Sicherheitsgeräte die volle Kontrolle über Ihr virtualisiertes Rechenzentrum. Ein virtuelles Intrusion Detection and Prevention System für Netzwerke ist für ein modernes, softwarezentriertes Rechenzentrum unerlässlich.

Deaktivierte virtuelle Maschinen

Jedes Mal, wenn Sie eine virtuelle Maschine deaktivieren, werden die darauf installierten herkömmlichen Endpoint-Sicherheitslösungen nicht mehr aktualisiert. Nach der Wiederaufnahme des Betriebs wird die betreffende virtuelle Maschine zum Schwachpunkt in der IT-Sicherheitskette eines modernen Rechenzentrums. Zudem müssen Sie ausgeschaltete virtuelle Maschinen weiterhin im Auge behalten. Möglicherweise befindet sich auf ihnen Malware, die in Aktion tritt, wenn eine VM wieder eingeschaltet wird. Sie benötigen eine zuverlässige Lösung, die jede VM unabhängig von ihrem aktuellen Betriebszustand scannen kann.

Bedrohungen für die Golden Images der VDI

Desktop-Virtualisierung bietet viele Vorteile und steigert die Effizienz. Mit einem einzigen Golden Image lassen sich innerhalb weniger Minuten Hunderte von virtualisierten Desktops erstellen. Allerdings kann jede Beschädigung oder Infektion des Golden Image dazu führen, dass Hunderte gefährlicher virtueller Maschinen erstellt werden, auf denen Benutzer unter Umständen mit geschäftskritischen Daten arbeiten. Außerdem machen Sie sich die VDI-Administratoren nicht zum Freund, wenn Sie sie darum bitten, „Golden Images" jeden Tag zu aktualisieren, nur weil Ihre Sicherheitssysteme aktualisiert wurden. Für die Administratoren ist dies eine enorme und ressourcenintensive Aufgabe. Ihre Sicherheitslösung benötigt die richtige Architektur, um einen solchen verschwenderischen Umgang mit Ressourcen zu vermeiden und dennoch jeden VDI-Rechner optimal zu schützen.

Datenspeichersysteme in Gefahr

Die meisten modernen NAS-Geräte (Network Attached Storage) sowie beliebte Dateiserver bieten erweiterte Datensicherheitsfunktionen. Benötigt wird allerdings eine zusätzliche, speziell für kritische Daten entwickelte Lösung – vorzugsweise eine Lösung, die speziell für Datenspeichersysteme entwickelt wurde und die Systemleistung nicht beeinträchtigt. Darüber hinaus können Sie nie gewährleisten, dass herkömmliche Lösungen alle Dateien in Ihrer Infrastruktur durchsuchen. Bestimmte Dateien auf den PCs Ihrer Unternehmensbenutzer könnten den Endpoint-Sicherheitslösungen verborgen bleiben. Sie benötigen ein Sicherheitstool, das in das Speichergerät selbst integriert ist und alles „sehen" kann, was vom oder zum Speicherort gelangt – jede einzelne Dateioperation, unabhängig von ihrem Ursprung.

Exzessiver Ressourcenverbrauch

Das Prinzip moderner softwarezentrierter Rechenzentren beruht darauf, die Effizienz der Systeme zu verbessern und eine hohe Konzentration von Computerressourcen zu erreichen. Die Installation einer speicherintensiven Sicherheitslösung führt zu einer enormen Belastung für jede virtuelle Maschine, was den Ressourcenbedarf von Virtualisierungs-Hosts (Hypervisors) erheblich erhöht. Somit kann eine schlecht gewählte Sicherheitslösung leicht alle Vorteile zerstören, die das Unternehmen mit dem Projekt zum Aufbau eines eigenen modernen, softwarezentrierten Rechenzentrums erreichen wollte.

Schutz für das moderne Rechenzentrum

Kaspersky Lab bietet eine dedizierte Sicherheitslösung für moderne Rechenzentren, die sowohl virtualisierte Umgebungen (virtuelle Server und Endpoints) als auch die Datenspeichersysteme von Unternehmen schützt. Kaspersky Security for Virtualization und Kaspersky Security for Storage sind jeweils Bestandteile der Lösung und wurden von Anfang an so entwickelt, dass sie sich mit den Technologien integrieren lassen, die zum Aufbau von Rechenzentren und zur optimalen Nutzung der Ressourcen eingesetzt werden.

Die einzigartige Architektur der Lösung wurde im Hinblick auf die Funktionsweise moderner Rechenzentren entwickelt, um sicherzustellen, dass die Systemleistung möglichst wenig beeinträchtigt wird. Sie trägt zur Aufrechterhaltung hoher Konsolidierungsraten bei und steigert die Effizienz beim Aufbau des Unternehmens-Rechenzentrums. Ein wichtiger Vorteil der Lösung ist die Integration mit den im Rechenzentrum eingesetzten Technologien und die zentrale Verwaltung von einer einzigen Konsole aus – dies hilft Systemadministratoren, Sicherheitsrichtlinien schneller umzusetzen.

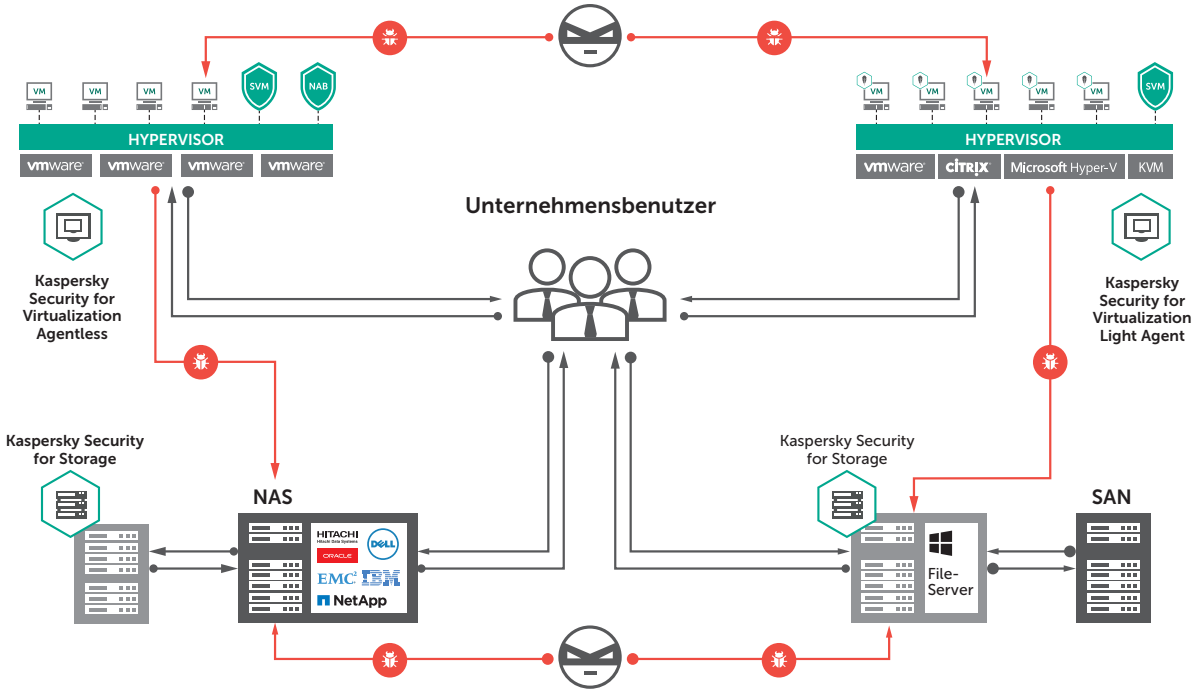


Abbildung 4: Architektur der Lösung

Kaspersky Security for Virtualization Einsatz von VMware NSX für vSphere

Die VMware vSphere-Plattform mit NSX-Technologien bildet das Netzwerk des Rechenzentrums mithilfe eines softwarezentrierten Modells ab. So kann die Netzwerktopologie in Sekundenschnelle erstellt oder neu konfiguriert und im Handumdrehen eine Sicherheitsstrategie für das Rechenzentrum auf Basis des „Zero Trust"-Modells umgesetzt werden. Die gemeinsame Lösung von Kaspersky Lab und VMware macht es einfach, einen integrierten Schutz für die Infrastruktur eines modernen Rechenzentrums bereitzustellen.

Kaspersky Security for Virtualization Agentless wurde speziell für den Schutz softwarezentrierter Rechenzentren entwickelt, die auf VMware-Technologien basieren. Da kein zusätzlicher Agent auf geschützten VMs installiert werden muss und die Prozesse, die für die virtualisierte Umgebung „überflüssig" sind, auf dedizierte Sicherheitseinrichtungen ausgelagert werden, die Datei- und Netzwerkverkehrs-Scans bereitstellen, sind die Auswirkungen der Lösung auf die Systeme eines softwarezentrierten Rechenzentrums minimal, und jede VM ist sofort nach dem Start geschützt.

Integrierte VMware NSX-Services	
Verteilte Firewall	Virtualisierte Netzwerke (VXLAN)
Überwachung der Serveraktivität	VPN (IPSec, SSL L2VPN)
Kaspersky Security for Virtualization	
Malware-Schutz	IDS/IPS für virtualisierte Netzwerke
Sicherheitsautomatisierung	Richtlinienbasierte Integration
Integration von Sicherheitsmarkierungen	Vollständiger Infrastrukturscan selbst für ausgeschaltete VMs

„Im Vergleich zu herkömmlichen Lösungen verbraucht Kaspersky Security for Virtualization Agentless 40 % weniger VM-Speicher und 80 % weniger Festplattenspeicher. Das Ergebnis ist ein effizienter und sicherer Betrieb der Unternehmenssysteme."

Die Lösung kommuniziert über eine dedizierte API mit der VMware-Infrastruktur und bietet nicht nur Schutz vor Malware für jede virtuelle Maschine sowie Erkennung und Blockierung von Netzwerkbedrohungen, sondern auch eine tiefgreifende Integration mit den Prozessen innerhalb der Infrastruktur.

- **Automatisches Deployment** vereinfacht die Arbeit des IT-Personals und IT-Sicherheitspersonals drastisch und ermöglicht die vollständige Automatisierung von Sicherheitsgeräten auf Hypervisoren auf Basis der für jede VM definierten Sicherheitsrichtlinien.
- **Eine enge Integration von Sicherheitsrichtlinien** bedeutet, dass jede VM jetzt die Schutzfunktionalität erhält, die von der IT-Sicherheitsrichtlinie des Unternehmens vorgegeben wird.

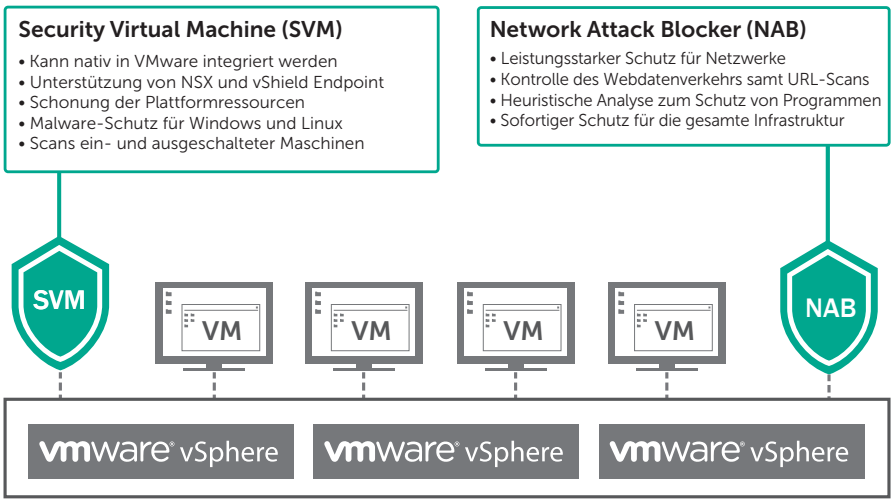


Abbildung 5: Agentenlose Sicherheitslösung

- **Die Integration mit NSX-Sicherheitsmarkierungen** erweitert die Grenzen der „Kommunikation" zwischen der Infrastruktur und den sie schützenden Tools. So kann das Rechenzentrum vollautomatisch und in Echtzeit auf IT-Sicherheitsvorfälle reagieren, Verwaltungsentscheidungen treffen und die Netzwerktopologie des softwarezentrierten Rechenzentrums in Sekundenschnelle neu konfigurieren.
- **Sowohl laufende als auch deaktivierte VMs** werden in einem vollständig agentenlosen Modus gescannt, sodass das gesamte Rechenzentrum des Unternehmens rund um die Uhr geschützt ist.

Die Architektur der Lösung wurde von Anfang an so konzipiert, dass sie den Betrieb unternehmenskritischer Server nahezu ohne Auswirkungen auf die Ressourcen ermöglicht und gleichzeitig erweiterten Schutz bietet.

Patentierte Light-Agent-Technologie

In einigen virtualisierten Umgebungen, die in Rechenzentren von Unternehmen gehostet werden, fehlt es an Integrationsprotokollen, die die Infrastruktur mit der Sicherheitslösung verbinden. Die Sicherheit dieser Umgebungen muss jedoch unbedingt gewährleistet werden.

Darüber hinaus erfordern virtuelle Desktop-Infrastrukturen (VDI) Technologien, die jedem Benutzer zuverlässigen Schutz bieten, unabhängig davon, wie bewusst sich dieser Benutzer der relevanten Bedrohungen und Präventionsmethoden ist.

„Der Light Agent kontrolliert die Programmausführung und schützt virtuelle Endpoints vor Crypto-Viren und anderen Bedrohungen."

Kaspersky Security for Virtualization Light Agent übernimmt die Prinzipien der agentenlosen Lösung, bietet aber zusätzliche Schutzebenen. Die Lösung unterstützt die gängigsten Virtualisierungsplattformen, wie z. B. VMware vSphere, Microsoft Hyper-V, Citrix XenServer sowie KVM, und bietet jedem virtualisierten Endpoint eine ausgewogene Kombination aus völlig neuen Schutztools und Technologien, die die Leistung von VDI-Plattformen wie VMware Horizon und Citrix XenDesktop nicht beeinträchtigen.

- Malware-Schutz und IDS/IPS für virtualisierte Server und VDI
- Sicherheit für VMware-, Citrix-, Microsoft- und KVM-Plattformen
- Leistungsstarker und ressourcenschonender Schutz für XenDesktop und Horizon
- Arbeitet im Verbund mit Ihrer bestehenden Infrastruktur.
- Hochgradig ausbalancierter Schutz ohne Beeinträchtigung der Systemleistung

Der dedizierte Schutz-Server, die Security Virtual Machine (SVM), ermöglicht ein zentrales Scannen aller VMs. Gleichzeitig können mit dem auf jeder VM installierten Light Agent nicht nur die Dateien, sondern auch Arbeitsspeicher und Prozesse gescannt werden. Durch den Einsatz des Light Agent auf VDI-Rechnern lassen sich erweiterte Sicherheitsfunktionen wie Programmkontrolle, Gerätekontrolle, URL-Kontrolle sowie heuristische Module zur Analyse des E-Mail- und Internetverkehrs aktivieren. Darüber hinaus bieten die patentierten Schutztechnologien, auf denen der Light Agent basiert, virtuellen Endpoints Schutz vor ausgeklügelten Angriffen, einschließlich Crypto-Viren.

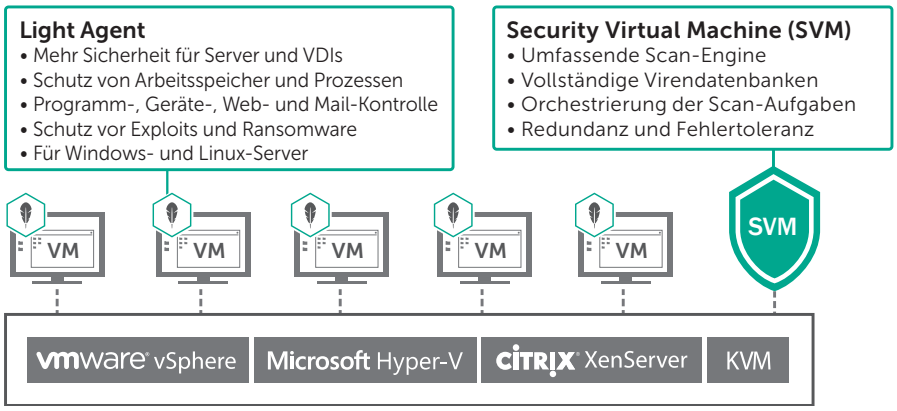


Abbildung 6: Funktionsprinzipien des Light Agent

Schutz der Datenspeichersysteme von Unternehmen in Rechenzentren

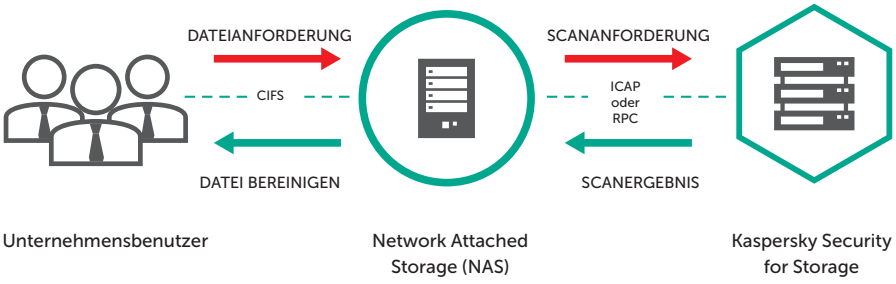
Selbst mit dem fortschrittlichsten Schutz von Endpoints – virtualisierten Servern oder Workstations – sollten Probleme im Zusammenhang mit dem Schutz hoher Datenmengen, die in modernen Unternehmensrechenzentren gespeichert sind, mithilfe spezieller Schutztools gelöst werden.

Kaspersky Lab hat hierfür **Kaspersky Security for Storage** entwickelt, das über ICAP- und RPC-Protokolle in zahlreiche netzwerkgestützte Datenspeichersysteme auf Unternehmensebene integriert ist und robusten, leistungsstarken und skalierbaren Schutz für jede Dateioperation bietet. Die Architektur der Lösung und die sehr leistungsfähige Engine eliminieren potentielle Risiken im Zusammenhang mit einer möglichen Malware-Infektion wichtiger Unternehmensdateien.

„Die Sicherheitslösung für Speichersysteme schützt nicht nur NAS-Systeme, sondern auch Dateiserver."

Egal, welcher Benutzer welche Dateiaktivität ausführt, alle Aktionen werden von der Antiviren-Engine von Kaspersky Security for Storage verarbeitet.
Die leistungsstarke von Kaspersky Lab entwickelte Antiviren-Engine scannt jede Datei, die aufgerufen oder geändert wird, auf sämtliche Arten von Malware, einschließlich Viren, Würmer und Trojaner. Eine fortschrittliche, ganzheitliche Analyse erkennt selbst neue und bisher unbekannte Bedrohungen.

Die Lösung nutzt eine flexible Scan-Steuerung und unterstützt so genannte „vertrauenswürdige Zonen", die vom Scannen ausgeschlossen werden können, sowie bestimmte Dateiformate und Prozesse wie z. B. das Erstellen von Sicherungskopien.



Zusammenfassung

Kaspersky Lab nutzt seinen vielfach ausgezeichneten Malware-Schutz, um damit jede einzelne Komponente eines softwarezentrierten Rechenzentrums abzusichern und gleichzeitig ein Höchstmaß an Systemeffizienz aufrechtzuerhalten. Die Lösung ist für alle führenden Hypervisoren geeignet, z. B. VMware vSphere mit NSX, Microsoft Hyper-V, Citrix XenServer und KVM, und ist mit Standardlösungen für die Desktopvirtualisierung, VMware Horizon und Citrix XenDesktop, kompatibel.

Neben spezieller Sicherheit für Virtualisierungsplattformen bieten wir auch eine Lösung zum Schutz von Network Attached Storage (NAS) und File-Servern in Unternehmen. Hierdurch wird sichergestellt, dass jeder Vorgang für eine Datei, woher diese auch stammt, abgesichert wird.

Mit der Lösung Kaspersky Data Center Security definieren wir die Interaktion zwischen der Infrastruktur des Rechenzentrums und der zugehörigen Sicherheitslösung neu, verbinden ihre Stärken und schaffen so eine sichere und effiziente virtualisierte Umgebung. Dank seiner Integrationsmöglichkeiten erweitert Kaspersky Data Center Ihre virtualisierte Umgebung um hochmoderne Schutzfunktionen, die genau darauf abgestimmt sind, wie und wo Ihre Daten gespeichert sind, und jeden einzelnen Dateivorgang absichern. Das Rechenzentrum Ihres Unternehmens ist also jederzeit einsatzbereit und umfassend abgesichert.

Kaspersky Lab
Cybersicherheit für Unternehmen:
www.kaspersky.de/enterprise-security
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **www.kaspersky.de/blog/b2b**

#truecybersecurity
#HuMachine

www.kaspersky.de