KASPERSKY lab

SICHERHEIT FÜR RECHENZENTREN: SELBST DAS RUDER ÜBERNEHMEN

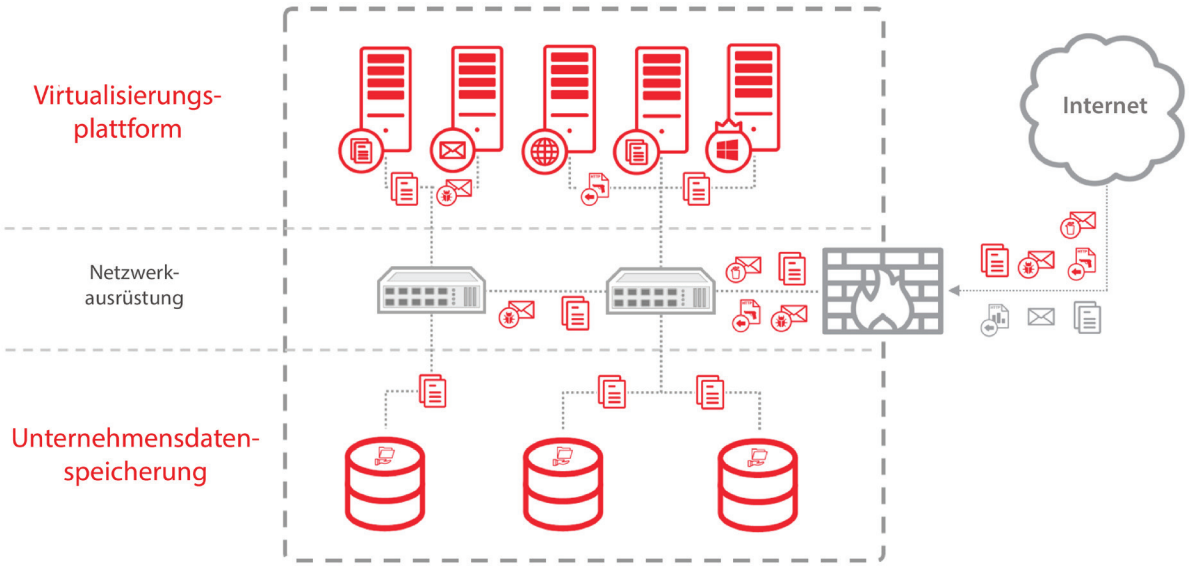
EINLEITUNG

Der Betrieb eines Rechenzentrums besteht aus einer Unmenge hochkomplexer Abläufe, von denen die Sicherheit nur einer ist. Die Sicherheit speziell von virtuellen Umgebungen und Datenspeichern ist für das moderne Rechenzentrum von heute von ausschlaggebender Bedeutung. Die Sicherung dieser beiden Bereiche ist zwar von Natur aus anspruchsvoll, sich diesen Herausforderungen jedoch nicht zu stellen, kann unerfreuliche Folgen haben, sowohl für Ihre Kunden als auch für das Rechenzentrum selbst. Leider sind einige dieser Probleme nicht ganz so offenkundig oder werden ignoriert, bis es zu spät ist. Lassen Sie sie uns einmal im Detail anschauen und überlegen, wie wir sie schon vor ihrer Entstehung verhindern können.

VIRTUALISIERUNGSSICHERHEIT: FEHLER UND IHRE FOLGEN

Die Virtualisierung unterschiedlicher Unternehmensressourcen ist ein schnell wachsender Trend, der eine optimale Ressourcenauslastung, größere Flexibilität und Skalierbarkeit ermöglicht. Und viele Szenarien, in denen eine virtualisierte Infrastruktur eine Rolle spielt, lassen sich gut an ein Rechenzentrum abgeben. Da ein Rechenzentrum jedoch in der Regel mit einer großen Bandbreite unterschiedlicher Aktivitäten betraut ist, fällt die Sicherheit dieser Ressourcen oft nicht in seinen Aufgabenbereich.

Hierfür kann es unterschiedliche Gründe geben. Die Kunden könnten sich mit ihrer eigenen, traditionellen Art und Weise, wie sie Sicherheit handhaben, wohler fühlen bzw. zögern, die Verwaltung der Sicherheit an Dritte abzugeben. Oder der Anbieter selbst zieht es vor, keine Verantwortung für die Sicherheit von gehosteten Ressourcen zu übernehmen.



Ein Rechenzentrum bietet seinen Kunden unterschiedliche Arten von Ressourcen, die allesamt geschützt werden müssen.

Derartige Einstellungen können ernsthafte Konsequenzen haben. „Die Dinge auf traditionelle Weise zu handhaben", kann zu einem ineffizienten Wirrwarr aus Sicherheitslösungen unterschiedlicher Kunden führen, die für die Virtualisierung ungeeignet sind und alle auf demselben Host ausgeführt werden – oder, noch schlimmer, dazu, dass überhaupt keine Sicherheitslösung vorhanden ist. Dieser Verzicht lässt sich durch die überraschend hartnäckige Legende erklären, virtualisierte Umgebungen seien „von Natur aus sicher" und Malware können „nicht auf virtuellen Maschinen ausgeführt werden".

In Wahrheit trifft natürlich genau das Gegenteil zu: virtuelle Maschinen (VMs) sind von den meisten Angriffsformen betroffen und bieten sogar zusätzliche Schwachstellen. VDIs (virtualisierte Desktop-Infrastrukturen), die in der Regel ganz genau so genutzt werden wie ihre physischen Pendants (einschließlich Webzugriff und der damit verbundenen Gefahren), sind besonders anfällig für die Infektion mit Schadsoftware. Ungeschützte Schwachstellen können in kürzester Zeit zu einem Malware-Befall führen, der dann nicht nur den ursprünglich angegriffenen Kunden, sondern auch andere betrifft, deren Ressourcen auf demselben Host bereitgestellt werden. Ein plötzlicher Anstieg der Ressourcenauslastung durch Virenbefall kann zu Verzögerungen, ja sogar zum Ausfall des Hosts insgesamt führen – besonders ärgerlich für nicht infizierte Kunden.

Eine bestimmte virtualisierte Infrastruktur im Rechenzentrum kann sogar als Sprungbrett für weitere Attacken genutzt werden. Dies führt dazu, dass ganze IP-Adressbereiche gesperrt werden, die Aufmerksamkeit der Behörden erregt und der reibungslose Betrieb des Rechenzentrums nachhaltig gestört wird.

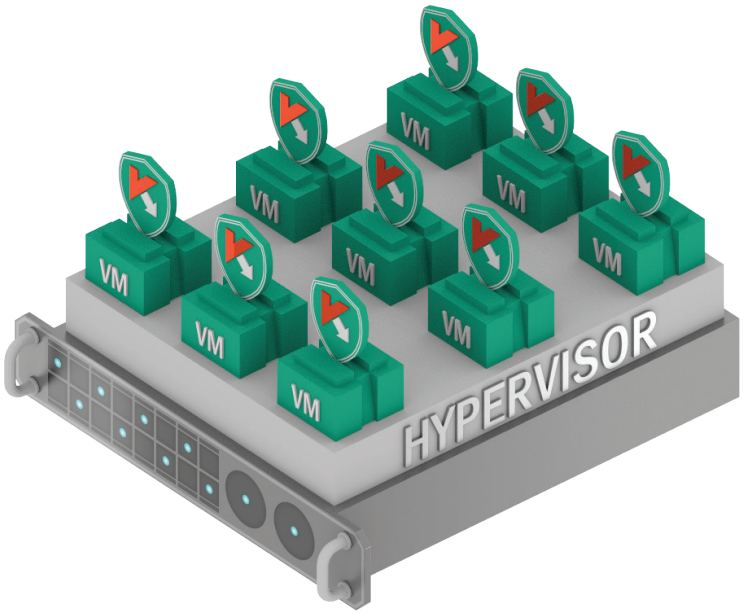
Die Installation von Sicherheitslösungen, die nicht speziell für virtualisierte Umgebungen geeignet sind, kann jedoch ganz eigene Probleme verursachen.

Diese beinhalten:

- Exzessiver Ressourcenverbrauch, da jede geschützte VM die gesamte Ausstattung an Sicherheitskomponenten besitzt: eine Scanning-Engine, eine lokale Signaturdatenbank, eine hostbasierte Angriffsüberwachung etc. Und wenn Cloud-basierte Feeds mit Bedrohungsinformationen verwendet werden, wird für jeden von ihnen Bandbreite benötigt.
- Unvorhersagbare Spitzen in der Ressourcenauslastung, so genannte „Update-Storms", die durch die zeitgleiche Ausführung ähnlicher Aufgaben, z. B. Aktualisierungen oder Dateisystem-Scans, auf einer Vielzahl von VMs hervorgerufen werden. Dies kann zu erheblichen Verzögerungen oder sogar zu Service-Ausfällen im gesamten Hostsystem führen.
- Panik-Attacken: Malware-Ausbrüche führen oft zu Panikreaktionen, z. B. ungeplanten Scans, einer Erhöhung der Scantiefe, etc. Die resultierende Verschlechterung der Performance kann alle VMs auf demselben Server betreffen.

- „Instant-on"-Sicherheitslücken: Einige VMs verbleiben im Standby-Modus, bis sie benötigt werden. In diesem Zustand können auf ihnen keine Updates ausgeführt werden (hierzu gehören das Vulnerability Patching und Sicherheits-Updates). Direkt nach dem Systemstart ist die VM bis zum Abschluss des Aktualisierungsvorgangs also anfällig – Zeit genug, um sich mit Malware zu infizieren.
- Inkompatibilität. Obwohl VMs in vielerlei Hinsicht ihren physischen Pendants ähneln, unterscheiden sie sich auch in einigen Aspekten. Virtualisierungsunspezifische Sicherheitslösungen sind beispielsweise nicht für dynamisch zugewiesenen Speicher oder die VM-Migration ausgelegt – dies kann zu Aussetzern, aber auch zu schwerwiegenderen Fehlern führen.

Es muss klar und deutlich gesagt werden, dass der Serviceanbieter letztendlich für die hier beschriebenen Konsequenzen verantwortlich gemacht wird. Die Tatsache, dass Sie keine Kontrolle über die von Ihnen gehosteten Ressourcen haben, ist in diesem Fall keine Verteidigung. Dies gilt umso mehr, weil es tatsächlich Methoden gibt, die Sicherheit in virtualisierten Umgebungen effizient zu kontrollieren.



1. Verursacht „Update-Storms"
2. Verursacht „Scan-Storms"
3. „Instant-on"-Lücken
4. Exzessiver Ressourcenverbrauch
5. Geringere VM-Dichte
6. Kein Schutz für Netzwerkressourcen

Nicht speziell auf Virtualisierung ausgelegte Sicherheitslösungen verursachen eine Vielzahl von Problemen, angefangen bei der ineffizienten Ressourcennutzung.

Die Antwort besteht in der Verwendung von Sicherheitslösungen, die von Anfang an auf Virtualisierungstechnologien ausgelegt sind.

SCHUTZ, DER IHREN BEDÜRFNISSEN ENTSPRICHT

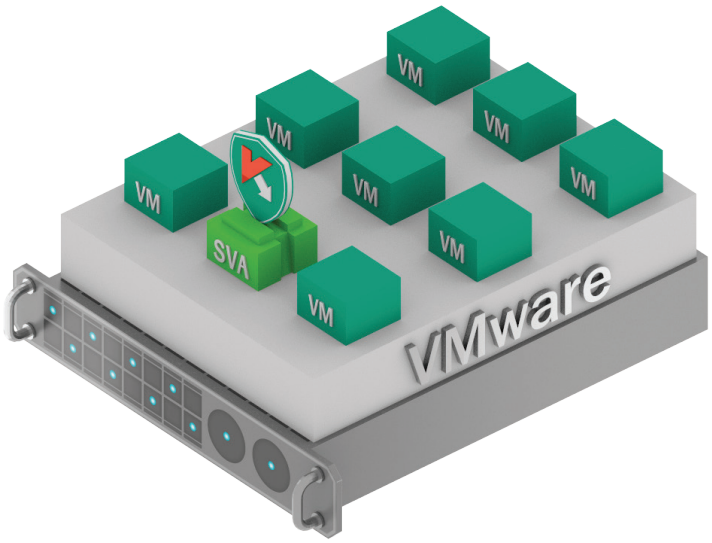
Kaspersky Security for Virtualization wurde mit einem genauen Verständnis der Besonderheiten von virtuellen Infrastrukturen entworfen. Unsere Lösung wurde von uns an diese Art von Umgebung angepasst, um Probleme, die durch ungeeignete, unzweckmäßige und ineffiziente Lösungen entstehen, zu vermeiden.

Zunächst wird die Redundanz eliminiert, die durch identische Komponenten auf jeder einzelnen VM entsteht. Eine spezielle VM, die so genannte **Security Virtual Appliance (SVA)**, enthält zentral sowohl die Scanning-Engine als auch die Sicherheitsdatenbank und schützt so alle VMs, die unter demselben Hypervisor ausgeführt werden. Sie wird fortlaufend aktualisiert und nutzt eine intelligente Zeitplanung für das Scanning, um „Storms" zu vermeiden.

Natürlich muss die SVA irgendwie auf die geschützten VMs zugreifen. Kaspersky Security for Virtualization hat hierfür zwei unterschiedliche Methoden vorgesehen:

Agentless

Diese Option funktioniert nur in VMware-basierten Umgebungen. Wie der Name schon verrät, ist es bei dieser Lösung nicht erforderlich, einen Software-Agenten auf der VM zu installieren. Es wird die systemeigene vShield-Technologie genutzt. Bei der agentlosen Lösung wird **jede VM** ab dem Zeitpunkt des Systemstarts **automatisch geschützt**, während eine weitere SVA für die **Angriffsüberwachung (IPS)** auf Netzwerkebene sorgt.



Agentenlose Lösungen bieten umgehenden Schutz, ohne etwas auf einer VM installieren zu müssen

Sie empfiehlt sich besonders bei Kunden, die Bedenken haben, fremde Software auf ihren Systeme zu installieren, bzw. ausschließlich mit vorgegebenen Anwendungen arbeiten. Bei Kunden, die strikt gegen den Einsatz von Sicherheitslösungen sind, ist dies unter Umständen die einzige Möglichkeit, klaffende Sicherheitslöcher zu vermeiden.

Es gilt jedoch auch hier einige Aspekte zu bedenken. Bei agentenlosen Verfahren kann die Sicherheitslösung keine Prozesse überwachen, die im Arbeitsspeicher einer VM ausgeführt werden: Die vShield-Technologie hat lediglich Zugriff auf das Dateisystem der VM und bietet deshalb gegen hoch entwickelte Malware (z. B. körperlose Varianten) nur eingeschränkt Schutz.

Darüber hinaus ist es nicht möglich, zusätzliche Sicherheitsschichten, etwa Anwendungs-, Geräte- oder Webkontrollen, zu installieren. Für einige Szenarien, z. B. im Fall von virtualisierten Desktop-Infrastrukturen (VDI), die physische Workstations zunehmend verdrängen, empfehlen wir eine andere, in Kaspersky Security for Virtualization enthaltene Option: den Schutz durch Light Agents.

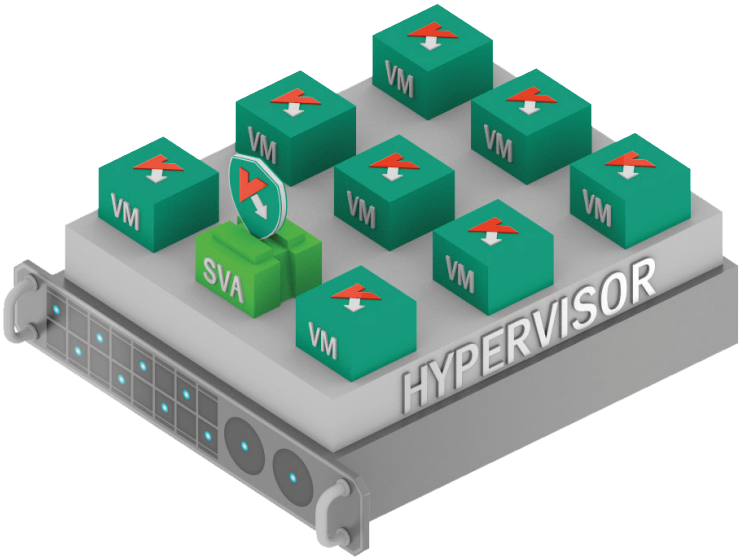
Light Agent

Im Gegensatz zur agentenlosen Sicherheit ist diese Option nicht von einer **plattformabhängigen Zwischenschicht** abhängig und ist deshalb auch mit zusätzlichen Hypervisoren kompatibel, so z. B. mit Microsoft Kerpen-V und Central. Hierzu wird ein **„schlanker" Software-Agent** auf der zu schützenden VM bereitgestellt. Mit diesen Agenten hat die Anti-Malware-Engine der SVA nicht nur direkten Zugriff auf die geschützten VMs, es steht auch eine viel größere Bandbreite an Sicherheitstechnologien zur Verfügung, sodass annähernd ein Sicherheitsniveau entsteht, **das einer umfassenden Endpoint-Sicherheitslösung** wie z. B. Kaspersky Endpoint Security for Business entspricht.

Unter anderem bietet Kaspersky Security for Virtualization | Light Agent Ihnen Folgendes:

- Kontrolle über die Prozesse im Arbeitsspeicher der VM unter Verwendung hoch entwickelter verhaltensanalytischer Mechanismen
- Abwehr von Exploits durch AEP-Technologie (Automatic Exploit Prevention)
- Web-Virenschutz durch Cloud-gestütztes Anti-Phishing
- Vollständige Sicherheitskontrollen, über die Sie explizit auf einzelnen VMs festlegen können, welche Programme, Webressourcen und Geräte für diese zulässig sind.
- Ein verbesserter Netzwerkschutz durch Blockierung von Netzwerkangriffen, hochentwickelte Firewalls und Monitore sorgt für ein Höchstmaß an Sicherheit für jede VM innerhalb von virtualisierten Netzwerken.

Trotz dieser Leistungsfähigkeit sind die eingesetzten Agenten sehr schlank – die SVA übernimmt nach wie vor das Update- und Scan-Management, eliminiert Redundanzen und reduziert die agentenbasierte Aktivität auf den VMs auf das zur Gewährleistung von Sicherheit erforderliche Minimum.

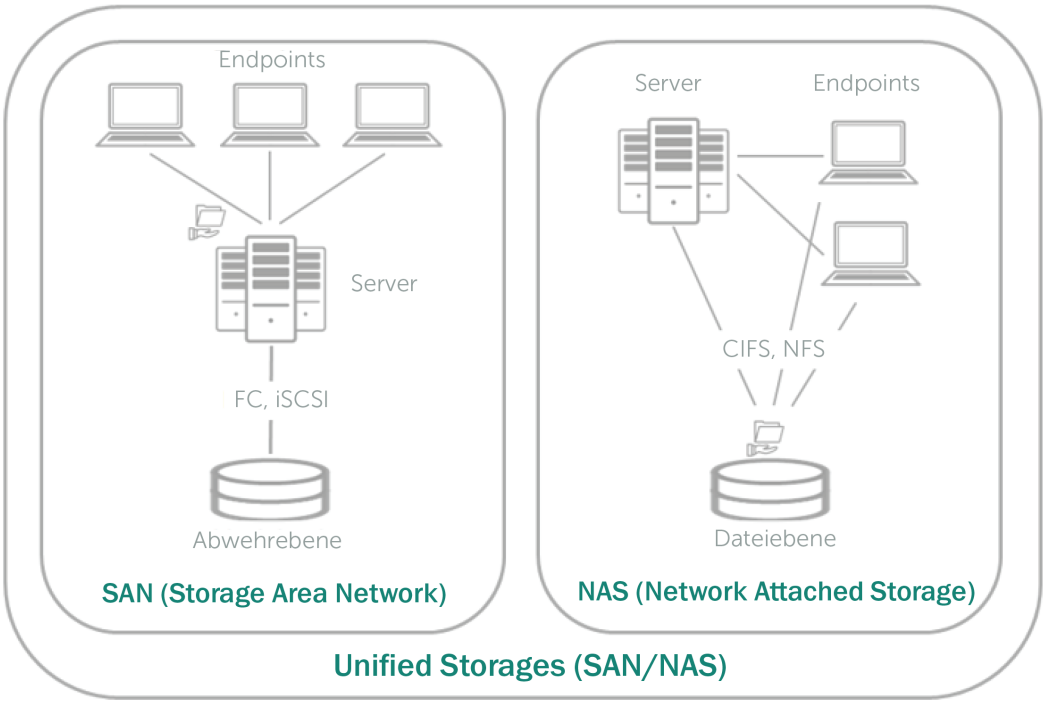


Eine Light-Agent-Lösung garantiert hochwertigen Schutz mithilfe von schlanken Anwendungen für die einzelnen VMs. Diese Anwendungen können in den VM-Images vorinstalliert werden.

Für Szenarien mit höherem Risiko und breiteren Angriffsflächen (z. B. virtualisierte Desktops mit vollständiger Internet-Funktionalität), ist ein solcher mehrstufiger Schutz ein Muss – und nicht nur wegen der gestiegenen Angriffswahrscheinlichkeit. Da virtualisierte Netzwerke weitaus effizienter sind, können sich Infektionen blitzartig ausbreiten, und der Angreifer erhält in kürzester Zeit die Kontrolle über eine schlecht gesicherte Infrastruktur. Eine gut geschützte virtualisierte Infrastruktur ist hingegen ein weitaus weniger attraktives Ziel, selbst für Hacker, die zielgerichtet angreifen und auf der Suche nach dem schnellen Gewinn sind.

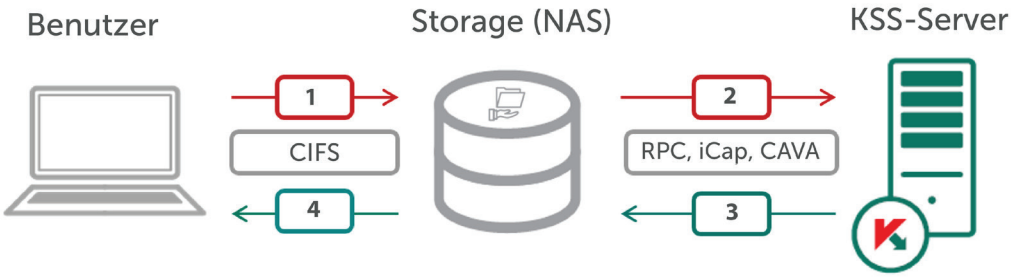
SICHERUNG DES DATENSPEICHERS – VIRTUALISIERT ODER NICHT

Der Datenspeicher darf bei der Rechenzentrumssicherheit nicht außer Acht gelassen werden. Große Mengen von Daten werden gespeichert, aktualisiert und ausgetauscht – eine potentielle Gefahrenquelle für alle Benutzer, sollte nur einer von ihnen achtlos oder sogar in böswilliger Absicht handeln. Bedenken Sie außerdem, dass es möglicherweise auch Benutzer gibt, die sich außerhalb des geschützten Perimeters befinden. In diesem Fall hat das Rechenzentrum überhaupt keine Kontrolle oder Informationen über seine Sicherheitsstellung. Es sollten also spezielle Maßnahmen ergriffen werden, um unterschiedliche Arten von Datenspeichern zu sichern, insbesondere dann, wenn nicht alle von ihnen virtualisiert sind und durch eine virtualisierungsspezifische Lösung geschützt werden.



Unterschiedliche Arten von Speicher erfordern ebenfalls Schutz

Während der Schutz von **Storage Area Networks (SAN)** relativ unkompliziert ist, da sie nur über Server zugänglich sind, gestaltet sich die Absicherung von **netzwerkgebundenen Speicherlösungen (NAS)**, auf die vom Netzwerknutzer direkt zugegriffen werden kann, schon schwieriger.



Der Schutz von NAS ist komplizierter als der von SAN

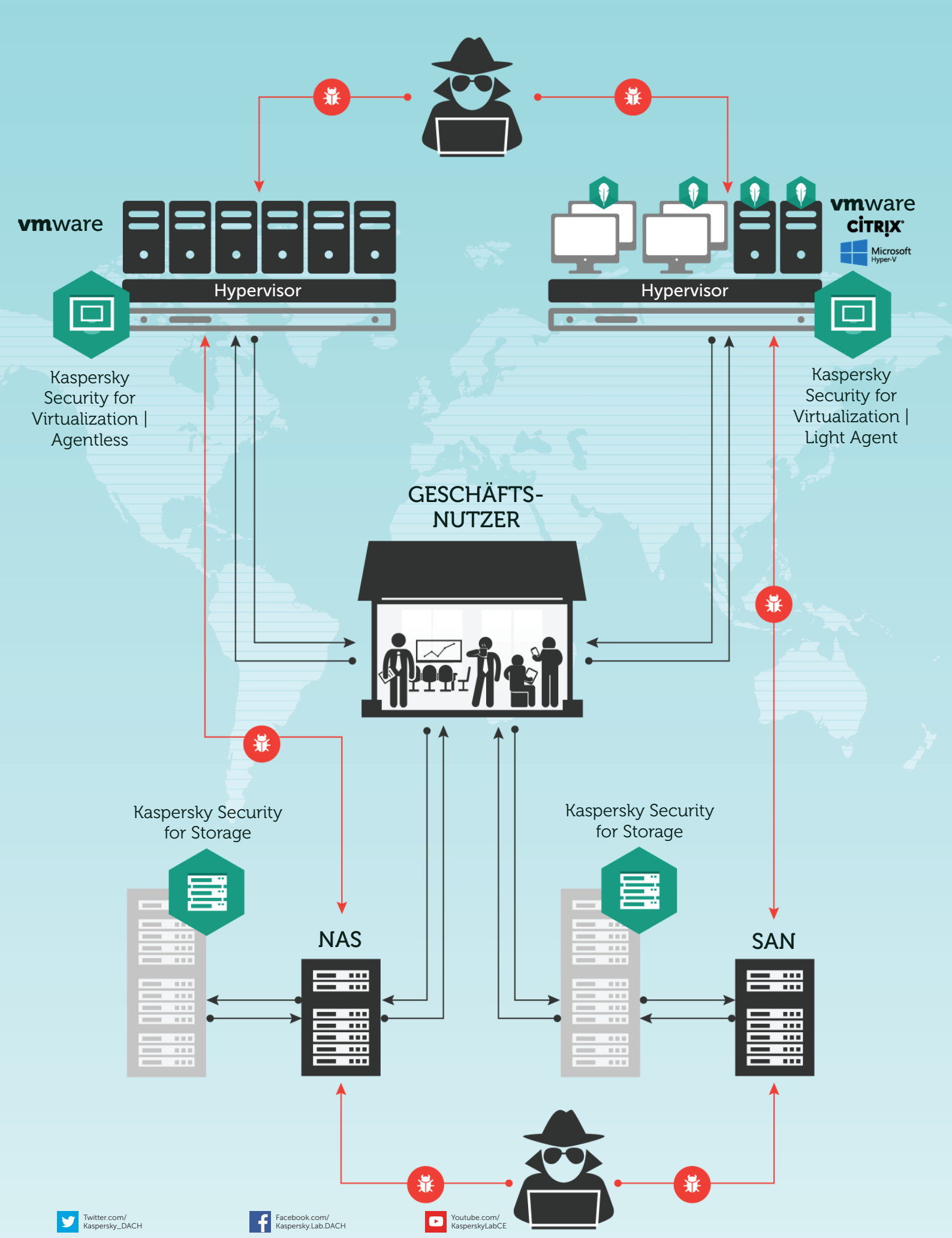
Glücklicherweise gibt es spezielle Sicherheitslösungen, die Schutz für beides bieten. Ein gutes Beispiel hierfür ist Security for Storage. SAN-Ressourcen werden genau wie herkömmliche Dateisysteme gesichert, jedes Objekt, das an einen NAS-Datenspeicher gesendet oder von dort abgerufen wird, wird zunächst von der Kaspersky-Lösung überprüft. Auf Basis der Einschätzung durch unsere Sicherheitslösung kann das NAS dann den angeforderten Vorgang zulassen oder verweigern. Um mit umfangreicheren Datenströmen zurechtzukommen, können auch mehrere Instanzen der Lösung bereitgestellt werden, wobei das Load Balancing dann vom NAS selbst übernommen wird.

EINE KONSOLE, UM SIE ALLE ZU BEHERRSCHEN

Angesichts der wachsenden Anzahl und zunehmenden Raffinesse von modernen Cyberattacken, ist es von ausschlaggebender Bedeutung, den Überblick über die gesamte Infrastruktur des Rechenzentrums zu behalten, damit Bedrohungen zeitnah erkannt und bekämpft werden können. Hier liefern Lösungen von Kaspersky Lab einen weiteren Vorteil: alle Sicherheitsparameter werden über eine einzige flexible Konsole – das Kaspersky Security Center – überwacht und verwaltet. Ein optionaler, rollenbasierter Zugriff gibt Ihren Kunden die Möglichkeit, ihren eigenen Sicherheitsstatus bei Bedarf selbst zu verwalten, ohne die Rechenzentrumssicherheit insgesamt in Gefahr zu bringen.

FAZIT

Egal ob Sie mit virtualisierten oder physischen Ressourcen arbeiten, mit der Kaspersky-Sicherheitslösung für Rechenzentren (die Teil unserer Enterprise Security Platform ist) wird IT-Sicherheit zu einer attraktiven und profitablen Option, die Sie in Ihr Portfolio an Rechenzentrumsservices aufnehmen können. Eines sollte aber klar sein: Beim Thema Sicherheit für Ihr Rechenzentrum das Ruder selbst in die Hand zu nehmen, ist Grundvoraussetzung dafür, aufziehende Stürme zu überstehen.



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

© 2016 Kaspersky Lab. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber. Lotus und Domino sind Marken der International Business Machines Corporation und als solche in vielen Rechtsgebieten weltweit eingetragen. Linux ist das eingetragene Markenzeichen von Linus Torvalds in den USA und anderen Ländern. Google ist eine eingetragene Marke von Google, Inc.

KASPERSKY lab