

# RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL,  
NETZWERKE

Wenn die Standortfrage  
eine zentrale Rolle spielt

**SDN 1: Wozu Software  
Defined Storage gut  
sein soll**

Seite 8

**Virtualisierung:  
Wie Kopien auf die  
Performance wirken**

Seite 12

**Code of Conduct:  
Was intelligente  
Verkabelung bewirkt**

Seite 18

**Kühlung: Worauf es  
beim Brandschutz  
besonders ankommt**

Seite 22

**SDN 2: Worauf das  
Software Defined  
Datacenter basiert**

Seite 10

**Energieverbrauch:  
Warum Messungen  
so wichtig sind**

Seite 16

**Sicherheit: Was eine  
Next Generation  
Firewall besser kann**

Seite 20

**Ausblick 2015:  
Wohin die Reise für  
Rechenzentren geht**

Seite 25



Server & Storageysteme

Wir schaffen Platz für das wirklich Wichtige!



# Storage Unlimited



## BigFoot Storageysteme

Die Idee: Es sollte ein Storage-System geben, das in zahlreichen Anwendungsgebieten einsetzbar ist, durch nahezu endlose Speicherkapazitäten Platz für Daten und Anwendungen schafft und dabei dank flexibler Prozessorleistung dennoch leichtgewichtig und schnell arbeitet.

Aus dieser Idee hat die Rausch Netzwerktechnik GmbH die BigFoot-Produktfamilie entwickelt. Die vier verschiedenen Basiskonfigurationen eignen sich als Datenbankserver genauso, wie als Enterprise-Storage-Server, Nearline-Storage, als Virtual Tape Library zur Langzeitarchivierung oder ebenso für den Einsatz im Cloud Computing oder bei Big-Data-Anwendungen.

**Überzeugend in Leistung und Preis – das und mehr schafft die BigFoot-Storage-Familie in nur 4HE.**



Rausch Netzwerktechnik GmbH  
Englerstraße 26 · D-76275 Ettlingen  
Telefon (07243) 5929-0 · Telefax -14 · info@rnt.de  
[www.rnt.de](http://www.rnt.de)

**RAUSCH NETZWERKTECHNIK** ▲▲  
[www.rnt.de](http://www.rnt.de) ▲▲

*Sympathisch und gut beraten. Bestens betreut.*

**>> Mehr erfahren!**

# Wenn die Standortfrage eine zentrale Rolle spielt



**K**aum hatten wir die vorige Ausgabe von Rechenzentren und Infrastruktur im Kasten, erfuhren wir davon: Das deutsche Rechenzentrum von Amazon Web Services (AWS) ist im Oktober 2014 wenige Monate nach Ankündigung tatsächlich online gegangen. Wo genau es in Frankfurt am Main steht, weiß keiner. Aus Sicherheitsgründen. Was wir in Erfahrung bringen konnten, hat der freiberufliche Journalist Roland Freist auf Seite 4 zusammengefasst. Nur so viel steht fest: Amerikanischer Anbieter, Safe Harbor und Geheimdienste hin oder Datenschutz her – damit dürfte einer der schärfsten Konkurrenten für deutsche RZ-Betreiber bittere Realität geworden sein, seitdem die Standortfrage eine zentrale Rolle spielt.

Doch damit nicht genug: Wer die Zukunft in dieser Branche meistern will, muss auf seinen Speicher achten. Software Defined Storage ist der nächste Schritt zum virtualisierten Rechenzentrum. Obwohl die Vorstellungen schwammig sind, ist nahezu jedes große Unternehmen in der Branche auf diesen Zug aufgesprungen, weiß Freist ab Seite 8 zu berichten. Eine Story später bleiben wir auf dem Weg zum Software Defined Datacenter: Welches Speichermedium für bestimmte Daten am besten geeignet ist, beantwortet Hans Schramm von Dell ab Seite 10.

Um Datenlawinen und Kostenexplosionen geht es ab Seite 12. Wie die Virtualisierung von Datenkopien einzelne Elemente sowie die Gesamtperformance eines Rechenzentrums beeinflusst, hat Ash Ashutos, CEO und Gründer von Actifio, auf den Punkt gebracht: Anstatt für immer mehr Geld immer mehr Speicherplatz zu kaufen und zu verwalten, sollten RZ-Betreiber sich dem Thema Datenkopien widmen. Durch geschickten Umgang mit den (notwendigen) Kopien lassen sich Zeit, Aufwand und Geld sparen. Zudem steigt die Sicherheit, da weniger unkontrollierte Kopien herumvagabundieren.

Den Energieverbrauch im Blick hat Frank Leinhoss von Colt ab Seite 16. Mit genauen Messungen lässt sich seinen Erfahrungen nach dieser erheblich senken. André Engel, von trans data elektronik vertieft ab Seite 18

seine grünen Aussichten auf Rechenzentren, die intelligent verkabelt sind und so unter anderem die Energiekosten senken. Mit dem Code of Conduct wollen Teilnehmer und Befürworter einer europäischen Initiative für das Thema Green-IT sensibilisieren und Möglichkeiten des Energiesparens aufzeigen, bei der unter anderem die Verkabelung eine wichtige Rolle spielt.

Ab Seite 20 nimmt sich Thorsten Henning von Palo Alto Networks Zeit für mehr Sicherheit, die Next Generation Firewalls versprechen. Ein wesentlicher Grund für die nächste Generation sind zeitgemäße Abwehrmaßnahmen, die vor aktuellen Angriffsszenarien schützen.

Noch einen Blick auf die Sicherheit wirft Katrin Strübe von der Wagner Group: Wie sich mit einem System zur indirekten Freien Kühlung ein effektiver Brandschutz bewerkstelligen lässt, steht im Praxisbeispiel ab Seite 22 geschrieben.

Wie der Verband der Ersatzkassen sensible Datentransfers verschlüsselt, weiß Svenja Borgschulte von Rohde & Schwarz auf Seite 24 zu berichten. Damit Sozialversicherungsdaten nicht in falsche Hände geraten, hat insbesondere auch der Transfer von Backups eine immer wieder gern vernachlässigte Aufmerksamkeit verdient.

Mit einem Ausblick auf 2015 beendet Bernd Hanstein von Rittal die erste Ausgabe von Rechenzentren und Infrastruktur im neuen Jahr. Sein Fazit: In Sachen Effizienz liegt vieles im Argen. Es wird Zeit für eine Modernisierung. Doch es kommt Bewegung in die Branche. AWS in Frankfurt ist der Beweis.

*Thomas Jannot*

## MAN RECHNET DEUTSCH: AWS IN DEUTSCHEM RZ

In der zweiten Oktoberhälfte 2014 hat Amazon für seine Amazon Web Services (AWS) in Frankfurt am Main sein erstes deutsches Rechenzentrum in Betrieb genommen. „EU-Frankfurt“, wie die offizielle Bezeichnung lautet, ist die insgesamt elfte globale Region, die AWS seinen Kunden zur Auswahl anbietet, und nach Irland die zweite Region im europäischen Rechtsraum. Amazon reagiert damit auf die vermehrten Kundenwünsche nach einem Datacenter auf deutschem Boden. Für den Standort Frankfurt sprachen laut dem Cloud-Anbieter die Nähe zum deutschen Internet-Knoten DE-CIX und die daraus resultierenden kurzen Latenzzeiten.

Preislich liegt Frankfurt im weltweiten Vergleich im Mittelfeld der AWS-Regionen, ist jedoch teurer als etwa Irland. Als Beispiel sollen die Gebühren für Amazon S3 dienen: Für Datenmengen bis zu einem Terabyte zahlt der Kunde pro Gigabyte in den Regionen US Standard, USA West (Oregon), Irland, Asien-Pazifik (Singapur) 0,03 US-Dollar im Monat. In Frankfurt sind es bereits 0,324 US-Dollar. Noch teurer ist allerdings die Nutzung der Rechenzentren in USA West (Nordkalifornien), Asien-Pazifik (Tokio) und Asien-Pazifik (Sydney): Dort wird der Kunde mit 0,033 US-Dollar pro Gigabyte und Monat zur Kasse gebeten.

An der Spitze der Preisskala steht schließlich Südamerika (São Paulo) mit 0,0408 US-Dollar. Der Grund für die unterschiedliche Preisgestaltung in den Regionen ist zum einen, dass Amazon in den USA auch Besitzer der Rechenzentren ist, während das Unternehmen an anderen Standorten teilweise auf die Infrastruktur von lokalen Part-

nern zurückgreift. Hinzu kommen differierende Kosten für Strom, Grundstücke, Gehälter und so weiter.

Die genaue Adresse und Ausstattung des Rechenzentrums hält Amazon wie üblich unter Verschluss. Das Unternehmen gab jedoch bekannt, dass die neue Region zwei Availability-Zones umfasst, also aus zwei räumlich getrennten Datacentern besteht. Das garantiert eine Hochverfügbarkeit der Daten, da beim Ausfall eines Standorts sofort der zweite einspringt. Die installierte Infrastruktur der Rechenzentren ist identisch, sämtliche Daten werden 1:1 gespiegelt. Beide Zentren werden unabhängig voneinander mit Energie, Kühlungstechnik und Netzwerkdiensten versorgt. Die Einrichtung erfolgte gemäß den Compliance-Standards ISO 27001, SOC 1 und PCI DSS Level 1.

Für die deutschen Kunden hat die neue AWS-Region laut Amazon mehrere Vorteile:

- Die neue Region verbessert und stabilisiert die Verbindung in die Amazon-Cloud – ein Faktor, der im Wettbewerb mit anderen Anbietern zunehmend an Bedeutung gewinnt.
- Unternehmen können ihre Anwendungen nun in zwei AWS-Regionen zur Verfügung stellen. Ihre Kunden können sich für die Region entscheiden, die ihnen die kürzeren Latenzzeiten bietet. Die Daten verlassen dennoch nicht den europäischen Rechtsraum.
- Anwender haben die Gewissheit, dass ihre Daten gemäß den strengen deutschen Datenschutzregeln behandelt werden.

Umstritten ist jedoch, ob ein deutscher Standort die Daten tatsächlich vor dem Ausspionieren durch NSA und GCHQ schützt. Amazon selbst gibt an, dass amerikanische Behörden keinen Zugriff auf seine Rechenzentren haben. Kritiker verweisen hingegen auf den amerikanischen Patriot Act, der den USA das Recht gebe, amerikanische Unternehmen zur Herausgabe auch solcher Daten zu zwingen, die bei ausländischen Niederlassungen gespeichert sind.

## FREIKÜHLUNG MIT INDIREKTER VERDAMPFUNG

Emerson Network Power setzt bei Liebert EFC auf eine Kombination aus Freikühlung mit indirekter Verdampfung und einem Luft-Luft-Wärmetauscher, die in einer einzigen Einheit integriert sind. Durch den Wasserverdampfungsprozess soll ein pPUE-Wert von 1,03 erreicht und so die CO<sub>2</sub>-Emissionen gesenkt werden. Konzipiert sei das Gerät für mittelständische Unternehmen und Colocation-Center.

Mithilfe der patentierten Steuerlogik von Emerson Network Power könne Liebert EFC das interne Luftvolumen und die Lufttemperatur entsprechend den jeweiligen Serveranforderungen optimieren. Der Luftstrom wird dabei genau dem Bedarf des Servers angepasst. Damit werde sichergestellt, dass beim Umwälzen oder Kühlen von nicht benötigter Luft keine Energie verschwendet werde. Zudem analysiert laut Emerson die iCOM-Regelung, um ein möglichst effizientes Gleichgewicht zwischen Wasser- und Stromversorgung herzustellen und so weitere Kosteneinsparungen zu ermöglichen. Die Berechnung basiert auf dem Versorgungsbedarf des Rechenzentrums und berücksichtigt Schwankungen bei den Wasser- und Strompreisen.

Liebert EFC besitze außerdem Betriebsmodi, die für den Einsatz unter unterschiedlichen Umgebungsbedingungen vorgesehen sind. Darüber hinaus werde durch die Einheit die räumliche Trennung zwischen der inneren und der äußeren Umgebung jederzeit aufrechterhalten. Somit könne der Betrieb ohne das Risiko einer Verunreini-

gung der Luft durch veränderliche äußere Faktoren wie starke Verschmutzung oder Rauch weitergeführt werden.



Quelle: Emerson Network Power

Die Kühlungslösung Liebert EFC soll Luftvolumen und Lufttemperatur entsprechend den jeweiligen Serveranforderungen regeln können.



Besuchen Sie uns auf der CeBIT 2015:  
16. bis 20. März 2015 in Hannover  
Halle 12 / DCD@CeBIT

**FNT**

// when transparency matters.



Software für Data Center Infrastructure Management

## Wir bringen Transparenz und Effizienz in Ihr Rechenzentrum.

Sie wollen Rechenzentren effizient betreiben. Kapazitäten, Aus- und Umbau verlässlich planen können. Sie benötigen Transparenz – vom Gebäude, der Energieversorgung über die IT-Systeme bis zu den Services und Prozessen. In Echtzeit, jedes Detail, integriert, auf Knopfdruck visualisiert.

Unsere DCIM-Softwarelösung bietet das – dank des einzigartigen, durchgängigen FNT Datenmodells.

Jetzt informieren: [www.fntsoftware.com](http://www.fntsoftware.com)

## UMLUFTKÜHLUNG VON 5 BIS 200 KILOWATT

Mit den Präzisionsklimaanlagen Uniflair AM für kleine IT-Umgebungen (5 bis 20 Kilowatt) und Uniflair LE für mittelgroße und große Datacenter (20 bis 200 Kilowatt) bietet Schneider Electric nach eigener Auskunft flexible Lösungen zur Umluftkühlung. Die Klimaanlagen sollen eine bedarfsgerechte Anpassung an wachsende und wechselnde Ausstattungen im Datacenter ermöglichen. In Kombination mit Warm- oder Kaltgangeinhausungskonzepten sorgen die Kühllösungen laut Hersteller für mehr Energieeffizienz und verbessern die Leistungsdichten.

Die Geräte zur Kühlung von IT-Umgebungen von 5 bis 20 Kilowatt bietet Schneider Electric in unterschiedlichen Bauformen: als luft-, wasser- oder glykolgekühltes System und in den Konfigurationen mit Luftstrom nach oben oder unten. Durch die elektronisch kommutierten Lüfter (EC) sollen die Uniflair AM bei gleicher Kühllast den Gesamtenergieverbrauch des Datacenters senken. Das elektronische Expansionsventil reguliert laut Anbieter das eingesetzte Kältemittel und steigert so den COP-Wert (Coefficient of Performance). Die Wärmetausch-Register seien derart dimensioniert, dass der Anteil der sensiblen Leistung gegenüber der Gesamtkühlleistung hoch sei. Weitere Eigenschaften der Anlagen: Die Geräte sollen die Luft nur bei Bedarf entfeuchten und so eine gleichmäßige Luftverteilung ohne Verringerung des Luftstroms sicherstellen. Durch die Mikroprozessor-Regelung solle mit bis zu zehn Einheiten, die in einer Gruppe arbeiten, auf Raumbene für Redundanz gesorgt werden. Die Geräte seien kompatibel mit den gängigen Protokollen der Gebäudeleittechnik inklusive BACnet und Modbus.

Die Umluftkühler von 20 bis 200 Kilowatt wurden laut Schneider Electric speziell für Datacenter mit einem 24-Stunden-Betrieb entwickelt. Auch sie gibt es in verschiedenen Bauformen: als luft-, wasser- oder glykolgekühltes, doppelt gekühltes oder Energiesparsystem. Das Energiesparmodell besitze zwei Wärmetauscher und eigne sich idea-

lerweise für kleinere Rechenzentren. Im Sommer wird es als ein wassergekühltes Direktverdampfungsgerät benutzt. In kühleren Jahreszeiten schaltet laut Hersteller ein internes Ventil um und ermöglicht so die indirekte freie Kühlung. Somit sind die Investitionskosten geringer als bei einem Kaltwassergerät mit Chiller. Bei Bedarf könne das Direktverdampfungs-system auch zur Entfeuchtung genutzt werden und der Montageaufwand ist niedriger, da hier bereits zwei Systeme enthalten sind.



Quelle: Schneider Electric

**Die Umluftkühler Uniflair LE (20 bis 200 Kilowatt) wurden speziell für Rechenzentren mit einem 24-Stunden-Betrieb entwickelt.**

## OPNSENSE: FIREWALL GRATIS

Laut Anbieter Deciso kombiniert OPNsense die Vorteile von Open-Source-Firewalls mit denen von Closed-Source-Produkten. Die Initiative will die Funktionalität kommerzieller Angebote zusammen mit den Vorteilen offener und verifizierbarer Quellen in einer einfachen BSD-Lizenz kombinieren.

Wenn zwei Vorgaben beachtet werden, können Unternehmen mit OPNsense eine markenspezifische Version erstellen, den Funktionsumfang der Software erweitern oder eine Gabelung (Forking) erstellen und auf der gleichen Codebasis aufbauen. Zu den Funktionen von OPNsense gehören Lastausgleich, hohe Verfügbarkeit und ein Captive Portal. Alle Quellen und Build-Tools sollen ohne Sonderklauseln und Lizenzkosten frei verfügbar sein.

**OPNsense ist eine quelloffene Firewall samt Bedienung per Webinterface, deren Code quasi beliebig angepasst werden kann.**



Quelle: OPNsense.org

## IBM MIT CLOUD-RZ IN FRANKFURT

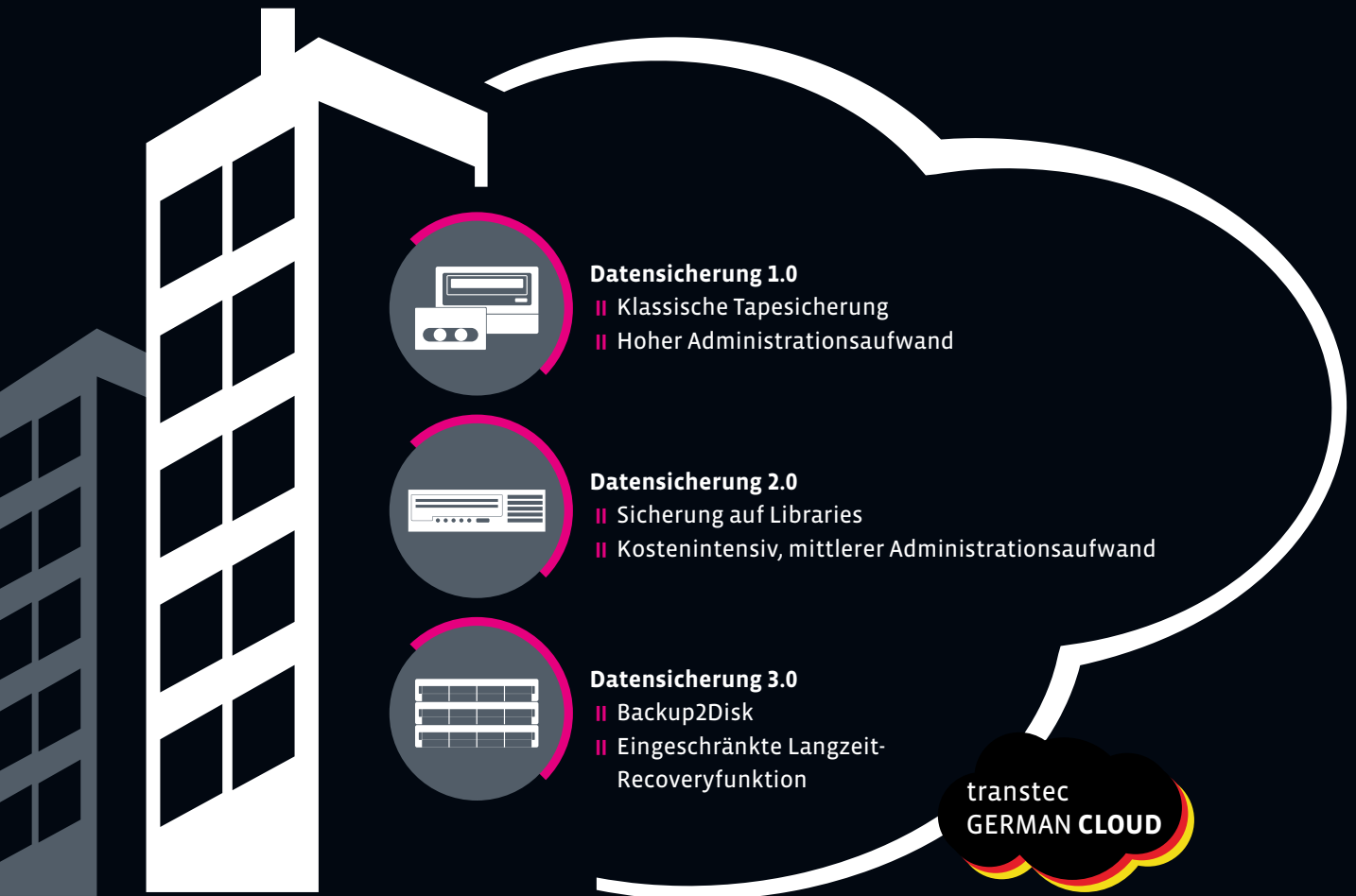
Nicht nur Amazon versorgt seine Kunden seit Neuestem mit einem Cloud-Rechenzentrum in Frankfurt – auch IBM erweitert ihr Cloud-Netz und eröffnet unter anderem in Frankfurt am Main ein Cloud-Zentrum. Die neuen IBM Cloud-Center in Frankfurt, Mexiko-Stadt und Tokio seien Teil einer 1,2 Milliarden US-Dollar hohen Investition, die IBM in den globalen Cloud-Ausbau steckt. So wolle man lokale Kundenanforderungen an Leistung, Sicherheit und Datenschutz erfüllen.

2014 habe IBM zahlreiche Cloud-Investitionen getätigt und Partnerschaften geschlossen, um ihre Cloud-Präsenz auszubauen oder auch Softwareentwickler mit der PaaS-Plattform (Platform as a Service) Bluemix zu unterstützen. So hat IBM nach eigener Auskunft einen Cloud-Marktplatz eröffnet, um das eigene Angebot mit Services von Drittanbietern zu ergänzen. Die Partnerschaft mit Equinix füge sich in eine Reihe weiterer Cloud-Vereinbarungen, die IBM in jüngster Zeit mit namhaften Unternehmen wie SAP, Microsoft, Tencent Cloud, AT&T oder Intel geschlossen habe. Zusätzlich will IBM nach eigener Auskunft auch seine Private-Computing-Services über die IBM OpenStack-Service-Plattform an OpenStack und Cloud Foundry Foundations liefern.

Im Jahr 2013 habe IBM mit der Cloud einen Umsatz von 4,4 Milliarden US-Dollar weltweit und wachse jährlich um knapp 70 Prozent. Zu den neuen Cloud-Kunden von IBM gehöre seit Kurzem auch die Lufthansa.

# Das transtec Backup-Konzept

## Höchste Sicherheit mit Backup-as-a-Service



### Datensicherung 4.0

- || Zusätzliche Auslagerung in die transtec German Cloud
- || Höchste Datensicherheit und -verfügbarkeit
- || transtec360 Service: Monitoring des Backups



CALLEO APPLICATION SERVER 2280S

Alle Informationen unter:  
[www.transtec.de/go/backup](http://www.transtec.de/go/backup)



Intel® Xeon® Prozessor

Intel, das Intel Logo, Xeon, und Xeon Inside sind Marken der Intel Corporation in den USA und anderen Ländern.



# Storage nach Wunsch

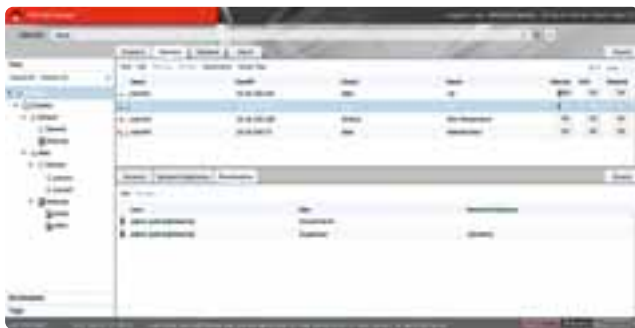
## Software Defined Storage ist der nächste Schritt hin zum virtualisierten Rechenzentrum

Storage, wie man ihn gerade benötigt – das ist das große Versprechen der softwaregesteuerten Storage-Lösungen. Obwohl die Vorstellungen davon oft noch schwammig sind, ist nahezu jedes große Unternehmen in der Branche auf diesen Zug aufgesprungen. Ein Leitfaden durchs derzeitige Dickicht.

Nachdem das Software Defined Networking (SDN) eines der großen Themen des Jahres 2013 war, nahm in den vergangenen Monaten der Software Defined Storage (SDS) seinen Platz ein. Beides ist eng miteinander verwandt, schließlich bauen beide auf Virtualisierungs-Techniken auf. Zusammen mit virtualisierten Servern bilden sie das Grundgerüst für das komplett per Software definierte RZ, das seine Services weitgehend automatisiert anbietet. Allerdings existiert nach wie vor keine einheitliche Definition von SDS. Trotzdem wollen nahezu alle größeren Hersteller auf diesen Zug aufspringen, was in den letzten Monaten dazu führte, dass teilweise bestehende Produktlinien einfach umgedeutet wurden in der Hoffnung, in der Diskussion um SDS Beachtung zu finden. Der Begriff wird zumindest momentan noch so schwammig verwendet, dass jede Software, die Storage verwaltet oder virtualisiert, als SDS durchgeht. Das soll sich nach dem Willen der Storage Networking Industry Association ändern. Sie hat den Entwurf für einen SDS-Standard vorgelegt, der unter anderem verschiedene Attribute und Funktionen vorschreibt. Ob und wann dieser Standard jedoch verabschiedet wird, steht derzeit noch in den Sternen. Allerdings ist es dem Anwender nur mit einer festen Definition von SDS möglich, verschiedene Systeme, die den Anforderungen entsprechen, miteinander zu vergleichen und das für ihn passende auszuwählen.

### Weitgefasste Kriterien

Bis der Standard verabschiedet ist, müssen einige weitgefasste Kriterien genügen, um SDS zu beschreiben. Der zentrale Punkt dieses Konzepts: Speichern und Verwalten der Daten sind von der zugrunde liegenden Hardware getrennt. Software und Hardware werden also als unterschiedliche Instanzen behandelt. Die Storage-Software stellt Services wie eine Orchestration, Provisionierung und Datenschnittstellen bereit



Quelle: IDC

Der Software Defined Storage ist ein Baustein für den Aufbau eines kompletten, per Software gesteuerten Rechenzentrums.

und bietet automatisch arbeitende Funktionen für die Verwaltung. Sie lässt sich auf nahezu beliebiger Storage-Hardware installieren und ermöglicht ein Scale-out der Ressourcen. Ziel einer SDS-Lösung ist es, Speicher-Ressourcen einfach und je nach Bedarf hinzufügen und bereitstellen zu können. Der physische Speicher wird dabei zu einem Pool zusammengefasst, der sich über mehrere Systeme erstrecken und unterschiedliche Medien wie SSDs und Festplatten umfassen kann.

Software Defined Storage darf dabei nicht verwechselt werden mit Storage-Virtualisierung: Letztere trennt durch das Bilden von Pools lediglich die Kapazität von den einzelnen Systemen. SDS dagegen abstrahiert sämtliche Services und Funktionen von der Hardware. Der große Vorteil von SDS ist die erhöhte Flexibilität. Werden Storage-Software und -Hardware voneinander getrennt, bedeutet das beispielsweise, dass Controller und Speichersysteme nicht mehr länger vom gleichen Hersteller bezogen werden müssen. Stattdessen kann der Controller an beliebiger Stelle innerhalb der Storage-Infrastruktur betrieben werden, auf einem dedizierten Server genauso wie in einem Hypervisor oder in einer Cloud. Die Unternehmen bekommen damit die Möglichkeit, Hardware verschiedener Hersteller zu kombinieren und preiswerte Standard-Systeme einzukaufen. Allerdings: Obwohl die Einrichtung einer SDS-Infrastruktur prinzipiell mit jeder Hardware möglich ist, empfehlen Experten, getestete Enterprise-Systeme der führenden Hersteller zu verwenden und mit Händlern zusammenzuarbeiten, die entsprechendes Know-how vorweisen können.

### Hilfe durch definierte Service-Level

Ein weiterer Vorteil von SDS ist, dass viele Standardaufgaben automatisiert oder einfach dem Anwender überlassen werden können. Er gibt beispielsweise an, welche Kapazität er benötigt, ob die Daten gespiegelt oder mit Snapshots gesichert werden sollen, und bekommt anschließend einen auf seine Ansprüche zugeschnittenen Storage vom System zugewiesen. Damit das funktioniert, definiert der Administrator verschiedene Service-Levels für die vorhandenen Systeme. Er teilt die Arrays über die Storage-Software etwa in mehrere Performance-Klassen ein, gibt an, welche durch Snapshots überwacht werden, wo überall eine Replikation eingerichtet ist und bei welchen Systemen die Daten dedupliziert werden. Über ein Portal klickt sich der Anwender dann die benötigten Eigenschaften für seinen Storage zusammen, die Software macht den Rest.

Schließlich reizt an SDS auch die Möglichkeit, die vorhandene Storage-Infrastruktur per Scale-out zu erweitern. Während einzelne Systeme bei Performance, Kapazität und Funktionalität oft schnell an ihre Grenzen stoßen und schließlich ersetzt werden müssen, kann ein Unternehmen mit einer SDS-Infrastruktur einfach weitere Systeme hinzufügen. Theoretisch jedenfalls. Denn dazu bedarf es letztlich eines



übergreifenden, herstellerunabhängigen Standards, den es derzeit noch nicht gibt – siehe oben.

## Ursprünge in der Storage-Software

Der SDS-Pionier heißt Datacore. Die amerikanische Firma brachte bereits im Jahr 2000 mit SANsymphony eine offene Storage-Management-Plattform für Unternehmen auf den Markt. Im Jahr 2011 veröffentlichte sie das weiterentwickelte SANsymphony-V, das auch eine Option zur Virtualisierung enthielt und damit das erste vollwertige SDS-Produkt darstellte. Allerdings wird es nicht als Software Defined Storage vermarktet, sondern als Virtual SAN – gleiche Technik, anderes Schlagwort. Die aktuelle Version SANsymphony-V10 lässt sich bis auf 50 Millionen IOPS und 32 Petabyte skalieren, integriert Festplatten genauso wie SSDs und bietet Funktionen für automatisches Failover und Failback. Gegenüber anderen SDS-Produkten zeichnet sie sich unter anderem dadurch aus, dass sie sowohl ein virtuelles SAN aufspannen und gleichzeitig physische SANs verwalten kann.

Auf Seiten der Software-Hersteller geht auch VMware das Thema SDS an und stellte die Software Virtual SAN (VSAN) vor. Sie ist in den Kernel von VMware vSphere integriert und fasst Festplatten und SSDs in x86-Servern zu Pools zusammen, die virtuellen Storage-Cluster können bis zu 4,4 Petabyte groß werden. Über eine richtlinienbasierte Kontrollebene lassen sich Aufgaben wie etwa die Provisionierung oder das Management des Storage automatisieren. VSAN ist zwar hardwareunabhängig, unterstützt jedoch nicht sämtliche Geräte auf dem Markt. VMware hat daher Kompatibilitätslisten für bestimmte Server-Konfigurationen und einzelne Komponenten zusammengestellt.

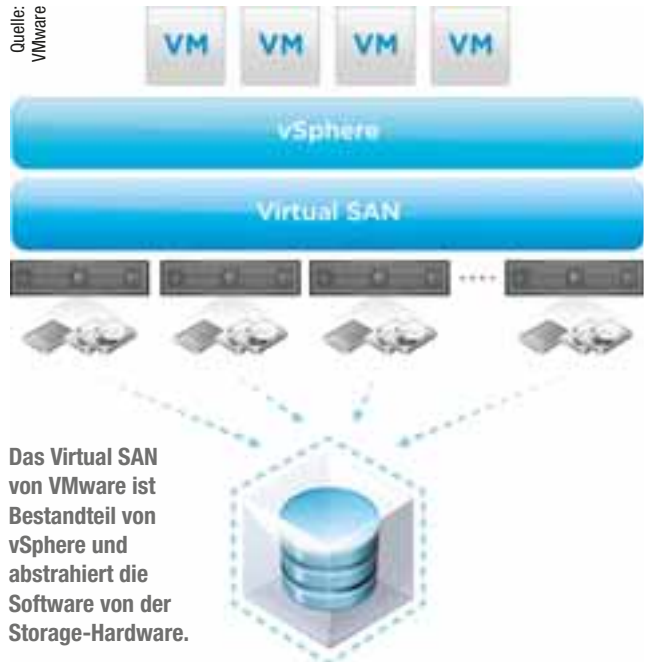
## SDS bei den Storage-Herstellern

Auch Linux-Hersteller Red Hat engagiert sich stark auf dem SDS-Markt und hat 2014 im Abstand von einem halben Jahr gleich zwei Versionen seines Red Hat Storage Server vorgestellt. Die Version 3 basiert auf dem Dateisystem GlusterFS und dem Betriebssystem Red Hat Enterprise Linux 6 und sei damit für Kapazitäten bis in den Petabyte-Bereich ausgelegt, teilte das Unternehmen mit. Zudem hebt es die einfache Integration in Apache Hadoop heraus und sieht Einsatzmöglichkeiten vor allem in den Bereichen Big-Data-Analyse, Kollaboration und Filesharing.

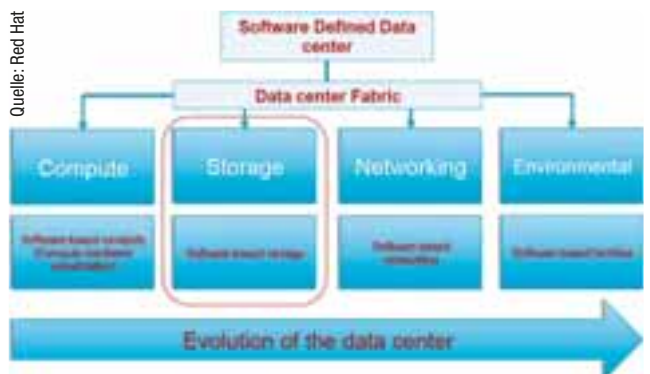
Von den Storage-Herstellern erkannte EMC als einer der ersten den SDS-Trend. EMC stellte 2013 seine Software-Lösung ViPR vor, mit der Unternehmen ihren Storage zu Pools zusammenfassen und von der Hardware abstrahieren können. Im Unterschied zu Virtual SAN unterstützt sie nicht nur die VMware-Technik, sondern auch Microsoft Hyper-V und die offene Cloud-Lösung OpenStack. Eine REST-basierte Standard-API ermöglicht einen direkten Zugriff auf die von ViPR verwalteten Ressourcen und Daten. Die Software ist sogar herstellerunabhängig. Neben den hauseigenen Array-Reihen Isilon, VMAX und VNX soll die Lösung auch zu den Systemen konkurrierender Firmen wie Hitachi Data Systems, NetApp, HP, IBM, Dell oder Oracle kompatibel sein.

Sehr aktiv im SDS-Umfeld ist HP und hat gleich einige entsprechende Software-Pakete im Programm. Das führende Produkt der Firma nennt sich HP StoreVirtual VSA (Virtual Storage Appliance) und ist laut HP die erste SDS-Lösung, die auch Daten-Tiering unterstützt: Häufig angeforderte Daten packt es beispielsweise automatisch auf die schnellen, aber auch teuren und zumeist kleineren SSDs, seltener nachgefragte Blöcke verschiebt es auf preiswertere, größere, aber auch langsamere SATA-Festplatten. StoreVirtual VSA läuft sowohl in VMware- wie auch in Microsoft-Hyper-V-Umgebungen.

Quelle: VMware



Quelle: Red Hat



Ein solches Tiering bietet auch Elastic Storage von IBM. Elastic Storage soll nahezu unbegrenzt skalierbar sein und sowohl lokalen als auch Cloud-Speicher einbeziehen können. IBM sieht die Software vor allem im Big-Data-Umfeld und generell überall, wo sehr große Datenmengen verarbeitet werden wie etwa bei Erdbeben-Vorhersagen oder der Analyse von Finanzdaten. Konsequenterweise bietet sie daher Schnittstellen sowohl zu OpenStack als auch zu Hadoop.

Und was bleibt unterm Strich?

Die neuen SDS-Lösungen weisen vielversprechende Ansätze auf und geben dem Anwender mehr Freiheiten beim Aufbau seiner Storage-Infrastruktur. Ob sie allerdings die hochgesteckten Erwartungen und Versprechen der Industrie tatsächlich alle erfüllen können, ist zumindest fraglich. Denn ohne einen allgemein akzeptierten Standard wird die Flexibilität des Anwenders immer eingeschränkt bleiben.

*Roland Freist,  
Freier IT-Fachjournalist*

# Auf dem Weg zum Software Defined Datacenter

## Elementarer Bestandteil des softwarebasierten RZ ist Software Defined Storage

Welches Speichermedium ist am besten für bestimmte Daten geeignet? Auf diese Frage konzentriert sich die Diskussion bei Storage-Systemen. Die Antwort soll Software Defined Storage liefern, das letztendlich auch die Grundlage ist für die nächste Generation der RZ-Infrastruktur – das Software Defined Datacenter.

Die Auswahl der passenden Speicherlösung spielt eine wichtige Rolle in den IT-Abteilungen: Daten sind das Lebenselixier in jedem Unternehmen. Verfügbarkeit, Zuverlässigkeit und der Schutz der Daten bestimmen die Speicherstrategie und -architektur und liefern das Fundament für die Produktivität in den Fachabteilungen. Wenn es um rasche Datenzugriffe geht, sind NAS und SAN flexibler, aber auch DAS (Direct Attached Storage, lokale Festplatte) ist immer noch aktuell.

Mit dem Aufkommen der Server-Virtualisierung für x86-Systeme ist in den Rechenzentren vieles in Bewegung geraten. Bei Storage zielt die Virtualisierung darauf ab, den vorhandenen Speicherplatz besser auszunutzen, um so Leistungsspitzen abzufangen. Zugleich lassen sich durch Storage-Virtualisierung der Verwaltungsaufwand, die Ausfallrisiken und die damit verbundenen Kosten reduzieren.

### Die Flut der unstrukturierten Daten

Gemeinsam genutzter Storage ist oft durch Systeme charakterisiert, die auf proprietären Hardwarekomponenten und einer nahtlosen Einbindung der Firmware basieren. Daher bleiben viele Speichersysteme unflexibel, komplex und verursachen beträchtliche Kosten im Betrieb. Das Aufkommen von softwarebasierten Techniken in den letzten Jahren wie Deduplizierung, Replikation, Snapshots, Cloning oder Thin Provisioning hat wichtige Fortschritte bei der Modernisierung der Datenspeicherung gebracht. Traditionelle, hardwaredefinierte Systeme eignen sich für Umgebungen mit einem vorhersehbaren und nur leicht

steigenden Datenwachstum. Exemplarisch für diese Szenarien sind Datenbanken, in denen strukturierte Datensätze entstehen und verwaltet werden.

In vielen Unternehmen hat sich in den letzten Jahren jedoch das Verhältnis zwischen den auf Storage-Medien vorgehaltenen strukturierten und den unstrukturierten Daten drastisch gewandelt: Waren beide Segmente bis vor Kurzem in etwa gleich groß, entfallen heute rund 90 Prozent des Speichervolumens auf unstrukturierte Daten. Diese Herausforderung muss die IT angehen. Einen Ansatz dazu bieten zukunftsfähige softwarebasierte Storage-Lösungen, die ausbaufähig, kosteneffizient, hoch verfügbar und einfach zu verwalten sind.

### Software Defined Storage baut Brücken

Bei Software Defined Storage (SDS) geht es im Kern um das Trennen von Hardware und Software, um flexibler zu werden. SDS arbeitet mit standardbasierten Komponenten, und die Storage-Software dient dazu, Daten schneller und flexibler bereitzustellen. Dafür existiert in den Unternehmen eine deutliche Nachfrage, für die es verschiedene Lösungsvarianten gibt. Dabei lassen sich zwei Anwendungsszenarien unterscheiden: erstens bereits vorhandene Umgebungen, die um Software Defined Storage aufgewertet werden, und zweitens reine Software-Umgebungen.

Die Akzeptanz bei den Anwendern wäre nur sehr gering, wenn keine stufenweise Migration möglich wäre. Es werden auch weiterhin

## EINSATZGEBIETE VERSCHIEDENER SOFTWARE-DEFINED-STORAGE-LÖSUNGEN

	Dell XC Web-Scale Converged Appliance mit Software von Nutanix	Microsoft Storage Spaces	Nexenta NexentaStor	Red Hat Inktank Ceph und Red Hat Enterprise Linux OpenStack	VMware EVO: RAIL
Anforderungsniveau	Geschäftskritisch, Hosting	Geschäftskritisch, Hosting	Geschäftskritisch, Hosting	Geschäftskritisch, Hosting	Geschäftskritisch, Hosting
Anwendungsszenarien	Einfach, skalierbar und leistungsstark für VDI; Abteilungs-Virtualisierung; gemischte Umgebungen mit Hypervisor und Private Cloud; Hypervisor-Migration	Unternehmen sowie Provider, die Microsoft-Kunden sind, und Entwicklungs- und Testumgebungen sowie eine kosteneffiziente Speicherumgebung benötigen	Unternehmen, die eine ZFS-Speicherlösung für sehr große Datenmengen benötigen	Skalierbarer Speicher in Private und Public Clouds	VMware-Kunden mit Schwerpunkt VDI sowie Test- und Umgebungen
Profil der Anwendungsszenarien	Gutes Preis-Leistungs-Verhältnis	Kostenoptimiert, aber auch gutes Preis-Leistungs-Verhältnis	Kostenoptimiert	Kostenoptimiert	Gutes Preis-Leistungs-Verhältnis

Hardware- und Software-definierte Welten koexistieren. Bei einem evolutionären Weg sind etwa serverseitiger Speicher, externe SANs, virtualisierter Speicher, physische und virtuelle Appliances gefragt. Eine höhere Effizienz und Flexibilität sowie eine einfache Verwaltung schützen die Investitionen, die Unternehmen bereits getätigt haben.

### Modulare Speichersysteme fördern Migration

Ein Kernbestandteil von SDS-Lösungen sind flexible, modulare Speichersysteme. Intelligente Software folgt dem Modell des dynamischen Tierings und legt Daten automatisch ihrer Bedeutung für bestimmte Anwendungsszenarien entsprechend auf einem Speicherbereich mit sehr kurzen Zugriffszeiten oder einem kostengünstigen Speicherbereich ab.

Häufig benötigte Informationen befinden sich auf schnellen, kleinen und teuren Medien (zum Beispiel SAS-Festplatten oder SSDs). Daten, die nur selten benötigt werden, platziert die Software auf großen, aber kostengünstigen Medien (beispielsweise Nearline-SAS-Platten). Das geschieht natürlich auch umgekehrt. Steigen die Zugriffe auf Informationen, werden sie wieder auf schnelle Medien verlegt.

Ein weiterer Vorteil des dynamischen, automatisierten Tierings: Müssen die Kapazitäten erweitert werden, weil die Menge der langfristig zu speichernden Daten steigt, benötigen Unternehmen nur große, kostengünstige Festplatten. Eine weitere Variante besteht darin, dass selten benötigte Daten oder solche, die sicher mit Geschäftspartnern oder Kunden geteilt werden sollen, in die Cloud verlagert werden. Gleichzeitig ist die Cloud auch einer der Auslöser für innovative Software-Defined-Storage-Lösungen, die eine hohe Flexibilität bezüglich der Rechen- und Speicherkapazitäten erfordern.

Der eher revolutionäre Weg eignet sich vor allem für neue Applikationsszenarien und umfasst reine Softwarelösungen, hyperkonvergente, vollkommen neu aufgesetzte Infrastrukturen, die Server, Speicher, Netzwerkkomponenten und Virtualisierungssoftware in einem Gehäuse kombinieren oder auch skalierbare Lösungen in Public Clouds und SaaS-Umgebungen. Durch flexible Hardwarekonfigurationen bezüglich der Anzahl der Prozessorkerne, der Größe des integrierten Cache- und des Flash-Speichers für Lese- und Schreibvorgänge lassen sich solche Lösungen an verschiedene Anwendungsszenarien anpassen.

### Ausblick: Software Defined Datacenter

Bei neuartigen Anwendungsszenarien geht der Trend in Richtung hyperkonvergenter, hochintegrierter Systeme, die vermehrt auf Open-Source-Lösungen setzen. Hier sind Hauptspeicher, Rechen- und Speichernetzwerkfunktionen in einer reinen Softwarelösung oder einer Appliance zusammengefasst. Alle konvergenten beziehungsweise hyperkonvergenten Systeme zeichnen sich dadurch aus, dass sie zusätzlich zur Integration von Rechen- und Speicherfunktionen in einem Knoten oder einem Cluster einen Hypervisor für das Datenmanagement nutzen. Das Spektrum der verfügbaren Lösungen reicht von konvergenten Infrastrukturlösungen für einzelne Rechenzentren, über eine Private oder Hybrid Cloud, bis hin zu hyperkonvergenten Web-Scale-Umgebungen.

Software Defined Storage wird so zu einem zentralen Puzzleteil, mit dem ein durchgängiges Software Defined Datacenter entsteht, das Server, Storage-Systeme und Netzwerke umfasst. Die höhere Flexibilität und eine einfachere Verwaltung, die sich als die wichtigsten Vorteile einer Software Defined Infrastructure erweisen, sprechen dafür, dass Unternehmen einen flexiblen und offenen Ansatz auf dem Weg zu einem Software Defined Datacenter verfolgen.

*Hans Schramm,  
Field Product Manager Enterprise, Dell*



## Rechenzentrums- Infrastruktur für das nächste Jahrzehnt

Nutanix macht IT kompromisslos einfach, so dass Sie sich auf Ihr Geschäft konzentrieren können. Stellen Sie jede Anwendung bereit, in jedem Maßstab mit höchster Effizienz und optimierten Gesamtbetriebskosten (TCO). Erfahren Sie, warum Ihr Unternehmen Web-Scale Infrastruktur braucht - und weshalb gerade jetzt.



Besuchen Sie uns:  
Halle 2, Stand B29  
16.-20. März 2015, Hannover

[nutanix.com/dcinfrastructure](http://nutanix.com/dcinfrastructure)

**NUTANIX**™

# Wider die Datenlawinen und Kostenexplosionen

## Wie die Virtualisierung von Datenkopien einzelne Elemente sowie die Gesamtpformance eines Rechenzentrums beeinflusst

Anstatt für immer mehr Geld immer mehr Speicherplatz zu kaufen und zu verwalten, sollten RZ-Betreiber sich dem Thema Datenkopien widmen: Durch geschickten Umgang mit den (notwendigen) Kopien lassen sich Zeit, Aufwand und letztendlich Geld sparen. Zudem steigt die Sicherheit, da weniger unkontrollierte Kopien herumvagabundieren.

Das Rechenzentrum unterliegt einem radikalen technischen Wandel. Bei den Speichermedien geht der Trend von Bandspeicher und Festplatte (HDD) zu Flash-Speicher (SSD). Manche Unternehmen entscheiden sich vorerst für einen Mischbetrieb, was jedoch das Daten-, Storage- und Performance-Management aufwendiger macht. Die Komplexität der IT-Landschaft im Rechenzentrum nimmt ohnehin zu. Gleichzeitig steigt der Kostendruck, so dass Computing-, Storage- und Netzwerk-Ressourcen konsolidiert werden müssen.

Energiekosten sind dabei ein wichtiges Thema, daher gilt es den Betrieb des Rechenzentrums effizient zu gestalten. Dies ist umso dringlicher, da die Datenlawine anwächst und sich die Verwaltung des zunehmenden Speicherbedarfs in den Betriebskosten deutlich niederschlägt. Gleichzeitig wollen Unternehmen – Stichwort „Big Data“ – wertvolle Erkenntnisse aus dem Datenberg ziehen.

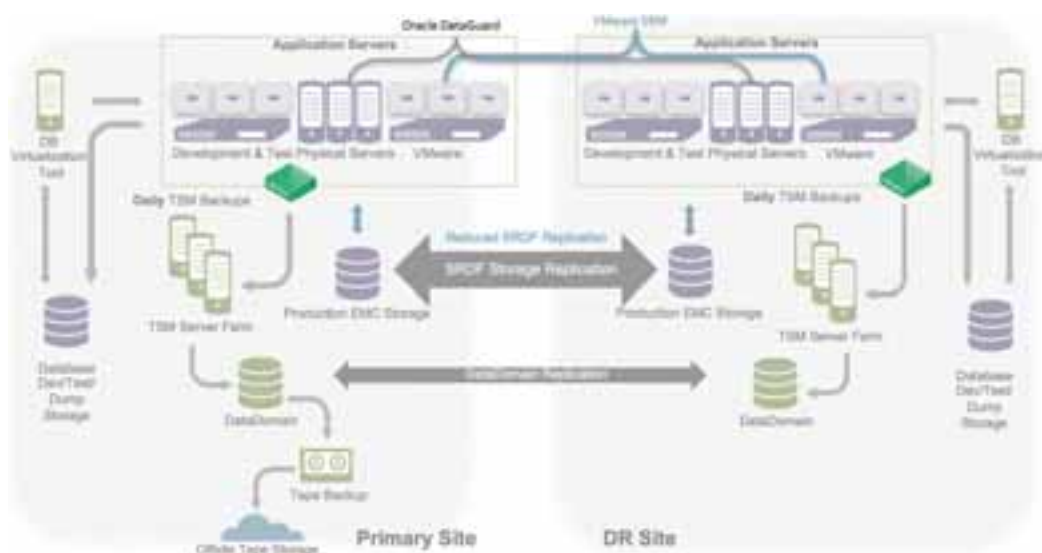
Schließlich kommt noch das Thema Sicherheit hinzu. Die wachsende Menge an Daten muss sowohl zugänglich als auch sicher sein. Dies ist eine schwierige Gratwanderung und sie ist umso schwieriger, je mehr Datenkopien es gibt, da sich damit auch die Angriffsfläche vergrößert. Würden also weniger Kopien im Ansatz erstellt werden,

würde sich die Anzahl der sicherheitsrelevanten Ziele drastisch verringern. Hinzu kämen geringere Administrations- und Betriebskosten, wenn sich das Datenwachstum durch effizientere Datenverwaltung eindämmen ließe.

### Reichlich (überflüssige) Kopien

Das Datenvolumen wächst nicht nur aufgrund täglich neuer Daten, sondern exponentiell durch die ungebremste Vermehrung von Datenkopien. Doch woher kommt die Flut an Datenkopien? Traditionelle Systeme für Datensicherung, Wiederherstellung im Notfall, Test und Entwicklung, Analyse, Snapshots oder Migrationen erstellen alle redundante Kopien von Anwendungsdaten in separaten Silos.

So können in Unternehmen bis zu 120 Kopien bestimmter Produktionsdaten in Umlauf sein. In einer Studie aus dem Jahr 2013 schätzte IDC, dass der Umgang mit der Flut an Datenkopien weltweit 44 Milliarden US-Dollar an Kapital verschlingt. Insgesamt fließen laut IDC 85 Prozent der Investitionen in Speicherhardware und 65 Prozent in Speichersoftware in die Bewältigung überzähliger Datenkopien. Deren Ma-

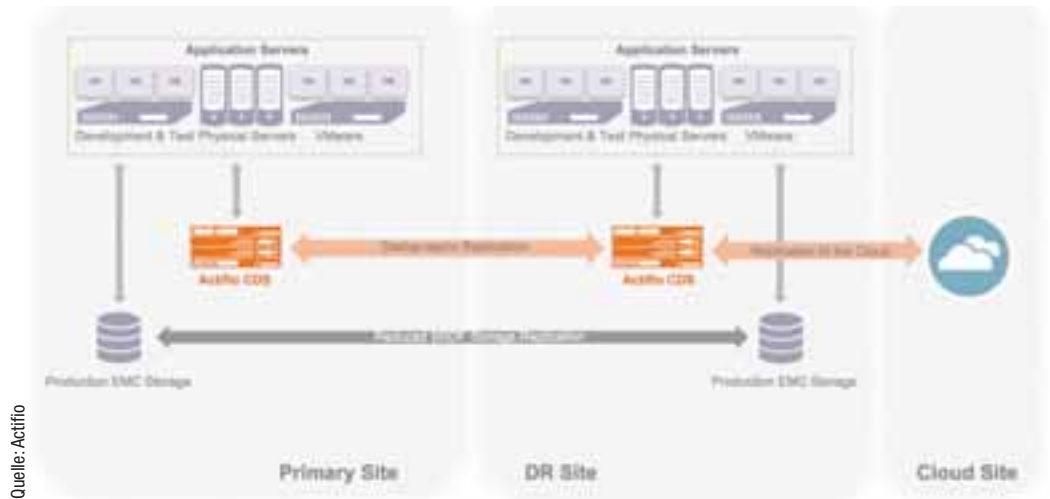


Quelle: Actifio

Die klassische Architektur im Data Center weist eine Vielzahl an Daten-silos für einzelne Anwendungen sowie eine große Zahl an Datenkopien auf.

# STRATEGIE

Durch die Virtualisierung von Datenkopien entfällt eine Vielzahl identischer Datenbestände, wodurch die Übersichtlichkeit der Infrastruktur steigt und die Komplexität des Datenmanagements sinkt.



management nimmt in Unternehmen inzwischen mehr Ressourcen in Anspruch als die Verwaltung der eigentlichen Produktionsdaten.

Die Virtualisierung von Datenkopien hat sich als effektive Maßnahme erwiesen, um die Datenverwaltung bereits im Ansatz deutlich effizienter zu gestalten. Durch die gleichzeitige Integration von Datenduplizierung und ein Maximieren der Netzwerknutzung ist ein sehr effizientes Datenhandling möglich. Da weniger Bandbreite und Spei-

cher erforderlich ist, lassen sich zusätzlich sehr kurze Wiederherstellungszeiten realisieren.

Ein mögliches Prinzip ist dabei der Einsatz einer sogenannten „virtuellen Daten-Pipeline“. Dabei handelt es sich um ein verteiltes Objektdateisystem, in dem die wichtigsten Grundlagen der Datenverwaltung – Kopieren, Speichern, Verschieben und Wiederherstellen – virtualisiert werden. Auf diese Weise können aus der Sammlung ein-

## Gezielte Luftführung

## Optimale Energiebilanz

## Variable Installation von Hardware

dtm.  
group

### Zukunftssichere Verkabelung



### Kabelmanagement QuickLink



Lückenlose Beratung, Planung und Ausführung **energieeffizienter** Rechenzentren





Quelle: Actifio

**Wurde das Datenmanagement vereinfacht, genügt eine App fürs Tablet, um die Daten im RZ zu verwalten oder Backups zu steuern.**

deutiger Datenblöcke jederzeit virtuelle Kopien von zeitspezifischen Daten erstellt werden.

Müssen die Daten wiederhergestellt werden, wird das zugrunde liegende Objektsystem von der Copy Data Virtualisierungs-Lösung analysiert und anschließend an einem vom Benutzer festgelegten Wiederherstellungspunkt in einem beliebigen Anwendungsformat extrahiert. Dadurch, dass die wiederhergestellten Daten direkt auf einem Server gemountet werden, ist keine Datenverschiebung erforderlich, was ebenfalls zur geringen Wiederherstellungszeit beiträgt. Die wiederhergestellten Daten stehen somit unmittelbar zur Verfügung.

## Mehr Effizienz beim Daten-Handling

Die virtuelle Datenpipeline dient dazu, Daten so effizient und effektiv wie möglich zu erfassen, verwalten und zur Verfügung zu stellen. Nach dem Erstellen und Speichern eines einzelnen, vollständigen Snapshots werden mithilfe von Change Block Tracking nur die geänderten Blöcke der Anwendungsdaten erfasst, nach einem Incremental-forever-Prinzip. Die Datenerfassung erfolgt auf Blockebene, da dies der effizienteste Weg ist, um Änderungen zu verfolgen und zu übertragen. Die Daten werden in ihrem nativen Format verwendet, daher werden sie auch in ihrem nativen Format gespeichert. Somit besteht keine Notwendigkeit, Daten aus Backup-Dateien zu erstellen oder wiederherzustellen.

Erfasst werden die Daten auf der Basis von SLAs, die vom Administrator festgelegt werden. Diese beinhalten die Häufigkeit der Snapshots oder Speicherung, der Typ Speicher, in dem sie gespeichert werden sollen, und die Dauer der Speicherung. Ebenso lässt sich festlegen, ob sie an einen Remote-Speicherort oder bei einem Cloud-Serviceanbieter repliziert werden sollen. Sobald ein SLA erstellt wurde, kann eine beliebige Anwendung oder virtuelle Maschine auf die Daten zugreifen.

Zur Datenverwaltung wird ein physisches „goldenes“ Image oder eine Master-Kopie der Produktionsdaten vorgehalten und auf Basis des SLA ständig aktualisiert. Diese „goldene Kopie“ steht immer zur Verfügung. Eine virtuelle Kopie ausgewählter Produktionsdaten für Tests, Entwicklung oder Analyse kann dann innerhalb von Minuten ohne Beeinträchtigung der Produktion bereitgestellt werden. Die „goldene Kopie“ kann an einen ausgelagerten Standort für die Wiederherstellung im Notfall gespiegelt werden.

## Positive Auswirkungen auf das Rechenzentrum

Die Virtualisierung von Datenkopien im Rechenzentrum entlastet Produktionssysteme und unterstützt die Datensicherung, Wiederherstellung im Notfall und Geschäftskontinuität. Was das Server-Backup be-

trifft, so wird das herkömmliche NDMP-(Network Data Management Protocol)-Backup für Server obsolet. Vollständige Sicherungen sind nicht mehr nötig, da das Mounten von Images eines beliebigen Zeitpunkts jederzeit möglich ist. Für das langfristige Aufbewahren von Images kommt bei der Copy Data Virtualisierungs-Lösung effiziente Deduplizierung und Komprimierung zum Einsatz. Ältere Images lassen sich ebenfalls auf einfache Weise mounten und verlorene oder beschädigte Daten innerhalb von wenigen Minuten wiederherstellen.

So unterstützt das Verwalten von Datenkopien auch die Disaster-Recovery-Anforderungen im Unternehmen: Daten lassen sich unter Einsatz verschiedener Techniken an einen entfernten Ort replizieren, je nach Anforderung des Unternehmens. Synchrone oder asynchrone LUN-Spiegelung ist ebenfalls möglich. Mit spezieller Dedup-Async-Replikation kann die für die Datenwiederherstellung erforderliche Bandbreite erheblich reduziert werden. Bei der Dedup-Backup-Replikation wird nur der erforderliche Block, der bereits dedupliziert und komprimiert wurde, für die langfristige Aufbewahrung über das WAN transferiert.

Copy Data Management entlastet damit auch den Primärspeicher, da Datenkopien separat aufbewahrt werden können. Nachdem viele Unternehmen auf SSD für den Primärspeicher umsteigen, ist die Wirtschaftlichkeit besser, wenn keine Datenkopien diesen beanspruchen. Der Primärspeicher verwaltet die Leistungsanforderungen der Produktionsdaten, während die Copy Data Management-Lösung sich um alle anderen Datenbelange kümmert.

Bei Anwendungsentwicklung, Tests und Analyse spielt das Verwalten virtueller Datenkopien ebenfalls seine Stärken aus: Das Mounten eines virtuellen Images auf jedem Gerät erfolgt unmittelbar und ohne die Notwendigkeit, eine vollständige physische Kopie vorzuhalten. Daraus resultiert eine wesentlich schnellere Verfügbarkeit und geringerer Speicherbedarf. Ebenso lässt sich ein Klon der virtuellen Kopie erstellen, wenn eine neue Produktionsversion benötigt wird oder für Vorproduktionstests.

## Das Verfahren zahlt sich aus

Copy Data Virtualisierung kann für eine Teilmenge der Datensicherung genutzt werden, in Koexistenz mit vorhandenen Anwendungen und Infrastrukturen oder lediglich für Tests und Entwicklung zum effizienten Einsatz kommen. Das größte Effizienzpotenzial entfaltet sich jedoch, wenn vorhandene Silolösungen nach und nach eliminiert werden können. Eine einheitliche Copy Data Management-Plattform wird dann zur effizienten Drehscheibe für die Datenverwaltung und beseitigt auf elegante Weise das Problem der Verwaltung einer rasant zunehmenden Menge an redundanten Datenkopien.

Wer hingegen kontinuierlich das rapide Datenwachstum mit Investitionen in zusätzliche Speicherhardware abfangen will, wird früher oder später durch die Kostenexplosion und zunehmende Komplexität der Verwaltung und Kompromisse in der Sicherheit ausgebremst. SSD als neue effiziente, aber derzeit noch kostenintensive Speichertechnik ist zu schade, um mit überflüssigen Datenkopien in Richtung Kapazitätsgrenzen zu steuern. Durch Copy Data Virtualisierung wird der Datenhaushalt komprimiert und von Redundanzen befreit. Dies verschafft den vorhandenen Speicherressourcen für die wichtigen Produktionsdaten viel Luft, um auch das Datenwachstum der nächsten Jahre zu bewältigen. Gleichzeitig wird eine schnelle und zuverlässige Datenverfügbarkeit und damit Geschäftskontinuität sichergestellt. All das geht mit reduzierten Betriebskosten, effektiverer Verwaltung und einer erhöhten Sicherheit für das Rechenzentrum einher.

*Ash Ashutos,  
CEO und Gründer, Actifio*

## UNSER STANDARD: PERFEKTION IM DETAIL



**47 nutzbare HE**

**Traffic Commitment**  
100 Mbit inklusive

**Zahlenschloss** mit eigener  
3-stelliger Kombination

**Uplink Switchport** 1 Gbit/s  
(bis zu 10 Gbit/s redundant)

**+ Hochsicher**

Mehrfach redundante Technik- und Sicherheits-Systeme

**+ Schnell**

Eigener DarkFibre City Ring mit über 50 Gbit/s IP-Transit

**+ Individuell**

Maßgeschneiderte Lösungen nach genauer Bedarfsanalyse

**+ Effizient**

30% weniger Stromkosten durch innovative Kaltgangeinhausung

**799,00 €\***  
PRO MONAT



[WWW.INTERNETX-HOUSING.COM](http://WWW.INTERNETX-HOUSING.COM)

Tel. +49 941 59559-483

vertrieb@internetcx-housing.com



\*Das Angebot, Rack inkl. Traffic Commitment 100 Mbit, gilt bis zum 28. Februar 2015 mit einer Laufzeit von 12 Monaten. Die Einrichtungsgebühr entfällt. Das Angebot richtet sich nur an Unternehmer und versteht sich zzgl. ges. MwSt.

# Den Energieverbrauch im Blick

## Mit den richtigen Maßnahmen – beispielsweise Messungen – lässt sich der Energieverbrauch im Rechenzentrum erheblich senken

Zahlreiche Serracks, optimale Kühlung, Sicherheitssysteme und eine unterbrechungsfreie Stromversorgung – all das ist essentiell für den Betrieb eines Rechenzentrums und frisst eine Menge Energie. Steigende Energiepreise und der gleichzeitige Druck, Kosten zu senken, um wettbewerbsfähig zu bleiben, stellen die RZ-Betreiber vor große Herausforderungen in Sachen Energiemanagement.

Um in RZ Energie effizient zu nutzen, gibt es mehrere Ansatzpunkte. Untersuchungen zeigen, dass die eigentliche IT nur rund 50 Prozent des Energieverbrauchs ausmacht, der Rest ist durch Infrastruktur wie Klimatisierung, Licht oder Sicherheitssysteme bedingt.

Im Schnitt fließen mindestens 20 Prozent der gesamten Energiekosten eines Rechenzentrums in die Kühlung der Anlage. Der richtige Aufbau der Serracks sowie moderne Mess- und Kühltechnik können diesen Anteil allerdings deutlich senken. Die richtige Klimatisierung der Räume ist also ein wesentlicher Aspekt in Sachen Energiemanagement – und entscheidend dafür ist die optimale Luftführung.

### Optimale Luftführung und Temperatur

Server saugen an ihrer Front kalte Luft ein und geben nach hinten warme Abluft ab. Eine Kaltgangeinhausung und Abdichtungen an Racksöffnungen oder im Doppelboden sorgen dafür, dass Zu- und Abluft sich nicht durchmischen. Über perforierte Bodenplatten wird die kühle Luft aus dem Doppelboden direkt in die Kaltgänge geleitet. Die Abluft wiederum strömt über die Schränke und wird zu den Kühlgeräten zurückgeführt – so weit, so bekannt. Dabei muss die Luftführung immer an die tatsächliche Serverbestückung angepasst werden.

Die Kühlluft wird von Umluftkühlgeräten erzeugt. Diese Ventilatoren laufen 24 Stunden am Tag und somit 8760 Stunden im Jahr – also auch eine effektive Stellschraube zum Energiesparen. Früher waren die Ventilatoren nicht regulierbar, sondern liefen immer mit voller Leistung. Und volle Leistung heißt doch optimale Kühlung, oder?



Quelle: Cofit

Mit modernen Servern lassen sich im Vergleich zu alten Modellen 20 bis 35 Prozent Energie einsparen – zumal der Leistungsschub durch neue Hardware sicher auch willkommen sein dürfte.

### Keine Server-Kühlschränke mehr

Falsch. Heute nutzt man in der Regel drehzahlregelte Ventilatoren, die im Schnitt nur mit einer Leistung von 30 bis 50 Prozent laufen. Setzt man mehrere Geräte mit entsprechend reduzierter Drehzahl ein, kann man erheblich Energie einsparen. Zudem ist die Ventilatorsteuerung des Kühlgeräts mit dem Ventil des Kaltwasserzustroms gekoppelt und wird entsprechend reguliert. Je weniger Kaltwasser durch das Ventil fließt, desto weniger Leistung erbringt der Kühler. Eine große Einheit, die auf niedriger Stufe läuft, ist dabei effizienter als mehrere kleine Kühlgeräte. Wie viele Umluftkühler eingesetzt werden, hängt von der Größe, Auslastung und Ausstattung des Rechenzentrums ab.

Früher glichen Rechenzentren Kühlschränke. Die Temperatur wurde sehr niedrig gehalten, damit Server- und Speichertechnik reibungslos funktionierten. Doch die Technik hat sich weiterentwickelt und die Komponenten vertragen heute höhere Temperaturen und auch mehr Luftfeuchtigkeit: 2004 lag die empfohlene Ansaugtemperatur für technische Geräte in Rechenzentren bei 20 bis 25 Grad Celsius, zehn Jahre später liegt sie zwischen 22 und 26 Grad Celsius.

Kein großer Unterschied? Wenn man bedenkt, dass jedes Grad erhöhte Raumtemperatur dazu führt, dass bis zu vier Prozent Energie gespart werden können, hat das doch deutliche Auswirkungen auf die Energiekosten. Basis für das Erhöhen der Temperatur ist das eingangs erwähnte Trennen von Warm- und Kaltluft. Dabei gilt generell: Je höher die Rücklufttemperatur, desto energieeffizienter arbeitet die An-



Quelle: Cofit

Die Luftführung sollte stets an die tatsächliche Serverbestückung angepasst sein. Um eine Vermischung von Kalt- und Warmluft zu verhindern, müssen Lücken in den Racks geschlossen werden.



lage. Auch die Außentemperatur hat Einfluss auf die Kühlleistung. Daher sollte der Betreiber des Rechenzentrums den Zeitpunkt für die Umschaltung von Sommer- auf Winterbetrieb bewusst wählen.

## Kontinuierliches Monitoring

Das beschriebene Regulieren der Kühlung in Rechenzentren läuft heutzutage automatisch. Exakte Messungen von Raumtemperatur, Luftdruck und Luftfeuchtigkeit machen es möglich. Im Schnitt sollte die Rücklufttemperatur im Raum rund 26 Grad betragen, dies wird direkt am Umluftkühlgerät gemessen. Der Luftdruck der Kühlluft wird sowohl im Doppelboden als auch in den Kaltgängen erfasst. Diese Werte geben Aufschluss darüber, mit welcher Geschwindigkeit die kalte Luft zu den Servern gelangt. Das Zusammenspiel von Temperatur und Druck ist maßgeblich für die Drehzahl und Ventilatorstellung der Umluftkühler. Die Luftfeuchtigkeit wird ebenfalls gemessen, ist aber in erster Linie relevant für das elektronische Equipment.

Die kontinuierlich erfassten Daten werden von einer Software ausgewertet. Dieses Monitoringsystem enthält die zulässigen Grenzwerte. Werden diese überschritten, werden automatisch Gegenmaßnahmen eingeleitet. Steigt zum Beispiel die Temperatur über den Grenzwert, wird automatisch die Kühlung verstärkt. Bei Störungen oder extremen Abweichungen gibt es automatische Meldungen an die Servicetechniker. Die Software visualisiert die erfassten Daten. So lassen sich der Verlauf des Energieeinsatzes und mögliche Spitzenverbräuche leichter nachvollziehen und entsprechend in Zukunft besser regeln.

## Bei der PUE nach RZ-Typ unterscheiden

Dieses kontinuierliche Monitoring des Energieverbrauchs ist Basis für ein effizientes Energiemanagement. An allen Messstellen werden die Werte erfasst und ausgewertet, um den Energiekoeffizienten PUE (Power Usage Effectiveness) zu bestimmen. Der Wert gibt das Verhältnis von Gesamtenergieverbrauch und dem Energieverbrauch der IT an.

Dieser Wert ist mittlerweile für Kunden ein entscheidendes Kriterium bei der Auswahl des Rechenzentrums. Dabei sollte allerdings nicht vergessen werden, dass Rechenzentren heutzutage verschiedene Aufgaben erfüllen. Der PUE eines Rechenzentrums, das nur mit einem Typ von Servern betrieben wird, ist dementsprechend anders zu bewerten als ein Rechenzentrum, das im Wesentlichen Colocation-Fläche zur Verfügung stellt. Vor allem die Kapazitätsauslastung des Rechenzentrums ist für die Berechnung des PUE entscheidend. Zudem spielt auch das Klima am Standort eine wichtige Rolle, denn der Betrieb eines Rechenzentrums im Süden Europas erfordert mehr Kühlung als im kalten Norden.

Um den Energieverbrauch auch für die Kunden transparent zu machen, werden die Energiekosten nicht wie früher pauschal nach Rack abgerechnet, sondern nach dem tatsächlichen Verbrauch. An den Abgängen zu dem jeweiligen RACK befinden sich Messstellen, die die entsprechenden Daten per WLAN oder LAN direkt übermitteln. Per Software kann der Kunde seinen Stromverbrauch sogar in Echtzeit einsehen. Zudem erhalten Kunden einen monatlichen Report über den Energieverbrauch und können nachvollziehen, wie sich dieser auf ihre Kosten auswirkt. Diese Transparenz sensibilisiert sie zunehmend für das Thema Energieeffizienz.

## Modernes Equipment und ausmisten helfen

Das ist wichtig, denn auch die Kunden selbst haben einen wesentlichen Anteil am Energieverbrauch des Rechenzentrums, da dieser wie

## IT-ENTSCHEIDER: ENERGIEEINSPARUNG IST EIN MUSS

Auch für die Kunden, also die IT-Entscheider auf Seiten der Unternehmen, nimmt das Thema Energiemanagement in Rechenzentren eine wichtige Rolle ein, wie die von Colt in Auftrag gegebene Studie „Four Forces of Data Centre Disruption“ aus dem Frühjahr 2014 belegt. Befragt wurden dabei 503 IT-Entscheider in Unternehmen aus Deutschland, Frankreich, Großbritannien und den Niederlanden. Die Untersuchung ergab, dass im Durchschnitt 64 Prozent der Befragten den Energieverbrauch als zunehmend wichtigen Einfluss auf die IT-Strategie ansehen.

In Deutschland sind 57 Prozent der Teilnehmer dieser Meinung. Zudem gaben 67 Prozent an, dass sie Energiemanagement als wichtigen oder sehr wichtigen Faktor einschätzen, um Sparziele zu erreichen. Hier liegen die Teilnehmer aus Deutschland auf dem europäischen Schnitt. Die Ergebnisse zeigen, dass aus Sicht der Entscheider Energiemanagement den zweitwichtigsten strategischen Einsparungsbereich für die IT nach der Netzwerkeffizienz darstellt.

beschrieben maßgeblich von der eingesetzten IT bestimmt wird. Ist diese modern und energieeffizient, lassen sich Energiekosten deutlich senken. Server, die technisch up-to-date sind, sparen im Vergleich zu alten Modellen 25 bis 30 Prozent Energie. Das ist zwar anfangs mit Investitionen verbunden, diese amortisieren sich aber relativ schnell, sodass neues Equipment auf Dauer Energiekosten spart.

Wird moderne Hardware eingesetzt, ist des Weiteren zu betrachten, wie genau diese genutzt wird. Es sollten generell nur die Geräte in Betrieb sein, die tatsächlich benötigt werden. Denn der Standby-Modus vieler Server verbraucht bis zu 70 Prozent der Energie, die er bei voller Auslastung benötigen würde. Läuft auf einem Server nur eine Applikation, wird seine restliche Kapazität verschwendet. Konsolidierung und Virtualisierung können also die Geräte optimal auslasten und so den Energieverbrauch senken. Virtualisierung ermöglicht einen Konsolidierungsgrad von bis zu 1:10. Das entspricht rund 80 Prozent weniger Energieverbrauch der Server.

Auch das Datenmanagement der Kunden hat Auswirkungen auf den Energieverbrauch: Werden veraltete und unnötige Daten konsequent gelöscht, kann die Infrastruktur optimal genutzt werden, da nur tatsächlich benötigter Speicherplatz besetzt wird. Diese Konsolidierung ermöglicht es im nächsten Schritt, dass nicht genutzte Server einfach abgeschaltet werden können. Das wiederum beeinflusst Raumkühlung und Luftstrom. Wenn mehrere Server abgeschaltet werden, können einzelne Umluftkühlgeräte möglicherweise ebenfalls abgeschaltet oder zumindest heruntergeregelt werden.

Für effektives Energiemanagement ist kontinuierliches Monitoring also unabdingbar, denn was nicht gemessen wird, kann man auch nicht optimieren. Erfahrungen zeigen, dass durch richtige Planung, Bau, Ausstattung und Betrieb eines Rechenzentrums, Einsparungen der Energiekosten von rund 20 Prozent und mehr zu erzielen sind. Dabei sollten die Kapazitäten optimal genutzt werden. Das bedeutet, einerseits Leerstände zu vermeiden und andererseits unnötige Geräte abzuschalten. Dabei sind Rechenzentrumsbetreiber genauso gefragt wie ihre Kunden.

*Frank Leinhoss,  
Operations Manager Germany, Data Center Services, Colt*

# Grüne Aussichten

## Rechenzentren intelligent verkabeln und so unter anderem die Energiekosten senken

Mit dem Code of Conduct für Rechenzentren wollen Teilnehmer und Befürworter der europäischen Initiative für das Thema Green-IT sensibilisieren und Möglichkeiten des Energiesparens aufzeigen. Energieeffizienz im Rechenzentrum beginnt bereits mit der Verkabelung: Intelligent gewählt, spart sie Ressourcen und schont die Umwelt.

Ohne Strom läuft nichts in Serverräumen und Rechenzentren: 1,8 Prozent der gesamten hierzulande verbrauchten Energie beanspruchen Serveranlagen und IT-Bereiche. Eine nur auf den ersten Blick niedrige Zahl. Denn tatsächlich steckt die jährliche Stromproduktion von umgerechnet vier mittelgroßen Kohlekraftwerken dahinter, um den jährlichen Stromhunger deutscher Datenzentren zu decken. Ein enormer Kostenfaktor, der durch den teuer gewordenen Strom inzwischen den Großteil der Kosten im IT-Bereich ausmacht und zugleich die Umwelt belastet. Energieeinsparungen rechnen sich daher doppelt.

### EU-Initiative liefert Anwendungsempfehlungen

Zugleich steigen Datenvolumina und Rechenleistung seit Jahren kontinuierlich an. Um mit dieser Entwicklung Schritt zu halten und wettbewerbsfähig zu bleiben, sind Unternehmen zunehmend auf leistungsfähige Server angewiesen. Der daraus resultierende Energiebedarf ist enorm: Auf etwa 104 Terawattstunden soll der jährliche Energieverbrauch in Westeuropa bis zum Jahr 2020 Schätzungen zufolge ansteigen. Ein beachtlicher Teil davon entfällt auf den Betrieb von Rechenzentren, Enterprise-Servern, ITK-Ausstattung, Kühlsysteme und Antriebsaggregate.

Bereits 2007 hat die Europäische Kommission den sogenannten europäischen Code of Conduct ins Leben gerufen – eine Reaktion auf

den zunehmenden Energieverbrauch in Rechenzentren. Gegründet vom Joint Research Center und Institute for Energy der Europäischen Kommission setzt sich der Code of Conduct für den Aufbau eines standardisierten Systems zur grünen Rechenzentrumsoptimierung in Unternehmen ein.

Ziel ist es, Betreiber und Eigentümer von Rechenzentren für das Thema Green-IT zu sensibilisieren und Möglichkeiten des Energiesparens aufzuzeigen. Zudem liefert die Europäische Kommission mit Best-Practice-Beispielen Anwendungsempfehlungen, wie sich Infrastrukturen konkret verbessern lassen. Schließlich ist kostensparender und effizienter Einsatz der Energie eines der wichtigsten Themen des 21. Jahrhunderts – und die größte Herausforderung für Unternehmen: Sie müssen betriebliche Prozesse optimieren, ohne negative Auswirkungen auf unternehmenskritische RZ-Funktionen. Potenzial gibt es genug: Untersuchungen belegen, dass sich 35 Prozent der Energie in Datenzentren einsparen ließe, wenn Unternehmen ihr Energiemanagement gezielt angingen und die IT entsprechend umrüsteten.

Um den Grundgedanken des Code of Conduct weiter voranzutreiben, adressiert die europäische Initiative zwei Zielgruppen: Unternehmen und Institutionen, die ihre Rechenzentren nach streng energieökonomischen Gesichtspunkten betreiben, zertifiziert sie als sogenannte Participants. Dienstleister und Hersteller energieeffizienter Komponenten können sich als Endorsers oder auch Befürworter listen lassen.

Intelligente IT-Hardware spielt beim Schaffen energieeffizienter Rechenzentren eine entscheidende Rolle. Bereits mit der Wahl des richtigen Verkabelungssystems sparen Unternehmen nachweislich Kosten: Rechenzentren lassen sich insgesamt kleiner auslegen, wenn das Kabelvolumen gering und die Packungsdichte in den Netzwerkschränken hoch ist. Zugleich sinkt der erforderliche Klimatisierungsaufwand.

### Strukturierte Verkabelung senkt den Energieverbrauch

Dabei spielt vor dem Hintergrund steigender Übertragungsraten bereits die Wahl der Kabelart eine wichtige Rolle: Glasfaser bietet hier auf unterschiedlichen Ebenen Vorteile und ist die erste Wahl, wenn Übertragungsraten von 40, 100 oder mehr GbE erreicht werden sollen. Denn LWL-Kabel verbrauchen mit zunehmender Übertragungsgeschwindigkeit weniger Strom als Kupferkabel. So sind bei 10 GbE über Kupfer bereits zehn Watt nötig, um das ankommende Nutzsignal nicht im Rauschen untergehen zu lassen. Demgegenüber fallen bei Übertragungen von 10 GbE über LWL lediglich zwei Watt an. LWL-Kabel sind zugleich frei von Störeffekten wie Übersprechen oder dem Skin-Effekt, bei dem die äußeren Bereiche der Kupferkabel überbelastet werden.



Quelle: trans data elektronik GmbH

Das modular aufgebaute Verkabelungssystem besteht aus den drei Kernkomponenten Modul, Trunkkabel und Modulträger.

## VERKABELUNG

Da LWL-Kabel auch einen deutlich dünneren Durchmesser als kupferbasierte Kabel besitzen, haben sie auch ein geringeres Volumen. Dadurch ergeben sich gleich zwei zentrale Vorteile: Die Belüftungswege in den Netzwerkschränken sind weniger blockiert, wodurch sich Energieeinsparungen erzielen lassen. Zugleich reduzieren sich die Brandlasten in Rechenzentren, je kleiner die Kabeldurchmesser sind.

### Vorgefertigte Verkabelungssysteme im Kommen

Rechenzentren sollten bei der Konzeption stärker als bisher auf eine strukturierte Verkabelung setzen. Deshalb geht der Trend von klassischen Einzelverkabelungen zu vorgefertigten, modularen Verkabelungssystemen. Solche flexiblen Systeme bieten nicht nur Investitionsschutz, sondern helfen auch, Ressourcen einzusparen und die Umwelt zu schonen: Sind Systemkomponenten vorkonfektioniert und getestet, lassen sie sich dank Plug and Play innerhalb kürzester Zeit und dadurch sehr viel effizienter installieren.

Zugleich können Netzwerktechniker jederzeit Änderungen vornehmen und dieselben Komponenten wiederverwenden. In Verbindung mit modularen Plug and Play-Verkabelungsplattformen mit hoher Packungsdichte sind Patchkabel-Management-Systeme unumgänglich. Geeignete Patchkabel-Management-Systeme schaffen eine geordnete und flexible Patchkabelführung im Netzwerkverteiler. Hochwertige Systeme integrieren eine Zugentlastung, schützen die Kabel vor mechanischer Beanspruchung und verhindern überflüssige Dämpfungserhöhungen durch Faserstress. Dies ist vor allem aufgrund niedriger Dämpfungsbudgets bei hohen Übertragungsraten vorteilhaft. Umso wichtiger ist dies, da sich viele Unternehmen mit beengten Platzverhältnissen konfrontiert sehen und die vorhandenen Räume optimal für die gestiegenen Rechnerleistungen nutzen müssen.

### Erste Erfolge sichtbar

Energie sparen und die Umwelt schonen: Hersteller und Zulieferer von Komponenten sowie Betreiber von Rechenzentren überdenken aktuell ihre bisherigen Produkte und IT-Infrastrukturen und gehen sensibler auf Green-IT ein. Eine Entwicklung, die bereits Wirkung zeigt: Laut Branchenverband Bitkom ließ sich 2012 bereits 1,4 TWh Energie einsparen. Einerseits hat die IT ihre Energieeffizienz verbessert und den Stromverbrauch von Servern durch Virtualisierung senken können. Andererseits benötigen qualitativ hochwertige Systeme weniger Energie

Quelle: trans data elektronik GmbH



Das gezeigte Patchkabel-Management-System trägt zu einer effizienten Lüftung des Serverschranks und damit zu mehr Green-IT im RZ bei.

Quelle: trans data elektronik GmbH



Im RZ lassen sich 35 Prozent der Energie einsparen, wenn auf Energiesparen optimierte Produkte – zum Beispiel Kabelsysteme – zum Einsatz kommen.

für die Klimatisierung. Die eingesparte Energie spart nicht nur Kosten, sondern trägt auch dazu bei, künftig wettbewerbsfähig zu bleiben. Den Anfang dazu machen Unternehmen schon mit der Wahl des richtigen Verkabelungssystems für ihr Rechenzentrum.

*André Engel,  
Geschäftsführer, trans data elektronik GmbH*



Fernstudiengang Seminare Konferenzen Online-Kurse

isits AG International School of IT Security

**Bleiben Sie fit im Job – nutzen Sie unsere Weiterbildungsangebote!**

Melden Sie sich jetzt zu unseren aktuellen Terminen an:

- |                |  |
|----------------|--|
| 02.-06.03.2015 | Zertifikat: BCM Manager – Business Continuity Management             |
| 11.-13.03.2015 | Einführung eines zertifizierungsfähigen ISMS nach ISO/IEC 27001:2013 |
| 13.-18.04.2015 | TÜV-Zertifikat: T.I.S.P. TeleTrust Information Security Professional |
| 15.04.2015     | Semesterstart Fernstudiengang M.Sc. „Applied IT Security“            |
| 15.04.2015     | Start Onlinekurse (Forensik, Virenschutz, Programmanalyse uvm.)      |
| 20.-24.04.2015 | ISMS Auditor/Lead Auditor nach ISO/IEC 27001:2013                    |

Ihre Ansprechpartnerin:

Yasemin Gülsuyu  
Tel.: 0234 32 22675  
E-Mail: guelsuyu@is-its.org

[www.is-its.org](http://www.is-its.org)



# Zeit für die nächste Generation

## Next Generation Firewalls versprechen mehr Sicherheit als die Vorgänger

Dass Netzwerke trotz Firewall ständig von Kriminellen geknackt werden, ist eine Binsenweisheit. Wobei es hier zu unterscheiden gilt, ob eine althergebrachte Firewall das RZ schützt, oder eine Next Generation Firewall. Letztere versprechen aufgrund eines moderneren Konzepts mehr Schutz vor aktuellen Angriffstaktiken.

Die Kombination aus Web-basierten Anwendungen, Virtualisierung, Cloud Computing, Mobile Computing und technischem Fortschritt sorgt dafür, dass sich die Netzwerkbandbreite und der Durchsatz immer weiter erhöhen. Fast ein Viertel der Unternehmen sind der Meinung, dass dieser Anstieg des Netzwerkverkehrs die Netzwerksicherheit immer schwieriger macht (Enterprise Strategy Group, 2014).

Zusätzlich zur grundlegenden Zunahme des Verkehrsaufkommens verändern sich die Kommunikationsmuster. Neben klassischer Client-Server-Kommunikation müssen Unternehmen heute auch Verkehrsspitzen zwischen Nutzern, mobilen Geräten und Cloud-basierten Anwendungen bewältigen.

Die Sicherheitsarchitekturen mussten in den letzten zehn Jahren – als Antwort auf eine Vielzahl von neuen Bedrohungen und Angriffstaktiken – immer wieder ergänzt werden. So ist ein Sammelsurium entstanden aus Stateful-Inspection- oder Port-basierten Firewalls, IDS/IPS, Netzwerk-Proxys, Gateways, Sandboxes oder Endpoint Security Suites. Im Laufe der Zeit hat sich erwiesen, dass dieses schlecht integrierte Arsenal immer schwieriger zu verwalten ist. Zudem ist es nicht mehr effektiv genug, um gegen die Vielzahl von Exploits, Viren, Spyware, Malware und Advanced Persistent Threats (APTs) gewappnet zu sein. Denn Angreifer haben längst diverse Mittel und Wege gefunden, um die bekannten Schutzmechanismen verlässlich auszuhebeln.

### Auf die Granularität kommt es an

Der Schutz des Ein- und Ausgangs des Rechenzentrums und das effektive Absichern auf Applikationsebene sind entscheidend, um mögliche Angriffsvektoren von Haus aus zu minimieren. Die Hauptrolle, wenn es um zeitgemäße IT-Sicherheit geht, spielen heute daher Next Generation Firewalls (NGFW), eingebunden in eine moderne Enterprise-Security-Plattform.

Next Generation Firewalls können alle relevanten Filteraktivitäten parallel verarbeiten, ohne die Netzwerkperformance nennenswert zu beeinträchtigen. Sie gehen aber auch ein anderes Problem effektiv an: Cloud Computing, Virtualisierung und mobiles Arbeiten führen dazu, dass sich einzelne User nicht mehr klar definierten IP-Adressen zuordnen lassen. Ebenso wenig sind beispielsweise Web-2.0-Applikationen mit fixen TCP-Ports verbunden, sie lassen sich mit herkömmlichen Schutzmechanismen daher nur bedingt kontrollieren. Es ist also mehr Granularität notwendig.

Während herkömmliche Firewalls sich meist auf die Kontrolle von IP-Adressen, Ports und Protokollen beschränken, unterstützen Next Generation Firewalls auch Filterregeln, die Anwendung, Inhalt und Benutzeridentität mit einbeziehen. Auch SSL-/TLS- und SSH-Verkehr lässt sich verzögerungsfrei und mit hoher Granularität analysieren. Die Anwendungserkennung ist dabei unabhängig von Portnummern: So

bald eine Anwendung identifiziert ist, sind non-konforme Daten wie Viren, Angriffssignaturen und verdächtiger Verkehr leichter erkennbar.

### Klassifizierung von Sicherheitsrichtlinien

Eine exakte Klassifizierung des Datenverkehrs bildet das Kernstück jeder NGFW. Das Ergebnis wird zur Grundlage der Sicherheitsrichtlinie. Dazu werden mehrere Klassifizierungsmechanismen auf den Verkehrsstrom angewendet, sobald das Gerät diesen sieht, um die Identität von Anwendungen im Netzwerk zu erkennen. Während die Anwendungen und ihre Subfunktionen durch aufeinanderfolgende Mechanismen identifiziert werden, stellt die Richtlinienprüfung fest, wie sie behandelt werden müssen: Blockieren, Zulassen oder sicheres Aktivieren.

Das Erstellen und Verwalten von Sicherheitsrichtlinien erfolgt dabei basierend auf der Anwendung und der Identität des Benutzers, unabhängig von Gerät oder Standort. Das verspricht mehr Schutz, als sich nur auf Port und IP-Adresse zu stützen. Durch die Integration in interne Benutzer-Repositories lässt sich die Identität der Benutzer ermitteln, die über Microsoft Windows, Mac OS X, Linux, Android oder iOS auf die Anwendung zugreifen. Reisende oder entfernt arbeitende Benutzer werden nahtlos durch die gleichen, durchgängig geltenden Richtlinien geschützt, die auch im lokalen beziehungsweise im Unternehmensnetzwerk eingesetzt werden.

Dank der Kombination aus Transparenz und Kontrolle der Aktivität eines Benutzers in Bezug auf eine Anwendung ist das sichere Aktivieren von Oracle, BitTorrent, Google Mail oder einer beliebigen anderen Anwendung im Netzwerk möglich, egal von wo oder wie der Benutzer darauf zugreift. Das gilt sowohl für die Bürokommunikation als auch den Übergang zum Rechenzentrum.

### Suchen, erkennen und handeln

NGFWs können Applikationen im Netzwerk mit verschiedenen Mechanismen erkennen: Es werden Signaturen auf zulässigen Verkehr angewendet, um jede Anwendung basierend auf eindeutigen Anwendungseigenschaften und zugehörigen Transaktionsmerkmalen zu identifizieren. Stellt die Firewall fest, dass eine Verschlüsselung zum Einsatz kommt, so wird die Anwendung entschlüsselt. Anschließend werden auf den entschlüsselten Traffic erneut die Applikations-Signaturen angewendet. Im Anschluss werden Decoder für bekannte Protokolle verwendet, um mit Hilfe kontextbasierter Signaturen weitere Anwendungen zu ermitteln, die möglicherweise das Protokoll durchtunneln (beispielsweise Yahoo! Instant Messenger über HTTP). Die Identität von nicht über erweiterte Signatur- und Protokollanalysen zu fassende Applikationen lässt sich durch heuristische oder Verhaltensanalysen ermitteln.

## Zentrale Mechanismen

Zu den wichtigsten Funktionalitäten beim Suchen und Erkennen von Malware gehören Content-ID, IPS-Funktion, Virenschutz, Anti-Spyware und URL-Filterung. Content-ID bietet voll integrierten Schutz vor Exploits in Bezug auf Sicherheitslücken, Malware sowie durch Malware generierten Command-and-Control-Traffic. Die Gefahrenabwehr wird dabei über den gesamten Applikations- und Protokollkontext angewendet – für den gesamten Traffic und alle Ports. So kann sichergestellt werden, dass Bedrohungen trotz aller Umgehungsversuche erkannt und blockiert werden. Gefahrenabwehrtechniken müssen folgende Elemente umfassen:

- **IPS-Funktionen:** Sie blockieren Exploits in Bezug auf Sicherheitslücken, Pufferüberläufe, DoS-Angriffe und Port-Scans. Weitere Fähigkeiten, wie etwa die Abwehr ungültiger oder deformierter Pakete, IP-Defragmentierung und TCP-Reassembly schützen vor Umgehungs- und Verschleierungsmethoden.
- **Virenschutz für Netzwerke:** Bekannte Malware wird durch eine streambasierte Engine ermittelt, die die In-Line mit hohem Tempo blockiert. Dies erfolgt über eine Vielzahl von Protokollen, einschließlich HTTP, SMTP, IMAP, POP3, FTP und SMB.
- **Anti-Spyware:** Neben der Kontrolle von Viren und Malware werden auch Spyware und Malware-Kommunikation unterbunden, wie zum Beispiel Botnet-Kommunikation, Browser-Hijacks, Adware, Backdoor-Verhalten, Keylogger, Datendiebstahl, Netz-Würmer, Peer-to-Peer-Traffic. Anti-Spyware soll auch in der Lage ein, DNS-Anfragen passiv zu analysieren, um eindeutige Muster von Botnets zu identifizieren. Dadurch werden infizierte Benutzer erkannt und es wird verhindert, dass Daten aus Unternehmen herausgelangen.

Eine vollintegrierte URL-Filterungsdatenbank ermöglicht eine einfachere und wirksamere Durchsetzung der Richtlinien zum Browsen im Internet. Diese ergänzt die richtlinienbasierte Anwendungstransparenz und -kontrolle. Transparenz- und Richtlinienkontrollen zur URL-Filterung können mit Unternehmens-Verzeichnisdiensten wie Active Directory, LDAP und eDirectory mit bestimmten Benutzern verknüpft werden. Protokollanalysen und benutzerspezifische Reports sorgen für noch mehr Transparenz bei der URL-Filterung.

## Filtern von Daten und Dateien

Mit Hilfe der Datenfilterungsfunktionen lassen sich Richtlinien implementieren, welche die mit dem Transfer unautorisierter Daten und Dateien verbundenen Risiken reduzieren. Wichtig: Dateitypen müssen durch Nutzlastanalysen erkannt werden – nicht durch die Dateieindung.

Dadurch ist eine genaue Kontrolle über die Dateiübertragung innerhalb einzelner Anwendungen möglich. Hierbei werden der Einsatz der Applikation gestattet, aber unerwünschte eingehende und ausgehende



Quelle: Palo Alto Networks

Die NGFW PA-7050 schützt Rechenzentren mit einem Firewall-Durchsatz von bis zu 120 Gbps sowie vollem Bedrohungsschutz bei Geschwindigkeiten bis zu 100 Gbps.

Datentransfers verhindert. Zusätzlich kann der Transfer sensibler Datenmuster, wie Kreditkarten und Sozialversicherungsnummern, in Applikationsinhalten oder Anhängen erkannt und verhindert werden.

Moderne Angreifer verwenden zunehmend zielgerichtete und neue, unbekanntere Varianten von Malware, um herkömmliche Sicherheitslösungen zu umgehen. Durch Ausführen verdächtiger Dateien in einer virtuellen Umgebung und Beobachten des Verhaltens kann Malware schnell und präzise identifiziert werden, selbst wenn die entsprechende Malware noch nie zuvor gesichtet wurde.

Ist eine schädliche Datei erkannt, müssen automatisiert Schutzmaßnahmen generiert werden, die umgehend nach der Erkennung an alle NGFWs verteilt werden. Den IT-Mitarbeitern sind umfangreiche forensische Erkenntnisse zur Verfügung zu stellen, anhand derer exakt festgestellt werden kann, wer angegriffen wurde, über welche Applikation und welche URLs bei dem Angriff involviert waren.

## Virtualisierte Firewall für virtualisierte Umgebungen

Aus der Virtualisierung erwachsen ganz spezifische Herausforderungen. Hierzu zählt der Mangel an Transparenz, was den Ost-West-Verkehr von VM zu VM betrifft. Manuelle, prozessintensive Netzwerkkonfigurationen, um Sicherheitsfunktionen in der virtualisierten Umgebung zu implementieren, erweisen sich als sehr aufwendig. Es kann dadurch auch zu einem Leistungsabfall in virtuellen Umgebungen kommen. Ein weiteres Problem ist, dass herkömmliche Sicherheitsplattformen nicht mit der Geschwindigkeit der Veränderungen in virtuellen Umgebungen mithalten können oder erforderliche Features fehlen.

Unternehmen, die beispielsweise mit VMware ESXi oder Citrix NetScaler arbeiten, benötigen eine virtualisierte Firewall, die diese Plattformen explizit unterstützt.

Aktuelle virtualisierte Firewalls können Ost-West-Traffic untersuchen. Damit auch bei hohem Verkehrsaufkommen der Zugriff auf die Administrationsfunktionen gewährleistet bleibt, sollten die Daten- und Steuerungsebene voneinander getrennt sein. Das Verarbeiten aller Sicherheitsfunktionen in einem einzigen Durchlauf sorgt zusätzlich für geringe Latenz. Funktionen wie beispielsweise dynamische Adressengruppen und VM-Monitoring ermöglichen das nahtlose Einbinden von Sicherheitsrichtlinien, egal ob beim Hinzufügen, Verschieben und Ändern virtueller Maschinen oder beim Erzeugen virtueller Workloads.

Zum Beispiel sind in einem 3-Schichten-Anwendungsmodell alle Webserver-VMs mit dem Web Logical Switch verbunden, die Anwendungslogik-VMs mit dem App Logical Switch und die Datenbank-VMs mit dem DB Logical Switch. Gast-VMs können in jedem ESXi-Host instanziiert werden, solange die VXLAN-Erreichbarkeit auf diese Hosts erweitert wird. In Bezug auf die Verkehrssteuerung würden dann der Verkehr zwischen Web-, App- und DB-Schicht von der Gast-VM umgeleitet und von der virtuellen Firewall verarbeitet werden.

## Mit neuen Anforderungen Schritt halten

Nicht nur das Beispiel der Virtualisierung zeigt, dass die Sicherheitsanforderungen immer komplexer werden. Gleiches gilt für die Sicherheit auch bei Cloud und Mobile Computing. Während sich viele Unternehmen für neue Technologien öffnen, gilt es jetzt auch, sicherheitstechnisch den Anschluss nicht zu verpassen. Next Generation Firewalls werden hier die zentrale Rolle übernehmen.

*Thorsten Henning,  
Senior Systems Engineering Manager  
Central & Eastern Europe, Palo Alto Networks*

# Freie Kühlung ganz sicher

## Blick hinter die Kulissen: Durchdachte Brandschutzkonzepte für grüne Lösungen

Der Kühlung kommt beim Betrieb des Rechenzentrums nicht nur im Hinblick auf die Lebensdauer der Hardware eine entscheidende Rolle zu. Auch zum Senken der Energiekosten sind clevere Kühlungskonzepte entscheidend. Wie aber lässt sich beispielsweise bei einem System zur indirekten Freien Kühlung ein effektiver Brandschutz im Rechenzentrum bewerkstelligen? Ein Praxisbeispiel zeigt, wie es geht.

Die größten Stromfresser in der IT-Branche und damit hauptverantwortlich für CO<sub>2</sub>-Emissionen sind Rechenzentren mit deren Servern. Leistungsstark und hochverfügbar müssen sie sein – wie zum Beispiel nach der Verfügbarkeitsklasse 4 des BSI, die lediglich eine Ausfallzeit von rund fünf Minuten pro Jahr erlaubt.

Doch die leistungsstarken Rechner und die hohe Verfügbarkeit haben auch ihren Preis: Um die geringen Ausfallzeiten sicherstellen zu können, ist eine redundante Ausführung der Versorgungstechnik unabdingbar. Das kostet jedoch nicht nur in der Anschaffung, sondern verbraucht selbst im Standby-Betrieb Energie. Kosteneffizienz und ein schonender Umgang mit Ressourcen sind hier nur schwer möglich.

Die Klimatisierung hingegen bietet einen hervorragenden Ansatzpunkt, ein Rechenzentrum deutlich effizienter und grüner zu betreiben. Gerade der Einsatz der sogenannten indirekten Freien Kühlung amortisiert sich betriebswirtschaftlich meist in kurzer Zeit. Anstatt die warme Luft innerhalb des Rechenzentrums aufwendig herunterzukühlen, bedient man sich der in der Regel deutlich kühleren Außenluft. In Nord- und Mitteleuropa funktioniert dies – mit Ausnahme weniger Tage im Hochsommer – das gesamte Jahr hindurch.

### Herausforderung für den Brandschutz

Im Rechenzentrum werden in der Regel Gaslöschanlagen mit dem natürlichen Löschgas Stickstoff verbaut. Stickstoff bietet zahlreiche Vorteile wie beispielsweise ein schonendes, rückstandsfreies Löschen ohne Beeinträchtigungen für die IT-Hardware. Schäden wie sie beispielsweise beim Einsatz wassergeführter Systeme auftreten, bleiben beim Löschen mit dem Inertgas aus. Im Fall einer Branddetektion wird

durch die Löschgaszufuhr der Sauerstoff in den zu schützenden Bereichen verdrängt und der Brand erstickt.

Im Hinblick auf den Brandschutz sind Methoden zur Freien Kühlung wie das KyotoCooling (siehe Kasten) eine besondere Herausforderung. Denn beim Einsatz einer Löschanlage ist im Brandfall entscheidend, dass eine löschfähige Gaskonzentration aufgebaut und auch über einen ausreichenden Zeitraum hinweg aufrechterhalten werden kann. Um eine erneute Entzündung zu vermeiden, fordert das unabhängige Prüfinstitut VdS Schadenverhütung GmbH in EDV-Bereichen eine Haltezeit von zehn Minuten. Die dafür notwendige Raumdichtigkeit ist jedoch beim Einsatz einer Freien Kühlung durch die Abströmverluste am Wärmetauscher nicht gegeben.

Im neuen RZ der network AG in Nürnberg wurde KyotoCooling erstmals in einem deutschen Rechenzentrum eingesetzt. Nach einer Risikoanalyse und der Definition des entsprechenden Schutzziels wurde für die noris network AG ein individuelles Brandschutzkonzept entwickelt: Der Hersteller Wagner hatte zum Zeitpunkt der Kontaktaufnahme durch die noris network AG in einer zweijährigen Testreihe bereits Erfahrungen zum Einsatz von KyotoCooling im Zusammenspiel mit einer Brandschutzlösung gesammelt. Daher war bekannt, dass die konventionellen Konzepte der Gaslöschtechnik beziehungsweise Brandvermeidung in diesem Fall jeweils allein nicht geeignet waren.

### Keine Standard-Lösung

Die Abströmverluste beim Betrieb eines Rotationswärmetauschers machen den Einsatz einer konstanten Sauerstoffreduzierung unwirtschaftlich. Mit dem konventionellen Einsatz einer Gaslöschanlage hin-



Quelle: noris network AG

Die noris network AG betreibt in Nürnberg mit NBG6 eines der modernsten Rechenzentren Europas.



Quelle: noris network AG

Die Brandfrüherkennung erfolgt über ein Ansaugrauchmeldesystem. Beim Brand wird die Schnellabsenkung auf 16 Vol.-% eingeleitet.

Quelle: noris network AG



**Im NBG6 sorgt eine Brandvermeidungsanlage für die notwendige Sauerstoffreduzierung.**

gegen hätte man aufgrund der sehr starken Druckunterschiede beim Betrieb der Ventilatoren des Kühlsystems keine löschtfähige O<sub>2</sub>-Konzentration über eine ausreichende Zeitspanne aufrechterhalten können. Große Sorge bereitete den Planern auch ein möglicher Eintrag kontaminierter Außenluft über die Freie Kühlung.

Ein wichtiger Eckpfeiler für den Schutz der beiden Bereiche mit insgesamt 16.000 Kubikmetern war eine frühestmögliche Branderkennung. Dazu werden Ansaugrauchmeldesysteme in Zwei-Melder-Abhängigkeit eingesetzt: Sie detektieren einen Brand täuschungsalarmsicher bereits in der Frühphase – ein Alarm wird jedoch erst ausgelöst, wenn beide Melder einen Brand detektieren. Zudem wurden die Ansaugrauchmelder zur Überwachung der Luftqualität im Außenluftkreislauf des KyotoCooling-Systems installiert.

## Brandrisiken und Folgen

Die Abwärme der IT-Racks, die hohe Energiedichte der elektrischen Anlagen und damit verbundene technische Defekte stellen, ebenso wie von außen mit der Frischluft zugeführte Partikel durch das freie Kühlsystem, in der Regel das größte Brandrisiko dar. Von umso größerer Bedeutung ist daher eine frühestmögliche und täuschungsalarmsichere Branddetektion.

Im Rechenzentrum der noris network AG werden Ansaugrauchmelder sowohl im Schutzbereich selbst, als auch in den Bereichen eingesetzt, in denen der Luftaustausch aufgrund der indirekten freien Kühlungsmethode stattfindet. Auch gegebenenfalls kontaminierte Außenluft muss überwacht werden. Die verwendeten Melder detektieren im Brandfall so früh wie möglich und sollen für eine deutliche Schadensbegrenzung sorgen.

Im Fall einer Detektion wird nach Möglichkeit schnellstens die Energiezufuhr unterbrochen, um dem Feuer die Stützenergie zu entziehen sowie die Löschung und das anschließende Halten eingeleitet. Der Betrieb des Rechenzentrums bleibt dabei erhalten, Daten sind weiterhin verfügbar und Schäden werden minimiert beziehungsweise vermieden. Größer als die Angst vor dem Brandschaden selbst war für den Betreiber die Vorstellung einer Unterbrechung der IT-Prozesse durch ein Stromlosschalten der gesamten IT-Infrastruktur, da den Kunden eine durchgängige Verfügbarkeit von Rechenkapazität und gespeicherten Daten vertraglich zugesichert wird. Ein Stromlosschalten kam daher nicht in Frage.

## HINTERGRUND: KYOTOCOOLING

Ein Beispiel für eine indirekte Freie Kühlung ist das Prinzip Kyoto-Cooling. Bei dieser Lösung, die speziell für Rechenzentren entwickelt wurde, kommen Rotationswärmetauscher aus Aluminium mit einem Durchmesser von sechs Metern zum Einsatz. Die kalte Außenluft wird über die Aluminiumlamellen der Räder geführt und diese somit gekühlt. Im Inneren des Rechenzentrums wird die warme Innenluft angesaugt und ebenfalls über die Lamellen geleitet. Der Effekt: Das Aluminium gibt die Kälte an die Rechenzentrumsluft ab, nimmt die Wärme aus dem Inneren auf und gibt sie in der Folge durch die Rotation wieder an die Außenluft ab. Dabei nutzt KyotoCooling aus, dass zu 95 Prozent des Jahres die Außenlufttemperatur niedriger ist als die Raumluft im IT-Zentrum. Als Kosten fallen nur die Antriebsenergie des Wärmetauscherrads und der Ventilatoren an. Als Ersatzsystem und für die wenigen Stunden im Jahr, in denen die Außenluft zu warm zur Kühlung ist, lassen sich Luft-Wasser-Wärmetauscher zuschalten.

## Kontrollierte Abläufe im Alarmfall

Bei Auslösen des empfindlichen Voralarms werden bereits erste Brandfallsteuerungen eingeleitet, zu denen ein Stoppen des Kyoto-Rades, Aktivieren der Abdichtungen, Umschalten auf Ersatzkühlung und Schließen der Brandschutzstore gehören.

Beim ersten Hauptalarm löst die erste Stufe der Löschanlage aus und leitet Stickstoff aus 70 Druckgasflaschen in vier Minuten in den Bereich ein. Bei der Schnellabsenkung von 20,9 Vol.-% auf 16,0 Vol.-% O<sub>2</sub> zeigt sich bereits ein deutlich reduziertes Brandverhalten, sodass sich die üblichen Stoffe in einem IT-Raum nicht mehr entzünden. Die angeschlossene OxyReduct-Anlage hält den Sauerstoffgehalt dann kontinuierlich auf diesem Niveau.

Erkennt ein zweites Ansaugrauchmeldesystem, dass der Brand nicht vollständig erstickt wurde, werden ein zweiter Hauptalarm und die zweite Stufe der Löschanlage ausgelöst. Das O<sub>2</sub>-Niveau wird dann innerhalb von weiteren vier Minuten auf eine Konzentration von 13,5 Vol.-% abgesenkt. Das System kann dieses Niveau für theoretisch unbegrenzte Zeit halten, was Rückzündungen verhindert, ohne dass der betroffene Bereich stromlos geschaltet werden muss.

## Raumdichtigkeit sichergestellt

Nur in einem dichten Raum kann die erforderliche Gaskonzentration lange genug aufrecht gehalten werden, damit im Brandfall das Löschen effektiv und sicher erfolgt. Selbst wenn zum Zeitpunkt der Inbetriebnahme eine ausreichende Dichtigkeit nachgewiesen wurde, so ergeben sich beispielsweise durch Anpassungen der Hardware oder durch Bewegungen des Gebäudes im Laufe der Zeit unbemerkte Leckagen, die den Brandschutz dramatisch gefährden können.

Mit dem im Rechenzentrum installierten System kann regelmäßig die Dichtigkeit des Bereiches und so die Wirksamkeit der Löschanlage getestet werden. Dazu wird zu bestimmten Zeiten auf die Ersatzkühlung umgeschaltet und der Sauerstoffgehalt leicht gegenüber dem Normalniveau reduziert. Aus der erforderlichen Zeit zum Aufbau der vorab definierten Sauerstoffkonzentration können Rückschlüsse auf die aktuelle Dichtigkeit des Bereiches gezogen werden – ein nicht zu unterschätzendes Sicherheitsplus.

*Katrin Strübe,  
Kommunikation, Wagner Group GmbH*

# Sicher nach draußen

## Wie der Verband der Ersatzkassen sensible Datentransfers verschlüsselt

Sozialversicherungsdaten enthalten höchst private Informationen – etwa Name, Geburtsdatum, Familienstand –, die nicht in unberechtigte Hände geraten dürfen. Gerade bei der elektronischen Übertragung muss jederzeit die Vertraulichkeit und Integrität zum Schutz der Daten gewährleistet sein. Der vdek löst den Transfer zum Backup-RZ mittels Verschlüsselungstechnik.

Darauf legt auch der Verband der Ersatzkassen e.V. (vdek) – Interessenverband und Dienstleistungsunternehmen aller Ersatzkassen in Deutschland – höchsten Wert. „Wir sehen uns in der Pflicht, stets die sichersten Verschlüsselungstechniken einzusetzen, um auch für die Zukunft einen zweifelsfreien Schutz der uns anvertrauten Daten garantieren zu können“, erklärt Peter Neuhausen, Abteilungsleiter IT des Verbandes. Der vdek trägt die Verantwortung für Dienstleistungen, die eine reibungsfreie, bundesweite Versorgung von 26 Millionen Versicherten der Ersatzkassen unterstützen.

Zum Sicherstellen der Verfügbarkeit der immer größer werdenden Datenmengen hat der vdek unter anderem ein Remote-Backup in einem externen Datenzentrum eingerichtet. Dieses ist mehrere Kilometer von der Zentrale entfernt und über bestehende öffentliche Glasfaserverbindungen kostengünstig angebunden. Dies erfordert aber spezielle Schutzmaßnahmen: „Sensible Daten dürfen nicht unverschlüsselt über öffentlichen Grund und Boden übertragen werden“, unterstreicht der Experte des vdek. „Die Gefahr eines unberechtigten Zugriffs wäre einfach zu hoch.“

### Anforderungen: schnell, sicher, effizient

Neben dem größtmöglichen Schutz ihrer Daten ist für die Mitgliedskassen des vdek auch ein hoher Datendurchsatz und ein rasches Agieren auf sich ändernde Anforderungen wichtig. „Eine schnelle, effiziente und sichere Verschlüsselungslösung ist elementar für uns, um Massendaten in kürzester Zeit verarbeiten und bereitstellen zu können“, sagt Neuhausen.

Für die Entscheidung zwischen den Bewerbern der bundesweiten Ausschreibung waren darüber hinaus eine BSI-Zulassung, hohe Verfügbarkeit und Service entscheidend. Um ein späteres aufwendiges und teures Nachrüsten zu vermeiden, sollte die Lösung bereits jetzt eine synchrone Spiegelung der Daten ermöglichen. Entscheidende Faktoren hierfür waren eine hohe Bandbreite bei gleichzeitig geringer Latenz.

Diese Anforderungen konnte nur die SITLine ETH-Produktfamilie der Rohde & Schwarz SIT GmbH erfüllen, die die Ausschreibung zusammen mit ihrem Integrationspartner, der Pan Dacom Direkt GmbH, gewann und damit zukünftig Sozialversicherungsdaten zwischen den

Rechenzentren schützt. Die Pan Dacom Direkt GmbH übernimmt vom Einbau der Hardware-Lösungen über den Anschluss an die bereits bestehenden Glasfaserleitungen bis zur Betreuung vor Ort ebenfalls die Funktion des direkten Ansprechpartners für die systemorientierte Lösung.

### Mitlesen verhindern

Zum Absichern der Sozialversicherungsdaten kommt konkret der Ethernet-Verschlüssler SITLine ETH40G zum Einsatz, der über das zentrale Sicherheitsmanagement SITScope eingerichtet und administriert wird. Das SITLine ETH40G wurde speziell für den verschlüsselten Austausch großer Datenmengen in Echtzeit entwickelt. Durch die bislang einmalige Durchsatzrate von 40 Gigabit pro Sekunde bei einer Latenz von drei Mikrosekunden für die Verschlüsselung, erfüllt die Hardware die Anforderungen im Rechenzentrumseinsatz.

Zum technischen Hintergrund: Die Verschlüsselung erfolgt bereits auf der Sicherungsschicht (Layer2), was einen zusätzlichen Vorteil bringt: Der Security-Overhead gegenüber IP-Verschlüsselung (Layer3) ist um bis zu 40 Prozent reduziert und spart so Bandbreite. Damit ist die Geräteklasse für den vdek gut geeignet, da die Leistung den Anforderungen genügen soll.

### Gut zu integrieren

Die Sicherung des Datenverkehrs mit Verschlüsseln der SITLine ETH-Gerätefamilie ist in der Praxis mit wenig Aufwand verbunden: Außer den Sicherheitsparametern sind keine weiteren netzwerkspezifischen Konfigurationen erforderlich. Sicherheitsmanagement und Netzwerkmanagement sind voneinander getrennt, sodass die Geräte gut in bestehende IT-Systeme integriert werden können. Dadurch entfällt eine aufwendige Anpassung der Netzwerkinfrastruktur.

Die Verschlüssler sind aber nicht nur bei Punkt-zu-Punkt-Verbindungen oder Sternstrukturen einsetzbar: Durch die Gruppenverschlüsselung kann auch die Übertragung in vollvermaschten „switched networks“ abgesichert werden. Verbände und Unternehmen können so Speicherlösungen ungefährdet auf mehrere geografisch entfernte Standorte verteilen. Dabei spielt es sicherheitstechnisch keine Rolle, ob sie zur Vernetzung gemietete oder eigene Leitungen einsetzen. Ein weiterer Pluspunkt: Die Netzwerkverschlüssler von Rohde & Schwarz SIT sind vom BSI für die Verarbeitung von Daten der Vertraulichkeitsgrade VS-NfD und NATO Restricted zugelassen. Gesetzliche Vorschriften zum Schutz personenbezogener Daten werden damit eingehalten.

*Svenja Borgschulte,  
für Rohde & Schwarz SIT GmbH*



Quelle: Rohde & Schwarz

Die vom vdek verwendeten Verschlüssler arbeiten auf Layer 2 mit 40Gbit/s Datendurchsatz.



# Ausblick 2015: Mittelständler wollen energieeffiziente RZ

## In Sachen Effizienz liegt in deutschen RZ vieles im Argen – es wird Zeit für eine Modernisierung

Seit Jahren ist in der RZ-Branche die Rede vom Energiesparen. Doch augenscheinlich ist der Mittelstand in Deutschland derzeit gar nicht in der Lage, die viel beschriebenen Maßnahmen umzusetzen: Die verwendete Infrastruktur ist zu alt. Allem Anschein nach kommt jedoch Bewegung in die Sache: Modernisierungsprojekte stehen an. Zum Glück.

Wenn es um Energieeffizienz geht, sind Rechenzentren bei weitem nicht auf dem aktuellen Stand der Technik. Dies hat eine Umfrage von IDC im Auftrag von Rittal in fünf europäischen Ländern unter mittelständischen Unternehmen ergeben: Zwei Drittel der befragten IT-Organisationen betreiben ihre Rechenzentren zu kalt. Mit durchschnittlich 15,5 Grad Celsius verbrauchen sie somit unnötig Energie für die Kühlung. Ist die Temperatur zu niedrig, führt dies zu einem ungünstigen PUE-Wert (Power Usage Effectiveness), der bei der Befragung im Durchschnitt bei über 2,0 lag.

Der PUE-Wert setzt die im Rechenzentrum verbrauchte Energie ins Verhältnis zur Energieaufnahme der Rechner: Je näher der PUE-Wert der Zahl 1 kommt, desto effizienter arbeitet das Rechenzentrum. Industrieweit gilt ein PUE-Wert von 1,4 als ausgezeichnet, während große IT-Dienstleister mit optimierten Anlagen auch Werte von 1,2 oder weniger erreichen.

### Ein Muss: Optimierung des Stromverbrauchs

39 Prozent der Befragten legen daher im kommenden Jahr eine hohe Priorität auf die Optimierung des Stromverbrauchs im Rechenzentrum. Das Reduzieren des Energiebedarfs dürfte jedoch schwierig werden, da die Rechenzentren laut Umfrage im Schnitt sieben Jahre alt sind. Die vorhandenen Konzepte für Klimatisierung und Energieversorgung sind daher überholt und erschweren eine energietechnische Sanierung.

Abhilfe kann ein Modernisieren durch modulare Rechenzentren schaffen: 25 Prozent der IT-Experten erwarten niedrigere Betriebskosten durch den künftigen Einsatz modularer Rechenzentren. Modulare Rechenzentren bestehen aus vorkonfigurierten Infrastrukturkomponenten für Energie- und Notstromversorgung, Energieverteilung und Klimatisierung. Durch die aufeinander abgestimmten Komponenten wird beispielsweise der Energieverbrauch für die Klimageräte optimiert, sodass sich IT-Infrastrukturen mit insgesamt verbesserter Energieeffizienz betreiben lassen.

Zum Hintergrund: Rechenzentren verbrauchen in Deutschland rund 1,8 Prozent des gesamten Stroms, also rund 10 Terawattstunden jährlich. Der Branchenverband BITKOM schätzt, dass davon rund ein Fünftel in älteren Rechenzentren für Kühlung und Stromversorgung benötigt wird. Würde die Effizienz dieser Anlagen nur um 10

Prozent erhöht, so spart dies rund 200 Gigawattstunden im Jahr, umgerechnet 115.000 Tonnen Kohlendioxid.

### Auch auf dem Wunschzettel: IT-Sicherheit

Mittelständische Unternehmen aus Deutschland gelten auf vielen Spezialgebieten als Weltmarktführer. Daher hat der Mittelstand auch bei der IT-Sicherheit vergleichbare Anforderungen wie große Unternehmen. Beispielsweise müssen Rechenzentren auch in mittelständischen Betrieben hochverfügbar arbeiten, da immer mehr Prozesse entlang der Wertschöpfungskette auf unterbrechungsfreie IT-Lösungen angewiesen sind. Dies stellt besonders hohe Anforderungen an den Rechenzentrumsbetrieb. Diese müssen einerseits einen hohen physischen Schutz unterstützen und andererseits die Hochverfügbarkeit der IT durch redundante Stromversorgung und Klimatechnik sicherstellen.

Eine im April 2014 veröffentlichte Studie der Beratungsgesellschaft PwC zeigt, dass besonders der deutsche Mittelstand auf Hackerangriffe, Datendiebstahl und Cyber-Kriminalität nur unzureichend vorbereitet ist. So rückt der Mittelstand als Innovationstreiber verstärkt in den

Quelle: Rittal



Modulare Rechenzentren wie RiMatrix S sind eine kosteneffiziente und schnelle Alternative zum individuellen Rechenzentrumsbau.

Fokus von Industriespionage: 31 Prozent der mittelständischen Unternehmen bis 499 Mitarbeiter wurden bereits Opfer von Hackerangriffen. Dies meldete der BITKOM im Oktober 2014. Damit ist der Mittelstand von Datendiebstahl stärker betroffen als Großunternehmen. Die durch Wirtschaftsspionage entstandenen Schäden schätzte die Bundesregierung im Jahr 2013 auf bis zu 50 Milliarden Euro jährlich.

## Nachholbedarf bei der Ausfallsicherheit

Welche Sicherheitsaspekte mittelständischen Unternehmen in Europa besonders wichtig sind, zeigt eine im Auftrag von Rittal in fünf europäischen Ländern durchgeführte Studie der Analysten von IDC. Die Untersuchung gibt Einblicke in den Stand der IT mittelständischer Unternehmen und zeigt, dass insbesondere bei der Ausfallsicherheit im Rechenzentrum erheblicher Nachholbedarf besteht.

So halten im Schnitt 24 Prozent der befragten IT-Experten ihr Redundanzkonzept für nicht ausreichend und planen, die Ausfallsicherheit im Rechenzentrum zu verbessern. Deutlich kritischer erscheint die Situation bei mittelständischen Unternehmen der Fertigungsindustrie. Hier sehen 46 Prozent aller Befragten eine Verbesserung der Verfügbarkeit der IT-Systeme als wichtig oder sehr wichtig an.

Beim Ausbau der Rechenzentren über Public-Cloud-Angebote wird sich der Mittelstand auch im Jahr 2015 zurückhalten. Die IDC-Umfrage zeigt, dass 60 Prozent der Befragten vor den Risiken einer Public Cloud zurückschrecken. Das eigene Rechenzentrum gilt für viele Unternehmen (93 Prozent) auch weiterhin als wesentlicher Schlüssel

## HINTERGRUND ZUM MODULAREN RECHENZENTRUM

Das Konzept für ein modulares Rechenzentrum kommt der Anforderung von Unternehmen entgegen nach mehr Agilität und Skalierbarkeit. So lassen sich kürzere Produktlebenszyklen, die Inbetriebnahme neuer Systeme oder das Implementieren neuer Vorschriften rasch umsetzen. Auch wenn diese Konzepte noch relativ neu auf dem Markt sind, nimmt der Bekanntheitsgrad weiter zu. Laut IDC verzeichnete das Marktsegment in den letzten Jahren ein starkes Wachstum im zweistelligen Bereich. In EMEA wurden Investitionen im Wert von dreistelligen Millionenbeträgen getätigt. Die vorkonfigurierten Module oder Container können laut IDC im Vergleich zu einem herkömmlichen Rechenzentrumsneubau kostengünstiger sein und lassen sich innerhalb weniger Wochen einrichten.

für den wirtschaftlichen Erfolg. Der Ausbau der IT-Kapazitäten wird daher verstärkt über Private-Cloud-Lösungen im eigenen Rechenzentrum erfolgen. Modulare Rechenzentren können helfen, da sich hiermit sehr schnell Cloud-Kapazitäten mit hoher IT-Sicherheit im eigenen Haus aufbauen lassen.

*Bernd Hanstein,  
Hauptabteilungsleiter Produktmanagement IT, Rittal*

### Impressum Themenbeilage Rechenzentren und Infrastruktur

#### Redaktion just 4 business GmbH

Telefon: 080 61/348 111 00, Fax: 080 61/348 111 09,  
E-Mail: tj@just4business.de

#### Verantwortliche Redakteure:

Thomas Jannot (v. i. S. d. P.), Uli Ries (089/68 09 22 26)

#### Autoren dieser Ausgabe:

Ash Ashutos, Svenja Borgschulte, André Engel, Roland Freist, Bernd Hanstein, Thorsten Henning, Frank Leinhoss, Uli Ries, Hans Schramm, Katrin Strübe

#### DTP-Produktion:

Enrico Eisert, Kathleen Tiede, Matthias Timm, Hinstorff Verlag, Rostock

#### Korrektur:

Silke Peters, Hinstorff Verlag, Rostock

#### Technische Beratung:

Uli Ries

#### Titelbild:

kubais, shutterstock

#### Verlag

Heise Zeitschriften Verlag GmbH & Co. KG,  
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;  
Telefon: 05 11/53 52-0, Telefax: 05 11/53 52-129

#### Geschäftsführer:

Ansgar Heise, Dr. Alfons Schröder

#### Mitglied der Geschäftsleitung:

Beate Gerold

#### Verlagsleiter:

Dr. Alfons Schröder

#### Anzeigenleitung (verantwortlich für den Anzeigenteil):

Michael Hanke (-167), E-Mail: michael.hanke@heise.de

#### Assistenz:

Stefanie Bels -205, E-Mail: stefanie.bels@heise.de

#### Anzeigendisposition und Betreuung Sonderprojekte:

Katharina Kraft -534, E-Mail: katharina.kraft@heise.de

#### Anzeigenverkauf:

PLZ-Gebiete 0-1 und Ausland: Tarik El-Badaoui -395, E-Mail: tarik.el-badaoui@heise.de,  
PLZ-Gebiete 2-3, 8-9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de

#### Anzeigen-Inlandsvertretung:

PLZ-Gebiete 4-7: Karl-Heinz Kremer GmbH, Sonnenstraße 2,  
D-66957 Hilst, Telefon: 06335/ 9217-0, Fax: 06335/9217-22,  
E-Mail: karlheinz.kremer@heise.de

#### Leiter Vertrieb und Marketing:

Bianca Nagel

#### Druck:

Dierichs Druck + Media GmbH & Co. KG, Kassel

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages verbreitet werden; das schließt ausdrücklich auch die Veröffentlichung auf Websites ein.

Printed in Germany

© Copyright by Heise Zeitschriften Verlag GmbH & Co. KG

## Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich. Redaktionelle Gründe können Änderungen erforderlich machen.

Bytec	<a href="http://www.bytec.de">www.bytec.de</a>	S. 28	Isits	<a href="http://www.is-its.org">www.is-its.org</a>	S. 19
dtm Group	<a href="http://www.dtm-group.de">www.dtm-group.de</a>	S. 13	InternetX	<a href="http://www.internetx.de">www.internetx.de</a>	S. 15
FNT	<a href="http://www.fnt.de">www.fnt.de</a>	S. 5	NUTANIX	<a href="http://www.nutanix.com">www.nutanix.com</a>	S. 11
			Rausch	<a href="http://www.rnt.de">www.rnt.de</a>	S. 2
			Transtec	<a href="http://www.transtec.de">www.transtec.de</a>	S. 7

# WIR TRINKEN DEN KAFFEE #000000.

iX. WIR VERSTEHEN UNS.



**Jetzt Mini-Abo testen:**  
3 Hefte + Kinogutschein nur 13,50 Euro  
[www.ix.de/test](http://www.ix.de/test)



Sie mögen Ihren Kaffee wie Ihr IT-Magazin: stark, gehaltvoll und schwarz auf weiß! Die iX liefert Ihnen die Informationen, die Sie brauchen: fundiert, praxisnah und unabhängig. Testen Sie 3 Ausgaben iX im Mini-Abo + Kinogutschein für 13,50 Euro und erfahren Sie, wie es ist, der Entwicklung einen Schritt voraus zu sein. **Bestellen Sie online oder unter Telefon +49 (0)40 3007 3525.**

# Data Protection 4 You

## Fujitsu Primergy SX Storage Systems

SECURITY

ECONOMICAL

BEST  
VALUE

RELIABILITY

HIGH  
PERFORMANCE



The Informatics Network

BYTEC GmbH Tel. 07541/585-0 [www.bytec.eu](http://www.bytec.eu)

bytec