Eine Themenbeilage der
Heise Medien GmbH & Co. KG

III
2015

RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Was künftige Rechenzentren von heutigen unterscheidet

www.rechenzentren-infrastruktur.de

powered by:

Server & Storagesysteme

Wir schaffen Platz für das wirklich Wichtige!

Storage Unlimited

BigFoot® Storagesystem XXLarge

BigFoot® Storagesystem Flash

BigFoot® Storagesystem XXCold

BigFoot® Storagesystem Object

BigFoot® Storagesystem XXFast

BigFoot Storagesysteme

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 Konfigurationsmöglichkeiten nahezu allen Anforderungen gerecht wird.

Aus dieser Idee hat die Rausch Netzwerktechnik GmbH die BigFoot-Produktfamilie entwickelt. Die fünf 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.

Wir konfigurieren auch Ihren BigFoot passend zu Ihren Anforderungen.

Überzeugend in Leistung und Preis – das und mehr schafft die BigFoot-Storage-Familie.

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

>> Mehr erfahren!

RAUSCH NETZWERKTECHNIK
www.rnt.de

Sympathisch und gut beraten. Bestens betreut.

Was künftige Rechenzentren von heutigen unterscheidet

Als ich vor etwas mehr als 35 Jahren meinen ersten Aufsatz darüber schrieb, wie ich mir das Jahr 2000 vorstelle, fühlte ich mich wie Ray Bradbury. Mit dem kleinen aber feinen Unterschied, dass ich weniger als keinen blassen Schimmer hatte. Das war das peinliche Ergebnis, als ich mein Geschreibsel bei einem Klassentreffen vor wenigen Jahren nachzulesen bekam.

Gründlich daneben lag ich auch, als ich kurz nach der Inauguration von Michail Gorbatschow zur Zukunft der Sowjetunion im Allgemeinen und der DDR im Besonderen gefragt wurde. Dass alles so bleiben und noch schlimmer würde, war meine feste Überzeugung. Seitdem bin ich sehr skeptisch, was langfristige Prognosen betrifft. Insbesondere dann, wenn es um digitale Einflüsse auf analoge Werte geht. Dennoch müssen und wollen wir es in dieser Ausgabe wagen.

Den Anfang macht Dr. Peter Koch von Emerson Network Power. Er beschreibt das Rechenzentrum im Jahr 2025. Sein Blick in die Glaskugel stützt sich auf Erfahrung. Branchenexperten gehen davon aus, dass sich Rechenzentren im Verlauf des kommenden Jahrzehnts im Vergleich zu ihrer bisher bekannten Form stark verändern werden. Insbesondere erwarten sie – wen wundert's – eine Zunahme bei der Nutzung von Solarenergie und Cloud-Diensten.

Die Münchner Journalistin Ariane Rüdiger hat auf der Datacloud Europe in Monaco mindestens einen deutlichen Trend ausgemacht. Ab Seite 8 berichtet sie über neue Wege zum Rechenzentrum. Verschiedenste Ansätze konkurrieren, um bestehende und neue Data Center umweltfreundlicher und nachhaltiger aus- oder neu zu bauen. Mit der Berechnung der Power Usage Effectiveness (PUE) allein sei es jedenfalls nicht mehr getan. Neben Standortfragen spielen vor allen Dingen das Sicherheitskonzept und der effektive IT-Betrieb eine wichtige Rolle. Prämierte Beispiele aus Europa belegen, dass digitale Nachhaltigkeit durchaus machbar ist.

Das bestätigt auch Thorsten Henning von Palo Alto Networks. Er schwört auf Sicherheit: „Hybride Rechenzentren ganzheitlich schützen", heißt sein Beitrag ab Seite 12, in dem es darum geht, wie sich gemischte physische und virtuelle Umgebungen gegen (künftige) Angriffe sichern lassen. Denn Rechenzentren entwickeln sich immer mehr zu einem Mix aus physischen und virtuellen Rechen-, Netzwerk- und Speicherkomponenten. Angreifern ist das egal. Deshalb stellt sich die Frage, ob zum Schutz der Daten neue Konzepte nötig sind.

Der Münchner Journalist Roland Freist hinterfragt ab Seite 15 einen Hype, der vielleicht doch keiner ist: Hyper-converged. Hyperkonvergente Infrastrukturen versprechen vereinfachte Administration und geringere Kosten. Doch das Konzept hat seine Grenzen. Ronald Timmermans von Schleifenbauer macht im Anschluss auf ein Problem aufmerksam, das gerne unterschätzt wird. Fehlerströme sind eine Gefahrenquelle, die im europäischen Ausland oftmals keine Rolle spielt, in Deutschland aber durchaus relevant ist. Warum Differenzströme gefährlich sein können, steht ab Seite 17 geschrieben.

Bleiben wir bei fließendem Strom. Er bringt unweigerlich elektromagnetische Felder mit sich, die HF-Strahlung abgeben. Elektrische Geräte können von den starken Feldern negativ beeinflusst werden. Aber auch schwache Felder sind eine Gefahr, weil Informationen bei unerwünschten Mithörern landen können. Schutz versprechen IT-Sicherheitsräume, schreibt Hartmut Lohrey von Rittal ab Seite 20.

Auf Seite 23 geht es um Diversifikation, die sich bei der Auslagerung von Rechenzentren auszahlen soll. Wie sich ein möglichst schneller Zugriff auf ausgelagerte Daten herstellen lässt, beschreibt Matthias Hain von Colt. Den Abschluss macht Tony Thompson von Silver Peak. Ab Seite 24 geht es darum, ob Multi-Protocol Label Switching (MPLS) zu teuer, wenig flexibel und nur unzureichend für Techniken wie Cloud Computing ausgelegt ist. Eine Alternative könnte Software-Defined WAN auf Grundlage von kostengünstigen Breitband-Internetverbindungen sein, da beide Technologien kombinierbar sind.

Die Frage ist, was tatsächlich Zukunft hat. Wenn kein Schwarzer Schwan Rechenzentren und Infrastrukturen völlig überflüssig macht, dürfte ihre künftige Entwicklung einigermaßen absehbar sein, weshalb ich den Ausführungen der Autoren dieser Ausgabe sehr wohl mehr Glauben schenke als meinen eigenen von damals. ;-)

Thomas Jannot

Das Rechenzentrum im Jahr 2025

Einen Blick in die RZ-Glaskugel werfen Fachleute und zeichnen so das Bild vom Rechenzentrum der Zukunft

Branchenexperten gehen davon aus, dass sich Rechenzentren im Verlauf des kommenden Jahrzehnts im Vergleich zu ihrer bisher bekannten Form stark verändern werden. Insbesondere erwartet man eine Zunahme bei der Nutzung von Solarenergie und Cloud-Diensten.

Mehr als 800 Rechenzentrumsspezialisten aus aller Welt beteiligten sich an der Online-Umfrage „Rechenzentrum 2025: Sondierung der Möglichkeiten“. Viele weitere Experten äußerten ihre Gedanken zum Thema in Interviews, E-Mails und Videos. Folgende Trends lassen sich aus der „Data Center 2025“-Umfrage ableiten: Der Großteil der Branche sieht der zukünftigen Entwicklung des Rechenzentrums optimistisch entgegen und geht von kontinuierlichen Innovationen im IT-Bereich und darüber hinaus aus. Das Managen hochkomplexer und dynamischer Rechenzentrumsumgebungen bleibt eine echte Herausforderung. Dabei sind die obersten Ziele stets das Aufrechterhalten der Verfügbarkeit, das Steigern der Effizienz sowie das Senken von Kosten. So sind sich 64 Prozent der Branchenkenner sicher, dass das Rechenzentrum 2025 deutlich weniger beziehungsweise weniger Energie bei gleicher Leistung benötigen wird. Es verwundert daher nicht, dass das Augenmerk der Rechenzentrumsbetreiber früher viel mehr auf den Investitionskosten lag und jetzt auf den Ausgaben im laufenden Betrieb. Denn Strom wird immer teurer. Deswegen sollten Server auch regelmäßig ausgetauscht werden, weil neue Modelle bei gleicher Leistung immer weniger Strom verbrauchen.

Tiefgreifende Veränderungen bei der RZ-Stromversorgung

Rechenzentren werden gemäß den befragten Experten künftig über einen Energiemix mit Strom versorgt. Die Solarenergie wird dabei künftig den größten Teil einnehmen, gefolgt von einem jeweils etwa gleich großen Anteil an Kern-, Erdgas- und Windenergie. Zum heutigen Zeitpunkt wird beispielsweise in den USA nur 1 Prozent der Energie durch Solarenergie gewonnen. Die Experten erwarten hier eine Steigerung um rund 20 Prozent in den nächsten zehn Jahren. Außerdem gehen 65 Prozent der Befragten weltweit davon aus, dass der Strom für Hyperscale-Anlagen in Zukunft mit eigenen Komponenten erzeugt werden wird. Gleichzeitig erwarten 58 Prozent, dass bis 2025 die Größe der Stromanlagen lediglich die Hälfte oder weniger des gesamten Rechenzentrums ausmachen wird.

Quelle: Emerson Network Power

Laut Studie wird die Leistungsdichte pro Rack bis zum Jahr 2025 erheblich ansteigen.

Von der Kühlung zum Temperaturmanagement

Zwei Drittel der Rechenvorgänge in Rechenzentren im Jahr 2025 werden nach Expertenmeinungen über Cloud-Dienste abgewickelt. Das liegt insbesondere an dem stets steigenden Bedürfnis nach mehr Flexibilität, was vor allem bei der Verwaltung der Kapazitäten innerhalb von Rechenzentren eine Herausforderung ist. Laut dem globalen Cloud-Index von Cisco entfielen 2013 rund 54 Prozent der Arbeitslast von Rechenzentren auf Cloud-Dienste. Bis 2018 soll dieser Anteil auf 76 Prozent ansteigen.

Was früher Kühlung war, hat sich in den letzten fünf Jahren dramatisch weiterentwickelt und wird immer mehr durch ein umfassendes Temperaturmanagement ersetzt. Es geht darum, möglichst energieeffizient zu kühlen und Abwärme zu nutzen. Die Kühlmethoden beziehungsweise das Temperaturmanagement werden ausgereifter und passen sich anderen Trends wie mehr Leistungsdichte an. Insgesamt verträgt IT-Equipment heutzutage höhere Temperaturen im Vergleich zu früher und produziert auch weniger Wärme. Gekühlt wird je nach Rechenzentrumsgröße und Lage unterschiedlich, wobei Luftkühlung weiterhin dominieren wird und Kühlungen mit Kältemittel aufgrund der Umweltproblematik abnehmen werden.

Automation in den Rechenzentren: DCIM wird wichtiger als erwartet

Indirekte freie Kühlung, insbesondere in Verbindung mit adiabater Verdunstungskühlung, wird stark an Bedeutung gewinnen. Innovative Ansätze wie Immersionskühlung werden zwar relevanter, aber zumindest vorerst eine Nischenanwendung bleiben.

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

Der Grad der Automation in den Rechenzentren wird weiter ansteigen. Viele Geräte der Rechenzentrumsinfrastruktur werden bereits heute schon ohne menschliche Unterstützung betrieben. Auch die Ergebnisse der aktuellen Studie unterstreichen diese Entwicklung: 43 Prozent erwarten, dass Rechenzentren in naher Zukunft selbstständig Fehler beheben und Optimierungsschritte durchführen können. Weitere 29 Prozent der befragten Experten gehen von einer alle Systeme und Schichten umspannenden Transparenz aus. Insgesamt sind damit 72 Prozent der Experten der Ansicht, dass bis 2025 in einem gewissen Umfang DCIM-Lösungen eingesetzt werden. Das ist eine deutlich höhere Einschätzung als bisher angenommen.

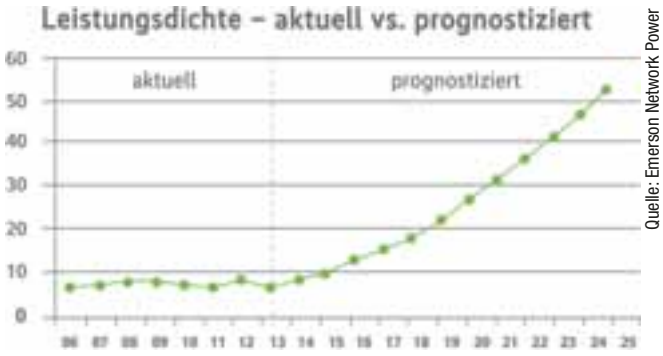
Die bereits erwähnte höhere Transparenz soll auch die Gesamtleistung von Rechenzentren effizienter machen. Effizienz in Rechenzentren ist bereits heute schon wichtiger denn je und dieser Aspekt wird sich in Zukunft noch verstärken. 72 Prozent der befragten Experten meinen, dass die Auslastung von IT-Ressourcen eines Rechenzentrums im Jahr 2025 mindestens bei 60 Prozent liegen wird. Schätzungen zufolge beträgt die durchschnittliche Auslastungsquote derzeit gerade einmal sechs bis zwölf Prozent, wobei ein idealer Wert zwischen 30 und 50 Prozent liegt.

Enorm erhöhte Dichte pro Rack realistisch?

Die befragten Experten prognostizieren im Rahmen der Studie unter anderem eine Steigerung der Leistungsdichte im Rechenzentrum bis 2025 auf durchschnittlich 52 Kilowatt pro Rack. Obwohl die durchschnittliche Leistungsdichte seit knapp zehn Jahren im Bereich von maximal sechs Kilowatt verharrt. Das zeigt die von Emerson Network Power gesponserte Data Center Users' Group, welche Enduser dabei unterstützt, die großen Herausforderungen beim Entwickeln und Verwalten von kritischen IT-Prozessen und Infrastrukturen zu bewältigen. Die erhöhte Leistungsdichte soll außerdem einen tief greifenden Wandel in der physischen Umgebung von Rechenzentren bewirken.

Allerdings ist fraglich, ob sich eine derartige Steigerung tatsächlich realisieren lässt. Branchenkenner und Rechenzentrumsverantwortliche sind hier geteilter Meinung: Denn ein Steigern der Leistungsdichte im Rack von sechs auf 52 Kilowatt pro Rack würde eine jährliche Erhöhung um mehr als 20 Prozent innerhalb der nächsten zehn Jahre voraussetzen. Zum Vergleich: 2001 lag die Dichte pro Rack bei einem Kilowatt, 2014 erreichte man hier gerade einmal eine Steigerung auf sechs Kilowatt pro Rack.

Interessant sind auch die Ergebnisse der Umfrage in Bezug auf die Innovationstreiber in Rechenzentren des Jahres 2025. Branchenexperten sehen die potenziellen Motoren für Neuerungen im nächsten Jahrzehnt bei unternehmenseigenen Rechenzentren, Hyperscale-Rechenzentren sowie bei Softwareanbietern. Weiterhin sind in diesem Zusammenhang auch IT-Geräte- und RZ-Infrastrukturhersteller wichtige Innovationsmotoren. Allerdings wird neue Technik in Rechenzentren nur schleppend umgesetzt. Die Erfahrung zeigt, dass in nur ungefähr 20 Prozent State-of-the-Art-Technik eingesetzt wird. Viele Rechenzentrumsbetreiber planen auch heute noch mit veralteter Technik – zum einen, weil es zu wenig ganzheitliches Wissen dazu gibt, zum anderen, weil niemand ein Risiko eingehen will. Außerdem fehlt es hier auch an konkreten Normen und Vorgaben.



Quelle: Emerson Network Power

Angesichts der bisherigen Entwicklung der Leistungsdichte scheint es unwahrscheinlich, dass diese bis 2025 so stark zunimmt, wie es die Studie nahelegt.

Quelle: Emerson Network Power

Der Prozentsatz der IT-Operationen, die in die Cloud ausgelagert werden, soll bis zum Jahr 2025 erheblich ansteigen.

Auch weiterhin: Für jeden Zweck das jeweils passende Rechenzentrum

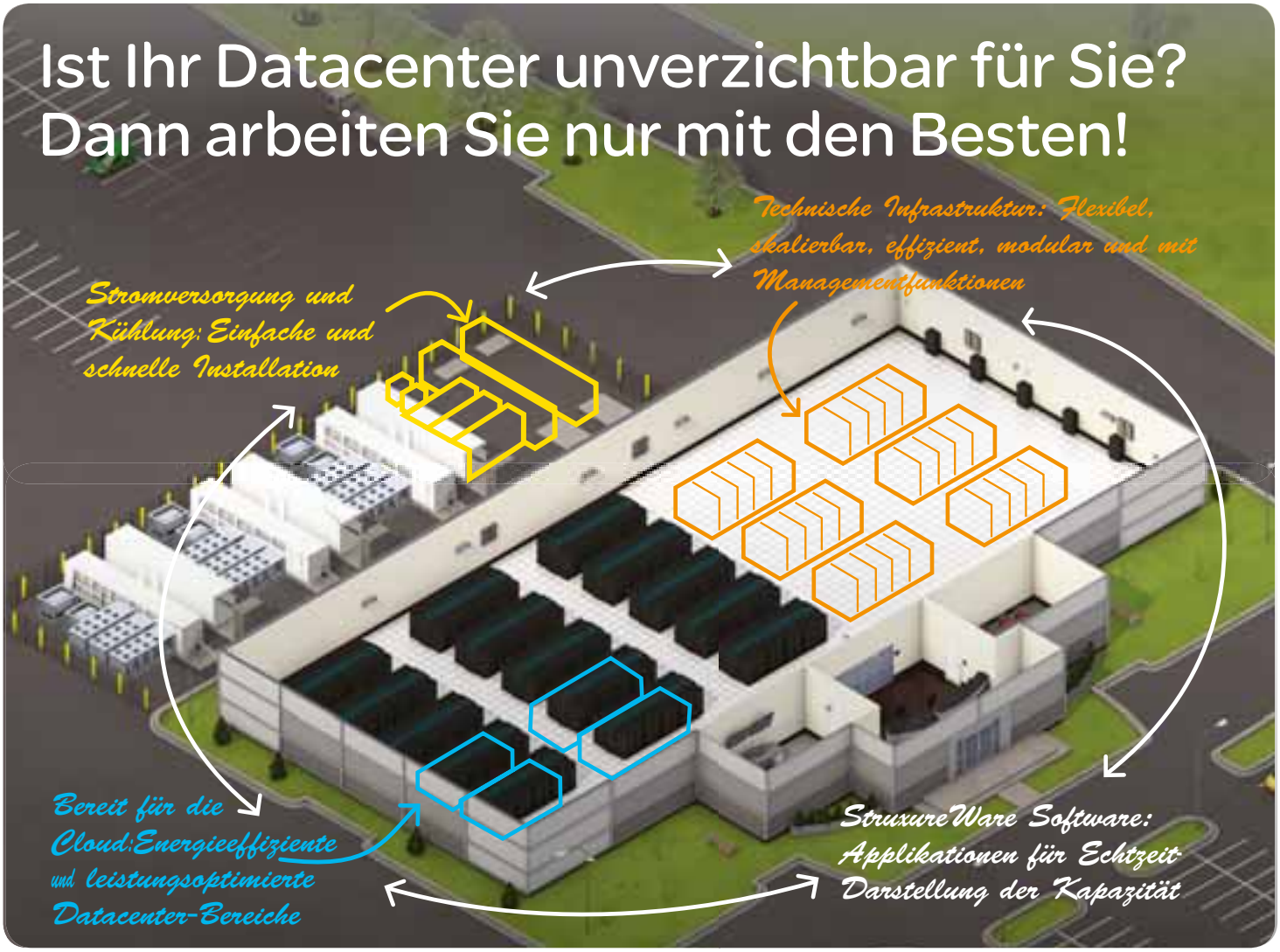
Sicher ist nach Analyse der Studie nur eines: Es wird auch im Jahr 2025 nicht das eine typische Rechenzentrum geben. Dies lässt sich gut mit dem Transportwesen vergleichen: Auf der Straße sind Sportwagen, Familienautos, Busse und Lastwagen unterwegs. Sie werden von unterschiedlichen Motoren angetrieben, sind mit unterschiedlichen Sitzen ausgestattet und weisen unterschiedliche Eigenschaften in den Bereichen Energieverbrauch und Zuverlässigkeit auf. So werden auch in Zukunft je nach Verwendungszweck und Betriebsmodell klassische Rechenzentren (beispielsweise von mittelgroßen Unternehmen), neben Collocation-Standorten (hier werden Platz und Infrastruktur an Kunden vergeben), Superrechenzentren (von großen Betreibern) und Supercomputing-Standorten (Hochleistungsrechenzentren mit wenig Platzbedarf) existieren.

Außerdem verlangen steigende Anforderungen von Anwendern an hohe Bandbreiten und kurze Latenzzeiten verstärkt kleinere, dezentrale Standorte beziehungsweise Minirechenzentren. Diese Entwicklung setzt sich nicht zuletzt auch durch andere Trends wie höhere Sicherheitsanforderungen, Industrie 4.0 (IT integriert in die Produktion) und dem Internet der Dinge (IoT) immer mehr durch. Oft sind große Rechenzentren auch einfach zu komplex. Allerdings sorgt hier ein anderer Trend für Abhilfe: Die IT wandert stärker in die Endgeräte.

Außerdem gewinnen modulare Rechenzentren an Bedeutung. Sie haben den Vorteil, dass die einzelnen Module flexibel skalierbar, sehr schnell implementierbar, einfach up-to-date zu halten und gut ausgelastet sind. Es bleibt also spannend hinsichtlich der künftigen Entwicklungen im Rechenzentrumsumfeld.

Dr. Peter Koch,
Sr. VP Engineering & Product Management, Racks & Integrated Solutions, Emerson Network Power in EMEA

Ist Ihr Datacenter unverzichtbar für Sie? Dann arbeiten Sie nur mit den Besten!



Schneider Electric bietet die Komplettlösung für optimale Energieeffizienz und Ausfallsicherheit.

Unsere modulare DCPI ist nur der Anfang.

Die technische Datacenter-Infrastruktur (DCPI) von Schneider Electric™ können Sie einfach an Ihre individuellen Anforderungen anpassen und gleichzeitig Ihr gesamtes Datacenter exakt dimensionieren. Von den hocheffizienten InRow™ Kühlsystemen über die innovativen EcoBreeze™ Economiser-Module bis zu den skalierbaren Dreiphasen-USV-Systemen – unsere DCPI eignet sich für die unterschiedlichsten Anforderungen an Ausfallsicherheit und Kapazität. Doch unsere herausragende, modulare DCPI ist nur der Anfang.

Kapazität für heute und die Zukunft planen.

Wenn Sie sich für Schneider Electric entscheiden, können Sie mit Ihrem Datacenter neue Maßstäbe hinsichtlich Effizienz und Rentabilität setzen. StruxureWare for Data Centers, unsere Software für Datacenter-Infrastrukturmanagement, zeigt Ihnen in Echtzeit, welche Bereiche und wie viel Kapazität aktuell verfügbar sind. Darüber hinaus steigert die Lösung die Ausfallsicherheit, optimiert die Performance und verbessert die Effizienz im Datacenter.

Umfassende Serviceleistungen von einem echten Lösungsanbieter

Bei Schneider Electric erhalten Sie Serviceleistungen für den kompletten Datacenter-Lebenszyklus aus einer Hand – von der Planung über die Inbetriebnahme bis zum Betrieb, der Überwachung, Analyse und Optimierung. Da wir sämtliche Komponenten für die technische Infrastruktur Ihres Datacenters liefern, wissen Sie immer, an wen Sie sich wenden können, wenn es mal ein Problem gibt. Dann sind wir schnell vor Ort, da wir global mit zahlreichen Servicecentern präsent sind. Schneider Electric bietet Ihnen komplette Lösungen und die Sicherheit, die Sie in den heutigen dynamischen IT-Umgebungen benötigen.

Business-wise, Future-driven.™

Sicherheit mit der StruxureWare Software und Life Cycle Services für Ihr Datacenter

Die StruxureWare Data Center Operation Software und unsere Life Cycle Services vereinfachen den Betrieb und machen Ihr Datacenter effizienter als je zuvor. Warum?

- Sie können schneller und fundierter über neue Projekte entscheiden durch Echtzeit-Darstellung der verfügbaren Kapazitäten.
- Flexible Servicepläne für jedes Budget unterstützen Sie in allen Phasen des Datacenter Life Cycle.

APC™ by Schneider Electric

APC by Schneider Electric gehört zu den Pionieren der modularen Datacenter-Infrastruktur und innovativen Kühltechnologien.

Planung optimieren und Betriebskosten senken mit DCIM Best Practices!

Laden Sie unser White Paper herunter und GEWINNEN Sie mit etwas Glück ein Power Pack!
Besuchen Sie www.SEreply.com Schlüsselcode: 57860p

Schneider Electric™

Neue Wege zum nachhaltigen Rechenzentrum

Verschiedenste Ansätze existieren, um bestehende und neue Rechenzentren umweltfreundlicher und nachhaltiger zu machen

Mit der Berechnung der PUE (Power Usage Effectiveness) allein lassen sich ökologische Nachhaltigkeit von Rechenzentren und Kostenoptimierung nicht erreichen. Neben Standortfragen spielen vor allen Dingen das Sicherheitskonzept und der effektive IT-Betrieb eine wichtige Rolle. Beispiele aus Europa belegen, dass Nachhaltigkeit machbar ist.

Die durchschnittliche PUE US-amerikanischer Unternehmens-Rechenzentren liegt auch heute noch nur bei 2,73, ergab eine aktuelle Umfrage von IDC unter 400 US-Unternehmen. Das ist nicht berauschend. Deutlich anders dürfte es in Europa auch nicht aussehen, doch ist der Trend nach unten eindeutig: Neu gebaute Infrastrukturen und auch RZs, die einer durchgreifenden Modernisierung unterzogen werden, landen in der Regel irgendwo zwischen 1 und 2, am weitesten unten große Provider- und Kollokation-RZs. Für die Datacloud Europe, der 2015 zum zehnten Mal veranstalteten Rechenzentrumsmesse, sind grüne Rechenzentren traditionell eines der wichtigen Themenfelder. Im Vorfeld der Veranstaltung werden regelmäßig die Awards des European Code of Conduct for Datacentres, einer von der EU ausgehenden Nachhaltigkeitsinitiative für RZs, vergeben. Die Preisträger zeigen, was heute möglich ist: Beispielsweise wurde Kimcell (Großbritannien) für ein unterirdisch in bereits bestehenden Gebäuden angelegtes RZ prämiert, weil dies den Bauaufwand minimiert und das RZ gleichzeitig von äußeren Klimaeinflüssen abschirmt. Überschüssige Wärme heizt ein Bürogebäude, es wird ein Freikühlsystem genutzt. Leere Stellen in Racks werden konsequent durch Blenden geschlossen.

Quelle: GSI

Das im Bau befindliche Rechenzentrum des GSI Helmholtzzentrum für Schwerionenforschung bringt 800 Racks auf sechs Etagen in einem Gebäude von nur 21 Meter Höhe unter und wird keine USVs besitzen.

Das Licht bleibt aus – und die Temperatur bei konstant 24 Grad

Der zweite Preisträger des EU-Code of Conduct war in diesem Jahr das Rechenzentrum Sevenoaks, ebenfalls in Großbritannien angesiedelt. Dort ist der Rechnerraum in Bereiche mit niedriger (1000 Watt pro Quadratmeter) und hoher Stromdichte (10 000 Watt pro Quadratmeter) unterteilt, was das leistungsangemessene Auslegen von Stromversorgung und Kühlung erleichtert. Warm- und Kaltluft werden durch warme und kalte Gänge im Rechnerbereich getrennt. Die ständige Betriebstemperatur liegt bei 24 Grad Celsius. Um Strom zu sparen, ist das Licht standardmäßig abgeschaltet. Die Kühleinheiten arbeiten abwechselnd, sodass die Auslastung und damit Abnutzung gleich ist. Die Kühlpumpen arbeiten mit variabler Drehzahl. Bei Außentemperaturen von unter 9 Grad Celsius wird Außenluft genutzt, um das Kühlwasser zu kühlen. Die Kühlaggregate laufen so nur 70 Prozent der Zeit. Die Rechner stecken in geschlos-

senen Rechnerschränken (APC Cubes). So können sich warme und kalte Luft nicht mischen.

Einen der verliehenen DataCloud Awards erhielt in der Kategorie „Eco“ Michael Würth, Global Head of Data Centres bei SAP SE. Er wurde ausgezeichnet, weil es trotz steigendem Umsatz von SAP gelang, die Energieeffizienz der Rechenzentren jährlich um zehn Prozent zu steigern und deren Kohlendioxidausstoß zwischen 2003 und 2015 um 40 Prozent zu senken. Die Preisträger verschwenden kaum noch Energie für Heizung und Kühlung. Ein weiterer DataCloud Award ging an das neue Rechenzentrum des GSI Helmholtzzentrum für Schwerionenforschung (siehe folgende Seite).

Was passiert eigentlich mit der Energie im RZ?

Noch mehr könnte gehen, wenn innovative Ansätze mit einbezogen werden. Dieser Meinung sind etwa Marta Chinnici, Senior Researcher ENEA, und Alfonso Capozzoli, Senior Assistant Professor am Polytechnikum Turin. Ihre These: Bisher berücksichtigten die für Effizienzmessungen verwendeten Parameter lediglich den Energieinput eines RZ, nicht jedoch, was mit der Energie im RZ geschieht. Dabei gebe es auch hier Effizienzpotenziale, die sich allerdings nicht korrekt beziffern ließen.

Capozzoli beschäftigt sich beispielsweise mit Energieverlusten innerhalb des belüfteten Bereiches, die durch undichte Lüftungskanäle zustande kommen. So fließe Kaltluft an falsche Stellen, was wiederum die vorgesehenen Warmluftströme behindere und zu lokalen Hot- und Cold-Spots führe, die bei der Temperatursteuerung der Kaltluftzufuhr außer Betracht bleiben. Energieverluste könnten auf dieses Weise auch in der Klimatisierungseinheit oder innerhalb der Racks entstehen. Ihre Berechnung erfolgt mit aufwändigen Algorithmen aus der Strömungsdynamik und erfordert eine ausreichend dichte Ausstattung des Rechenzentrums mit Sensoren. Der Lohn der Mühen: die Lufttemperatur der Kaltluftzufuhr lässt sich optimal steuern.

Weiter bemängelt der Wissenschaftler, dass es derzeit noch keine Maßzahl dafür gilt, wie viel nützliche Arbeit ein Rechenzentrum tatsächlich in Verhältnis zum Gesamt-Energieaufwand verrichte (Datacenter Energy Productivity). Da jedoch die verschiedenen Applikationen in einem RZ unterschiedliche Leistungsparameter haben können, weil sie unterschiedliche Aufgaben verrichten, könne man die Leistungen der einzelnen Applikationen nicht zu einem einzigen Parameter aufsummieren. Man benötige einen Normalisierungsfaktor, wie er auch verwendet wird, um die in verschiedenen Energieträgern steckenden Energiemengen vergleichbar zu machen. Doch genau dieser fehle derzeit.

Besser heiße Luft produzieren

Zudem kann das einseitige Starren auf die PUE auch sinnvolle Ansätze zur Wärmewiederverwendung blockieren. Denn je geringer die Temperatur von Heißwasser oder Warmluft am RZ-Ausgang und damit die Überschussenergie, desto weniger kann man damit anfangen und desto näher sollte der Wärmeverbraucher liegen. Mit Ausgangstemperaturen von 24 Grad lässt sich ein Fernwärmesystem nur dann speisen, wenn die Luft energieintensiv erhitzt wird – was aber angesichts des Gesamtziels, Energieverschwendung zu minimieren, wiedersinnig wäre. Ist eine effiziente Abwärmenutzung möglich, wie vielerorts in Dänemark, wo jetzt Apple ein Großrechenzentrum betreibt, sollte das RZ also eher heißere Luft produzieren, als die PUE-Minimierung ausreizen.

Quelle: Tobin

In einigen europäischen RZ-Märkten gibt es Überkapazitäten.

Oft genug fehlen allerdings in der Nähe von RZs entweder Verbraucher oder Gasnetze, sodass als Wärmeverbraucher allenfalls die Büros oder andere Einrichtungen direkt am Datacenter in Frage kommen. Nur die genaue Analyse aller Energieströme kann also ermitteln, was vernünftig und sinnvoll ist. Ein weiterer wichtiger, oft aber nicht ausreichend beachteter Faktor ist die Effizienz des IT-Betriebs. Das Problem wurde in Bezug auf den Kohlendioxid-Ausstoß von Rechenzentren in der Wissenschaft bereits 2013 erkannt: Ein Forscherteam belegte, dass eine ausgeprägte Effizienz im Betrieb, wozu auch eine optimale Auslastung gehört, die negativen Effekte nicht nachhaltiger Energieträger durchaus kompensieren kann. Minimieren lässt sich der Kohlendioxidausstoß freilich nur dann, wenn alles stimmt: der Energieträger, die Auslastung und der Betrieb.

Eine Möglichkeit einer Gesamteffizienzbewertung besteht darin, die Kosten des RZ-Kunden zum Maß der Dinge zu machen. Das schlägt Jakob Carnemark, CEO des US-amerikanischen Rechenzentrumsbetreibers Aligned Energy, vor. „Der PUE-Wert als Verhältnis zwischen der Energie für die übrige Infrastruktur zur Rechenenergie bildet nicht ab, ob die Rechenenergie überhaupt effizient genutzt wird“, kritisiert er. „Dabei sind die meisten Rechenzentren nur zu maximal 30 bis 40 Prozent ausgelastet.“ Der Kunde zahle mithin meist 60 bis 70 Prozent mehr, als er tatsächlich nutze.

Kunden zahlen, was sie nutzen

Bei Aligned Energy verwende man deshalb eine neuartige Effizienzmetrik und ein Preissystem, das den Kunden nur den tatsächlichen Nutzungsgrad der Systeme in Rechnung stellt. Carnemark schlägt als neuen vereinheitlichen Messwert für die Gesamteffizienz des Rechenzentrums die sogenannte TCUE (Total Cost of Use Efficiency) vor. Dabei wird die Summe aus Gesamtstromverbrauch und Gesamtmietkosten für die Infrastruktur geteilt durch die Summe aus den fürs Rechnen angefallenen Stromkosten und den Leasingkosten für die tatsächlich genutzte Infrastruktur.

Ein günstiges Verhältnis zwischen Rechen- und Kühlenergie ist hier nur einer von mehreren Faktoren, der eine schlechte Auslastung nicht mehr kompensieren kann. Umgekehrt kann eine gute Auslastung schlechte Kühleffizienz oder nicht nachhaltige Energieträger partiell kompensieren. Freilich lassen sich günstige Werte im TCUE auch beispielsweise durch simples Preisdumping erzielen, was auf den konkurrenzintensiven RZ-Märkten möglicherweise durchaus eine Option ist, um Kunden zu binden. Dann wäre zwar den Kunden geholfen, aber nicht der Umwelt.

Wer braucht Tier IV wirklich?

Dass solche Dumpingpreise in überlaufenen Märkten denkbar sind, legt der Konzentrationstrend auf den Rechenzentrumsmärkten nahe. So wurde Telehouse jüngst von NTT übernommen, und just zur DataCloud Europe verkündete Equinix den Aufkauf von Telecity. In europäischen Großstädten, speziell in London, steigen seit Jahren die Leerstandsraten im RZ-Bereich, in Frankfurt und Paris dagegen ist die Tendenz trotz aktuellen Zubaus relativ stabil.

Ein wesentlicher Stolperstein auf dem Weg zum effizienteren Rechenzentrum ist auch das sicherheitstechnische Überdimensionieren. Denn, so viele Fachleute, kaum jemand brauche ein ausfallsicheres Tier-IV-Rechenzentrum, in dem wirklich alles doppelt ausgelegt und bei laufendem Betrieb auswechselbar ist. Tier-II- bis Tier-III-Rechenzentren, die für die meisten Aufgaben durchaus ausreichen, ließen sich aber auch mit erheblich weniger Aufwand als bisher üblich errichten. Ein Beispiel dafür ist das bereits mehrfach preisgekrönte eCube-Konzept. Hier versorgen Strom- und Kühlungsrohre jeweils die über und die unter ihnen liegende Etage, was eine geringere Höhe der RZ-Etagen und damit Materialeinsparungen möglich macht. Außerdem werden die Komponenten nach dem n+1-Prinzip ausgelegt statt doppelt. Allerdings verbinden zwei Stromzuführungen das Rechenzentrum mit zwei unterschiedlichen Providern.

Im neuen Datacenter des GSI Helmholtzzentrum für Schwerionenforschung entsteht gerade der Green-Cube, ein nach eCube-Prinzipien ausgelegtes Rechenzentrum für 800 Racks auf sechs Etagen, das auf diese Weise mit 21 Metern Höhe auskommt. Dort sparte man sich auch die gesamte USV-Anlage. Der pragmatische Ansatz lautet: Fällt der Strom aus, tut dies auch der unterirdische Beschleunigerring, dessen Versuchsdaten das Rechenzentrum auswerten soll. Da das Rechenzentrum nicht laufen muss, wenn keine Daten anfallen, kann man die USV weglassen und damit auch deren Energie- und Materialverbrauch sparen. Außerdem verwendet der Bau teilweise ein Stahl-Gebäudegerüst und nur in den Versorgungsbereichen Betonwände. Es steht auf Stahlstelzen, massive Stahl-Querträger wurden nicht eingesetzt. Auf diese Weise sank der Materialbedarf an energieintensiv erzeugten Stahl um viele Tonnen.

Nordeuropa nach wie vor hoch im Kurs

Metall spart auch der aus Schweden stammende Anbieter des RZ-Kühlsystem Oasis. Das Kühlaggregat des Systems besteht im Kern aus einem aus speziellem Kunststoff gefertigten Wärmetauscher. Die RZ-Abwärme durchströmt das Aggregat nicht wie üblich in Kurven, sondern gerade. Gekühlt wird das Wärmetauscher-Aggregat je nach Tem-

peratur von der Außenluft, die den Wärmetauscher äußerlich umströmt. Zusätzlich lässt er sich mit Wasser benetzen, das dann verdunstet und den Kühleffekt erhöht. Bei Spitzentemperaturen kann das Wasser zuvor auch noch gekühlt werden. Eine Kühlzelle führt 300 Kilowatt Wärme ab, für mehr ist eine zweite Zelle erforderlich. Warm- und Kaltluft bleiben bei diesem Design komplett getrennt, es können also keine Stäube oder Gase ins RZ eindringen. Die wieder gekühlte RZ-Luft wird am Ende wieder den Rechnern zugeführt. In tropischen Bereichen lässt sich die Lösung wegen der hohen Außentemperaturen allerdings nicht verwenden.

Da haben es andere Länder besser. Gerade die nordeuropäischen Staaten machen sich derzeit heftige Konkurrenz um investitionswillige Cloud- und RZ-Betreiber: Die meist reichlich vorhandene Wasserkraft verspricht auf Dauer günstige Energiepreise. Den Vogel schießen in dieser Beziehung Island mit einer Energieversorgung aus 75 Prozent Wasser- und 25 Prozent Geothermie sowie Norwegen (100 Prozent Wasserkraft) ab, auch Finnland ist reich mit Wasserenergie gesegnet. Der isländische Provider Verne Global wirbt daher mit dauerhaften Energiepreisen von vier Cent pro Kilowattstunde. Norwegen fehlten aber bisher die schnellen Glasfaseranbindungen an den Rest der Welt – dieses soll im Laufe des Jahres behoben sein.

In Schweden stecken dagegen noch 40 Prozent Atomenergie im Netz. Dänemark wirbt mit reichlich vorhandener regenerativer Windenergie und zudem einem ausgedehnten Wärmenetz, das es ermögliche, viel Abwärme weiterzuverkaufen. Dass günstige Energie ein wesentlicher Wettbewerbsfaktor auf dem Rechenzentrumsmarkt ist, haben inzwischen viele Ökonomien erkannt. Auch Malaysia wirbt für RZ-Investitionen. Nicht nur mittelfristige Steuererlasse und Wachstumsraten, sondern auch reichlich Wasserkraft in der Provinz Sarawak sollen RZ-Betreiber locken. Diese Region machte bisher übrigens bestenfalls durch martialische Auseinandersetzungen mit der dort lebenden Bevölkerung um Landrechte Schlagzeilen.

Erzeugt eigenen Strom!

In ferne Länder oder Regionen mit erneuerbarer Energie auszuweichen, ist freilich nicht die einzige Alternative, um als Betreiber von Rechenzentren zu einem kleineren Kohlendioxid-Fußabdruck zu kommen. Darauf weist Yahoo-Managerin Christina Page hin. Sie ist der Ansicht, dass man für Rechenzentren neue regenerative Energieanlagen bauen sollte, statt bereits vorhandene regenerative Energie zu nutzen oder einfach Zertifikate zu kaufen. Denn nur so steige das regenerative Erzeugungspotential. Yahoo lässt diesem Postulat derzeit Taten folgen: Own Energy, ein Stromprovider aus Kansas, baut in Rush County einen Windpark für Yahoo mit einer 15-jährigen Nutzungsvereinbarung. Weitere sollen folgen. Auch Amazon und Google haben massive Investitionen in eigene regenerative Energieerzeugungsanlagen angekündigt.

Ariane Rüdiger,
freie Journalistin, München

Hybride Rechenzentren ganzheitlich schützen

Wie sich eine gemischte physische und virtuelle RZ-Umgebung gegen Angriffe sichern lässt

Rechenzentren entwickeln sich immer mehr zu einem Mix aus physischen und virtuellen Rechen-, Netzwerk- und Speicherkomponenten. Angreifern ist das weitgehend egal, sie kommen dennoch ans Ziel. Für die RZ-Betreiber stellt sich jedoch die Frage, ob zum Schutz der Daten andere Konzepte nötig sind als bislang. Einige Überlegungen hierzu.

Aktuelle Sicherheitsvorfälle haben gezeigt, dass unabhängig von der Topologie des Rechenzentrums immer wieder Daten von Kriminellen extrahiert werden. Die jüngsten Angriffsszenarien bestätigen, dass sich Rechenzentren unter anderem durch moderne Firewall-Lösungen schützen lassen. Um das Bedrohungsrisiko zu mindern, empfehlen Sicherheitsexperten zunächst einige grundlegende Maßnahmen:

1. Bestandsaufnahme im Rechenzentrum: Welche Anwendungen sind vorhanden und kommunizieren miteinander?
2. Prävention gegen bekannte und unbekannte Bedrohungen in spezifischen Anwendungsprozessen im Rechenzentrum einrichten und seitliche Bewegung von Malware verhindern.
3. Zugriff auf Rechenzentrumsanwendungen immer auf Basis von Nutzeranforderungen und Anmeldeinformationen gewähren.
4. Sicherheitsrichtlinien müssen skalierbar sein und mit den dynamischen Veränderungen im Rechenzentrum Schritt halten können.

Das Umsetzen von Sicherheitsregeln auf Anwendungsebene innerhalb des physischen, virtualisierten oder Hybrid-Rechenzentrums kann die Sicherheitslage im Rechenzentrum verbessern. Die Komplexität und Variabilität vieler Rechenzentrumsarchitekturen stellt aber auch bestimmte Herausforderungen an die Netzwerkintegration.

Das vorliegende Beispiel einer zeitgemäßen Sicherheitsimplementierung im hybriden Rechenzentrum umfasst physische Firewalls am Rand der Rechenzentrumsumgebung, virtualisierte Firewalls für die Absicherung virtualisierter Arbeitslasten und eine zentrale Konsole zum Verwalten von Sicherheitsrichtlinien. Die Integration mit weiteren Komponenten des Rechenzentrums, wie etwa VMware-NSX-Netzwerkmanagement und Center-Host-Management, ermöglicht den Aufbau einer einheitlichen Sicherheitsarchitektur im Rechenzentrum. Um die Herausforderung der Integration zeitgemäßer Sicherheitsfunktionalität ins physische Netzwerk bewältigen zu können, unterstützen moderne Firewall-Plattformen eine Reihe von Netzwerk-Modi, darunter L2, L3, Virtual Wire und einen gemischten Modus. Spezielle Firewalls für die Netzwerk-Virtualisierungsplattform VMware NSX ermöglichen den Schutz der virtualisierten Umgebung mit anwendungsspezifischen Sicherheitsrichtlinien und erweiterten Threat-Prevention-Funktionen, die identisch mit denen in physischen Geräten sind. Eine zentrale Verwaltung gewährleistet die Regelkonsistenz für alle physischen und virtuellen Firewalls in einer RZ-Umgebung. Die Implementierungsvorschläge zeigen, wie sich eine Kombination aus Next-Generation-Firewall und fortschrittlicher Bedrohungsabwehr sowohl im physischen Teil des Rechenzentrums als auch in einer mit VMware NSX virtualisierten Umgebung einsetzen lässt. Die Aufgaben der einzelnen Komponenten in diesem Beispiel verteilen sich wie folgt: Zwei Firewalls an den Rechenzentrumsgrenzen sichern den Nord-Süd-Verkehr, der das Rechenzentrum durchquert. Die virtualisierte Firewall sichert den Ost-West-Verkehr. Eine zentralisierte Appliance als Management- und Reporting-Plattform sorgt für das einheitliche Verwalten der Sicherheitsumgebung.

Business-Anwendungen und -Services werden am häufigsten mit Exploits in Verbindung gebracht.

Quelle: Palo Alto Networks

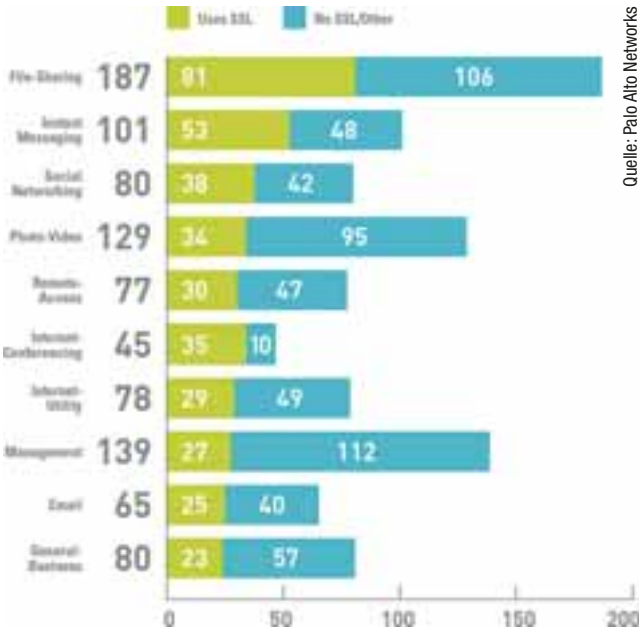
Zwei Firewalls sichern die Netzwerkgrenze

Zwei für Aktiv/Aktiv-Hochverfügbarkeit konfigurierte Firewalls sind zwischen dem Unternehmensnetzwerk und dem Kern-Rechenzentrum positioniert. Diese Systeme verarbeiten alle Daten, die in das Rechenzentrum kommen oder das Rechenzentrum verlassen, aber nicht den internen Datenverkehr. Der Virtual-Wire-Schnittstellenmodus ermöglicht das Verzahnen mit der bestehenden Umgebung. Ihre hohe Verarbeitungskapazität erzielen moderne Firewalls durch Bauteile wie Netzwerkverarbeitungskarte (Network Processing Card, NPC), First-Packet-Prozessor (FPP), Switch-Management-Karte (SMC) und Prozessverarbeitungskarte (Log Processing Card, LPC). Hierbei kommen sicherheitsspezifische Multi-Core-Prozessoren zum Einsatz. Die lineare Skalierbarkeit kommt durch das Entkoppeln der physischen Schnitt-

stellen an jeder NPC von den Sicherheitsprozessoren zustande. Somit agiert jede NPC als Verkehrsleit- und Verarbeitungsuntersystem, indem sie die gemeinsamen Ressourcen des gesamten Systems durch den FPP verfügbar macht, der eingehenden Traffic an die verfügbaren Ressourcen verteilt. Zum Erweitern der Kapazität ist nur das Hinzufügen einer weiteren NPC nötig. Die LPC nutzt RAID-1-Speicher, um Protokollierungsaktivitäten auszuführen, ohne die Verarbeitungsleistung von anderen Verwaltungsaufgaben zu beeinträchtigen. Wichtige Aufgaben für das Absichern der Netzwerkgrenze sind:

- die Auswahl des Schnittstellen-Modus (Virtual-Wire-, L2- oder L3-Firewall),
- die Konfiguration der Hochverfügbarkeit als aktiv/aktiv oder aktiv/passiv,
- das Anbinden an eine Managementkonsole.

Bei diesem Implementierungsbeispiel wurde Virtual Wire als Netzwerkmodus ausgewählt, somit muss das Netzwerk nicht neu konfiguriert werden. Virtual Wire stellt durch das Bündeln zweier Ports einen transparenten Modus bereit. Zwischen den Ports läuft der gesamte erlaubte Datenverkehr, ohne Switching oder Routing. So sind ein vollständiges Überwachen und die Kontrolle für den gesamten Verkehr möglich, ohne Netzwerkprotokoll-Konfiguration. Virtual-Wire-Konfigurationen arbeiten nahtlos mit hoher Verfügbarkeit und lassen sich durch das Hinzufügen neuer Port-Paare linear skalieren. Firewalls der neuesten Generation unterstützen sowohl Aktiv/Aktiv- als auch Aktiv/Passiv-Formen der Hochverfügbarkeit, um Anforderungen an die Hardwareredundanz



Quelle: Palo Alto Networks

Die Top-Ten-Kategorien mit der höchsten Konzentration an Anwendungen, die SSL nutzen können und damit für Firewalls schwerer zu kontrollieren sind.

zu erfüllen. Ein Hochverfügbarkeitspaar kann gemeinsam auf dem gleichen Switch oder getrennt, über ein L3-Netzwerk mit einem anderen Standort verbunden, installiert sein. Dedizierte Hochverfügbarkeits-Ports werden verwendet, um die Kommunikationsverbindung zwischen den beiden Systemen aufrechtzuerhalten. Der Aktiv/Aktiv-Modus wird häufig in geschäftskritischen Rechenzentrumsumgebungen verwendet. Diese Konfiguration liefert komplette Zustandsinformationen für beide Geräte. Im Falle eines Fehlers würde die funktionierende Firewall das Verarbeiten der bestehenden Verbindungen unterbrechungsfrei fortsetzen. Nach dem Neuaufsetzen der ausgefallene Einheit wird die Aktiv/Aktiv-Verbindung wieder hergestellt.

Virtuelle Firewall für virtualisierte Arbeitslasten

Eine virtuelle Firewall ist auf jedem physischen Host installiert, auf dem in diesem Fall VMware läuft. Die VMware-NSX-Virtualisierungsplattform ist ein integraler Bestandteil für den Schutz virtueller Workloads, da sie komplette L2- und L3-Switching-Funktionalität reproduziert, die von der zugrunde liegenden physischen Hardware entkoppelt ist. NSX hält dann die Firewalls vor und steuert den Datenverkehr zu den lokalen Firewalls für eine detailliertere Analyse basierend auf zentralen Regeln. In diesem Implementierungsbeispiel kommt daher eine virtualisierte Firewall unter NSX zum Einsatz. Das Bereitstellen einer Firewall erfolgt dann ebenso schnell wie das Bereitstellen neuer virtualisierter Arbeitslasten. Da sich diese immer wieder ändern, ermöglicht es eine solche integrierte Lösung, den Updateprozess für die Sicherheitsrichtlinien zu automatisieren, damit alle virtualisierten Anwendungen geschützt werden – egal wie schnell sich die virtuelle Umgebung ändert. Die wichtigsten Schritte beim Bereitstellen virtueller Firewalls sind:

- das Konfigurieren der Managementkonsole als neuen Dienst im NSX Manager,
- das Bereitstellen der virtuellen Firewalls über vCenter und NSX,
- das Konfigurieren von Traffic-Lenkungs-Richtlinien,
- das Synchronisieren des Rechenzentrumsstatus mithilfe von dynamischen Adressengruppen.

Der Einsatz von einzelnen virtuellen Firewalls ist ohne manuelle Eingriffe machbar, sobald das ursprüngliche Orchestrieren in Kraft gesetzt ist. API-Konnektivität zwischen den Management-Komponenten schafft sofortige Konnektivität, sodass für Änderungen in einer Umgebung nahtlos die Sicherheitsregeln angewandt werden. Dank dieser Orchestrierung entfällt die Notwendigkeit für mehrere administrative Schritte auf verschiedenen Management-Plattformen.

Quelle: Palo Alto Networks

Der Installations- und Exfiltrationsprozess von moderner Malware wie Smoke-Loadern umfasst sieben Schritte, die alle von Firewalls entdeckt werden sollten.

Zentrale Management-Appliance

Eine zentrale Management-Appliance bietet eine einzige Oberfläche zum Durchsetzen einer kohärenten, ganzheitlichen Sicherheitspolitik in physischen und virtuellen Firewalls. Eine derartige Schaltzentrale kann als virtuelle Appliance oder als dedizierte Appliance eingesetzt werden. Die Managementlösung sollte entsprechend den Unternehmensanforderungen hinsichtlich Firewall-Stellfläche, -Standort und -Compliance skalierbar sein. Zudem sollte es eine Schnittstelle zur API des NSX Managers geben. Dies sorgt für ein abgestimmtes Bereitstellen und dynamisches Aktualisieren von Veränderungen in der Umgebung. Konsistente Regeln und eine zentrale Protokollierung sind dabei wesentliche Bestandteile beim Schutz vor bekannten und unbekannten Bedrohungen. Ein entscheidender Vorteil des zentralen Managements gegenüber Lösungen, deren Verwaltung über verschiedene Programme mit unterschiedlichen Schnittstellen lauft: Konsistenz sowohl bei der Schnittstellen- als auch bei der Freigabeebene. Denn die Oberflächen der Management-Appliance und der einzelnen Geräte sollten das gleiche Erscheinungsbild aufweisen. Insgesamt können mit diesem Modell alle wichtigen Anforderungen zum Absichern eines hybriden Rechenzentrums erfüllt werden:

- Skalierbarkeit: Durch den modularen Aufbau einer modernen Firewall lassen sich Prozessorleistung und Kapazität nach Bedarf hinzufügen, ohne Beeinträchtigung der Verkehrsverarbeitung und mit einer einheitlichen Verwaltung der gesamten Firewall-Plattform. Virtuelle Firewalls, die im Tandem mit Datacenter-Hosts eingesetzt werden, erhöhen linear die Inspektionskapazität, wenn das Cluster wächst.
- Netzwerkintegration: Dank Virtual-Wire-Schnittstellen sind keine Netzwerkprotokolle oder Konfigurationen erforderlich, was den Einsatz der Firewall relativ einfach macht. Virtual Wire stellt einen transparenten Modus durch logisches Bündeln zweier Ports bereit, während uneingeschränkte Inspektion und Überwachung für den gesamten Verkehr möglich ist.
- Zuverlässigkeit: Aktiv/Aktiv-Hochverfügbarkeit sorgt dafür, dass beide Firewalls ständig ihre Konfigurations- und Sitzungsinformationen synchronisieren, sodass im Falle eines Hardwareausfalls kein Datenverkehr verloren geht und die Performance der Lösung sich nicht verschlechtert.
- Vereinfachtes Orchestrieren und Verwalten: Die direkte Integration mit VMware NSX durch vordefinierte APIs hilft beim Automatisieren der Firewall-Bereitstellung, während Tie-ins mit der Management-Appliance sicherstellen, dass die Richtlinien mit der Änderungsrate virtualisierter Arbeitsanforderungen Schritt halten können.
- Regelkonsistenz: die Management-Appliance dient als zentrale Konsole für alle Firewalls, sowohl physische als auch virtuelle. Regeln können zentral definiert und konsequent auf allen Geräten angewandt werden.

Ein entscheidendes Merkmal moderner Firewall-Plattformen ist, dass sie sowohl den Nord-Süd- als auch den zunehmenden Ost-West-Verkehr im Netzwerk schützen. Angreifer können somit nicht nur am Eindringen gehindert werden. Sondern auch dann, wenn sie sich seitlich im Rechenzentrum und durch das Rechenzentrum hindurch bewegen wollen. Damit wird ein nicht zu vernachlässigendes Szenario fortschrittlicher Angriffsmuster abgedeckt, mit denen sich Rechenzentrumsbetreiber heute konfrontiert sehen.

Thorsten Henning,
Senior Systems Engineering Manager, Palo Alto Networks

Und jetzt alles zusammen

In den Rechenzentren macht ein neues Zauberwort die Runde: hyper-converged. Was ist dran an dem Hype?

Eine hyperkonvergente Infrastruktur verspricht vereinfachte Administration und geringere Kosten. Doch das Konzept hat seine Grenzen und ist auch nicht für jedes Unternehmen die richtige Wahl.

Die immer weiter steigende Performance und Kapazität der Hardware, die enorme Rechenpower der modernen CPUs mit ihren Multicore-Architekturen genauso wie die mehreren Gigabytes Speicher, die aktuelle Festplatten und Flash-Systeme aufnehmen können, lassen das Konzept von All-in-One-Lösungen plötzlich wieder attraktiv aussehen. Heute ist es möglich, in ein einziges Chassis mit ein oder zwei Höheneinheiten Komponenten von einer Leistungsfähigkeit hineinzupacken, wie es sie früher nur in der Kombination aus mehreren Geräten gab. Das ist jedoch lediglich der nüchterne technische Hintergrund für die hyperkonvergenten Systeme, die in den letzten Monaten den Markt erreichten.

Damit sich dieser Trend durchsetzen konnte, war eine Veränderung der Sichtweise auf die Struktur des Rechenzentrums erforderlich. Voraussetzung dafür wiederum war zum einen der Siegeszug der Virtualisierung, die eine Trennung der Funktionen eines Datacenters von der physischen Hardware erlaubte. Vielleicht spielte aber auch das Beispiel der allgegenwärtigen Smartphones eine Rolle: Obwohl es sich um hochentwickelte Computer handelt, brauchen sich ihre Besitzer keine Gedanken über das Systemmanagement oder die Speicherverwaltung zu machen, wenn sie eine bestimmte Funktion benötigen. Stattdessen installieren sie einfach eine App. Das Gleiche gilt für eine hyperkonvergente Infrastruktur: Die Software ist der entscheidende Faktor, die darunter liegende Hardware tritt in den Hintergrund.

Wie sich Hyperkonvergenz definiert

Doch was ist nun der Unterschied zwischen einer konvergenten oder converged Infrastructure und einer hyperkonvergenten? Am einfachsten lässt es sich wohl folgendermaßen erklären:

- Eine converged Infrastructure wird über die Hardware definiert. Die Komponenten für Computing, Storage und Netzwerk – oft stammen sie von verschiedenen Herstellern – werden als Paket verkauft. Es handelt sich jedoch um eigenständige Geräte, die sich auch separat benutzen lassen. Der Anwender hat jedoch die Gewähr, dass ihre Schnittstellen und Funktionen aufeinander abgestimmt sind, der Aufwand für die Konfiguration ist dementsprechend sehr gering.
- Eine hyperkonvergente Infrastruktur hingegen definiert sich über die Software. Anbieter wie Nutanix oder VMware statten ihre Programme mit der nötigen Intelligenz aus, um Computing, Storage und Netzwerk über eine Bedienoberfläche zu steuern und zu verwalten. Die einzelnen Komponenten können von verschiedenen, aber auch vom gleichen Hersteller stammen. Im Unterschied zum konvergenten Ansatz lassen sie sich jedoch nicht aus dem System herauslösen. Stattdessen sind sie fest integriert.

Beispiel: In einem klassischen Rechenzentrum gibt es einen physischen Server, auf dem ein Hypervisor mehrere physische Maschinen verwaltet. Der zugehörige Storage ist über ein SAN oder als NAS angebunden. In einer konvergenten Infrastruktur ist der Storage dagegen direkt mit dem Server verbunden. In einer hyperkonvergenten Umgebung schließlich ist der Storage-Controller ein Dienst, den die Software bereitstellt, um die Daten auf den integrierten Platten und SSDs zu verwalten.

In einer hyper-converged Infrastructure sind sämtliche Komponenten virtualisiert, Server, Storage, Netzwerk, alles. Es gibt keinen Windows- oder Linux-Server, der direkt auf der Hardware aufsetzt. Sämtliche Funktionen werden von der Software als Dienste bereitgestellt, je nach Hersteller ist beispielsweise auch eine Deduplizierung verfügbar.

Scale-out statt Scale-up

Das große Argument für eine hyperkonvergente Infrastruktur ist das Vereinfachen. Hyperkonvergente Systeme sind Appliances. Sobald die Performance und/oder Kapazität einer dieser Appliances nicht mehr ausreicht, fügt man in einem Scale-out-Prozess einfach eine weitere hinzu, anstatt in einem Scale-up verhältnismäßig aufwendig CPUs oder Festplatten zu tauschen und einzurichten. Der gesamte, aufwendige Prozess mit der Definition von LUNs, Zoning oder dem Einrichten eines SAN entfällt.

Auch das Planen wird vereinfacht: Anstatt über das Jahr hinweg ständig an einer Stelle neue Speicherkapazitäten hinzuzufügen und an anderer einen neuen Server einzurichten oder den Netzwerkdurchsatz erhöhen zu müssen, werden lediglich zusätzliche Appliances angeschafft. Gleichzeitig macht auch die einheitliche Management-Oberflä-

Quelle: Dell

Mit der XC Appliance hat Dell ein hyperkonvergentes System mit Software von Nutanix im Programm.

che dem Administrator das Leben leichter. Er muss sich nicht mehr mit unterschiedlichen Tools und Bedienkonzepten auseinandersetzen, sondern kann sich auf eine Software konzentrieren.

Das hat auch Auswirkungen auf die Organisation der IT-Abteilung: In größeren Unternehmen besteht sie oft aus mehreren Teams, die sich getrennt voneinander um die Server-Hardware, die Storage-Systeme, die Virtualisierungs-Software und so weiter kümmern. Bei einer hyperkonvergenten Infrastruktur ergibt das keinen Sinn. Hier ist ein Team für alle Bereiche zuständig.

Neben diesen Vorteilen, die sich auch auf der Kostenseite niederschlagen können, hat das Konzept einer hyperkonvergenten Infrastruktur auch einige Nachteile gegenüber klassischen Ansätzen.

So entfällt die Möglichkeit, granulare Upgrades durchzuführen. Ganz gleich, wo der nächste Engpass droht, ob bei der Rechenleistung, dem Storage oder der Netzwerkkapazität: Der Administrator kann immer nur eine weitere Appliance hinzufügen. Es ist nicht vorgesehen, beispielsweise die Platten durch Modelle mit höherer Kapazität zu ersetzen oder zusätzlichen Flash-Speicher zu installieren. Das zeigt auch gleichzeitig, wo das Konzept an seine Grenzen stößt: Muss in einem Unternehmen beispielsweise schlagartig die Speicherkapazität um ein halbes Petabyte erhöht werden, so sind die Kosten in einer hyperkonvergenten Infrastruktur um ein Vielfaches höher als beim klassischen Scale-up, wo lediglich Festplattenkapazität hinzugefügt werden muss. Das wird auch nicht durch die Erleichterungen bei der Administration und Konfiguration aufgefangen.

Mehrere Software- und Hardware-Kombis

Unternehmen sollten zudem bedenken, dass die Entscheidung für oder gegen eine hyperkonvergente Infrastruktur immer ein Entweder-oder ist – Mischformen gibt es nicht. Es ist nicht möglich beziehungsweise ergibt keinen Sinn, bestehende Hardware wie Server oder NAS-Systeme in das Konzept miteinzubeziehen. Firmen haben also die Wahl, ob sie komplett auf hyperkonvergente Systeme umstellen oder weiterhin auf bestehende Konzepte vertrauen. Allerdings spricht nichts dagegen, lediglich einzelne, dafür geeignete Fachabteilungen auf eine hyper-converged Infrastructure umzustellen.

Quelle: VMware

VMware EVO:RAIL lässt sich über eine klar gegliederte Oberfläche in die VMware-Umgebung beim Anwender einpassen und konfigurieren.

Quelle: EMC

Die VSPEX Blue von EMC basiert wie ähnliche Systeme von HP, Fujitsu oder Hitachi auf dem EVO:RAIL-Softwarepaket von VMware.

Im Prinzip gibt es mehrere Möglichkeiten, um an ein hyperkonvergentes System zu kommen. Zum einen kann man sich an die Software-Hersteller wenden. Nutanix, SimpliVity oder Scale Computing bieten nicht nur die Software für das Management einer entsprechenden Appliance an, sondern verkaufen auch vorgefertigte Hardware-Lösungen mit ihrem Logo. Sie sind in verschiedenen Größen erhältlich und lassen sich laut den Herstellern in rund einer halben Stunde betriebsbereit machen. Vergangenen Herbst präsentierte auch VMware mit EVO:RAIL ein solches System. Bis zu acht Appliances in verschiedenen Ausbaustufen lassen sich dabei über ein 10-GBit-Netzwerk zu einem Cluster verbinden. Insgesamt kann ein hyperkonvergentes Rechenzentrum mit VMware EVO:RAIL bis zu 32 Knoten umfassen.

Im Mai 2015 präsentierte der Hersteller eine überarbeitete Version der Software, bei der auf Kundenwunsch das Monitoring verbessert wurde. Die Anwender können nun mit der Software den Status jedes einzelnen Knoten überwachen, zudem wird der aktuelle Zustand der SSDs, Festplatten, Netzwerk-Adapter sowie der ESXi-Bootlaufwerke angezeigt. VMware verkauft EVO:RAIL-Systeme unter seinem eigenen Namen, sie sind jedoch beispielsweise auch von Dell, HP oder Fujitsu erhältlich, die ihnen teilweise eigene Bezeichnungen geben. Auch die VSPEX BLUE von EMC basiert auf EVO:RAIL. Als Hypervisor wird bei den EVO:RAIL-Systemen natürlich nur vSphere unterstützt, hinzukommen VMware VSAN, vCenter Log Insight und die EVO:RAIL-Verwaltungssoftware selbst. Im Unterschied dazu lässt Nutanix seinen Kunden die freie Wahl, was den Hypervisor angeht. VMware wird genauso unterstützt wie Microsoft Hyper-V oder das zunehmend beliebtere KVM.

Der Kunde hat aber auch die Möglichkeit, lediglich die Software zu lizenzieren und die Hardware selbst zusammenzustellen. Dazu bekommt er etwa von Nutanix oder SimpliVity, aber auch von DataCore für die SANsymphony-V-Software, entsprechende Kompatibilitätslisten. Bei dieser Option bleibt zwar mehr Arbeit beim Anwender hängen, dafür erhält er jedoch mehr Kontrolle über Performance und Kapazität seiner Lösung.

Zum Dritten kann er sich jedoch auch an einen Hardware-Hersteller wie etwa Dell wenden. Das Unternehmen hat ein OEM-Agreement mit Nutanix abgeschlossen und bietet zwei vorkonfigurierte, hyperkonvergente Appliances mit der Software dieses Herstellers an. Das Dell-Konzept sieht ein Basispaket von drei Appliances vor, der Dell-XC-Serie. Alle drei speichern Daten lokal auf ihrem eigenen Storage und replizieren sie gleichzeitig zu einer zweiten Appliance, um Hochverfügbarkeit herzustellen. Sämtliche Server, Anwendungen und auch der Storage sind virtualisiert. Es wird erwartet, dass Nutanix entsprechende Agreements auch mit anderen Hardware-Herstellern abschließt. Ein heiß gehandelter Kandidat ist etwa HP.

Radikales Konzept

Hyperkonvergente Systeme werden den Rechenzentrums-Markt wahrscheinlich nicht im Sturm erobern. Dazu ist das Konzept letztlich zu radikal, zudem sind die Appliances für viele mittelständische Firmen schlichtweg zu teuer. In vielen Großunternehmen jedoch werden sie ihren Platz finden, da sie unter bestimmten Bedingungen klare Vorteile gegenüber klassischen Lösungen für sich verbuchen können.

Roland Freist,
freier Journalist, München

Gefahr im Rechenzentrum

Fehlerströme sind im RZ eine Gefahrenquelle, weil Fehlerstromschutzschalter aus verschiedenen Gründen ausgeschlossen sind

Was im europäischen Ausland oftmals keine Rolle spielt, ist in Deutschland durchaus relevant: Differenzströme sind in deutschen Rechenzentren ein intensiv diskutiertes Thema. Warum nimmt Deutschland hier eine Sonderrolle ein und warum können Differenzströme im Rechenzentrum gefährlich sein?

Ein wichtiger Unterschied zwischen Deutschland und seinen europäischen Nachbarn liegt bei den Themen Arbeitsschutz und Haftung: In Deutschland haften Arbeitgeber beziehungsweise leitende Angestellte unter Umständen persönlich, wenn sie die Regeln zur Arbeitssicherheit oder der Unfallverhütung missachten oder vernachlässigen.

Von der Unternehmensleitung wird also verlangt, umfangreiche Vorkehrungen zu treffen, um Unfälle zu vermeiden beziehungsweise im Fall von Betriebsunfällen abgesichert zu sein. Im konkreten Fall der elektrischen Sicherheit (Stichwort Differenzströme) sind Schutzeinrichtungen wie Fehlerstromschutzschalter vorgeschrieben, die bei drohender Gefahr den Strom automatisch abschalten – so zum Beispiel, wenn das System erkennt, dass Strom durch eine Person zur Erde fließt.

Die DIN VDE 0100, Teil 410 schreibt Fehlerstrom-Schutzschalter vor für „Steckdosen mit einem Bemessungsstrom nicht größer 20 A, die für die Benutzung durch Laien und zur allgemeinen Verwendung bestimmt sind.“ Ausnahmen sind nur für Steckdosen zulässig, die durch Elektrofachkräfte oder elektrotechnisch unterwiesene Personen überwacht werden oder Steckdosen, die jeweils für den Anschluss nur eines bestimmten Betriebsmittels errichtet werden. Steht der ausschließliche Einsatz der Steckdose für bestimmte Betriebsmittel in Frage, empfehlen sich ein Verzicht der Ausnahme oder der Festanschluss des Betriebsmittels.

Doch wie sieht es mit den speziellen C13- oder C19-Steckverbindungen in den heutigen Stromversorgungseinheiten (Power Distribution Units, PDUs) im Rechenzentrum aus? Sind sie nicht für den „Anschluss nur eines bestimmten Betriebsmittels errichtet“, also beispielsweise für IT-Hardware? Die Betriebsmittel, also IT-Hardware, wechseln häufig. Bestehen somit Zweifel? In diesem Fall müsste wiederum auf die Ausnahme verzichtet oder das Betriebsmittel fest angeschlossen werden. Dass dies gerade im Rechenzentrum nicht möglich ist, liegt auf der Hand.

Fürs RZ praxisfremde Regelungen

Eine weitere Vorschrift zwingt zur bewussten Stromabschaltung: die BGV A3-Prüfung. Bei der BGV A3 handelt es sich um eine Unfallverhütungsvorschrift der Berufsgenossenschaften, die Gesetzescharakter hat. Nach Paragraph 5 hat der Unternehmer dafür zu sorgen, dass die elektrischen Anlagen und Betriebsmittel auf ihren ordnungsgemäßen Zustand geprüft werden – vor der ersten Inbetriebnahme und nach einer Änderung oder Instandsetzung vor der Wiederinbetriebnahme.

Quelle: Schleifenbauer

Mit einem solchen Messgerät lässt sich der Differenzstrom direkt an der Stromverteilung (PDU) im Rack messen.

Quelle: Schleifenbauer

Der Residual Current Sensor (RCS) ist die Komponente, die für die eigentliche Messung des Differenzstroms zuständig ist.

Was nun speziell den Rechenzentren zu schaffen macht, sind die Überprüfung der elektrischen Anlagen und Betriebsmittel in bestimmten Zeitabständen: für elektrische Anlagen und ortsfeste Betriebsmittel alle vier Jahre, bei ortsveränderlichen Betriebsmitteln zwischen sechs Monaten bis zwei Jahren. Dabei werden alle Geräte in regelmäßigen Abständen vom Netz getrennt. Anschließend werden die entsprechenden Messungen vorgenommen und die Messergebnisse dokumentiert. Für ein Rechenzentrum ist dieser Ansatz wenig praktikabel.

Ebenso wenig sind Stromabschaltungen durch Fehlerstromschutzschalter eine Option für Rechenzentren, da sie die Verfügbarkeit der Geräte beeinträchtigen. Ein kleiner Differenzstromfehler könnte dann ganze Bereiche lahmlegen. Deshalb gibt es in Deutschland zum Vermeiden von Strom- und damit Betriebsunterbrechungen durch Fehlerstromschutzschalter zwei zugelassene (Um-)Wege zur Rettung.

Doch zunächst zur eigentlichen Bedeutung der Bezeichnung „Differenzstrom“: Sie meint die Differenz zwischen dem Phasen- und dem Nullstrom. Nach Messung beider Ströme (zufließender Strom und abfließender Strom) und Addition der Messwerte ist die Summe im Idealfall gleich null. Ist sie ungleich null, dann leckt irgendwo Strom, meistens zur Erde. Ein Mensch könnte dabei als Stromleiter fungieren und würde bei mehr als 30 Milliampere (mA) Schaden erleiden. Die Ursache von Differenzströmen kann in Fehlern im Gerät liegen; dann meist im Gehäuse, wobei Strom über den PE-Leiter (Protective Earth, Schutzerde) zur Erde abfließt. Nur wenn die Erdung nicht in Ordnung ist, kann es für den Menschen gefährlich werden.

Rettung fürs Rechenzentrum

Zu den bereits erwähnten Umwegen zum Vermeiden von Stromunterbrechungen in deutschen Rechenzentren zählt zum einen, den Zugang zu den elektrischen Einrichtungen nur speziell ausgebildetem Personal zu gewähren.

Der zweite Weg bezieht sich auf ein kontinuierliches Überwachen beziehungsweise Messen von Differenzströmen im Rechenzentrum. Alle Messungen werden in Datenlogs aufgezeichnet. Registriert das System einen anomalen Differenzstromwert, muss der verantwortliche Mitarbeiter sofort eingreifen, diese Maßnahmen dokumentieren und bei einem Zwischenfall später auch vorlegen können.

Aber nicht nur Fehler sind eine Ursache, denn eigentlich gibt jedes elektronische Gerät wegen der vielen elektronischen Schaltungen eine gewisse – wenn auch nur winzig kleine und damit ungefährliche – Menge Strom an die Erde ab. Aufgrund der hohen Anzahl elektrischer Geräte steht im Rechenzentrum eine große Anzahl solcher Erdschlussgeneratoren auf sehr engem Raum. Wie aber lassen sich unter diesen nun die problematischen Erdschlussströme orten? Wie immer lautet die Antwort: erst messen, dann regeln und steuern.

Versichert gegen Schadenersatzansprüche

Um einen Stromschluss zu orten, bevor er Mitarbeitern oder Kunden Schaden zufügen kann, ist also ein engmaschiges Messstellen-Netzwerk notwendig. Eine praktikable Lösung hierfür ist der Einsatz von Differenzstrom-Messgeräten für Stromversorgungseinheiten.

Ist eine PDU mit einem Differenzstrommessgerät (Residual Current Sensor, RCS) ausgerüstet, schickt diese die Messdaten vom RCS weiter an die Überwachung. So lässt sich ein Differenzstrom, der sich außerhalb der Sicherheitszone befindet, gleich am betroffenen Schrank oder sogar an einer bestimmten PDU zu erkennen. Dies vereinfacht es erheblich, den Ursprung des Fehlers zu finden und das Problem zu klären. Es ist sogar möglich, mehrere Messgeräte in eine PDU einzubauen, um so das Suchgebiet im Fehlerfall weiter einzugrenzen.

Sind alle Daten erfasst und werden bei Fehlern Maßnahmen getroffen und dokumentiert, ist das Risiko von Schadenersatzansprüchen geringer.

Umfassende Messungen notwendig

Das Thema „Differenzströme“ gestaltet sich jedoch noch umfangreicher, denn es gibt viele Arten von Differenzströmen. Da Schaltungen in der Elektronik das Sinussignal der Spannung stark beeinträchtigen, entstehen daraus sehr verschiedenartige Signale, unter anderem auch Gleichstrom (DC). Diese DC-Komponenten erschweren die Messungen ganz erheblich: Eine normale Messspule wird durch Gleichströme gesättigt und funktioniert dann nicht mehr zuverlässig. Daher werden spezielle Spulen benötigt, die nicht nur gegen Sättigung geschützt sind, sondern diese Gleichströme auch messen können.

Zum Messen von Differenzströmen wurde eine Klassifikation eingeführt: AC, A, F und B. In der letztgenannten Klasse werden bei der Messung alle Stromtypen berücksichtigt, also auch Differenzströme mit Frequenzen höher als 50 Hertz. Eine Überwachungseinheit vom Typ A erfasst diese harmonischen Ströme beispielsweise nicht, obgleich sie ebenso gefährlich sein können wie die Erdschlussströme von 50 Hz. Für ein wirklich gutes Bild müssen also auch diese Ströme gemessen werden. Fehlerströme stellen in Rechenzentren eine ernstzunehmende Gefahrenquelle dar, weil man aus den eingangs genannten Gründen auf Fehlerstromschutzschalter verzichten muss. Sie müssen also kontinuierlich überwacht und gemessen werden, um Personenschäden zu vermeiden. Differenzstromsensoren in Stromversorgungseinheiten sind ein praktikabler Ansatz, um Messungen durchzuführen und gleichzeitig einen unterbrechungsfreien Rechenzentrumsbetrieb zu gewährleisten. Je umfangreicher die Messung der Ströme dabei erfolgt, desto höher die Sicherheit und einfacher die Fehlersuche.

Ronald Timmermans,
Marketing Director, Schleifenbauer

Bock auf Basteln!

2 x Make mit 35 % Rabatt testen.

Ihre Vorteile:

- 2 Hefte mit 35% Rabatt testen
- Zusätzlich digital lesen über iPad oder Android-Geräte
- Zugriff auf Online-Artikel-Archiv*
- Versandkostenfrei

Für nur 12,90 Euro statt 19,80 Euro.

* Für die Laufzeit des Angebotes.

Jetzt bestellen und von den Vorteilen profitieren:

www.make-magazin.de/miniabo

Hier können Sie direkt bestellen und finden weitere Informationen.

Tel: 0541 80 009 125 E-Mail: leserservice@make-magazin.de

(Mo.-Fr. 8-19 Uhr, Sa. 10-14 Uhr)

Ausstrahlung? Nein, danke.

EMV-Schirmung von IT-Sicherheitsräumen schützt Informationen und Hardware

Fließender Strom bringt unweigerlich elektromagnetische Felder mit sich, die HF-Strahlung abgeben: Elektrische Geräte können von den starken Feldern negativ beeinflusst werden. Aber auch schwache Felder sind eine mögliche Gefahr, weil Informationen bei unerwünschten Mithörern landen können. Schutz versprechen IT-Sicherheitsräume.

Rechenzentren gelten normalerweise als Sicherheitshochburg in einem Unternehmen: Die dort gespeicherten Daten und laufenden Anwendungen sind das A und O für den Firmenerfolg. Dabei gibt es selbstverständlich auch Daten und Anwendungen, die noch sensibler sind als die Daten für das Tagesgeschäft – Entwicklungsunterlagen. IT-Sicherheitsräume stellen hier nicht nur eine gute Grundlage für IT-Equipment dar, sondern sie bieten auch mehr Platz, wenn schnell zusätzliche Hardware untergebracht werden muss und das Rechenzentrum das nicht hergibt.

Beim Schutz eines RZ denken die Betreiber sofort an offensichtliche Gefahren wie Feuer, Wassereintritt und Vandalismus. Aber auch ungewollte Abstrahlungen von elektrischen Feldern sind relevant. Die elektromagnetische Verträglichkeit (EMV) beschreibt auf der einen Seite wie Geräte vor Störstrahlungen aus anderen Quellen geschützt werden können. Es geht bei EMV aber auch darum, Abstrahlungen zu verhindern, aus denen Unbefugte wertvolle und sensible Informationen abgreifen können. Der Schutz vor solchen Strahlungen ist bei einem IT-Sicherheitsraum umfassend möglich, wenn er korrekt geplant und umgesetzt wurde und der Hersteller die notwendigen Vorkehrungen bei den kritischen Bauelementen getroffen hat.

CHECKLISTE: EMV-GERECHTER SICHERHEITSRAUM

- Bestehen definierte Anforderungen an die Schirmwirkung? Oder: Welche Anwendungen sollen darin betrieben werden?
- Kann das Hüllenmaterial mit der bestmöglichen Schirmwirkung genutzt werden oder bestehen Anforderungen, die ein anderes Material erfordern?
- Welche Schirmwirkung ist in welchem Frequenzbereich erforderlich (bei bekannter Größe und Baureihe)?
- Wird die Hülle in einer Umgebung mit Störstrahlung aussendenden oder gegen Störstrahlung empfindlichen Geräten oder Systemen eingesetzt? Oder: Welche Anlagen, Maschinen, elektrotechnischen Systeme befinden sich in der näheren (bis einige zehn Meter) Umgebung?
- Verlangen Sicherheitsanforderungen, dass störaussendende Komponenten besonders gekapselt werden?
- Sind für alle notwendigen Ausbrüche entsprechende HF-geschirmte Durchführungen erhältlich? Klimatisierungskomponenten gibt es in geeigneten Ausführungen (beispielsweise EMV-Filterlüfter), für Sichtflächen geschirmte Scheiben.

Widerstand auch gegen Strahlung

Ein IT-Sicherheitsraum ist ein Raum-in-Raum- beziehungsweise Haus-in-Haus-System. Es geht darum, eine existierende Gebäudeinfrastruktur zu nutzen und an den relevanten Stellen so zu verbessern, dass ein sicherer, geschützter Raum für den Rechenzentrumsbetrieb entsteht. Der resultierende IT-Sicherheitsraum übertrifft in der Regel hinsichtlich seiner Widerstandsfähigkeit gegenüber typischen Gefahren für die IT die Eigenschaften von gemauerten Gebäuden und Gebäudeteilen.

Hierfür sorgt mitunter ein Elementkern aus thermisch wirksamer Dämmsubstanz, der von robusten, gekapselten Stahlblechkassetten umgeben ist. Dazu sollte sich eine Verbindungstechnik gesellen, die mittels temperatur- und feuchtigkeitsbeständigen Profilen und Dichtungen zusammen mit Brandschutzklappen für hohe Temperatur- und Feuchtigkeitstoleranz sorgt.

Hieran schließen sich dann die Mechanismen gegen HF-Strahlung an: Jedes elektronische Gerät strahlt mehr oder weniger starke elektromagnetische Wellen ab. Diese Abstrahlung ist als Störstrahlung bekannt und ihre maximal zulässige Stärke ist im Allgemeinen gesetzlich geregelt. In Deutschland ist dafür das Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) anzuwenden. Dort wird die EMV-Strahlung wie folgt definiert: „Die elektromagnetische Verträglichkeit ist die die Fähigkeit eines Betriebsmittels, in seiner elektromagnetischen Umgebung zufriedenstellend zu arbeiten, ohne elektromagnetische Störungen zu verursachen, die für andere in dieser Umgebung vorhandene Betriebsmittel unannehmbar wären."

Einhalten von Grenzwerten ist nicht hinreichend

Informationsverarbeitende Geräte wie Computer, Switche oder Router strahlen über diese elektromagnetische Strahlung Hinweise auf die gerade verarbeiteten Informationen ab. Diese informationstragende Abstrahlung wird auch bloßstellende Abstrahlung genannt. Wenn ein Angreifer die bloßstellende Abstrahlung in einiger Entfernung, beispielsweise in einem Nachbarhaus oder auch in einem in der Nähe abgestellten Fahrzeug empfängt, kann daraus häufig die Information rekonstruiert werden und die Vertraulichkeit der Daten ist nicht mehr gewährleistet.

Die Grenzwerte der EMV-Normen reichen im Allgemeinen nicht aus, um das Abhören der bloßstellenden Abstrahlung zu verhindern. Gerade

deswegen müssen in Rechenzentren und vor allem in IT-Sicherheitsräumen zusätzliche Maßnahmen getroffen werden, um die HF-Strahlung so stark wie möglich einzudämmen.

Die Normung zur EMV legt für Produkte und Umgebungsbereiche Grenzwerte der Störaussendung in definierten Frequenz- und Feldstärkebereichen fest, zum Beispiel in DIN EN 55022 (VDE 0878-22):2011-12. Das System aus diesen Grenzwerten und den in DIN EN 55024 (VDE 0878-24):2011-09 beschriebenen abgestuften Anforderungen zur Störfestigkeit von Informationstechnischen Einrichtungen stellt im alltäglichen Betrieb die elektromagnetische Verträglichkeit zwischen Geräten aller Arten und den IT-Einrichtungen weitestgehend sicher.

Für natürlich entstehende Felder wie LEMP (Lightning Electro Magnetic Pulse), ebenso wie für künstlich hervorgerufene impulsförmige Hochfrequenzfelder, gibt es keine normativ festgelegten Schutzanforderungen. Es sind jedoch zum Abschätzen des Gefährdungspotentials Bedrohungswerte beschrieben, beispielsweise in der Norm VG 95371-10:2011-09 (für „Verteidigungs-Geräte“).

Komplette Schirmung

Zusätzlich muss bei hohem oder sehr hohem Schutzbedarf in Bezug auf die Vertraulichkeit geprüft werden, ob der Einsatz abstrahlarmer oder abstrahlgeschützter Geräte zweckmäßig oder sogar erforderlich ist. Dafür sind die sogenannten „TEMPEST“-Kriterien verantwortlich, die abstrahlgeschützte Geräte erfüllen müssen. Eine Liste von entsprechenden Herstellern und Geräten findet sich auf der Webseite des BSI in der offiziellen Produktübersicht BSI TL 03305. EMV in diesem Sinne umfasst übrigens keine Beeinflussung biologischer Systeme. Ob und ab welcher Stärke die Strahlung für Menschen schädlich ist, wird durch andere Normen definiert, unter anderem die Richtlinie 2004/40/EG zur EMF (EMVU) zum Schutz von Arbeitnehmern vor elektromagnetischen Feldern.

Abstrahlung zu verhindern oder zu vermindern bedeutet immer Schirmung. Ein komplett geschlossener metallischer Raum lässt keine Strahlung nach außen durch, das Problem der bloßstellenden Abstrahlung gibt es nicht. Die Schirmung einer schlitzfreien elektrisch leitenden Hülle beruht (nach einer einfachen Modellvorstellung) im hochfrequenten elektromagnetischen Feld auf Absorption. In der leitenden Schirmschicht werden Ladungsträger verschoben, was Ausgleichsströme bedeutet, die durch den Widerstand im Material der Hülle in Wärme umgewandelt werden.

Abschätzung zuverlässig vornehmen

Der Stromverdrängungseffekt (Skin-Effekt) bewirkt, dass die Ausgleichsströme – in Abhängigkeit vom Schirmmaterial und dem Frequenzspektrum des auftreffenden Feldes – nur bis zu einer berechenbaren Eindringtiefe geführt werden. Somit kann bei ausreichender Schirmdicke das Feld nicht in den Innenraum einkoppeln und von innen nach außen abstrahlen. Doch IT-Sicherheitsräume benötigen selbstverständlich Zugänge. Wandelemente müssen für die Installation und für spätere Änderungen abnehmbar sein, ausreichend große Türen sind ebenfalls notwendig, um den Zugang für die Hardware und Bedienpersonal zu erlauben. Negativ wirken sich zusätzlich Ausbrüche für Einbauelemente, Klimatisierungsmaßnahmen oder Sichtflächen aus sowie die eingeschränkte elektrische Leitfähigkeit der Materialien durch Korrosionsschutz.

Für einen IT-Sicherheitsraum ist in der Realität also ein Kompromiss erforderlich. Die Öffnungen in der Außenhülle müssen so klein wie

Quelle: Rittal

Für einen IT-Sicherheitsraum lässt sich eine existierende Gebäudeinfrastruktur nutzen und so verbessern, dass ein sicherer, geschützter und nach ECB-S-Regeln zertifizierter Raum für den RZ-Betrieb entsteht.

Quelle: Rittal

Die Schirmwirkung verbessert sich unter anderem, wenn mehr Befestigungspunkte für Wände und Scharnier- und Verschlussdruckpunkte für Türen vorhanden sind.

Quelle: Rittal

Auch die Aneinanderreihung von mehreren Sicherheitsräumen ist möglich. Hier befinden sich drei nebeneinanderliegende Technikbereiche in Grundschutzräumen.

möglich sein und den spezifischen Ausbreitungseigenschaften von hochfrequenten Schwingungen entgegenwirken. Dabei lautet ein Grundsatz: Je größer die schlecht geschirmte Öffnung, umso eher fällt die Schirmwirkung im betrachteten Frequenzbereich zu niedrigeren Werten ab. Bei rechteckige Öffnungen/Fugen ist hier die längste Seite zu betrachten, bei runden Öffnungen der Durchmesser.

Die charakteristischen Merkmale eines elektromagnetischen Feldes, das von einer IT-Einrichtung abgestrahlt wird oder von außen auf die IT-Einrichtung einwirken kann, sind in der Frequenz/dem Frequenzbereich und der Feldstärke gegeben. Meistens wird die elektrische Feldstärkekomponente, das E-Feld, in V/m zur Bewertung der Schirmung von elektromagnetischen Feldern mit Frequenzen oberhalb 30 MHz bis 3 (10) GHz herangezogen. Eine Abschätzung lässt sich vornehmen mit:

a = 20 log E0/E1

Bei der größten Länge l einer ungeschirmten Öffnung und der höchsten betrachteten Frequenz/kürzesten Wellenlänge ? gilt für l > ?/20: Schirmdämpfung a < 20 dB. Das heißt, zum Beispiel bei 1 GHz (0,3 m Wellenlänge) sinkt bereits bei einem Öffnungsdurchmesser von 1,5 cm die Schirmdämpfung unter 20 dB (und damit um den Faktor zehn).

Je höher die Frequenz des auftreffenden elektromagnetischen Feldes ist, desto negativer wirken sich Öffnungen in der Hülle aus. Daher sind einige Punkte wie das Verwenden spezieller Dichtungen und Kabeldurchführungen oder der Einsatz von Filter-Steckverbindern zu beachten. Grundsätzlich bestimmt dabei die konstruktive Ausführung des Dichtungssystems weitgehend die Schirmdämpfung. Je mehr Befestigungspunkte für Wände und Scharnier- und Verschlussdruckpunkte für Türen vorhanden sind und je gleichmäßiger damit der Anpressdruck und der Kontakt (niedrige Impedanz) von Hülle und Tür/Deckel entlang den Dichtungen sind, umso näher kommt man dem Ideal.

Höheren EMV-Schutz gewinnen

Leitende Spezialdichtungen aus Metallgewebe auf Schaumstoffkörper als Kombinationsdichtungen für EMV und IP-Schutzart erreichen hohe Schirmdämpfungswerte im Frequenzbereich bis 1 GHz oder darüber hinaus. Sie verbinden die metallisch-blanken Innenflächen von Türen und abnehmbaren Wänden, Dach- und Bodenblechen mit den metallisch-blanken Dichtkanten des Gehäusekörpers oder -gerüsts. Für die Kosten-Nutzen-Abwägung hat sich diese Methode als beste Lösung erwiesen. Alternativ können bei Neukonstruktionen oder bei besonders hohen Anforderungen stark überlappende Flächen und eine Trennung von EMV- und mechanischer (Umwelt-) Dichtung vorgesehen werden, wobei als EMV-Dichtung auch metallische Federdichtungen mit ihren besonderen Eigenschaften wählbar sind.

Durch bedarfsgerechte Maßnahmen können für IT-Sicherheitsräume Schirmdämpfungswerte von bis zu 60 dB im Frequenzbereich von 30 MHz bis 3 (10) GHz und damit ein erhöhter EMV-Schutz mit angemessenem Aufwand realisiert werden. Anforderungen mit darüber hinaus gehenden Schirmdämpfungswerten oder einem weiteren Frequenzbereich lassen sich nur mit erheblichem konstruktiven Einsatz erfüllen und sind nur in besonders sicherheitsrelevanten Anwendungen sinnvoll und vertretbar.

Schirmung beurteilen

Bei leeren Gehäusen oder IT-Sicherheitsräumen sind quantitative Urteile wenig aussagekräftig, da die Installation des elektrotechnischen Systems mit seinen Versorgungsleitungen, Klimatisierungsöffnungen und Sichtflächen die Schirmdämpfung stark beeinflusst. Trotzdem eignen sich verschiedene Messungen, um einen Anhaltspunkt für die Qualität der Schirmung zu gewinnen. Schirmdämpfungsmessungen sind nach mehreren Verfahren möglich, neben VG 95373, Teil 15, Messverfahren für Kopplungen und Schirmungen (Verteidigungsgerätenorm) auch die EN 61000-5-7, Schutzarten durch Gehäuse gegen elektromagnetische Störgrößen (mit Klassifizierung der Messergebnisse durch EM-Code) sowie IEC TS 61587-3, für Gehäuse für Elektronik-Anwendungen (mit Klassifizierung der Anforderungen durch „Performance Level“).

Hartmut Lohrey,
Leiter Marketing Training Support, Rittal

UNTERSTÜTZENDE MASSNAHMEN: ABSTRAHLARME GERÄTE

Häufig findet sich auf IT-Geräten der Begriff „abstrahlarm“ nach MPR II, TCO oder SSI. Diese Richtlinien berücksichtigen jedoch ausschließlich mögliche gesundheitsschädliche Auswirkungen der Gerätestrahlung. Sie stellen keine Bewertung der bloßstellenden Abstrahlung dar und dürfen nicht allein aufgrund dieses Siegels in Umgebungen mit hohem Schutzbedarf eingesetzt werden.

Es gibt aber durchaus speziell abstrahlgeschützte IT-Systeme. Diese Geräte wurden mit Hilfe eines detaillierten Konzepts des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geprüft. Ursprünglich wurde das Prüfkonzept des BSI zum Schutz staatlicher Verschlusssachen entwickelt. Aber auch die Privatwirtschaft profitiert vom hohen Sicherheitslevel entsprechend getesteter Geräte, wenn Daten mit hohem Schutzbedarf bezüglich Vertraulichkeit geschützt werden sollen.

Bei hohem oder sehr hohem Schutzbedarf in Bezug auf die Vertraulichkeit sollte deshalb geprüft werden, ob der Einsatz abstrahlarmer beziehungsweise abstrahlgeschützter Geräte zweckmäßig oder sogar erforderlich ist. Eine Liste solcher abstrahlgeschützter Geräte stelle das BSI auf seiner Webseite zur Verfügung (Produktübersicht BSI TL 03305).

Diversifikation zahlt sich aus

Schnelle und sichere Verbindungen zwischen Rechenzentren

Der Betrieb eines eigenen Rechenzentrums ist komplex – und schreckt oft ab. Umso attraktiver scheint es, den Betrieb auszulagern. Doch welche Punkte sind in diesem Fall zu beachten? Und wie lässt sich ein möglichst schneller Zugriff auf die ausgelagerten Daten herstellen?

Die Mehrheit der deutschen IT-Entscheider (83 Prozent) empfindet laut einer Umfrage das Planen einer RZ-Infrastruktur als komplex. Diese wahrgenommene Komplexität führt zu einer Unsicherheit, die dafür sorgt, dass die Entscheider mehr Zeit mit der Planung verbringen, als sie eigentlich sollten und sich strategische Entscheidungen entsprechend verzögern.

Doch wie setzt ein Unternehmen eine Rechenzentrumsstrategie auf? Grundsätzlich ist eine Reihe von Entscheidungen zu treffen, die Schritt für Schritt abgearbeitet werden können. Am Anfang steht die Entscheidung, ob man ein eigenes Rechenzentrum betreiben möchte oder die Daten auslagert. In Anbetracht der Entwicklung des Datenvolumens und des Datenverkehrs hat die Auslagerung vor allem in Hinblick auf die Investitionskosten Vorteile. Einem spezialisierten Rechenzentrumsbetreiber fällt es viel leichter, mit der Entwicklung der Speichertechniken, des Energiemanagements, der rechtlichen Vorgaben und weiterer Faktoren Schritt zu halten.

Auf den Standort kommt es an

Bei der Entscheidung für einen Anbieter und die Standorte sollte auch darauf geachtet werden, dass sogenannte carrierneutrale Rechenzentren genutzt werden. Das bedeutet, dass das Rechenzentrum an die Netzwerke verschiedener Anbieter angeschlossen ist. Das erhöht zum einen die Redundanz und Ausfallsicherheit, zum anderen ermöglicht es dem Unternehmen, unterschiedliche Dienstleister für Rechenzentrum und Netzwerk zu nutzen. Ein weiteres wichtiges Kriterium ist die Zahl der Drittrechenzentren, mit denen die Anlagen eines Anbieters verbunden sind. Die Verbindung zu vielen Rechenzentren über einen Netzprovider bietet eine höhere Flexibilität in der Auswahl von Standorten auch mit Blick auf die Zukunft, ohne dass dafür Verträge mit zusätzlichen Netzwerkprovidern erforderlich wären.

Datenschutz und Datensicherheit sind weitere wichtige Kriterien für die Rechenzentrumsstrategie, gerade in Hinblick auf gesetzliche Vorgaben und Compliance-Anforderungen. In diesem Bereich gibt es eine Reihe von Zertifizierungen, die bei der Auswahl eines Anbieters hilfreich sind. Neben dem technischen Standard der Einrichtung, den der TÜV mit der Tier Skala von II bis IV bewertet, gibt die „M&O“-Zertifizierung (Management & Operations) des Uptime Instituts Auskunft über die Führung und den Betrieb einer Anlage.

Daneben gibt es die DIN ISO 9001 als international anerkannten Qualitätsmanagementstandard und Nachweis für hochwertige Produkte und Dienstleistungen sowie die DIN ISO 27001, die die Einhaltung von Sicherheitsstandards zertifiziert. Das DQS-Zertifikat „Gütesiegel Datenschutz“ ist ein Nachweis über Gesetzeskonformität, Wirksamkeit und Angemessenheit der Datenschutz- und Datensicherheitsmaßnahmen. Das Testat PS 951 Typ B vom Institut der Wirtschaftsprüfer ist eine Prüfung des internen Kontrollsystems eines Dienstleisters für dorthin ausgelagerte Funktionen. Mit dem PCI-DSS schließlich bewertet die Kreditkartenindustrie die Sicherheit beim Bearbeiten von Kreditkartendaten.

Anbindung mit hoher Bandbreite

Eine zentrale Entscheidung betrifft die Anbindung der Rechenzentren. Für Unternehmen aus datenintensiven Branchen ist der Zugriff über das Internet nicht mehr zumutbar. Dabei mangelt es an Konnektivität, Bandbreite. Darüber hinaus genügt eine Internetanbindung auch nicht den Sicherheitsanforderungen, wie sie die oben beschriebenen Zertifizierungen verlangen.

Langsame, unzuverlässige und unsichere Verbindungen können aber katastrophale Folgen für die Unternehmen haben. Für einen Händler, der mit einer Promotion-Aktion Millionen von Kunden angesprochen hat, steht der Umsatz auf dem Spiel, für eine Bank beim Verlust von Kundendaten durch einen Hackerangriff die Reputation. Bei Buchungssystemen muss sichergestellt sein, dass Daten über räumlich verteilte Server zuverlässig und schnell abgeglichen werden. Wird beispielsweise in Hamburg ein Ticket verkauft, darf es auch in Berlin und allen anderen Verkaufsstellen nicht mehr zur Verfügung stehen, um Doppelbuchungen und die damit verbundenen Kosten und die Unzufriedenheit beim Kunden zu vermeiden. Der technische Schlüssel dazu ist das seit Jahren verwendete Carrier Ethernet. Mit Bandbreiten von 10 bis 100 Gigabit pro Sekunde erlaubt es die nahtlose Replikation großer Datenmengen zwischen verteilten Rechenzentren in Echtzeit.

Datenverkehr selbst lenken

Sind die ausgewählten Rechenzentren dank Carrier Ethernet mit entsprechender Bandbreite verbunden, lässt sich der Datenverkehr zwischen den verschiedenen Einrichtungen optimal lenken und an Lastspitzen anpassen. Das kann der Weihnachtsverkauf im Online-Handel sein, der Monatsabschluss bei einer Bank oder Versicherung oder der Ansturm auf die Tickets begehrter Künstler.

Aktuell wird der Datenverkehr noch vom Provider gelenkt. Das wird sich künftig ändern. Beim Software-defined Networking wird die Administration von der Hardware in die Software verlagert. Diese Software wird immer intuitiver, sodass Self-Service-Portale für die Anwender nur noch eine Frage der Zeit sind. Dort können sie den Datenverkehr in Echtzeit selbst lenken und zahlen wie bei der Cloud nur noch für den Verbrauch.

Matthias Hain,
Director Bandwidth & Ethernet Services, Colt

MPLS im Gespann

Weitverkehrsnetze um kostengünstige Internet-Verbindungen erweitern

Viele unternehmensweite Weitverkehrsnetze und RZ-Anbindungen basieren auf Multi-Protocol Label Switching (MPLS). Diese Technik ist jedoch teuer, wenig flexibel und nur unzureichend für Techniken wie Cloud Computing ausgelegt. Eine Alternative bieten Software-Defined WAN auf Grundlage von kostengünstigen Breitband-Internetverbindungen. Beide Technologien lassen sich zu einem Hybrid-WAN kombinieren.

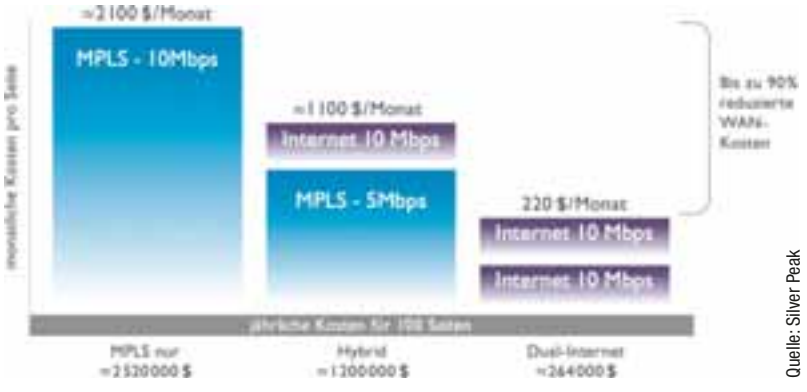
Viele unternehmensweite Weitverkehrsnetze basieren immer noch auf Multi-Protocol Label Switching (MPLS). Exakte Daten dazu, wie viele Enterprise-WANs diese Technik verwenden, sind Mangelware. Die amerikanische Marktforschungsgesellschaft Nemertes Research hat ermittelt, dass kleinere Unternehmen (40 Prozent) ausschließlich Internet-basierte WAN-Verbindungen nutzen. Unter den Großkonzernen sind es 25 Prozent, bei Mittelständler etwa 14 Prozent. Somit hat MPLS im Enterprise-Segment noch einen großen Marktanteil.

Ein MPLS-WAN wird meist von einem Service-Provider auf dessen eigener Netzwerk-Infrastruktur bereitgestellt. Das resultiert in einem hohen Sicherheitsniveau, weil der Service-Provider die Kontrolle über das Netz und die Vermittlungssysteme hat. Als weitere Pluspunkte führen MPLS-Anbieter die hohe Verfügbarkeit von 99,9 Prozent an, außerdem die Quality-oft-Service- und Class-of-Service-Funktionen (QoS, CoS).

Für jede Anwendung im Enterprise WAN lässt sich somit eine bestimmte Dienstgüte festlegen. Dadurch ist es beispielsweise möglich, Anwendungen mit hohen Anforderungen an die QoS wie Voice over IP oder Zugriffen auf Online-Transaktionsdatenbanken Vorrang vor E-Mails und Filetransfers einzuräumen.

Allerdings sehen sich Enterprise-Weitverkehrsnetze, die auf MPLS basieren, mit etlichen Herausforderungen konfrontiert. Dadurch wächst der Bedarf an preisgünstigen Alternativen zu MPLS. So liegen die Kosten eines Internet-basierten Enterprise WAN je nach Wirtschaftsregion um den Faktor 40 und mehr unter denen von MPLS-WAN-Strecken.

Dazu ein Beispiel: Ein Unternehmen mit 13 kleineren Außenstellen muss in den USA monatlich mit rund 9200 Dollar Verbindungsgebühren für eine MPLS-Infrastruktur rechnen. Nutzt dasselbe Unternehmen Breitband-Internet-Verbindungen, sind es etwa 1550 Dollar. Für die Kopplung zwei großer Standorte fallen pro Monat 15 000 Dollar bei MPLS an, rund 8000 Dollar WAN-Verbindungen via Internet.



Quelle: Silver Peak

Vergleich der Kosten zwischen MPLS- und Breitband-Internet-Verbindungen in San Francisco von Ende 2014.

Rechenzentren werden zum „Flaschenhals“

Hinzu kommt, dass eine wachsende Zahl von IT-Diensten und Anwendungsszenarien Internet-Verbindungen erfordern. Dazu zählen Mitarbeiter, die von unterwegs oder dem Home Office aus über mobile Endgeräte wie Smartphones, Tablet-Rechner und Notebooks auf Anwendungen im Unternehmensnetz zugreifen. Besonders kritisch ist die Situation bei Cloud-Diensten. Denn Cloud-Service-Provider stellen in der Regel ihre Dienste nur über Internet-Links zur Verfügung.

Zudem macht sich in diesem Fall die Backhaul-Struktur eines MPLS-Enterprise-WAN negativ bemerkbar: Greift ein Mitarbeiter über das Unternehmensnetze auf einen Cloud-Dienst zu, wird der gesamte Datenverkehr zunächst über die MPLS-Infrastruktur zu einem Unternehmensrechenzentrum übermittelt. Von dort aus erfolgt die Weiterleitung in das Internet. Der Grund für diese Art Umweg ist, dass meist nur das zentrale Datacenter oder wenige kleinere Rechenzentren in einem MPLS-WAN über eine Anbindung zum Internet verfügen.

Hier kommt ein weiterer Faktor ins Spiel: die mangelnde Flexibilität von MPLS-Netzen. So kann es bis zu 45 Tage dauern, bis ein Service-Provider eine MPLS-Verbindung der Kategorie E1/T1 (2,048 MBit/s beziehungsweise 1,544 MBit/s) bereitstellen kann. Nach Praxiserfahrungen von Silver Peak müssen Unternehmen bei Verbindungen mit noch höheren Bandbreiten bis zu sechs Monate Wartezeit veranschlagen. Technologien wie Big-Data-Analysen, Cloud Computing und die flexible Anbindung neuer Standorte erfordern jedoch eine WAN-Infrastruktur, die sich schnell an neue Anforderungen anpassen lässt – am besten innerhalb weniger Stunden.

Transfer von Virtual Machines über das WAN

Die aktuelle Situation sieht jedoch anders aus. So schätzt die Beratungsgesellschaft Gartner, dass in den kommenden Jahren der Bandbreitenbedarf in einem typischen Enterprise WAN um 28 Prozent pro Jahr steigt, vor allem wegen der zunehmenden Nutzung von Cloud-Diensten und mobilen Endgeräten. Bereits heute (2015) leiden laut Gartner 50 Prozent der Cloud-Dienste, die Unternehmen einsetzen, un-

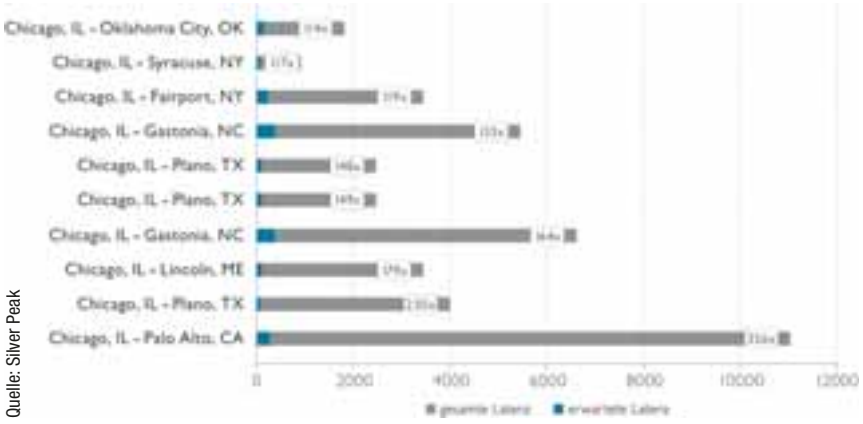
ter Performance-Engpässen der WAN-Infrastruktur.

Ein hoch flexibles WAN ist nach Angaben des amerikanischen Beratungsunternehmens ZK Research aus einem weiteren Grund erforderlich: der Entwicklung hin zum „Location-Independent Computing“ (LIC). Das heißt, Daten, Anwendungen und virtualisierte Ressourcen (Virtual Machines) werden im Unternehmensnetz dorthin verlagert, wo sie den optimalen Nutzen für Anwender bringen. Das kann ein Unternehmensrechenzentrum sein, aber auch ein Cloud-Datacenter in der Nähe eines Unternehmensstandortes oder die Außenstelle eines Unternehmens.

Mithilfe eines Breitband-WAN auf Basis von Internet-Verbindungen lässt sich die erforderliche Bandbreite dagegen schnell und kostengünstig bereitstellen. Vor diesem Hintergrund bietet es sich an, im Enterprise WAN zwei Techniken zu kombinieren:

- Ein Breitband-WAN auf Grundlage des Internets: Für weniger zeit- und unternehmenskritische Daten und Anwendungen oder Cloud-Services stehen Internet-Verbindungen bereit. Zudem stehen sie in vielen Regionen der Welt zur Verfügung, auch dort, wo keine MPLS-Links vorhanden sind.
- MPLS: Zeitkritische Applikationen, die eine garantierte Dienstgüte benötigen, sowie geschäftskritische Anwendungen nutzen die MPLS-Infrastruktur. Dazu zählen SAP-Applikationen, Online-Transaktionsverarbeitung, Voice und Video over IP sowie Unified Communications.

Das Resultat ist ein Hybrid WAN, das die klassische MPLS-Infrastruktur mit Internetverbindungen zu einem integrierten Weitverkehrsnetz zusammenfasst. Eine solche Infrastruktur bietet einen weiteren Vorteil: Hohe Ausfallsicherheit, weil zwei unterschiedliche Infrastrukturen verwendet werden, die zudem in der Regel von separaten Service-Providern betreut werden (Multi-Provider-Netzwerkstruktur). Zudem lassen sich die Kosten reduzieren, weil die MPLS-Links von Internet-Datenverkehr entlastet werden.



Quelle: Silver Peak

Die Latenzzeiten von Enterprise-WAN-Verbindungen auf Basis von Internet-Links sind nach Messung höher als erwartet, was sich unter anderen auf VoIP negativ auswirkt.

Das normale Internet reicht nicht aus

Allerdings wäre es wagemutig, würde ein Unternehmen für eine hoch kritische Ressource wie ein Hybrid-WAN auf das herkömmliche Internet zurückgreifen. Ein Grund sind die hohen Latenzzeiten der Internet-Verbindungen. Messungen von Silver Peak bei Internet-WAN-Verbindungen in den USA ergaben beispielsweise, dass die Verzögerungszeiten teilweise bis um den Faktor 300 höher lagen, als angesichts der Distanz zwischen den Messpunkten zu erwarten war.

Um solche Schwachpunkte der Internet-basierten Komponente von Hybrid-WANs zu kompensieren, können Unternehmen beispielsweise auf WAN-Optimierungslösungen zurückgreifen. Sie nutzen diverse Techniken, um IP-Pakete schneller und zuverlässiger über Internet-Verbindungen zu transportieren. Dazu zählt das Komprimieren und Zwischenspeichern (Caching) von Daten. Verfahren für die Optimierung der Latenzzeit sind unter anderem ein Messen der Round Trip Time (RTT) der Datenpakete und eine Überlastkontrolle (Congestion Control).

Um die Paketverlustrate zu minimieren, setzten WAN-Optimierungssysteme Verfahren wie Forward Error Correction (FEC) ein. Dabei wird zusammen mit einer bestimmten Zahl von Paketen ein Fehlerkorrektur-Paket übertragen. Die Netzwerksysteme beim Empfänger sind mithilfe dieses Pakets in der Lage, Datenpakete zur rekonstruieren, die ein Router oder Switch „weggeworfen“ hat.

Lösung: Ein Software-Defined WAN

Einen Ausweg bietet ein Software-Defined WAN (SD-WAN). Es besteht aus einem sicheren Overlay-Netzwerk (SD-WAN Fabric), das folgende Anforderungen erfüllt:

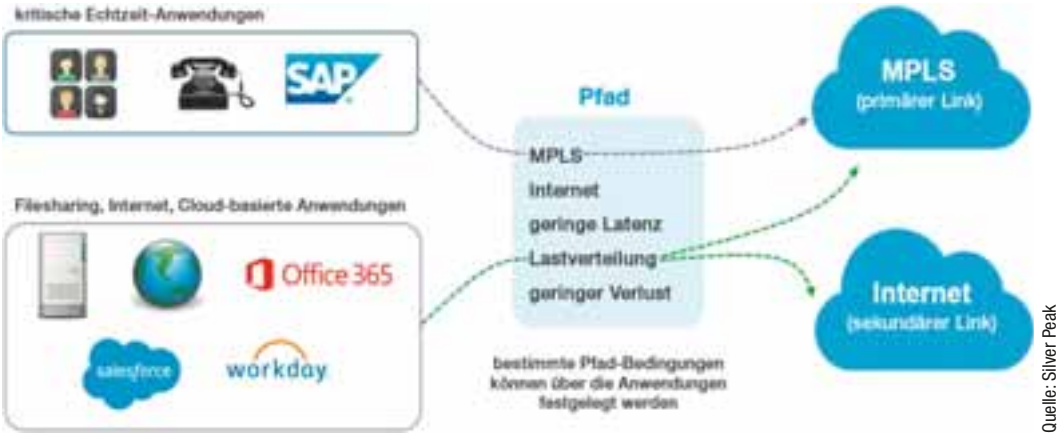
- Es muss unterschiedliche Connectivity-Arten unterstützen, beispielsweise über DSL- und Breitband-Mobilfunkverbindungen sowie Glasfasernetze.
- Es sollte Systemverwaltern die Möglichkeit geben, alle Anwendungen zu erkennen und zu kontrollieren.
- Es muss Nutzern eine konsistente Performance zur Verfügung stellen.
- Und es sollte Sicherheitsfunktionen bieten, beispielsweise das Abwickeln von Datenverkehr durch 256-Bit-SSL-Tunnel.

Eine zentrale Funktion eines Hybrid-Weitverkehrsnetzes, in dem Internet- und MPLS-Verbindungen gemeinsam genutzt werden, ist eine automatische Pfadkontrolle (Dynamic Path Control, DPC). Mit ihr lässt sich steuern, welche Daten über welche Weitverkehrs-Links transportiert

CLOUD-DIENSTE IN DEUTSCHLAND

Cloud Computing ist ein Faktor, der den Einsatz von Internet-basierten Weitverkehrsverbindungen fördert. In Deutschland setzen laut der Studie Cloud-Monitor 2015 des deutschen Digitalverbandes Bitkom und der Beratungsgesellschaft KPMG bereits 70 Prozent der Großunternehmen Cloud-Computing-Services ein. Von den mittelständischen Unternehmen sind es mehr als 50 Prozent. Insgesamt nutzten 2014 an die 44 Prozent der Unternehmen in Deutschland Cloud-Dienste, weitere 24 Prozent planen dies in naher Zukunft.

Vor allem Hybrid-Clouds erfreuen sich in der Deutschland besonderer Beliebtheit. In Deutschland nutzten laut IDC im Jahr 2014 rund 15 Prozent der Unternehmen diese Form der Cloud. Weitere 54 Prozent wollen das bis 2016 tun. Auf Cloud-Services greifen Nutzer in der Regel über Internet-Verbindungen zu. MPLS-basierte Enterprise WANs eignen sich dafür weniger, unter anderem deshalb, weil Cloud-Service-Provider diese Form der Anbindung an ihre Rechenzentren in der Regel nicht unterstützen.



Ein Hybrid-WAN mit MPLS- und Internet-Verbindungen: MPLS für kritische Anwendungen, kostengünstigere Zugänge für Cloud-Applikationen wie Office 365

Quelle: Silver Peak

werden. Für zeitkritische Daten wie VoIP oder Video kann ein Administrator beispielsweise festlegen, dass sie über WAN-Links mit besonders niedrigen Latenzzeiten und Paketverlustraten laufen. Außerdem lassen sich für bestimmte Anwendungen und Daten feste Pfade vorgeben.

Eine solche SD-WAN Fabric kann auf Appliances basieren, die an den Unternehmensstandorten und bei Service-Provider platziert werden. Diese Systeme ermitteln in Echtzeit, welcher Pfad durch das Internet oder die Netzwerkinfrastruktur eines Providers der optimale ist und lenken den Datenverkehr über die adäquaten Links.

Vorteil Hybrid

Eine Hybrid-Infrastruktur hat für den Nutzer mehrere Vorteile. So profitiert er weiterhin von den Vorzügen eines MPLS-Netzes. Geschäftskritische Anwendungen können somit weiterhin über Multi-Protocol Label Switching bereitgestellt werden.

Für den Zugriff auf Internet-basierte Applikationen, beispielsweise Cloud-Anwendungen wie Office 365 oder Salesforce.com, kommen dagegen preisgünstige lokale internet-Zugänge mit hoher Bandbreite zum Zuge. Solche lokalen „Break-outs“ erlauben es Unternehmen, auch abgelegene Standorte durch regionale oder lokale Internet-Service-Provider in das Enterprise WAN einzubeziehen.

Der Anwender hat im zweiten Schritt die Möglichkeit, das MPLS-Netz zugunsten eines Internet-basierten SD-WANs zu verkleinern. Dieser Trend zeichnet sich derzeit nach Angaben der Marktforschungsgesellschaft Gartner vor allem bei Unternehmen ab, die mehrere Standorte unterhalten. Durch das „Offloading“ von bandbreitenintensiven Internet-Anwendungen werden kostspielige MPLS-Verbindungen entlastet. In der Praxis lassen sich mithilfe dieses Verfahrens bis zu 70 Prozent der Bandbreite der MPLS-Verbindungen einsparen.

Tony Thompson,
Vice President Marketing, Silver Peak

Impressum
Themenbeilage Rechenzentren und Infrastruktur

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v. i. S. d. P.), Uli Ries (089 68092226)

Autoren dieser Ausgabe:
Roland Freist, Matthias Hain, Thorsten Henning, Dr. Peter Koch, Hartmut Lohrey, Ariane Rüdiger, Tony Thompson, Ronald Timmermans

DTP-Produktion:
Enrico Eisert, Kathleen Tiede, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

Technische Beratung:
Uli Ries

Titelbild:
kubais, shutterstock

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung:
Beate Gerold

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Die Inserenten

DENKEN SIE WEITER.

ALS HEFT ODER DIGITAL

3 Ausgaben Technology Review mit 34% Rabatt testen und Geschenk erhalten.

IHRE VORTEILE ALS ABONNENT:

- **VORSPRUNG GENIESSEN.**
  Früher bei Ihnen als im Handel erhältlich.
- **PREISVORTEIL SICHERN.**
  Mehr als 34 % Ersparnis im Vergleich zum Einzelkauf während des Testzeitraums.

WÄHLEN SIE IHR GESCHENK!

Zum Beispiel:
koziol Kaffeebereiter

GRATIS

Mit UNPLUGGED von Koziol wird die Kaffeezubereitung wieder richtig zelebriert und jede Tasse kann nach eigenem Gusto zubereitet werden.

JETZT AUCH KOMPLETT DIGITAL:

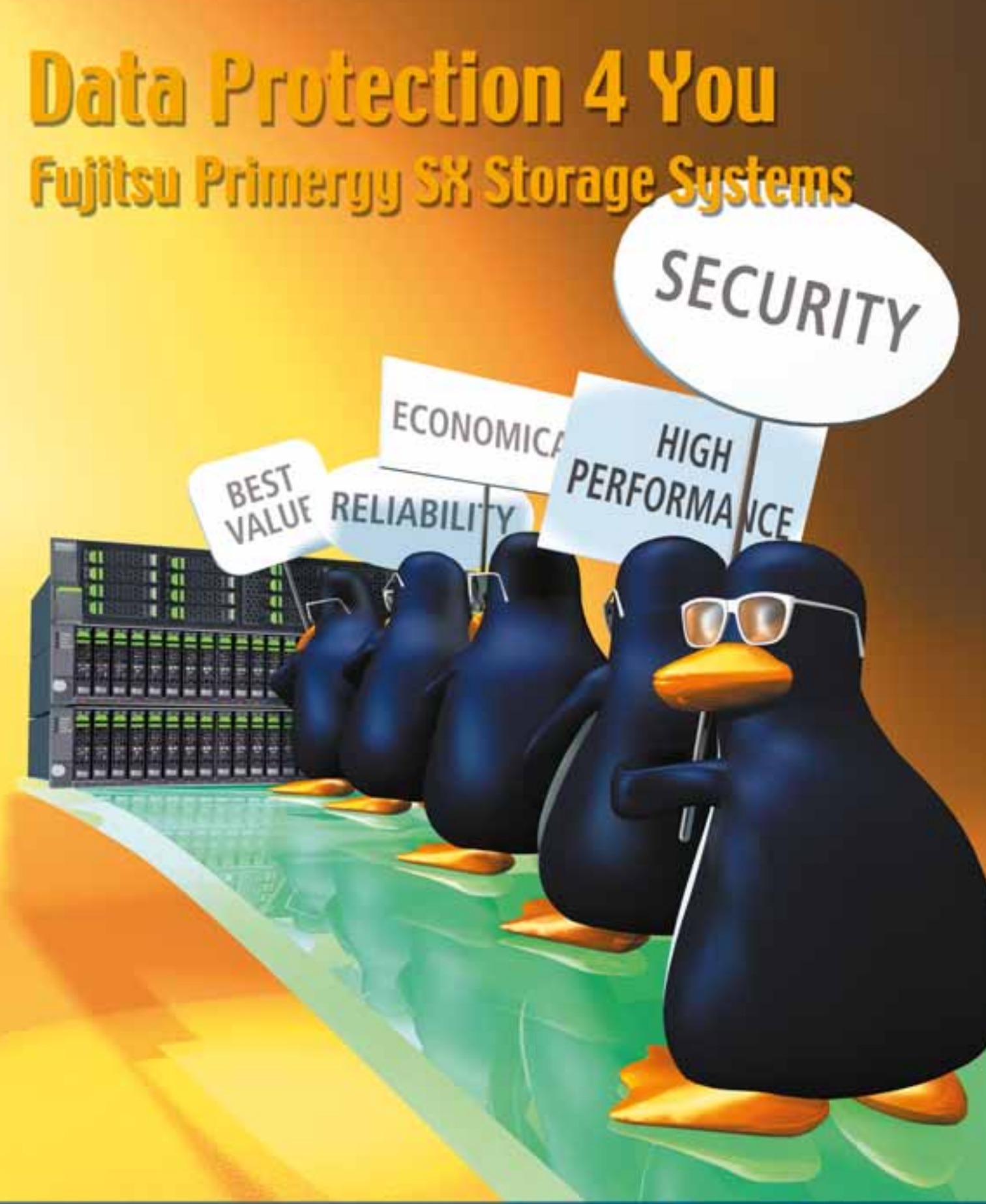
- Bequem auf Ihrem Tablet oder Smartphone
- Für Android, iOS oder Kindle Fire

Jetzt bestellen und von allen Vorteilen profitieren:

WWW.TRVORTEIL.DE

Data Protection 4 You

Fujitsu Primergy SX Storage Systems



The Informatics Network

BYTEC GmbH Tel. 07541/585-0 www.bytec.eu

bytec