Eine Themenbeilage der
Heise Medien GmbH & Co. KG

IV
2015

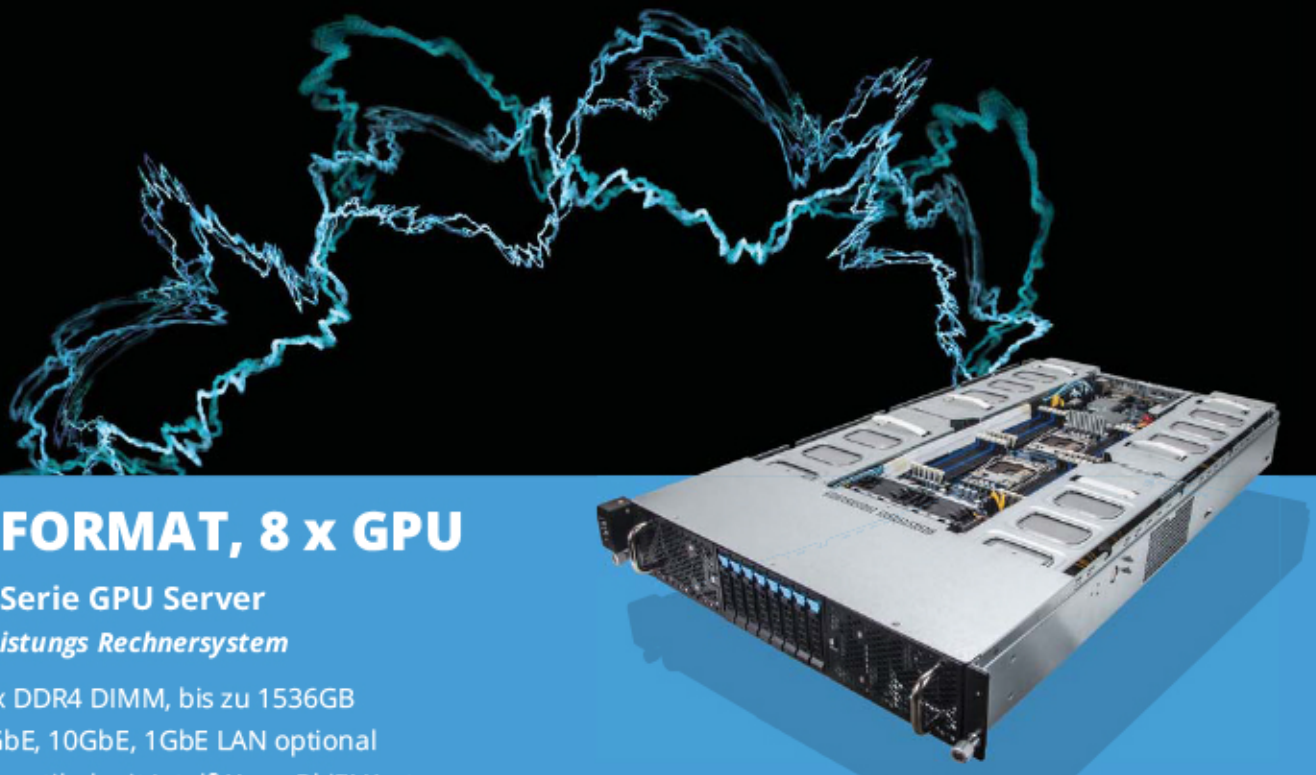
RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Wo der Kampf um Datenhoheit entschieden wird

powered by:

GIGABYTE™



2U FORMAT, 8 x GPU

G250 Serie GPU Server

Hochleistungs Rechnersystem

- 24 x DDR4 DIMM, bis zu 1536GB
- 56GbE, 10GbE, 1GbE LAN optional
- Kompatibel mit Intel® Xeon Phi™ Karten

Erhältlich bei:

MICROTRONICA A DIVISION OF ARROW

CTT HOME OF STORAGE

b2b.gigabyte.com

Mit Intel® Xeon® E5-2600 V3 Prozessor

Intel Inside®. Leistungsstarke Lösungen Outside.

intel XEON inside

Wo der Kampf um Datenhoheit entschieden wird

Es sollen herrliche Zeiten sein. Mit softwaredefinierten Netzwerken (SDN), die völlig frei an die Cloud anzuschließen und nahezu vollständig elastisch sind. Provider könnten damit ihre Lasten noch eleganter verschieben, ihre Ressourcen optimal verteilen und zugleich an Trends anschließen, die unter dem Namen „Internet of Things“ (IoT) mit umfassender Vernetzung drohen. Allerdings bricht damit die Virtualisierung auf einer neuen Ebene in die Rechenzentren ein, was einen deutlich schärferen Grad an Automatisierung und neue Sicherheitskonzepte erfordert – eben weil das System dann sehr viel offener ist. Frank Beckereit erörtert in seinem Schwerpunktbeitrag (S. 11), ob sich das lohnt – und zu welchem Preis. Ein konkretes SDN-Sicherheitskonzept legt dazu Christian Hentschel auf den Tisch (S. 16). Die Schlüsselrolle spielen dabei Next-Generation Firewalls, deren Regelsätze dank vorausgegangener Mikrosegmentierung mit jedem verschobenen Baustein mitwandern.

In jedem Fall lösen sich die physischen Komponenten damit nicht in Luft auf. Moderne Multimode-LWL bis 100 MBit müssen mit dem Traffic fertigwerden. Das können sie aber nur, wenn die Lichtleistung nicht in der Dämpfung verschwindet. Das auszuloten und den kritischen Stecker dingfest zu machen, ist mittlerweile ein eigenes Kunststück. Die Encircled-Flux-Metrik, erklärt Wilfried Schneider, kann dabei wertvolle Dienste leisten: Mit ihrer Hilfe lassen sich die sonst heftigen Messabweichungen auf unter 10 % drücken (S. 6).

Die zweite Großgruppe von Beiträgen berichtet direkt aus der Praxis. Der erste betrifft Data Center, die auf absehbare Zeit eine Großbaustelle in der Nachbarschaft haben. Dann nämlich stellen die Erschütterungen ein beträchtliches Risiko für den Betrieb der eigenen Anlagen dar, von der Haftungsfrage bei Ausfällen einmal ganz abgesehen. Das Team aus Friederike Busch, Markus Löffler und Andreas Gömmel stellt als Alternative zum Standardverfahren, das anfällig für (teure) Fehlalarme ist, ein erprobtes Monitoring-System vor, das im Vorfeld kalibriert und je nach Baufortschritt weiter betreut wird (S. 12). Mehrstufig angesetzte Grenzwerte lösen nicht erst den roten Alarm aus, sondern warnen die Arbeiter bereits, wenn sie mit ihren Maschinen ins Orange rumpeln.

Im zweiten Anwenderbeitrag schildert Simon Federle einen ungewöhnlichen Neubau: ein Rechenzentrum in den Speicherräumen eines aktiven Umspannwerks (S. 20). Stromversorgung und Gebäudesicherheit sind 1A, doch knapp einen Meter unter dem Boden fließen bis zu 1.000 Ampere und bauen ihr eigenes Magnetfeld auf. Dennoch verging vom ersten Auftrag bis zur Inbetriebnahme kein halbes Jahr.

Eine gute Nachricht haben wir noch zum Schluss: Das für produzierende Unternehmen verpflichtende Energieaudit gemäß DIN EN 16246-1 ist lästig, muss aber kein Angstgegner sein. Wer ein IT-gerechtes Energiemanagement samt Klimatisierung aufsetzt, sagt Karl-Heinrich Spiering, spart Stromkosten und kann die Untersuchung getrost auf sich zukommen lassen (S. 22). Und wer jetzt schon wissen will, wie die eigenen Systeme im Branchen- und Größenvergleich abschneiden, kann sich die Benchmark-Abfrage „Optimized Data Center“ vormerken, die wir auf S. 4 vorstellen. Außerdem hat Ariane Rüdiger – apropos Green IT – nachgesehen, wohin der nordamerikanische Markt geht. Speziell in Kalifornien können die Rechenzentren jedenfalls nicht so weiterwirtschaften wie bisher. Das Fazit: Die neuen US-Regularien könnten durchaus eine Chance für deutsche Effizienztechnik sein.

So scheint es zwar, als würde der bereits voll entbrannte Kontinentalkampf um die Datenhoheit auf der Facebook-Oberfläche von Smartphones ausgetragen. Entschieden wird er wohl eher ganz im Inneren: in den Rechenzentren. Wir informieren Sie weiter und wünschen eine anregende Lektüre.

Thomas Jannot

Potenzialanalyse in 90 Minuten

Wie schneidet das eigene Rechenzentrum im Vergleich mit anderen ab?

Rasant wachsende Datenvolumina und neue Sicherheitsrisiken geraten zum Dauerstresstest für Server, Speicher und Anbindung. Optimized Data Center heißt die systematische Benchmark-Abfrage, die aufzeigen kann, wo bei Management, Anbindung und Infrastruktur noch mehr herauszuholen wäre.

Optimized Data Center ist ein von der techconsult GmbH in Partnerschaft mit iX und Zusammenarbeit mit RZ-Experten entwickeltes Benchmark-System, welches Stück für Stück durch die verschiedenen Bereiche des Rechenzentrums führt. Dabei werden die für die jeweilige Sektion relevanten Prozesse und Aspekte evaluiert.

So entsteht die Möglichkeit, sich mit gleichartigen Unternehmen bezüglich ihres Rechenzentrums oder Serverraums zu vergleichen: angefangen beim Rechenzentrumsbetrieb über die physische und virtuelle IT-Infrastruktur bis hin zur Erfassung der Gebäudeinfrastruktur und der externen Anbindung. Jeder dieser Ausschnitte unterteilt sich in weitere Unterbereiche, die die RZ-Umgebung detailliert erfassen und abbilden.

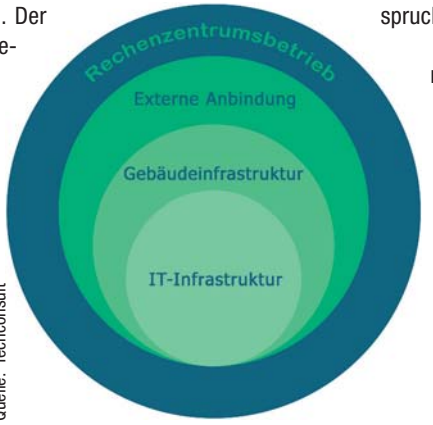
Management, Anbindung, Infrastruktur

Der Bereich Rechenzentrumsbetrieb umfasst die operativen und strategischen Aufgaben im Rechenzentrumsalltag. Dazu zählen das Rechenzentrums-Management samt unterstützender Werkzeuge, Personalfragen, das Management der heterogenen Clientlandschaft und das umfassende Monitoring verschiedener Messwerte und Umgebungen. Außerdem gehören dazu das Absichern der IT-Infrastruktur durch Backups und Redundanz sowie grundlegende organisatorischen Maßnahmen zur Rechenzentrumssicherheit.

In der nächsten Sektion unterscheidet die externe Anbindung zwischen dem Anschluss ans Internet, dem Zugriff auf externe Dienstleister zur Nutzung ergänzender Leistungen und der Anbindung mobiler Endgeräte an das Rechenzentrum.

Der Bereich IT-Infrastruktur konzentriert sich auf die Beschaffung und den Betrieb von Servern, Speichermedien und Netzwerkhardware sowie deren virtuellen Pendants. Der Gang durch das RZ wird mit der Erfassung der Gebäudeinfrastruktur abgeschlossen. Diese umfasst Prozesse und Maßnahmen zur Einhausung, Verkabelung, Klimatisierung, Energieversorgung, Gebäudetechnik, zum Brandschutz und den eingesetzten Serverracks.

Als Vergleichsreferenz zu den eigenen Angaben dient eine zuvor von techconsult durchgeführte Studie mit den identischen Inhalten des Optimized Data Center Benchmarks. Durch den Vergleich mit Rechenzentren beispielsweise gleicher Größe, gleicher Branche oder gleicher Leistung erlangen Betreiber wichtige Erkenntnisse über Optimierungspotenziale im eigenen Rechenzentrum oder Stärken gegenüber Konkurrenten.



Quelle: Techconsult

Die zum ganzheitlichen Erfassen des Rechenzentrums betrachteten Faktoren.

Die Fragen variieren dabei zwischen Selbsteinschätzungen und konkreten Detailfragen. Diese werden entweder zwecks besserer Übersichtlichkeit und Interpretation sinnvoll in aggregierte Indexwerte umgerechnet oder für eine direkte Gegenüberstellung visuell aufbereitet.

Selbsteinschätzung in drei Indizes

In der Methodik werden zum Zwecke des Vergleichs drei verschiedene Indizes als Referenzgrößen unterschieden: Der Effizienzindex spiegelt wider, welchen Aspekten von Betreibern die größte Priorität beigemessen wird und ob diese entsprechend ihrer Wichtigkeit umgesetzt werden. Der Innovationsindex verrät, ob und wie gut innovative Lösungen wie neueste Software oder aktuelle Standards ein- und umgesetzt werden. Mit dem Erfolgsindex ergibt sich schlussendlich eine Bewertung der eigenen Leistung anhand bereichsspezifischer Messgrößen, die der Betreiber für einen Dreijahreszeitraum einschätzt.

Der Benchmark fungiert neben seiner Vergleichsfunktion auch als eine Art selbstmoderierender Workshop. Bei selbstkritischer Beantwortung der Fragen, dem Erfassen der Informationen im eigenen Unternehmen und auch beim Sichten der Ergebnisse erkennen RZ-Betreiber ihre Prioritäten und erhalten neben dem direkten Vergleich auch einen umfassenden Überblick über alle Facetten des eigenen Rechenzentrums. Auf dieser Grundlage können Diskussionen, Verbesserungsmaßnahmen und Marketingentscheidungen angestoßen werden.

Optimized Data Center richtet sich dabei an Serverraumbetreiber aller Branchen, Größen und Geschäftsmodelle, also sowohl Colocation und Managed Service Provider als auch unternehmensinterne Rechenzentren zur Unterstützung der eigenen Wertschöpfung. Die vollständige Bearbeitung des Benchmarks wird etwa 90 Minuten in Anspruch nehmen.

Die Registrierung ist ab 22. Oktober 2015 geöffnet. Interessierte Teilnehmer können dann online (www.optimized-datacenter.de) den Benchmark unter Einhaltung aller Datenschutzkriterien anonym durchführen und erhalten im Anschluss ab 30. Oktober 2015 eine Ergebnisauswertung. Die zuvor getätigten Angaben können anonym zwischengespeichert werden.

Im Anschluss an den Benchmark erhält jeder Teilnehmer auf Wunsch nach Registrierung eine individuelle Detailauswertung. Ab Mitte November wird der fertige Studienbericht nach Registrierung ebenfalls kostenlos als Download auf dem Benchmarkportal zur Verfügung stehen. Die Optimized Data Center Studie wird jährlich wiederholt.

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

Streckentest im Lichtleiter

Die Multimode-Dämpfungsmessung mit Encircled Flux ergibt zuverlässige und reproduzierbare Resultate

InfiniBand- und Ethernet-Techniken mit bis zu 100 Gigabit und immer engeren optischen Dämpfungsbudgets umzusetzen, ist erst auf der Basis präziser, wiederholbarer Messergebnisse möglich. Doch diese differieren in der Praxis oft heftig. Die strikte Einhaltung der Encircled-Flux-Einkoppelbedingungen kann die Abweichungen bei der Lichtwellenleiterprüfung auf unter zehn Prozent senken.

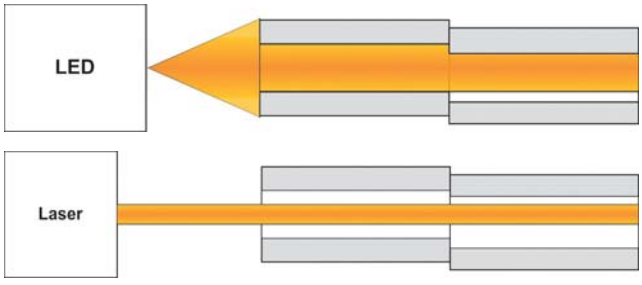
Angesichts steigender Datenmengen müssen Glasfaserkabel immer größere Datenmengen mit möglichst wenig Verlust übertragen. Sind die Datenstreuverluste zu hoch, können Multimode-Glasfaserkabel die Datenfluten nicht mehr bewältigen. Dämpfungsmessungen informieren Netzwerkadministratoren darüber, wie hoch der Verlust der in den Multimode-Fasern übertragenen Daten ist. Entsprechend der Messergebnisse können sie korrigierende Maßnahmen ergreifen.

Aber wie können Netzwerktechniker zuverlässig erkennen, ob ihr Netz ausgelastet ist oder wie viel Lichtleistung tatsächlich verloren geht? Die Lösung heißt Encircled Flux (EF). Dahinter steckt das strikte Einhalten von Einkoppelbedingungen für aussagekräftige und reproduzierbare Ergebnisse bei Multimode-Dämpfungsmessungen.

Technische Voraussetzungen für eine präzise Messung

Encircled Flux definiert die Anregungsbedingungen in Multimode-Glasfasern, indem das Verhältnis zwischen der eingekoppelten Sendeleistung und dem Radius des angeregten Teils des Faserkerns bestimmt wird. Um die auf der Verkabelungsstrecke verloren gehende Lichtleistung zu messen, verwenden Techniker eine Lichtquelle und einen Leistungsmesser oder ein OTDR (optische Zeitbereichsreflektometrie, Optical-Time-Domain-Reflectometry).

Die Messbarkeit verlässlicher und reproduzierbarer Einfügedämpfungswerte (IL =Insertion Loss) gestaltet sich in der Praxis jedoch schwierig. So hängt die Genauigkeit der Messergebnisse zunächst von qualitativ hochwertigen Komponenten wie Messkabel, Kupplungen und Stecker ab. Ebenso trägt ein falscher Messaufbau oder unterschiedliches Equipment zu IL-Messungenauigkeiten bei. Auch verschiedene Lichtquellen wie VCSEL (Vertical-cavity Surface-emitting Laser), Laser oder LED und Lichtenergien sind entscheidende Parameter für die Messung multimoder Fasern.



Quelle: trans data elektronik GmbH

Mode Fill Condition einer LED-Lichtquelle (oben) und einer Laser-Lichtquelle (unten).

Entscheidend für die Vergleichbarkeit von Dämpfungsmessungen sind die Einkoppelbedingung, unter der Licht in einen Stecker geleitet wird: Nur wenn der größte Teil des Lichtes in einem definierten Teilbereich des Faserkerns übertragen wird, sprechen Experten von Encircled Flux. Aufgrund des größeren Kerns der Glasfaser überträgt sich das Licht auf unterschiedlichen Wegen (Lichtmoden). Nur durch sorgfältig definierte Anregungsbedingungen für die Einkoppelung – wie sie Encircled Flux vorsieht – lassen sich Ungenauigkeiten bei Dämpfungsmessungen auf nachweislich unter zehn Prozent senken.

Neudefinition durch Encircled Flux

Ursprünglich wurde die Encircled-Flux-Metrik für die Simulation von Übertragungsbandbreiten entwickelt. In engem Zusammenhang steht die Entwicklung der Encircled-Flux-Metrik mit den Oberflächenemittern VCSEL: Diese kommen aufgrund ihrer hohen Datenrate seit 1999 als optische Sender für die High-Speed-Übertragung zum Einsatz, da sie sich gut für die analoge Breitband-Signalübertragung eignen. VCSEL-Lichtquellen arbeiten mit einer Wellenlänge von 850 Nanometern (nm), koppeln dabei das Licht aber anders ein als LEDs mit gleicher Wellenlänge. VCSELs emittieren einen schmalen Lichtstrahl, der in der Mitte des Glasfaserkerns am hellsten ist, nach außen hin schnell abdunkelt und den Kern nahe der Grenzschicht zum Mantel nicht mehr beleuchtet.

Die Wellenlänge von 850 nm hat das Institute of Electrical and Electronics Engineers (IEEE) auch für die Übertragung von VCSELs auf Multimodefasern für Gigabit Ethernet vorgegeben. Mit der Entwicklung des 10 Gigabit Ethernet kam es zur Festlegung der Encircled-Flux-Metrik: Sie definiert Encircled Flux als Einkoppelbedingung für eine ideale VCSEL-Lichtquelle, die ihre Lichtleistung stärker auf die Mitte des Faserkerns konzentriert als Laser oder LEDs.

Einkopplung unterschiedlicher Lichtquellen

Ideale Einkopplungsbedingungen liegen vor, wenn sich das Licht über den gesamten Faserkern verteilt. Tatsächlich aber verursachen unterschiedliche Lichtquellen „overfilled“ beziehungsweise „underfilled launch conditions“. Kommt als Lichtquelle eine Leuchtdiode (LED) zum Einsatz, wird die Energie gleichmäßig über die Multimode-Faser beziehungsweise ihren Kern verteilt. Da Strahlungsfläche und Winkelverteilung größer als der Faserkern sind, gehen sowohl das außerhalb des

Limited Time to Complete Your Next Data Centre Deployment?

ACCELER8

Corning, makers of EDGE™ solutions, the industry-leading Base-12 preterminated optical cabling system for your data centre, now offers EDGE8™ solutions. Combining the best-in-class density, speed of installation, and modular components of EDGE solutions with the superior network scalability, improved link performance, and 100 percent fibre utilisation of the first true Base-8 optical solution.

With **EDGE8™** solutions, less really is more.
www.corning.com/edge8

CORNING

Quelle: trans data elektronik GmbH

Bei Multimode-Dämpfungsmessungen unter Verwendung einer LED-Lichtquelle beseitigt Mandrel Wrap die Moden höherer Ordnung.

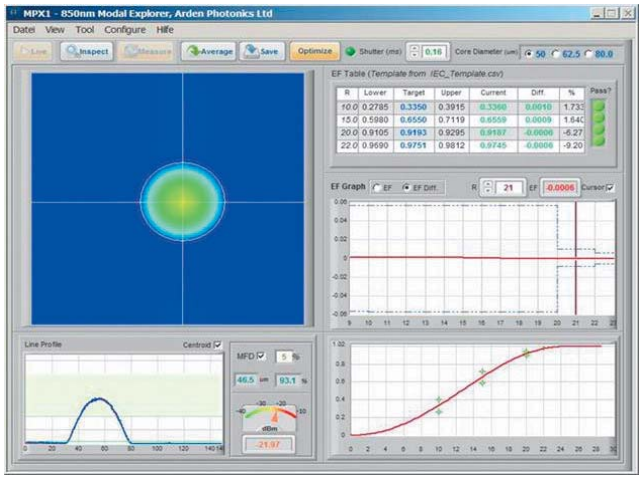
Faserkerns einfallende Licht als auch das in einem Winkel auftreffende und den Akzeptanzwinkel des Faserkerns übersteigende Licht für die Übertragung verloren. Die Vollanregung erzeugt tendenziell zu hohe Dämpfungswerte und damit zu pessimistische Messergebnisse.

Kantenstrahler wie Laser oder VCSEL-Hochleistungslaser hingegen übertragen die Lichtenergie nur in einen geringen Bereich des Kerns. Strahlungsfläche und Winkelverteilung des Lichtes sind bei diesen Lichtquellen kleiner als der Faserkern. Der Großteil der optischen Leistung konzentriert sich in der Mitte der Faser und leuchtet den Kern nicht vollständig aus. Die „underfilled launch condition" genannte Anregung erzeugt zu niedrige Dämpfungswerte. Die Messergebnisse sind in der Regel also zu optimistisch.

Genau zwischen der Overfill- und der Underfill-Anregung liegt Encircled Flux. Seit Juli 2009 definiert der IEC-Standard 61280-4-1 die Teilbereiche für die Energieverteilung des Lichtes im Kern. Da die Einkoppelbedingungen für unterschiedliche Lichtquellen variieren, müssen VCSEL- und LED-Dioden sowie Laser an die EF-Bedingung angepasst werden. Grundlage vieler Standards – wie IEE802.3, ANSI/TIA und ISO/IEC – bilden LED-Lichtquellen.

Die Dämpfungsmessung im Detail

In der Praxis läuft die IL-Messung von LWL-Steckern (S2) oder -Kabeln wie folgt ab: Netzwerktechniker verbinden einen Testjumper mit einer Lichtquelle. Am Ende des Testjumpers wird ein Stecker angebracht (S1) und mittels Kupplung mit dem Prüfling verbunden. Das Licht wird von der Lichtquelle über S1 in Stecker S2 eingekoppelt und so über das daran angeschlossene Kabel am anderen Ende aufgefangen und gemessen.



Quelle: trans data elektronik GmbH

Der Modal Explorer MPX1 von Arden Photonics zeigt beim Scan des Kern-Nahfelds oben rechts den nach IEC 61280-4-1 definierten Teilbereich des Faserkerns.

Mit diesem Testaufbau lässt sich der Energieverlust messen, der beim Einkoppeln der Lichtenergie von S1 in S2 entsteht. Da sich Encircled Flux abhängig von der verwendeten Faser oder weiteren Zwischenadaptierungen signifikant ändern kann, muss die Compliance zwingend am Ende des Testjumpers kontrolliert werden. Um vergleichbare Messergebnisse gewährleisten zu können, ist das regelmäßige Überwachen der Einkoppelbedingung notwendig, selbst wenn Hersteller von Dämpfungsmessgeräten die Einhaltung von EF garantieren. Auch bei baugleichen Messgeräten derselben Serienreihe und desselben Baujahrs können Unterschiede auftreten.

Testleitung mit LED-Lichtquelle

Kommt eine LED-Lichtquelle bei Multimode-Dämpfungsmessungen zum Einsatz, passiert dies mit sogenannten Mandrel Wraps. Aufgrund der überfüllten Fasern weisen diese mehr Moden auf, die sich nahe der Grenzschicht zwischen Kern und Mantel befinden. Diese Moden höherer Ordnung sind anfälliger für die Dämpfung durch das Biegen der Glasfaser und gehen auch an Verbindungsstellen zuerst verloren. Mandrels gewährleisten zuverlässige und reproduzierbare Ergebnisse: Hierbei wird das mit der Lichtquelle verbundene Anschlusskabel so um den zylindrischen Wickeldorn (Mandrel) gewickelt, dass der Einfallswinkel an der Biegung kleiner ist als der Grenzwinkel der Totalreflexion. Dadurch werden die Moden höherer Ordnung beseitigt, bevor das Testsignal in die zu prüfende Strecke eingekoppelt wird. Die gemessene Dämpfung verringert sich.

Für Multimode-Dämpfungsmessungen mit einer Laser-Lichtquelle muss laut IEEE802.3aq und FOTP-203-Standard zusätzlich ein Fiber Shaker eingesetzt werden. Er passt die helleren Sprenkel (Speckels) durch Änderung der differenzialen Weglänge der unterschiedlichen Moden in der Faser an: Dazu wird die Faser während des Messvorgangs kontinuierlich geschüttelt, um die Speckles auszumitteln

Durchgängig saubere Ergebnisse

Mit der Encircled-Flux-Metrik lassen sich Messunsicherheiten auf unter zehn Prozent senken und eine gute Performance in High-Speed-Netzen bei Verwendung von 850 nm VCSELs in 10 Gigabit Ethernet-Systemen erzielen. Das gilt auch für neue Techniken, bei denen opto-elektronische Module direkt auf den Leiterplatten montiert und über Prismenstecker angeschlossen werden.

Zugleich gewährleistet Encircled Flux auch die bessere Vergleichbarkeit von unterschiedlichen Messgeräten. Viele Messgeräte-Hersteller garantieren mittlerweile EF Compliance für ihre Messgeräte, jedoch gilt die Einhaltung nur für den Messgeräte-Ausgang. Wird ein Adapterkabel zwischen Messgeräte-Ausgang und Prüfling geschaltet, können sich die Einkoppelbedingungen ändern, die am zu messenden Stecker anliegen. Verursacht wird dies beispielsweise durch Fasertypen unterschiedlicher OM-Kategorien, deren Kombination, die Verbindungsanzahl oder sogar aufgrund unterschiedlicher Faserhersteller oder Kabellängen.

Deshalb ist Encircled Flux kein statischer Parameter – die Anregungsbedingung verändert sich dynamisch im Lauf einer Kabelstrecke. Für vergleichbare Messergebnisse müssen Hersteller und Netzwerkingenieure die Einkoppelbedingungen direkt vor dem zu messenden Stecker prüfen. Nur hier lässt sich Encircled Flux erfolgreich umsetzen.

Wilfried Schneider,
Technischer Leiter/CTO, tde – trans data elektronik GmbH

DAS SCHNELLERE, LEISTUNGSSTÄRKERE, UND SCHLANKERE DATA CENTER

200 erstklassige Referenten.
200 international führende Anbieter.
Reger Austausch mit den
wichtigsten IT-Entscheidungsträgern.
Ihr kostenloses Ticket im Wert von 1.500 EUR
wartet auf Sie!
www.datacentreworld.de/RZI

Deutschlands größtes Zusammentreffen von Data Center Spezialisten

Registrieren Sie sich jetzt für Ihre kostenlose Eintrittskarte im Wert von 1.500 Euro.

www.datacentreworld.de/RZI

DATA CENTRE WORLD

10. – 11. November 2015 Messe Frankfurt
www.datacentreworld.de

Konferenzsaal Sponsor: EMERSON Network Power

Gold Sponsoren: COMMSCOPE, E-LINE, EAE, dternity, HUBER+SUHNER, Munters, bulk, HUAWEI

Strategic Advisory Partner: bitkom

Event Partner: eco, EuroCloud Deutschland | eco

Analyst Partner: SNIA Europe, crisp

Zeitgleich mit: CLOUD EXPO EUROPE

Der (fast) abstrakte Abakus

Softwaredefinierte Netzwerke zwingen Betreiber zum Umdenken

Enorm elastisch, hoch automatisiert und gründlich gesichert: Software-defined Networking verbindet das Rechenzentrum der Zukunft bruchlos sowohl mit der Cloud als auch mit On-Premise-Systemen. Als Selbstläufer braucht das virtuelle System aber dynamischen Schutz und ein intelligentes Monitoring.

Bei der Entwicklung des eigenen Rechenzentrums von einer unflexiblen, schwer zu steuernden Infrastruktureinrichtung hin zum agileren Business Response Center setzen Unternehmen vermehrt auf Automatisierungslösungen. Diese versprechen ein Optimieren der Auslastung bei gleichzeitig hoher Flexibilität und Fehlerminimierung – und damit eine spürbare Reduktion laufender Kosten.

Noch vor zehn Jahren basierte Automatisierung fast ausschließlich auf Hardware. Nicht selten verwandte ein Unternehmen einen großen Teil seiner finanziellen und personellen Ressourcen ausschließlich auf das manuelle Bereitstellen zusätzlicher Kapazitäten und Systeme. Mittlerweile hat die Cloud die Sicht auf die Automatisierung umfassend verändert, sodass es jetzt mindestens im selben Maße darum geht, Anlagen zu verkleinern und flexibler zu gestalten.

Gradmesser der Automatisierung

Aber auch ein weiterer zentraler Aspekt hat sich grundlegend verändert: Noch vor fünf bis acht Jahren fand die Automatisierung im Unternehmen auf Funktionsebene statt, das heißt auf der Ebene eines spezifischen Servers oder einer bestimmten Technik. Dies erforderte Investitionen in qualifizierte Mitarbeiter für jedes einzelne Automatisierungs-Tool, wodurch lediglich – wenn auch für sich genommen automatisierte – neue Silos geschaffen wurden.

Heute machen sich Unternehmen Gedanken darüber, wie, wo und wofür die Automatisierung stattfindet: in der Cloud, auf einem neuen Server im eigenen Rechenzentrum oder einer virtuellen Maschine? Für eine spezifische Anwendung, Service-Stack oder einen kompletten Prozessablauf? Und wenn die Cloud genutzt wird, dann um Spitzenlasten auszugleichen oder um spezifische Geschäftssituationen wie Produktentwicklung, Data Analytics oder Expansion zu bewältigen? Entscheidend ist aber in jedem Fall die konkret zu automatisierenden Workloads und den daraus zu erwartenden geschäftlichen Nutzen zu bestimmen.

Es wäre wenig zielführend, diejenigen Systeme und Abläufe zu automatisieren, die das ganze Jahr über relativ statisch bleiben und für die bereits eine sehr gute Serverauslastung gegeben ist. Demgegenüber bieten sich Arbeitslasten, die sich häufig und wiederholt ändern oder für die aufwendige manuelle (und damit fehlerträchtige) Abläufe erforderlich sind, für die Automatisierung geradezu an.

Zu berücksichtigen ist natürlich auch, welche Anwendungen und Szenarien überhaupt dieselbe Infrastruktur im Rechenzentrum sinnvoll zeitgleich nutzen können und ob das Einführen einer bestimmten Arbeitslast zu übermäßiger Auslastung einzelner Komponenten (Netz- oder Storage-Traffic, CPU- oder RAM-Auslastung) führen würde; dies könnte die Performance kritischer, auf demselben Server laufender Workloads, beeinträchtigen.

SDN-Schwerpunkt Sicherheit

Den eigentlichen Mehrwert bringt aber die Automatisierung ganzer Prozesse im Rechenzentrum. Mit den geeigneten Prozessen lassen sich komplette Systeme von der Basis-Infrastruktur über Kommunikation und Sicherheit bis zur Anwendung provisionieren, Back-up- und Sicherheitsaufgaben automatisieren, Lifecycle Management betreiben

Quelle: Dimension Data

Cloud Enablement, Hybride IT oder das Rechenzentrum als IT Factory – alle Ansätze sollten Business-orientiert geplant und aufgebaut werden.

Quelle: Dimension Data

Log- und Analyse-Tools sind entscheidend für den Betrieb eines automatisierten Rechenzentrums, in dem sich häufig und wiederholt ändernde Abläufe automatisiert werden sollen.

und die Systemauslastung automatisch steuern und optimieren. Der Trend geht zu einer komplett aus der Ferne programmierbaren Umgebung, um Flexibilität und Skalierbarkeit zu optimieren und die IT jederzeit schnell an die sich rasch wandelnden Anforderungen des digitalen Zeitalters anpassen zu können.

Doch der Schwerpunkt beim Einsatz softwaredefinierter Netze lag bisher auf schnellem und einfachem Transport von Daten und hoher, statischer Verfügbarkeit und weniger auf Sicherheit; die traditionelle Methode der Trennung von Systemen durch Aufteilung auf verschiedene physische Netzwerkports ist auf heutige, hochgradig virtuelle und dynamische Infrastrukturen nicht mehr sinnvoll anwendbar.

Eine virtualisierte Struktur bietet allerdings auch erheblich mehr Angriffsfläche für unbefugte Zugriffe von außen als ein physisch abtrennbares System. Bei einer softwaredefinierten Infrastruktur werden die Sicherheitsmechanismen damit von der Physik der Hardware auf die Logik und Kommunikationsmuster der Software verlagert, weshalb der Fokus bei modernen SDN-Modellen auf dem sicheren Management der Netzwerkkommunikation auf Anwendungsebene liegt. Unerlaubtes Fremdeinwirken und das Einfügen von Schadsoftware soll sich so verhindern lassen.

Softwaredefinierter Komplettschutz

Als Antwort auf die Anforderungen programmierbarer Infrastrukturen setzen auch viele Anbieter von Sicherheitslösungen mittlerweile auf softwaredefinierten Schutz. Durch eine entsprechende Technik in der Software kann jede virtuelle Maschine eigene Sicherheitsrichtlinien anwenden, sodass diese direkt durch eine Firewall und Intrusionsschutz abgesichert ist.

Ein großer Vorteil ist dabei die Flexibilität, denn die Sicherheitseinstellungen lassen sich mit der virtuellen Maschine frei zwischen Abschnitten, kompletten Rechenzentren oder der Cloud transparent und regelbasiert transportieren. Somit lässt sich nicht nur eine agile und flexible, sondern auch in hohem Maße sichere Infrastruktur realisieren, die auch für den (späteren) Aufbau von Multi-Tenancy-Umgebungen genutzt werden kann.

Ein weiterer Vorteil ist die Möglichkeit, besonders sensible Datenströme im gesamten Netzwerk nach Bedarf – etwa durch Verschlüsselungsverfahren oder isolierte, virtuelle Netzwerkverbindungen – dynamisch zu schützen. Auf diese Weise können Unternehmen ihre Sicherheitsrichtlinien effektiver und effizienter anwenden und im Rahmen von Automatisierungslösungen als Teil des Gesamtkonzepts programmatisch oder Script-basiert einbinden.

Auch in der softwaredefinierten Welt wird es noch lange physische (sogenannte Bare Metal) Systeme geben, die sich aus den unterschiedlichsten Gründen nicht virtualisieren lassen. Wichtig ist, dass die Netzwerkautomatisierung für virtuelle und physische Systeme genutzt werden kann, um parallele Installationen von zusätzlichen Layern und Produkten zu vermeiden. Jede zusätzliche Schicht bringt weitere Komplexität und damit Kosten; Fehlerpotenzial und Aufwand den es zu vermeiden gilt.

Monitoring ist K.-o.-Kriterium

Bei allen Vorteilen der Automatisierung: Wenn doch einmal etwas nicht funktioniert, sind die richtigen Informationen der Schlüssel zur schnellen Fehlerbeseitigung. Mit Hilfe der richtigen Log- und Analyse-Tools lassen sich die wichtigsten Messdaten erfassen und zudem präemptiv Problembeseitigungsmaßnahmen durchführen. Es können Entscheidung getroffen werden, wann zusätzliche Kapazitäten automatisch hinzugefügt werden sollen oder eine Vorhersage, wann sich das Traffic-Volumen ändern wird. Der Einsatz von Analytics bedeutet das Ende der Abhängigkeit von einzelnen Mitarbeitern für die Bereitstellung dieser Informationen – ein entscheidender Schritt in Richtung der umfassenden Automatisierung des Rechenzentrums.

Vom Rechenzentrum zur IT Factory

Unternehmen, die ihre Rechenzentrumsumgebungen automatisieren wollen, tun sich oftmals schwer damit, Voraussetzungen und passende Ansatzpunkte zu identifizieren oder die Auswirkungen des Multi-Tenancy-Konzepts für interne Private-Cloud-Angebote zu verstehen respektive im Voraus abzuschätzen. Hier können – bei aller Rücksichtnahme auf die individuellen Gegebenheiten in der IT-Infrastruktur – externe Partner mit ihren Erfahrungswerten beratend zur Seite stehen.

Cloud Enablement, Hybride IT oder das Rechenzentrum als IT Factory – alle Ansätze haben ihre eigenen Herausforderungen und sollten Business-orientiert geplant und aufgebaut werden. Nicht die Produkte und Funktionen dürfen bei der Neudefinition im Mittelpunkt stehen, sondern der konkrete, messbare Nutzen den eine moderne, effiziente, dynamische und flexible IT dem Unternehmen heute und in Zukunft bietet.

Frank Beckereit,
Head of Next Generation Datacenter Solutions,
Dimension Data Deutschland

Draußen beginnt der Abbruch

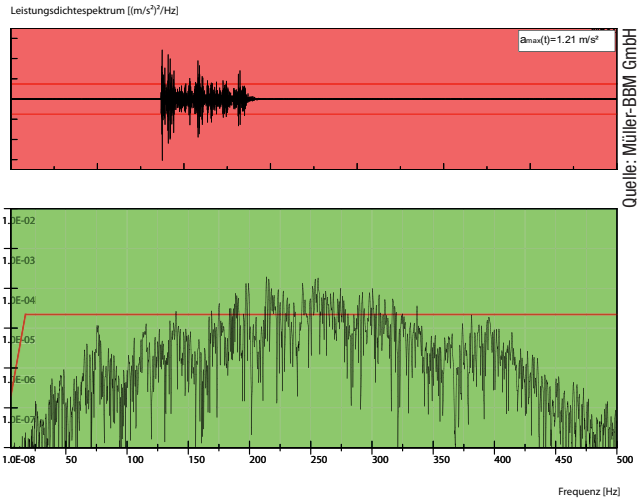
Ein kluges Erschütterungsmonitoring schützt die Server im Inneren und löst rechtzeitig Alarm aus

Bodenarbeiten bei Baustellen und donnernder Schwerlastverkehr gefährden den reibungslosen Betrieb des Rechenzentrums. Bewährt hat sich ein Mess- und Warnsystem, das man bereits im Vorfeld kalibriert und während der Arbeiten online anpassen kann. Denn Fehlalarme will sich niemand leisten.

Für den störungsfreien Betrieb von Rechenzentren existiert eine Vielzahl von Grenzwerten hinsichtlich zulässiger Erschütterungen („vibration limits“). Dabei können sowohl ganze Systeme als auch einzelne Bausteine wie Festplatten eigene, sehr unterschiedliche Kriterien aufweisen. Die Abbildung unten zeigt beispielhaft eine gemessene Erschütterung mit Bewertung im Zeitbereich (oben) sowie im Frequenzbereich (unten) als Leistungsdichtespektrum.

Erfahrung ohne Grenzwerte

In den einschlägigen deutschen Normungsunterlagen sind lediglich Anhaltswerte zum Beurteilen von ganzen Gebäuden (DIN 4150, Teil 3) oder der Einwirkungen auf den Menschen (DIN 4150, Teil 2) angegeben. Hinsichtlich der für die Rechenzentren zu bewertenden Gebrauchstauglichkeit, also der Funktionstüchtigkeit der Räume innerhalb der Gebäude werden beispielsweise in der VDI-Richtlinie 2038 diverse Grenzwerte und Kriterien für schwingungsempfindliche Produktionsumgebungen angegeben. Diese beziehen sich jedoch nicht auf Rechenzentren. Eine Beurteilung anhand der Spürbarkeitsschwelle des Menschen (zum Beispiel aus VDI-Richtlinie 2057) ist erwartungsgemäß ebenso nicht zielführend.



Zwei Grenzwerte (rote Linien) zur Bewertung der registrierten Erschütterungen. Die grüne Fläche stellt dabei den zulässigen, die rote den unzulässigen Bereich dar. Oben: Bewertung im Zeitbereich, unten: Bewertung im Frequenzbereich eines Leistungsdichtespektrums.

Im Regelfall stehen die Racks einzeln oder baulich zu festen Gruppen verbunden auf Doppelböden. Diese Anordnung ist erfahrungsgemäß um ein vielfaches anfälliger für externe Schwingungen als die Montage direkt auf Beton-Decken- oder Bodenplatten. Dennoch werden die Grenzwerte im Allgemeinen beim regulären Betrieb durch Eigenanregung nicht erreicht. Eine andere Situation ist jedoch gegeben, wenn die Erschütterungen aus anderen Gebäudeteilen oder von außen eingetragen werden.

Die Anregungsquellen, für die ein Monitoring sinnvoll ist, sind in der Regel Bauarbeiten. Sonstige interne Emissionsquellen wie Kältekompressoren oder andere Aggregate der Haustechnik emittieren mit ihrer stationären Anregungscharakteristik gut beherrschbare Schwingungen. Diese Emissionen lassen sich durch geeignete Maßnahmen an der Quelle reduzieren, beispielsweise mittels einer geeigneten elastischen Lagerung.

Bauarbeiten und schwere Lastwagen

Die Einwirkungen aus Bauarbeiten im Gebäudeinneren oder von benachbarten Baufeldern stellen mit ihrer sehr instationären, transienten Charakteristik eine schwer bis ins Detail vorherzusagende Anregung dar. Eine Aufstellung der IT-Geräte auf schwingungsisolierenden Federelementen ist aufgrund der vielen verschiedenen Arbeitsfrequenzen der Baumaschinen nicht immer zielführend. Bei einer falschen Auslegung der Federelemente und bestimmten Bauverfahren können die Schwingungsamplituden durch die Lagerung sogar verstärkt werden.

Bei den in Bezug auf die Erschütterungsruhe kritischen Bauarbeiten außerhalb des Rechenzentrumgebäudes handelt es sich vor allem um Abbrucharbeiten, Maßnahmen zur Errichtung von Baugrubenwänden und teilweise auch um LKW-Verkehr auf schlechten Fahrwegen. Temporäre, aber von der Charakteristik her eher stationäre Anregungsarten können aus Vibrationsrammungen oder Verdichtungsarbeiten (siehe Abbildung S.14, links oben) resultieren. Dabei liegen die Anregungsfrequenzen teilweise in Bereichen, in denen sich auch die Deckeneigenfrequenzen der Rechenzentren befinden. Durch die Überhöhung in Resonanzanregung können sich so auf den Deckenplatten höhere Amplituden als beispielsweise auf der Gründungsebene einstellen.

SMS, Sirene und Warnlicht

Ein individualisiertes Erschütterungsmonitoring erlaubt dabei die Identifikation von äußeren Einwirkungen auf die Rechenzentren und lässt auch das Festlegen von Warnstufen (zum Beispiel 50 bis 75 Prozent des eigentlichen Grenzwerts) zu. Werden sie überschritten, erfolgt eine

automatisierte Benachrichtigung der Betreiber des Rechenzentrums, ohne dass ein Schaden an den Anlagen zu befürchten ist. Eine weitere Alarmierung von Verantwortlichen auf der Baustelle kann ebenso oder zusätzlich durch Signalhörner und/oder Warnlichter im Freien (siehe Abbildung S. 14, rechts oben) erfolgen. Darüber hinaus kann die Benachrichtigung auch via E-Mail und/oder SMS passieren.

Potenzialfreie Ausgänge können außerdem an die Gebäudeleittechnik angeschlossen und so für weitere Benachrichtigungen oder zur Dokumentation der Alarmierung beipielsweise über Drucker genutzt werden. Gerade bei Bauarbeiten, die nicht im eigenen Auftrag erfolgen, ist es unter anderem zur Beweissicherung oder zur Klärung von Haftungsfragen wichtig, nachzuweisen, dass die Erschütterungseinwirkungen von außen eingeleitet wurden.

Starre Lösung mit Risiken

Für die klassische Gebäudeüberwachung bei Baustellenerschütterungen werden oft autarke Systeme verwendet, die aus einem Schwingungssensor, einem Datenspeicher und einer UMTS- beziehungsweise WLAN-Verbindungsmöglichkeit bestehen. Beim Überschreiten eines bestimmten Grenzwerts im Zeitbereich werden die Zeitrohdaten kurz vor und nach dem detektierten Ereignis gespeichert.

Diese Methode reicht aus zum Bewerten der Einwirkung auf die Baustruktur. Komplexere Grenzwerte von IT-Geräten, die im Frequenzbereich als Schmalband-, Terz- oder Leistungsdichtespektrum (siehe Beispiel in Abbildung S. 12) sowie meist auch noch zusätzlich im Zeitbereich als Absolut- und/oder RMS-Wert vorliegen, lassen sich damit jedoch nicht überwachen. Weiterhin ist die oben erwähnte, zweifelsfreie Identifizierung einer von außen eingeleiteten Erschütterungseinwirkung nur durch die parallele Erfassung mehrere Sensoren auf einem Messsystem möglich.

Durch Reparatur- oder Wartungsarbeiten am überwachten Gerät kann es zudem zu (folgenlosen) Überschreitungen der Gerätegrenzwerte kommen, die bei Einsatz nur eines Sensors einen Fehlalarm auslösen würden. Im Falle einer automatischen Benachrichtigung der Baustelle beziehungsweise eines Einsatzes von Warnleuchten führen diese Fehlalarme schnell zu einem Gewöhnungseffekt bei den ausführenden Unternehmen vor Ort. Mit der Zeit haben deshalb gegebenenfalls auch die relevanten Alarme keine Wirkung mehr, und die schädigenden Arbeiten werden trotz Alarmsignal nicht eingestellt.

Alternative Dauermessanlage

Fachlaute haben in der Vergangenheit gute Erfahrungen mit einem selbstentwickelten, individuell zu konfigurierenden Monitoring-System mit mehreren Schwingungssensoren gemacht, das auf die jeweils zu überwachenden IT-Geräte abgestimmt wird. Im Vorfeld der Einrichtung dieser Dauermessanlage ist eine vorbereitende Diskussion sowohl mit den Nutzern des Rechenzentrums als auch mit den Verantwortlichen der Baustelle über die vorgesehenen Bauverfahren und ihren zu er-

wartenden Einfluss auf das Rechenzentrum zu empfehlen. Weiterhin sollte mittels Prognoseberechnungen die zu erwartenden Erschütterungen im Rechenzentrum in Abhängigkeit der einzusetzenden Bauverfahren prognostiziert werden, um die Notwendigkeit eines Monitorings überhaupt festzustellen.

Bewährung in der Praxis

Das hier im Folgenden vorgestellte Dauermesssystem kann dabei individuell hinsichtlich der Grenzwerte sowie Warn- und/oder Alarmschwellen programmiert werden. Das zeitgleiche Erfassen mehrerer Racks und Raumrichtungen durch das parallele Erfassen verschiedener Sensoren ist möglich. Je nach Anforderung lassen sich dabei beliebig viele Grenzwerte parallel überwachen.

Üblicherweise erfolgt das Überwachen der Erschütterungen am Rack durch traxiale Beschleunigungssensoren. Weiterhin wird ein Triggermesspunkt auf dem Gebäudefundament (idealerweise unterstes Kellergeschoss an einer Außenwand in Richtung der Baustelle) installiert. Die Triggerschwelle wird in einer Größenordnung definiert, von der erfahrungsgemäß auszugehen ist, dass sie nur von den externen Bauarbeiten überschritten wird. Im Zweifelsfall, zum Beispiel bei inneren Anregungen durch Lagerarbeiten im Bereich der Triggersensoren, ist eine Feinjustage durch Eingangsmessungen möglich. Dabei werden die Einflüsse der potenziell gefährlichen Verfahren in Probearbeiten simuliert und erfasst. Gleichzeitig kann der (sichere) Ruhe- beziehungsweise Hintergrundpegel der Erschütterungen im Gebäude erfasst werden.

Der Alarm wird nur ausgelöst, wenn durch den Triggermesspunkt sichergestellt ist, dass die Überschreitung des Grenzwerts am Rack tatsächlich von außen kommt. Ein Überschreiten der Triggerschwelle muss dabei nicht zwangsläufig zu einer Alarmierung führen. Jedoch wird in diesem Fall die Abfrage zum Überschreiten der Gerätegrenzwerte aktiviert, die durch die Sensoren direkt am Rack kontrolliert werden.

Zur Sicherheit Funkkontakt

Um Fehlalarme mit vollständiger Sicherheit ausschließen zu können, ist ein Online-Zugriff auf den Messrechner möglich. Die Voraussetzung dafür ist mindestens eine stabile UMTS-Verbindung. Der Anschluss an ein in Rechenzentren zumeist vorhandenes Gästenetzwerk ist ratsam. Im Alarmfall können sich externe Spezialisten innerhalb weniger Minuten auf dem Monitoring-System einloggen und die aufgezeichneten Signale bewerten. Gleichzeitig wird dadurch der Versand von Kurznachrichten und/oder E-Mails sichergestellt.

Quelle: Müller-BBM GmbH

Links: Beispiel für erschütterungsintensive Bauarbeiten (Vibrationsverdichtung), rechts: Abbildung des eingebauten Warnlichts und des Signalhorns.

Quelle: Müller-BBM GmbH

Links: Foto eines Sensors am Rack, Mitte: Foto eines Triggermesspunkts, rechts: Messanlage im Rack eingebaut

Um Schäden an IT-Geräten zu verhindern, wird die Alarmschwelle bereits unterhalb der eigentlichen Grenzwerte definiert. Je nach eingesetzten Bauverfahren werden in der Regel 75 Prozent des Grenzwerts dafür angesetzt. Zusätzlich kann eine sogenannte Warnschwelle bei zirka 50 Prozent definiert werden. Das Auslösen der Warnschwelle kann zum Beispiel einem Geräteführer signalisieren, dass die Arbeiten mit größter Vorsicht weiterzuführen sind und jederzeit mit dem Überschreiten der Alarmschwelle zu rechnen ist. Durch die Kombination von Warn- und Alarmschwellen kann die Wahrscheinlichkeit einer grenzwertigen Belastung der IT-Geräte auf ein Minimum reduziert werden.

Voraussetzung für ein effektives Monitoring sind jedoch klare Handlungsanweisungen auf der Baustelle. Im Alarmierungsfall werden automatisch die für den Überschreitungszeitraum relevanten Messdaten vom Messrechner auf lokale Systeme beim überwachenden Dienstleister übertragen, durch eine vorbereitete Routine ausgewertet, grafisch aufbereitet und anschließend zusätzlich durch einen Messingenieur beurteilt. Eine Klassifizierung der Erschütterungscharakteristik und damit des Bauverfahrens ist damit in der Regel mit hoher Genauigkeit möglich. Ebenso können Fehlalarme identifiziert werden. Die Erfahrung zeigt, dass sich die Anzahl der Fehlalarme auf nahezu Null reduzieren lässt, wenn vor dem eigentlichen Baustellenbeginn Probearbeiten messtechnisch begleitet wurden.

Online nachjustieren

Die ständige Internetverbindung des Messrechners hat außer der unmittelbaren Auswertungsmöglichkeit in Echtzeit den Vorteil, dass das Messprogramm aus der Ferne angepasst werden kann. So können neue Grenzwerte oder neue Triggerschwellen problemlos und ohne Verzögerung eingefügt werden, ohne dass die Anlage vor Ort verändert werden muss.

Da sich die Bauarbeiten in der Regel über einen längeren Zeitraum erstrecken, werden die Überwachungszeiträume beispielsweise durch Wochenberichte dokumentiert. Als zielführend haben sich dabei Darstellungen von 30-sekündigen Maximalamplituden über die Zeit herausgestellt. Überschreitungen von Grenzwerten werden separat je nach Erfordernis im Zeit- oder Frequenzbereich dargestellt. Die Zeitrohdaten werden im Normalfall jeden Monat vom Messrechner übertragen und zentral gesichert. Ohne Überschreitungen der Grenzwerte werden sie üblicherweise nach zwölf Wochen gelöscht.

Alert bei Ausfall

Das beschriebene Monitoring-System wird unter anderem in Rechenzentren direkt neben langjährigen Großprojekten seit mehreren Jahren kontinuierlich betrieben. Die Zuverlässigkeit der Anlagen konnte durch die Erfahrungen dieser Zeit immer weiter verbessert werden. So wurde aufgrund dieser Praxiserfahrungen eine zweite Kontrollebene eingerichtet, die die Funktionalität des Monitoringsystems ständig überwacht. Es gibt beispielsweise bei Stromausfall oder dem Ausfall des Messprogramms (aufgrund von Speicherfehlern und anderen Problemen) einen GSM-basierten internen Alarm.

Über ein Funksignal lässt sich dann unter anderem der Messrechner neu starten und eine Ferndiagnose umsetzen. Da die GSM-Versorgung vor allem in Rechenzentren, die in Untergeschossen eingerichtet sind, fluktuiert, sind mittlerweile GSM-Karten im Einsatz, die sich in das jeweils stabliste Funknetz einwählen, was bei allen momentan überwachten Anlagen einen kontinuierlichen Kontakt zur Messanlage ermöglicht.

Zukünftige Anpassungen betreffen beispielsweise Grenzwerte, die nicht als konstanter Wert vorliegen, sondern die zum Beispiel eine Funktion über die Frequenz darstellen. Erste Ansätze lösen die Problematik entweder durch eine Transformation der Beurteilungsgrundlage in eine andere Schwingungsgröße, also beispielsweise von Schwingbeschleunigungen nach Schwingschnellen oder durch ein Aufteilen des Spektrums in verschiedene Bänder.

Besser unerschütterlich

Prinzipiell ist der beschriebene Monitoring-Ansatz aufwändiger als die Standardverfahren zur Überwachung von Gebäuden bei Bauarbeiten, jedoch ist der differenzierte Ansatz infolge der komplexen Grenzwerte der IT-Geräte auch notwendig. Die ständige Fern-Wartung der Anlage erlaubt weiterhin einen maximalen Schutz der Rechenzentren bei einer minimalen Beeinflussung der Baustelle und Bauzeiten. So kann der Aufwand sowohl für die Rechenzentren als auch für die Bauausführenden insgesamt jeweils sehr gering gehalten werden.

Dipl.-Ing. Friederike Busch,
Dipl.-Ing. (FH) Markus Löffler,
M.Eng., Dr.-Ing. Andreas Gömmel,
Müller-BBM GmbH

In der nächsten Generation geht der Schutz mit der Last

Mikrosegmentierung wird die entscheidende Sicherheitsmaßnahme im softwaredefinierten Rechenzentrum

Die Virtualisierung ist inzwischen beim Netzwerk angekommen. Das hat viele Vorteile, doch die bisherigen Sicherheitskonzepte sind mit dieser Entwicklung hoffnungslos überfordert. Damit Next-Generation Firewalls ihre Fähigkeiten ausspielen können, ist ein überlegtes Mikrosegmentieren bereits bei der Konzeption des Software-defined Data Centers sinnvoll.

Das Virtualisieren der Netzwerkkomponenten hat zum einen dazu geführt, dass in den Rechenzentren wesentlich weniger Hardware vorzufinden ist. Zum anderen haben sich die Rüstzeiten für neue Projekte oder Geschäftsanwendungen deutlich verringert. Ein Beispiel: Vor gut sieben Jahren wurden in einem mittelständischen Unternehmen immerhin noch einige Wochen veranschlagt, um einen Server zur Verfügung zu stellen. Dank Virtualisierung kann dies heute schon in wenigen Tagen oder gar Stunden erfolgen.

Durch den Einsatz von Techniken zum Realisieren des Software-defined Data Center (SDDC) lassen sich neue Systeme innerhalb kurzer Zeit, Template-basierend und auf Knopfdruck zur Verfügung zu stellen. Dies gilt für alle aktuellen Projektlösungen im SDDC-Umfeld, wie etwa VMWare NSX, OpenStack oder CloudStack. Das SDDC ist somit der nächste, logische Schritt in der Transformation der IT-Infrastruktur. Ziel ist es dabei, diese kostenoptimiert, standardisiert und äußerst flexibel zu betreiben.

Quelle: Fotolia

Nicht nur moderne Hardware, sondern auch auf Sicherheit ausgelegte Strukturen und Prozesse sind gefragt. Ein Beispiel dafür ist Mikrosegmentierung.

Was früher galt, nutzt heute wenig

Aufgrund des Wandels des herkömmlichen Rechenzentrums zum Software-defined Data Center haben sich auch die Anforderungen an das Infrastrukturdesign verändert. Auf der Infrastruktur betrieben werden verschiedene Applikationen, mit unterschiedlichen Anforderungen an Sicherheit und Audits. Sie laufen entweder virtualisiert auf einer Server-Hardware oder bei einer serviceorientierten Architektur (SOA) verteilt über die komplette Infrastruktur im Rechenzentrum.

Infolge dieser Transformation haben sich auch neue Bedrohungslagen ergeben und damit die Sicherheitsanforderungen verändert. Mangels Transparenz über das Netzwerk können Dienste und Anwendungen jedoch nicht mit dem erforderlichen Maß an Sicherheit, Schnelligkeit und Präzision bereitgestellt werden.

In den bisherigen Legacy-Umgebungen waren Applikationen und auch weitestgehend virtuelle Maschinen an die physische Hardware gebunden. Identifiziert wurden sie nach dem Old-School-Ansatz per IP- oder MAC-Adresse. Dies reicht in den heutigen Designs, etwa bei einer Service-orientierten Architektur, nicht mehr aus. Zum einen wird aufgrund der Kostenoptimierung gefordert, dass die Infrastruktur optimal und nachhaltig ausgelastet wird. Zum anderen bringen die Applikationsdesigns die Herausforderung mit sich, dass einzelne Komponenten/Dienste auf unterschiedlichen Teilen des SDDC liegen können.

Durch den SDDC-Ansatz lässt sich die Infrastruktur auf verschiedenste Weise gruppieren und mit Sicherheits- und Compliance-Regeln versehen. Eine solche Gruppierung kann nach VM-Namen, nach vir-

tualisierten Applikationen oder nach Security-Gruppen gestaltet werden. Genau an dieser Stelle wird das Thema Mikrosegmentierung interessant: Mittles dieser Gruppierungen ist man in der Lage, die virtuelle Infrastruktur als verteilte Bausteine abzusichern. Dabei kann auch die Mobilität der virtuellen Anwendungen und virtuellen Maschinen berücksichtigt werden.

Mikrosegmentierung bleibt beweglich

Ziel der Mikrosegmentierung ist es, die VM-zu-VM-Kommunikation zu schützen und eine sichere Bereitstellung von Applikationen zu realisieren. So können beispielsweise sogenannte virtualisierte Application PODs (Point of Delivery) mit der Mikrosegmentierung umgesetzt werden. Dies ermöglicht das sichere Bereitstellen von Applikationen und kann für Sichtbarkeit und Transparenz in der Infrastruktur sorgen. In den Legacy-Infrastrukturdesigns der vergangenen Jahre wurde kein besonderes Augenmerk auf diese Segmentierung gelegt. Wenn, dann wurde meist nur mit Layer-3-Segmentierung und ACLs (Access Control Lists) abgesichert.

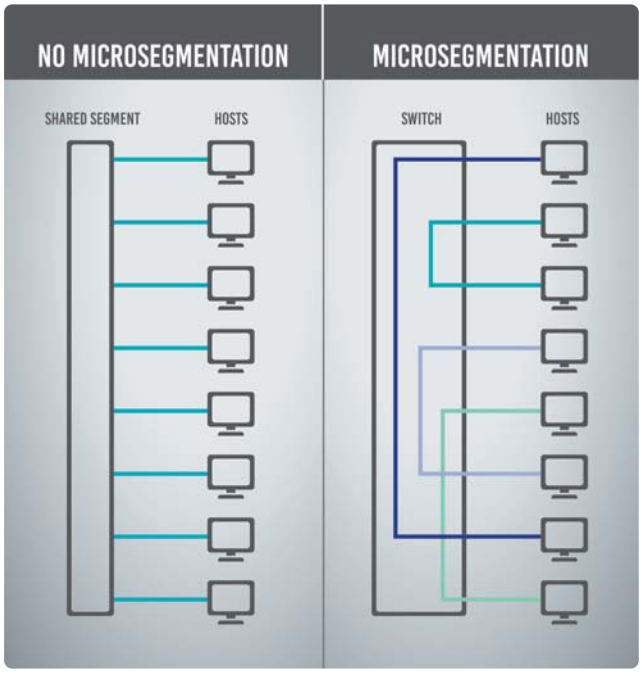
Mittels Mikrosegmentierung lässt sich eine Zero-Trust-Sicherheitszone zur Absicherung einzelner Ressourcen einrichten. In virtualisierten Netzwerken ermöglicht Mikrosegmentierung eine Firewall-Absicherung nicht nur für den Nord-Süd-, sondern auch für den Ost-West-Verkehr. Erst dank Mikrosegmentierung ist es somit möglich, fein abgestimmte Netzwerksicherheitsfunktionen für Segmente auf Layer-2-Ebene anzuwenden: Wird ein Node kompromittiert, können die Angreifer nicht auch noch auf andere Nodes im gleichen VLAN zugreifen.

Organisatorische Vorbereitung

Die Bedeutung der Mikrosegmentierung für das Rechenzentrum und die Infrastruktur zeigt sich in jüngster Zeit in Form der Integrationen in Virtualisierungsplattformen wie VMware, KVM oder auch Orchestration-Plattformen wie etwa OpenStack. Mikrosegmentierung fügt sich zudem nahtlos in den Zero-Trust-Ansatz für ein ganzheitliches Sicherheitskonzept für das Rechenzentrum und die Infrastruktur ein.

In Bezug auf Cloud Service Provider (CSP) kommt noch der Aspekt hinzu, dass das Thema SDDC die Möglichkeit bietet, die Infrastruktur an mehrere Kunden zu vermarkten. In diesem Fall wird von Multi-Tenancy-, also Mandanten-Fähigkeit gesprochen. Auch in diesem Bereich ist Mikrosegmentierung wichtig.

In der Praxis gestaltet sich das Segmentieren wie folgt: Zunächst ist eine organisatorische Vorbereitung notwendig, das heißt, es sollte bekannt sein, wie sich Applikationen, Datenbanken und andere Komponenten gruppieren lassen und welche Absicherung dadurch gewährleistet werden soll. Im nächsten Schritt muss die technische Grundlage innerhalb der VMWare-Umgebung geschaffen werden: NSX muss zur Verfügung stehen, eine Management-Plattform vorhanden und VM-basierende Firewalls einsatzbereit sein – je nach Anspruch von Sessions. Dann gilt es die Netzwerk-Topologie innerhalb von NSX zu berücksichtigen. Sobald diese Grundlagen vorbereitet sind, kann mit der Mikrosegmentierung begonnen werden.



Quelle: Palo Alto Networks

Mikrosegmentierung erschwert es selbst erfolgreichen Angreifern auf einen Schlag große Bereiche der Infrastruktur zu übernehmen.

Next-Generation-Firewalls

Herkömmliche Firewalls leisten Überwachungsmaßnahmen an physischen oder virtuellen „Engpässen“ im Netzwerk. Der Anwendungslastverkehr wird durch diese Kontrollpunkte geleitet, damit sich Regeln durchsetzen und Pakete entweder blockieren oder weiterleiten lassen. Mit dem herkömmlichen Firewall-Ansatz erreicht der Versuch einer Mikrosegmentierung schnell zwei entscheidende operative Barrieren: die Durchsatzleistung und das Verwalten von Operationen und Änderungen (Operations/Change Management).

Die erste Barriere könnte zwar mit herkömmlichen Firewalls überwunden werden, da es theoretisch möglich ist, genügend Firewalls anzuschaffen, um die zur Mikrosegmentierung erforderliche Kapazität zu erreichen. Dies dürfte aber den Kostenrahmen sprengen. Bei der zweiten Barriere wird es schon schwieriger. Die zu verwaltenden Operationen nehmen exponenziell mit der Anzahl der Arbeitslast und der zunehmend dynamischen Natur der heutigen Rechenzentren zu. Bei jedem Hinzufügen, Verschieben oder der Außerbetriebnahme einer virtuellen Maschine müssen Firewall-Regeln hinzugefügt, gelöscht und/oder modifiziert werden. Geschieht dies manuell, wäre die IT-Abteilung schnell überfordert. Genau diese Barriere hat schon viele Pläne für eine umfassende Mikrosegmentierung oder Zero-Trust-Strategie vereitelt.

Erst Firewalls der neuesten Generation („Next-Generation-Firewalls“) sind in der Lage, die Anforderungen an Datendurchsatz und Verwaltung für die Mikrosegmentierung praxisgerecht zu erfüllen. Automatisiertes Verschieben/Hinzufügen/Ändern ermöglicht es, die richtigen Firewall-Regeln umzusetzen, wenn eine Arbeitslast programmgesteuert erstellt wird. Diese Regeln folgen der Arbeitslast, wenn sie irgendwo im Rechenzentrum oder zwischen Rechenzentren verschoben wird. Wird die Anwendung stillgelegt, werden mit ihr zusammen die Sicherheitsregeln aus dem System entfernt. Dadurch kann die entscheidende Barriere überwunden werden, die eine konsequente Mikrosegmentierung zuvor unmöglich machte.

Die Integration beispielsweise der VMware-NSX-Plattform mit einer Next-Generation-Firewall macht es möglich, erweiterte Firewall-Funktionen lokal auf jedem Hypervisor zur Verfügung zu stellen. Es lassen sich Netzwerksicherheitsregeln definieren, die für einen Hypervisor bereitgestellt oder zu einem Hypervisor verschoben werden. Diese werden dann in die logische Pipeline des virtuellen Netzwerks eingesetzt. Nun

kommt das Feature-Set der Next-Generation-Firewall ins Spiel. Damit lassen sich Anwendungs-, Benutzer- und Inhalts-basierte Überwachung und Regeln an der virtuellen Schnittstelle des Workloads genau abgestimmt durchsetzen.

Integrierte Sicherheitsplattform für das moderne Rechenzentrum

Eine integrierte Sicherheitsplattform, die physische und virtuelle Formfaktoren umfasst und Next-Generation-Funktionen unterstützt: Dies ist die zeitgemäße Antwort auf die neuen Sicherheitsanforderungen im Rechenzentrum. Eine derartige Plattform liefert einen vollständigen Überblick zu den Anwendungen, die im Rechenzentrum verwendet werden und zu den Benutzern, die auf die diese Anwendungen zugreifen. Zudem sorgt sie für Schutz vor bekannten und unbekannten Bedrohungen.

Zwei entscheidende Maßnahmen für RZ-Sicherheit nach dem Next-Generation-Modell sind die Zonen-basierende Absicherung und das sichere Bereitstellen von Anwendungen:

- Beim Zonen-basierenden Absichern bieten sogenannte Zonenschutzprofile zusätzlichen Schutz zwischen bestimmten Netzwerkzonen, um diese vor Angriffen zu schützen. Das Profil muss auf die gesamte Zone angewandt werden. Daher ist das sorgfältige Testen der Profile wichtig, um Probleme mit normalem Datenverkehr zu verhindern, der diese Zonen durchquert. Mithilfe von Sicherheitszonen lässt sich beispielsweise der Oracle-basierte Speicher für Kreditkartennummern isolieren. Die Plattform zwingt Oracle-Traffic, über seine Standardports zu laufen und prüft auf Bedrohungen. Der Zugriff wird rein auf die Finanzabteilung beschränkt.
- Das sichere Bereitstellen von Anwendungen ist machtbar durch verbesserte Transparenz und genaueren Einblick in Anwendungen, Benutzer und Inhalte. Dies erleichtert es, herauszufinden, welche Anwendungen das Netzwerk durchqueren, wer sie nutzt und welche möglichen Sicherheitsrisiken drohen. Ausgestattet mit diesen Daten können Regeln für die sichere Bereitstellung von Anwendungen umgesetzt werden. Die entsprechenden Reaktionsmaßnahmen können feiner abgestimmt werden als nach dem klassischen Ansatz „Erlauben oder Verweigern“.

Dynamischer Schutz ist machbar

Perimeter-fokussierte Sicherheit wird weiterhin ihre Daseinsberechtigung haben. Die Kontrolle des Netzwerks zwischen dem Inneren des Unternehmens und dem Rechenzentrum ist jedoch entscheidend – und heute auch realisierbar. Bei einer modernen Sicherheitsplattform der nächsten Generation unterstützen dynamische, serviceorientierte Funktionen alle RZ-relevanten Sicherheitsanforderungen. Hierzu zählen Firewall, IPS, APT/Zero-Day-Bedrohungsabwehr – und insbesondere Mikrosegmentierung.

Am Beispiel der Mikrosegmentierung wird deutlich, dass sich heute eine wesentlich effektivere Absicherung im Rechenzentrum erzielen lässt. Mit herkömmlicher Sicherheitstechnik wäre dies nicht machbar. Integrieren sich die Sicherheitskomponenten in Virtualisierungsplattformen für die SDDC-Architektur wie etwa VMWare NSX, lassen sich Regeloptionen für die Mikrosegmentierung auf physische und virtuelle Workloads anwenden. Im Endeffekt steht Unternehmen damit eine ganzheitliche Lösung zur Verfügung: Damit können sie eine Mikrosegmentierung konsequent umsetzen und Regeln effizient verwalten.

Christian Hentschel,
Vice President EMEA, Palo Alto Networks

Projekt Transformator

Die badenIT GmbH ist mit einem Rechenzentrum ins Umspannwerk eingezogen

Strom im Überfluss und ein Sicherheitskonzept, das kaum zu überbieten ist – von daher bot es sich an, direkt in der Schaltzentrale des Energieversorgers einzuziehen. Allerdings verlaufen einen Meter unter dem Fußboden massive Stromleitungen. Das Neubauprojekt musste darum auch einige ganz spezielle Herausforderungen bewältigen, beim Brandschutz wie im Facility Management.

Das klingt nach einem Sicherheits-Jackpot für jeden Rechenzentrumsbetreiber: Direktschaltung zu Notrufbehörden. Security und Kameraüberwachung an 24 Stunden pro Tag, jeden Tag. Stahlbetonwände, die auch bei einem Direkteinschlag einer kleinen Propellermaschine nicht einstürzen.

Doch wie alles im Leben hat auch diese Medaille eine Kehrseite: Ein Meter unter dem Fußboden fließen bis zu 1.000 Ampere, die ganze Straßenzüge mit Strom versorgen. Dennoch: Für ihr neues Rechenzentrum entschied sich badenIT in Freiburg genau für diesen Standort – und verwandelte den Lagerraum eines Umspannwerkes kurzerhand in ein Rechenzentrum.

Argumente zum Projektstart

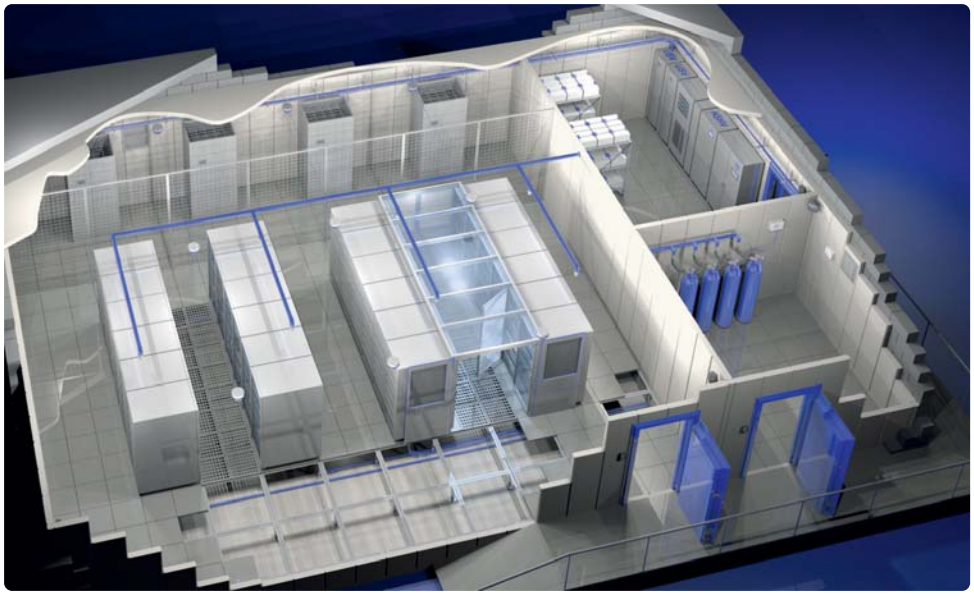
Die badenIT GmbH ist ein mittelständischer IT-Dienstleister. Zu seinem Portfolio gehören Private Cloud-Services, IT-Outsourcing, SAP sowie Rechenzentrums- und Telekommunikationslösungen. Daneben verfügt das Unternehmen über ein konzerneigenes Glasfaser- und Kupfernetz in Freiburg und bietet Breitbandanschlüsse an. Als hundertprozentige Tochter der badenova AG & Co. KG hat sich badenIT jedoch auch das Thema Energieeinsparung und Energieoptimierung auf die Fahnen geschrieben. So fiel im Rahmen einer Energieeffizienzanalyse des Dienstleisters proRZ auf, dass das Rechenzentrum des Unternehmens diesbezüglich kein unbedeutender Verbraucher ist. Gleichzeitig wurde klar, dass der Handlungsbedarf nicht nur energietechnisch, sondern auch sicherheitstechnisch besteht.

Also sollte ein zweites, neues Rechenzentrum geschaffen werden – geografisch getrennt vom ersten, in einem Bestandsgebäude der badenova. „In der Verbundwarte der badenova ist der Leitstand, der die Energieströme steuert und überwacht. Am Standort ist auch ein Umspannwerk des Energieversorgers, das 110.000 Volt auf 20.000 umwandelt. Der knapp 400 Quadratmeter große Lagerraum des Umspannwerks schien uns eine gute Grundlage für die physische Sicherheit des Rechenzentrums zu sein“, erklärt Ralf Held. Als Leiter der IT-/TK-Services bei badenIT hatte er den Auftrag das Projekt umzusetzen.

Da das Schalthaus zahlreiche Haushalte mit Strom versorgt, ist es entsprechend wichtig und gesichert: Einbruchmeldeanlagen, Videoüberwachung, 24-stündige Kontrolle aller kritischen Funktionen. Die massiven Stahlbetonwände des Gebäudes halten sogar dem Absturz einer zweimotorigen Turboprop stand, so Held.

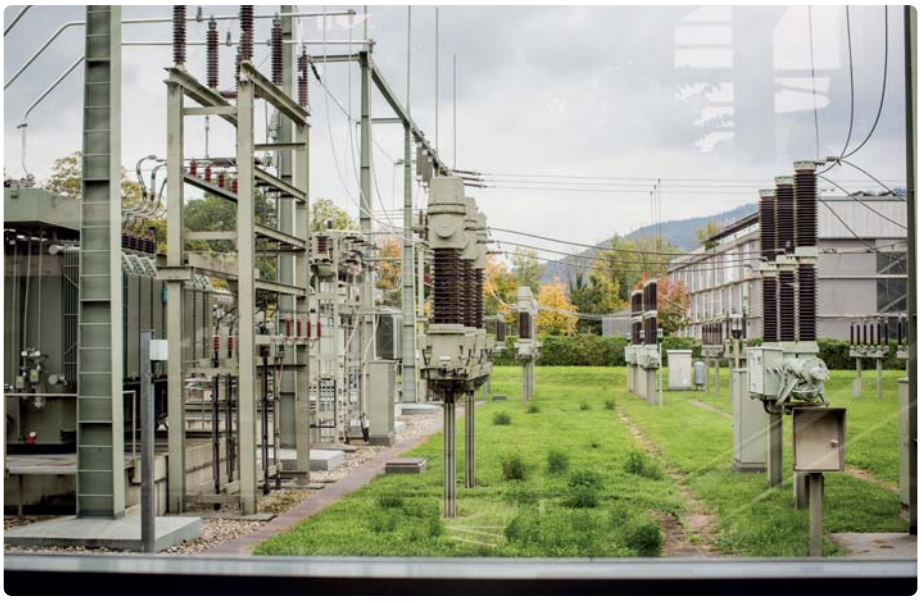
Energieversorgung samt Magnetfeld

Die Stromversorgung für das Rechenzentrum ist naturgemäß vorhanden. Sie kommt mittels zweier Trafostationen direkt von den 20.000 Volt des Umspannwerkes. Darüber hinaus können eine Netzersatzanlage mit 630 Kilovoltampere und 4.000 Liter Brennstoffvorrat die Leistung des Rechenzentrums für rund 45 Stunden aufrechterhalten. Jedoch war es wichtiger, sicherzustellen, ob ein Rechenzentrum in einem Lagerraum eines Umspannwerks überhaupt realisiert werden kann. Denn einen Meter unter dem Fußboden verlaufen massive Stromleitungen, mit weit-



Quelle: Data Center Group

Das Rechenzentrum der badenIT befindet sich in einem gesonderten Brandabschnitt. Auf rund 75 Quadratmetern sind 32 Serverschränke mit je 42 Höheneinheiten untergebracht.



Quelle: badenIT

Spannend: badenIT errichtete das neue Rechenzentrum im Gebäude eines Umspannwerks, was unter anderem besondere IT-Racks voraussetzt.

reichenden Konsequenzen für Brandvermeidung und -löschung sowie Facility Management.

Mithilfe einer Ausschreibung fand badenIT mit proRZ einen Partner, der die Entwicklung und Umsetzung des Rechenzentrums aus einer Hand unterstützen und begleiten kann. Der Dienstleister hat als Generalunternehmen das Planen, Realisieren und auch Warten des Rechenzentrumsbereichs übernommen. Held: „Uns war es wichtig, dass wir einen zentralen Ansprechpartner haben."

So analysierte proRZ zunächst die Situation. Eine Messung der Magnetfelddichte ergab zum Beispiel, dass gewöhnliche Serverschränke den elektromagnetischen Effekt der Stromleitungen verstärken würden, weshalb non-ferromagnetische Racks eingesetzt wurden. Daneben konnte durch zwei Standorte eine gänzlich neue IT-Strategie eingesetzt werden: Neue Technik ersetzte das bestehende Storage System an beiden Standorten. Zudem wurden alle physischen Systeme virtualisiert, die im Rahmen der Umzüge in den Räumlichkeiten angefasst werden mussten.

Ressourceneffizienz und Kühlung

Schließlich setzte badenIT auf eine Hochverfügbarkeits-Sicherheitslösung der RZproducts, einem Schwesterunternehmen der proRZ. Ausschlaggebend war, dass sich die einzelnen Bestandsgewerke des „QuartzITe-Raums" in die vorhandene Gebäudestruktur anpassen und integrieren ließen. So befinden sich die IT-Systeme in eigenen Sicherheitszellen: Einem Backup-Raum mit rund 18 Quadratmetern sowie zwei USV-Räumen von je elf Quadratmetern und 200 Kilowatt Leistung.

Das Rechenzentrum befindet sich in einem gesonderten Brandabschnitt. Auf rund 75 Quadratmetern sind 32 Serverschränke mit je 42 Höheneinheiten untergebracht. Die Klimaanlage belegt acht Racks des Rechenzentrums. Die InRow-Präzisions-Sidecooler mit je 31 Kilowatt werden von drei Kaltwassersätzen mit je 122 Kilowatt und sechs Klima-Innengeräten zu je zehn Kilowatt unterstützt. Die komplette Raum-in-Raum-Lösung weist einen Brandschutz mit Feuerwiderstand F90 gemäß der Normen DIN 4102 und EI90 nach EN 1363 auf. Zudem hält sie die Grenzwerte der EN 1047-2 für Temperaturanstieg und relative Luftfeuchtigkeit mindestens 30 Minuten ein.

Neben dem eigentlichen Energiebedarf des IT-Equipments, bei dem es nur geringes Optimierungspotenzial gibt, liegt der Hauptanteil des Strombedarfs bei der Kühlung und den Verlusten der Stromversorgung. Unter der Berücksichtigung des IT-Wachstums wollten die RZ-Betreiber den Strombedarf für den Einsatz von ITK im Rechenzentrum nachhaltig senken und gleichzeitig ein besonderes Augenmerk auf energieintensive Bereiche legen.

Kaltwassersätze zur Kälteerzeugung sowie InRows zu Kälteverteilung beispielsweise unterliegen einem komplexen Regelungsprozess, der bei sich ständig ändernden Rahmenparametern überwacht und gegebenenfalls korrigiert werden muss. Daher setzte proRZ auch eine Lösung für nachhaltiges Energiemanagement ein: Das Monitoring Tool „DC-ITMonitoring" ermittelt alle relevanten Energiekennzahlen, schafft Transparenz bei Verbräuchen und Anlagenfahrweisen und visualisiert diese. Damit kann badenIT nicht nur Optimierungspotenzial bei Energiekosten aufdecken und die Verfügbarkeit seiner IT-Infrastrukturen gewährleisten. Das Unternehmen kann durch die Daten ebenfalls eine langfristige Strategie erarbeiten, welche die Energie- und Ressourceneffizienz des Rechenzentrums erhöht. Das würde auch das Umweltsiegel „Blauer Engel für energiebewussten Rechenzentrumsbetrieb" testieren, welches badenIT ebenfalls anstrebt.

Fertigstellung und Regelbetrieb

„Wir haben den Auftrag für das Rechenzentrum im Januar erteilt. Vor der Inbetriebnahme hat proRZ alle Systeme einzeln und das Rechenzentrum als Ganzes in einem Lasttest geprüft. Schon im Juli konnten wir das Rechenzentrum dann abnehmen", sagt Held.

Der Bau eines Rechenzentrums ist jedoch nur ein Teil. Der anschließende Betrieb der Infrastruktur ist hinsichtlich Funktionalität und besonders Betriebssicherheit genauso wichtig. Allgemein gelten für den Betrieb des Rechenzentrums die Prozesse der ISO 27001 und der ISO 20000. Betreiber müssen die Systeme demnach laufend warten und an veränderte Betriebsbedingungen anpassen. Als Errichter der Anlage war es daher naheliegend, die proRZ auch mit der Wartung der Gebäudetechnik zu beauftragen.

Im Rahmen dieser Wartung beziehungsweise proaktiven Instandhaltung werden Auffälligkeiten vom Dienstleister an badenIT gemeldet. Zudem werden Maßnahmenvorschläge unterbreitet oder zum Teil sofort umgesetzt. Dazu überprüft der Anbieter alle Gewerke der Rechenzentrumsinfrastruktur außer der primären Energieversorgung sowie der Netzersatzanlage. Die Wartungsmaßnahmen und Zyklen richten sich dabei nach Art der Gewerke und Systeme. Diese sind die IT-Sicherheitsraumsysteme, das Elektromanagement inklusive Verteilung und Elektroinstallation sowie die Klima-, Kaltwasseraußen-, Be- und Entlüftungs-, USV-, Feuer-, Brandmelde- und Brandfrühst-Erkennungsanlage.

Simon Federle,
freier Autor, Augsburg

Keine Angst vor einem IT-Energieaudit!

Kleinen und mittleren Unternehmen hilft eine durchdachte Klimatechnik

Als ob die Stromkosten kein Argument wären, verpflichtet DIN EN 16246-1 produzierende Unternehmen zu einem jährlichen Audit. Wer aber weiß, wie sich ein IT-gerechtes Energiemanagement samt Klimatisierung planen und umsetzen lässt, darf die Untersuchung getrost auf sich zukommen lassen.

Der Energieverbrauch in Ihrem Unternehmen erfüllt nicht die Vorgaben der aktuellen DIN." Diese und ähnliche Aussagen müssen sich Geschäftsführer, RZ-Betreiber und IT-Leiter heutzutage anhören. Auf derartige Sätze folgt zumeist das Auflisten von Begrifflichkeiten, Zahlenfolgen und Anforderungen wie DIN, ISO, 50001. Dies steigert die Verwirrung des Zuhörers nur noch mehr. Kommt dann noch der Energieaudit ins Gespräch, wird es gänzlich unangenehm.

Der allgemeinen Verunsicherung beziehungsweise Verwirrung gilt es zunächst entgegenzuwirken. Dazu hilft es, Licht ins DIN-ISO-Dickicht bringen und einen kurzen Blick auf die Rechtslage werfen: Die DIN EN 16247-1 wurde im Oktober 2012 in deutscher Fassung veröffentlicht und beschreibt die Anforderungen an ein Energieaudit, mit dessen Hilfe ein Unternehmen seine Energieeffizienz verbessern und den Energieverbrauch reduzieren kann.

Quelle: Conect Informationssysteme

Bei der optimalen Raumausnutzung empfiehlt sich eine Rackbreite von 660 mm. In Kombination mit Trägerprofilen und den rundum offenen Gitterbahnen ergibt sich ein Innenskelett.

Seit dem 01.01.2013 sind kleine und mittlere Unternehmen (KMU) des produzierenden Gewerbes unter 250 Mitarbeitern verpflichtet, ein jährliches Energieaudit nach DIN EN 16247-1 durchzuführen, wenn sie staatliche Vergünstigungen im Rahmen des Spitzenausgleichs (vgl. 55 EnStG bzw. § 10 StromStG und SpaEfV) erhalten möchten. Das Audit dient in erster Linie dem Erkennen von Einsparpotenzialen und gibt dafür entsprechende Methoden vor.

Alternativ zum Energieaudit ist für KMU auch die Einführung eines Energiemanagementsystems nach DIN EN ISO 50001 möglich. Bei Nicht-KMU ist dies sogar verpflichtend, ein Audit also nicht mehr ausreichend. Auch die neue Ausgleichsregelung nach dem EEG 2014 erfordert für KMU des produzierenden Gewerbes ab einem jährlichen Energiebedarf von einer Gigawattstunde ein Energieaudit beziehungsweise ab fünf Gigawattstunden das Einführen eines Energie- oder Umweltmanagementsystems.

Belege, Begehung und Bericht

Nach der europäischen Norm EN 16247-1 ist ein Energieaudit eine „systematische Inspektion und Analyse des Energieeinsatzes und des Energieverbrauches einer Anlage, eines Gebäudes, eines Systems oder einer Organisation mit dem Ziel, Energieflüsse und das Potential für Energieeffizienz-Verbesserungen zu identifizieren und über diese zu berichten." Vor dem Audit müssen Ziele, Anforderungen, Anwendungsbereich und Grenzen des Energieaudits, Zeitraum der Durchführung und Anforderungen an die Daten, die vor Beginn des Audits zu sammeln sind, vereinbart werden.

Das eigentliche Audit besteht aus einer Einführungsbesprechung, dem Erfassen von Daten (historische Daten zum Energieverbrauch, vorherige Untersuchungen in Bezug auf Energie und Energieeffizienz, Energietarife und so weiter) und einer Begehung des zu prüfenden Objekts. Sodann folgt eine Analyse der ermittelten Energieflüsse und der Energiebilanz sowie der Faktoren, die den Energieverbrauch beeinflussen. Dies ist die Basis fürs Ermitteln geeigneter Energiekennzahlen und Energiesparmaßnahmen. Anschließend werden die wesentlichen Einsparpotenziale und -maßnahmen in einem Energiebericht zusammengefasst.

Der Begriff Energiemanagement umfasst die Summe aller Maßnahmen, die geplant und umgesetzt werden, um bei geforderter Leistung einen minimalen Energieeinsatz sicherzustellen. Ziel ist das kontinu-

ierliche Verbessern der Energieeffizienz im Unternehmen. Ein Energiemanagementsystem erfasst dazu systematisch die Energieströme und nimmt dann anhand der Ergebnisse Einfluss auf organisatorische und technische Abläufe sowie Verhaltensweisen.

Die DIN EN ISO 50001 ist ein solches systematisches Energiemanagementsystem. Es hilft insbesondere mittleren und größeren Unternehmen, ihren Energieverbrauch kontinuierlich und systematisch zu beobachten, regelmäßig nach Energieeffizienzmaßnahmen zu suchen und dies dann auch von einem externen Auditor zertifizieren zu lassen. Unter wirtschaftlichen Gesichtspunkten senkt ein Energiemanagementsystem somit den betrieblichen Gesamtenergieverbrauch sowie den Verbrauch von Grund- und Zusatzstoffen.

Auf Basis einer qualifizierten Energieanalyse lassen sich Möglichkeiten erkennen und entsprechende Verbrauchsminderungen umsetzen. Das Audit nach DIN EN 16247-1 ist jedoch keine Managementsystem-Norm. Sie ist weder mit der DIN EN ISO 50001 vergleichbar, noch eine Zertifizierung. Sie bewertet den Istzustand des Energieverbrauchs, gibt jedoch noch keine Anhaltspunkte für eine kontinuierliche Energieeinsparung, wie es in einem Managementsystem beabsichtigt ist. Nichtsdestotrotz ist ein Energieaudit nach dieser Norm ein erster Schritt für eine erfolgreiche Zertifizierung nach DIN EN ISO 50001. So entspricht die Vorgehensweise des Energieaudits weitgehend der energetischen Bewertung nach dem Managementsystem. Ein durchgeführtes Audit erleichtert insofern das Einführen eines Managementsystems.

Wer richtig kühlt, kann cool bleiben

Doch welche Komponenten gilt es zu optimieren, damit die Angst vor dem Audit gar der allgemeinen Vorfreude weicht? Neben baulichen Maßnahmen stehen hier insbesondere die gewerkeübergreifenden technischen Ausstattungen an erster Stelle: Klima, Energieversorgung und Sicherheit. Ebenfalls zu berücksichtigen sind Energie- und Betriebskosten.

Klimaanlagen beispielsweise sind längst übliche Geräte in den Serverräumen; doch oft werden sie mit der Hitzeentwicklung nicht fertig. Sie arbeiten bei vielen Anwendern am Anschlag und dabei ist ein Ende der Hitzewelle nicht abzusehen. Sowohl für den Betreiber als auch für die Anlage(n) selbst gilt aber: cool bleiben. Mit der energieeffizienten Kühlung steht und fällt das gesamte Energiemanagementsystem.

Die Herausforderung ist oft, neue Wege zu finden, insbesondere um die Kühlung einer Anlage zu sichern. Cool bleiben die Rechner und Hochleistungssysteme nur in einem optimal klimatisierten Umfeld. Oft helfen System- beziehungsweise Modullösungen, um einerseits die IT-Verfügbarkeit zu steigern und andererseits die Energie- und Betriebskosten zu senken. Es empfehlen sich Lösungskombinationen aus Kühltechnik, Luftführung, Energieverteiler und Monitoring-Systemen.

Generell gilt: Kompaktheit ist Trumpf; kompakt sowohl in den baulichen Dimensionen von Rack und Kühlung als auch in der Energieversorgung und im Bereich Datacenter Monitoring. Bestenfalls sind E-Verteiler mit grafischer Oberfläche – in 19-Zoll-Bauform und hinter Glastüren – direkt im Rackbereich integriert, mit kurzen Wegen zu PDU-Anschlusseinheiten und kompakten, steckbaren Abzweig- und Verteilerblöcken. Diese Konstruktion steigert die Flexibilität und sichert zudem den störungsfreien Betrieb.

Eine andere Maßnahme betrifft das Zusammenspiel zwischen Kühlluftführungen und Kaltgangausbildungen. So wird die Energieeffizienz des gesamten Serverraums beziehungsweise IT-Bereichs durch gezielte Kühlluftführungen deutlich verbessert. Auch empfiehlt sich eine offene Struktur ohne Schrankholme. Diese Bauart unterstützt den Anschluss aktiver Komponenten oder Core-Verkabelungen, ohne zugleich strömungshinderlich für Kühlluftführungen zu sein.

Quelle: Conect Informationssysteme

Es empfiehlt sich eine offene Struktur ohne Schrankholme, da es so nicht zu Hitzenesterbildung oder PDU-Betriebstemperaturüberschreitung kommt.

Das Ergebnis: Die Problematiken Hitzenesterbildung oder PDU-Betriebstemperaturüberschreitung treten in der Praxis nicht auf. Die mit solchen und ähnlichen Maßnahmen erreichten Werte beziehungsweise Einsparungen klingen aufs erste Gehör nicht sonderlich spektakulär. Wenn das RZ ein Kilowatt Einsparung im IT-Bereich erreicht, senkt das die Energiekosten im Mittel aber bereits um gut 1500 Euro im Jahr.

Gut für den Betrieb, gut fürs Klima

Die IT-gerechte Klimatisierung ist das größte Problem beim störungsfreien RZ-Betrieb. Innerhalb eines thermisch stark belasteten IT-Bereichs gilt es, ein Klima zu erzielen, in dem sich IT-Komponenten nicht nur störungsfrei, sondern auch schonend betreiben lassen. Voraussetzung ist eine stabile Temperatur zwischen 21 und 28 Grad Celsius sowie eine relative Luftfeuchtigkeit nach aktuellen Erfordernissen.

Über- beziehungsweise Unterschreitungen führen zu Störungen und Ausfällen, eine zu hohe Feuchte fördert Korrosionen, eine zu niedrige Feuchte kann statische Aufladung und Kurzschlüsse nach sich ziehen. Auch hier liegt die Lösung in der gezielten Luftzuführung, die in jedem Fall in einen Warm- und Kaltbereich ausgeführt sein sollte. Bei Bestandssystemen mit Doppelboden sollte der Planer grundsätzlich eine Luftführung von unten nach oben anstreben beziehungsweise gegebenenfalls nachrüsten. Die Zuluft wird dann über einen ausreichend dimensionierten Doppelboden zugeführt und über Schlitzplatten gezielt zu thermisch stark belasteten Stellen weitergeleitet.

Zugegeben: Die Rechtslage im DIN-ISO-Dschungel erscheint auf den ersten Blick verwirrend. Die Angst vor einem Energieaudit oder der Einführung eines Energiemanagementsystems ist jedoch unangebracht, wenn einige grundlegende Regeln beachtet und die Bereiche IT, Klimatisierung und Sicherheit stets im Zusammenspiel gesehen werden. Kompetente Planer wissen um dieses Zusammenspiel und können schnell beruhigen, sofern einige einfache Maßnahmen durchgeführt werden.

Karl-Heinrich Spiering,
Geschäftsführer, Conect Informationssysteme GmbH

Kalifornien rechnet schon auf Reserve

Für Anbieter von Effizienztechnik sind die USA ein attraktives Ziel

Der US-Rechenzentrumsmarkt wächst stark, besonders im Bereich Green IT. Brennpunkt der Entwicklung ist Kalifornien, wo die Regulierung von den Betreibern deutlich klima- und energiebewusstere Anlagen fordert. Darin kann auch eine Exportchance für deutsches Technik-Know-how liegen.

Der US-Markt ist für Anbieter von RZ-Technologien wegen seiner schieren Größe verheißungsvoll: Rund drei Millionen Rechenzentren aller Größenordnungen soll es dort geben. Und der RZ-Markt wächst weiter, nach Daten von JLL Research derzeit jährlich um 32 Prozent. 2017 soll er ein Volumen von etwa 36 Milliarden Dollar haben. Der Markt für Rechenzentrumsbau soll auf 18 Milliarden US-Dollar wachsen. Auch der Markt für energieeffiziente Rechenzentren legt mit 29 Prozent jährlich stark zu und soll nach Daten der Fast Company, die allerdings schon aus dem Jahr 2010 stammen, bis 2015 das Volumen von 13,81 Milliarden Dollar erreichen. Weltweit stehen rund 43 Prozent der Kollokationsflächen in Nordamerika. Die Zahl der Beschäftigten im US-RZ-Markt soll zwischen 2014 und 2019 nach Daten von JLL Research um 17 Prozent auf dann knapp 600.000 Beschäftigte steigen.

Eine aktuelle Analyse der Deutsch-Amerikanischen Handelskammern beschäftigt sich nun damit, wie die Gegebenheiten auf dem US-Rechenzentrumsmarkt im Detail aussehen und welche Chancen oder Risiken sich dadurch für deutsche Anbieter von Effizienztechniken für Rechenzentren eröffnen. Das kommt nicht von ungefähr: Die USA gehören seit jeher zu den wichtigsten Handelspartnern Deutschlands. 3500 deutsche Unternehmen sind laut der Studie dort aktiv und beschäftigen rund 580.000 Mitarbeiter. Deutschland ist der viertgrößte Investor in den USA und importierte 2014 Waren im Wert von rund 48 Milliarden US-Dollar aus den USA. In die USA wurden Waren im Wert von rund 95 Milliarden Euro exportiert. 2013 lag das Exportvolumen noch bei 83,66 Milliarden Dollar.

Land der unbegrenzten Vorschriften

Trotzdem hat der US-Markt auch einige Schlaglöcher für deutsche Importeure. Für Technik etwa gilt eine verwirrende Vielfalt an Standards. Beim ANSI (American National Standards Institute) sind über 250 Standard-Entwicklungsorganisationen akkreditiert. Es gibt neben nationalen auch staatliche Gesetze und lokale Regulierungen. International anerkannte Standards von ISO und IEC konkurrieren mit 800 weiteren Standards teilweise zu denselben Themen.

Dazu kommen in manchen Bereichen Verpflichtungen, lokal zu kaufen. Sie gelten beispielsweise für Stahl, der ja in der Regel beim Rechenzentrumsbau benötigt wird. Dazu können gegebenenfalls Zölle kommen. Zudem legen, so die Studie, US-Kunden mehr Wert auf Präsentation und einfache Nutzbarkeit als aufs technische Detail. Wer das nicht berücksichtigt, kann schnell Schiffbruch erleiden. Wegen der schieren geografischen Größe des Marktes ist es zudem gerade kleineren und mittleren Unternehmen anzuraten, mit lokalen Partnern zu arbeiten.

Der jährliche Energieverbrauch der USA betrug 2014 2,3 Milliarden Tonnen Öläquivalente. Erneuerbare Energien machen derzeit nur einen Anteil von 13 Prozent aus, wobei über die Hälfte aus Wasserkraft stammt. Hemmend für Effizienztechniken wirken sich die in den USA die durch die Förderung unkonventioneller Schiefergasvorräte steigenden Fördermengen fossiler Energieträger und die äußerst geringen,

Quelle: Deutsch-amerikanische Handelskammer/Fast Company

Dem Green-IT-Markt der USA prognostizierte Fast im Jahr 2010 ein Wachstum von 29 Prozent jährlich.

tendenziell weiter fallenden Energiepreise aus. Sie verlängern die Amortisationsperiode für Effizienzprodukte erheblich oder machen sie gar ganz unattraktiv.

Stromrechnung über 13,7 Milliarden US-Dollar

Zwei Prozent der elektrischen Energie wurden von Rechenzentren aufgenommen, die Hälfte davon von kleinen und mittleren Rechenzentren. Der Strombedarf von US-Rechenzentren soll 2020 laut einer Studie des National Resource Defense Council (NRDC) aus dem Jahr 2014 bei 139 Millionen Megawattstunden liegen. 26 1-Gigawatt-Kraftwerke wären erforderlich, um diesen Strombedarf zu decken. Die daraus resultierende Stromrechnung betrüge 13,7 Milliarden Dollar. Das sind 52,2 Prozent mehr Kosten als 2013. Die Strompreise für die Industrie lagen im Durchschnitt 2014 bei 7,1 US-Cent pro Kilowattstunden und dürften moderat steigen.

Das NRDC nennt folgende Gründe für den hohen Stromverbrauch und seinen Anstieg:

- Rund 20 bis 30 Prozent der Server sind veraltet oder werden nicht mehr genutzt, bleiben aber trotzdem am Strom,
- temporär ungenutzte Server werden nicht heruntergefahren, sondern bleiben eingeschaltet,
- Systeme werden für Spitzenlasten und höchste Verfügbarkeitsanforderungen dimensioniert und Virtualisierungslösungen sind noch längst nicht so verbreitet wie man annehmen dürfte. Daten von IDC und Gartner aus dem Jahr 2014 beispielsweise gehen davon aus, dass weltweit erst auf 30 Prozent der neu installierten physikalischen Server eine Virtualisierungstechnik läuft, die den Betrieb virtueller Maschinen oder Container gestattet.

Große Rechenzentrumsbetreiber beginnen inzwischen, sich der staatlichen Fördermöglichkeiten für Erneuerbare Energien in den USA zu bedienen. Davon gibt es vor allem zwei: RPS (Renewable Portfolio Standards) legen fest, welcher Anteil erneuerbarer Energien sich im Strommix eines Providers befinden muss. Dieser wird proportional erhöht. US-Bundesstaaten haben jeweils eigene RPS-Bestimmungen.

Ökoquoten und neue Standards

Mit Renewable Electricity Certificates (REC), dem zweiten Fördermechanismus, können Betreiber von Anlagen zur Erzeugung erneuerbarer Energie die Menge an Energie, die den durch RPS festgelegten Mindestanteil für erneuerbare Energien übersteigt, in Form von Zertifikaten an andere Stromversorger verkaufen, damit diese ihre Quoten einhalten. Rechenzentrumsbetreiber wie Yahoo beteiligen sich mittlerweile selbst am Bau von Wind- oder Solaranlagen oder kooperieren direkt mit Stromerzeugern, um von diesen Mechanismen zu profitieren, ihr Umweltimage zu verbessern und sich von den Unwägbarkeiten fossiler Energieversorgung unabhängig zu machen.

Die wichtigsten Gebäudestandards für den Bau von Rechenzentren sind die ASHREA-Richtlinien für Datenverarbeitungsumgebungen, die Zuluft-Temperaturen zwischen 18 und 27 Grad Celsius und Luftfeuchtigkeiten zwischen 60 und 80 Prozent relative Feuchte vorschreiben. Sie beschreiben zudem zwischen sechs Klassen von IT-Umgebungen, wobei die Klasen A1 bis A4 Rechenzentren betreffen.

Quelle: Deutsch-amerikanische Handelskammer

Wirksamkeit und Kosten von Energieeffizienz-Maßnahmen im Rechenzentrum.

Der noch in Arbeit befindliche ASHREA-Standardentwurf 90.4P macht Vorgaben für den Energiegebrauch in Rechenzentren mit Schwerpunkt auf Konstruktion, Planung, Betrieb, Wartung und Erneuerbarer Energie. Außerdem gelten in den USA die ISO-Standards 50001:2011 sowie 14001:2004. Ersterer fordert Richtlinien für die Energienutzung, datenbasierende Energieverbrauchsprognose und Effizienzverbesserung und den Einkauf energiesparsamen Equipments. Letzterer dient dem Vermeiden negativer Umwelteinwirkungen, unter anderem durch entsprechende Kontroll- und Managementsysteme.

Auch Rechenzentren können seit 2012 nach dem Umwelt-Gebäudestandard LEED (Leadership in Energy and Environmental Design) for Data Centres Existing Buildings: Operations & Maintenance zertifiziert werden, wovon einige Firmen wie Apple, VMware oder Digital Realty bereits Gebrauch gemacht haben. Zertifizierte Rechenzentren nutzen energiesparsame Kühlsysteme hohen Wirkungsgrads, sauberen Notstrom, verbrauchen weniger Energie und verwenden erneuerbare Energieträger. Sind die Server eines Rechenzentrums Energy-Star-zertifiziert, kann sich das Rechenzentrum und das Gebäude, in dem sich das RZ befindet, mit dem Energy-Star-Logo schmücken, was beispielsweise Equinix tut.

Effizienzförderung in den USA

Zudem zielen in den Vereinigten Staaten diverse öffentliche Förderprogramme und Initiativen darauf, die Effizienz von RZ zu erhöhen:

- Die Better Buildings Data Center Accelerator Initiative bietet zusammen mit dem Energieministerium der USA (DOE, Department of Energy) ein Programm an, bei dem sich die RZ-Betreiber verpflichten, den Energieverbrauch mindestens eines ihrer Rechenzentren um fünf Prozent innerhalb von fünf Jahren zu verringern und die Verbrauchsdaten regelmäßig zu veröffentlichen.

Quelle: Deutsch-amerikanische Handelskammer/Computerworld

STROMVERBRAUCH DER US-RECHENZENTREN 2013 UND 2020*

Jahr	Endverbrauch der Energie (in Mrd. kWh)	Stromrechnung (in Mrd. USD)	Kraftwerke (500 MW)	CO_2 (in Mio. T)
2013	91	9	34	97
2020	139	13,7	51	147
Anstieg	52,70 %	52,20 %	50 %	51,50 %

*Prognose

- Das National Data Center Energy Efficiency Information Program von EPA (Environmental Protection Agency, US-amerikanisches Bundesumweltamt) und DOE koordiniert diverse mit der Energieeffizienz von RZ befasste Initiativen und Verbände, unter anderem The Green Grid oder Uptime Institute. Es hilft, einheitliche Messprotokolle für RZ und Verbesserungsmöglichkeiten hinsichtlich der Energieeffizienz zu entwickeln. Weiter zertifiziert das Programm Experten, verleiht Best-in-Class-Awards an besonders effiziente Rechenzentren und führt Effizienzlogos für IT-Equipment ein.
- Das DOE hat zudem eine Online-Tool-Suite (online unter https://datacenters.lbl.gov/tools) zum Steigern der RZ-Effizienz entwickelt und führt eine Umfrage hinsichtlich der Energieeigenschaften von Rechenzentren durch. Im Rahmen einer US-weiten Initiative zur Verringerung der Abhängigkeit von Erdölexporten steckt das DOE rund 47 Millionen US-Dollar in RZ-Effizienzprojekte.

Dazu kommen Bestrebungen des privaten Sektors, beispielsweise die Open-Compute-Intitative oder Gelder, die etwa Microsoft an RZ-Effizienz-bezogene Forschungsprojekte vergibt. Auch einige Energieversorger bieten spezielle Incentive-Programme für Effizienzmaßnahmen von RZ-Providern an.

Kalifornien kämpft gegen den Kollaps

Kalifornien mit seinen mehr als 800, oftmals sehr großen Rechenzentren und seiner Agglomeration der IT-Industrie in San Francisco, Silicon Valley und Los Angeles, geht noch einige Schritte weiter. Das ist auch dringend anzuraten, da Rechenzentren in der Dürreregion im südlichen Kalifornien zunehmend wegen ihres hohen Energie- respektive Wasserverbrauchs ins Gerede geraten.

Gleichzeitig sind sie ein wichtiger Wirtschaftsfaktor: So gibt es im Silicon Valley insgesamt 3,6 Millionen Quadratmeilen RZ-Fläche, von denen 2014 nur 73.000 frei zur Verfügung standen. Nachgefragt werden diese Flächen primär vom (elektronischen) Handel, Technologiefirmen und Finanzdienstleistern (jeweils 20 Prozent).

Zum Senken des RZ-Energiebedarfs dienen insbesondere veränderte, seit 2014 gültige Bauregeln (Title 24 der Building Codes). Sie erfordern die Installation von Economizern in kleinen Serverräumen, die Nutzung adiabatischer Befeuchtungssysteme, begrenzen den Einsatz von Lüftersystemen in Computerräumen und fordern volumenstromvariable Klimaanlagen und Expansionssysteme für RZ.

Der Energieversorger Southern California Edison vergütet für die Reduktion von Verarbeitungslasten acht Cent pro Kilowattstunde. Dazu kommen diverse lokale oder regionale mit finanziellen Anreizen ausgestattete Effizienzprogramme, die auch für RZ-Betreiber sinnvoll sind.

Kontaktanbahnung für Exporteure

Aus alledem ergibt sich nach Meinung der Exportinitiative Energieeffizienz ein sehr gutes Chance-Risiko-Verhältnis für innovative deutsche Anbieter von effizienten Strominfrastruktur-Lösungen, Klimatisierungssystemen, Produkten für das Luftstrommanagement und Systemen, die IT an sich effizienter machen.

Deshalb organisiert die Berliner Agentur Energiewächter im Auftrag der Exportinitiative nun eine erste vom Bundesministerium für Wirtschaft und Umwelt subventionierte, Anfang November stattfindende Reise ins Silicon Valley. Zielgruppe sind Vertreter innovativer kleiner und mittlerer Unternehmen, die ihre Energieffizienz-Produkte für Rechenzentren gern dort präsentieren und in den US-Markt einführen möchten. Sollte die Reise erfolgreich im Sinne der Anbahnung von Kontakten und Partnerschaften verlaufen, werden weitere folgen.

Ariane Rüdiger,
freie Autorin, München

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:
Frank Beckereit, Friederike Busch, Simon Federle, Andreas Gömmel, Christian Hentschel, Markus Löffler, Ariane Rüdiger, Wilfried Schneider, Karl-Heinrich Spiering

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

AGIL ANS ZIEL.

iX. MEHR WISSEN.

Jetzt für nur 9,90 € bis 1.11. portofrei bestellen.

shop.heise.de/ix-it-projekte ✉ service@shop.heise.de

Auch als eMagazin erhältlich unter: shop.heise.de/ix-it-projekte-pdf

Generell **portofreie Lieferung** für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €

heise shop

shop.heise.de/ix-it-projekte