Eine Themenbeilage der
Heise Medien GmbH & Co. KG

IV
2017

RECHENZENTREN UND INFRASTRUKTUR

SERVER, KABEL, CLOUD-COMPUTING

Wo Datacenter gern Energie sparen

Klimatisierung: Wie effiziente Wasserkühlung arbeitet

Green Hosting: Wer ein Colocation-RZ im Windpark baut

Container Security: Wann Docker-Images sauber bleiben

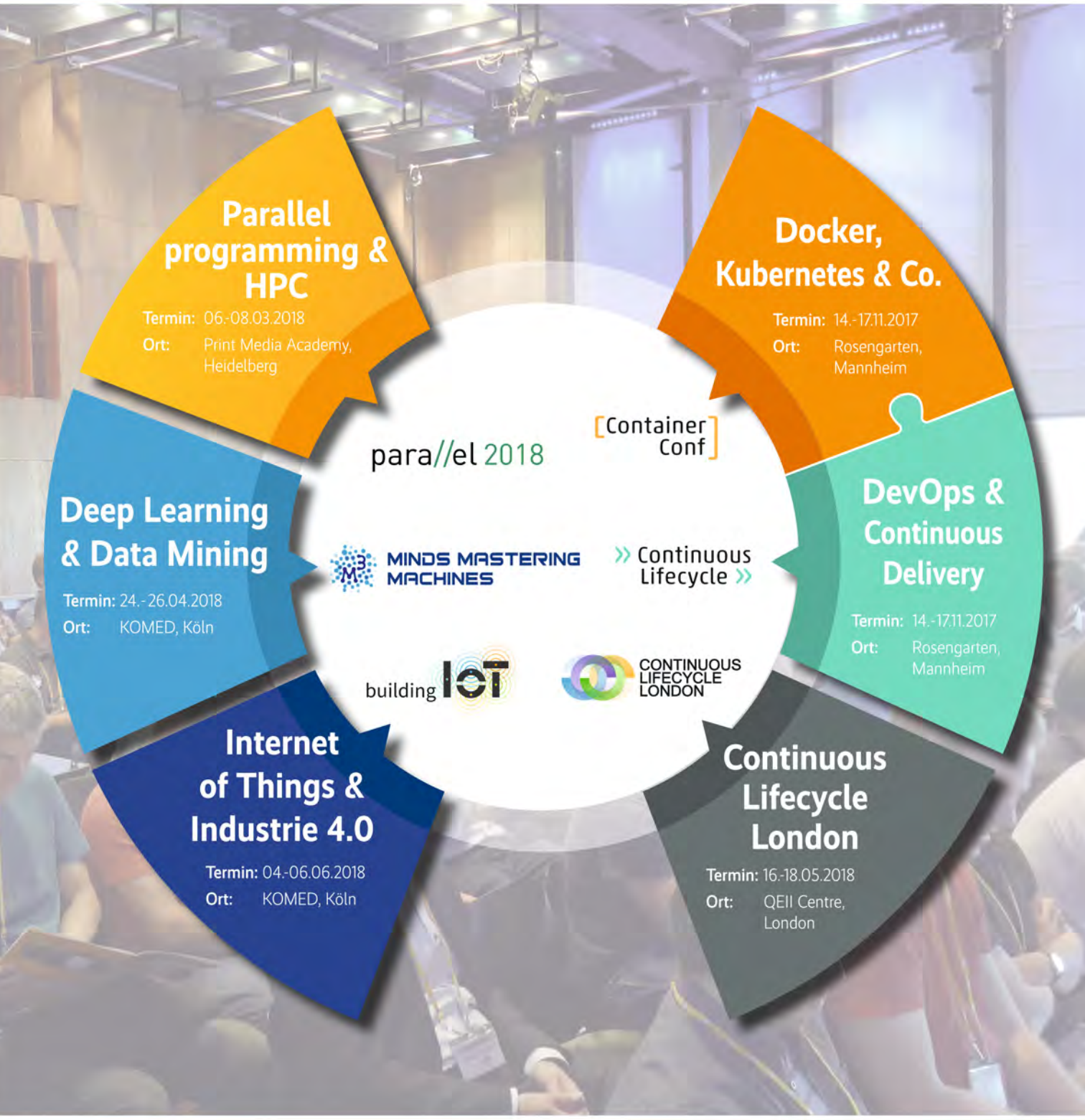
Verkabelung: Wer im Mesh-Layer den Durchblick behält

Fasermanagement: Wie ODFs im Verteilerschrank aufräumen

Hyperkonvergenz: Wie SecDL auf Plattformebene funktioniert

powered by

DEVELOPER-KONFERENZEN + -WORKSHOPS 2017/2018



Parallel programming & HPC

Termin: 06.-08.03.2018
Ort: Print Media Academy, Heidelberg

Docker, Kubernetes & Co.

Termin: 14.-17.11.2017
Ort: Rosengarten, Mannheim

Deep Learning & Data Mining

Termin: 24.-26.04.2018
Ort: KOMED, Köln

DevOps & Continuous Delivery

Termin: 14.-17.11.2017
Ort: Rosengarten, Mannheim

Internet of Things & Industrie 4.0

Termin: 04.-06.06.2018
Ort: KOMED, Köln

Continuous Lifecycle London

Termin: 16.-18.05.2018
Ort: QEII Centre, London

para//el 2018

[Container Conf]

MINDS MASTERING MACHINES

» Continuous Lifecycle »

building IoT

CONTINUOUS LIFECYCLE LONDON

Veranstalter:

Weitere Informationen unter:

www.heise.de/developer/

Das Kind im Rechenzentrum

In den Ausschreibungen (m & w) heißt es: „Sämtliche Bezeichnungen richten sich an alle Geschlechter." Aber die allermeisten RZ- und Netzwerktechniker sind genau das, nämlich Techniker, also Männer. Vielleicht hat es damit zu tun, dass die Datacenter lieber neues Spielzeug kaufen als in effiziente Energiespartechnologien zu investieren. Um genau zu sein: Energieeffizienz darf schon sein – aber nur, wenn sie beim neuen Server mit dabei ist. Das zumindest ist der unterschwellige Tenor der Titelgeschichte von Ariane Rüdiger ab Seite 4. Sie hat sich genau angesehen, was deutsche Rechenzentren mit der (voraussichtlich) 1 Milliarde Euro anfangen, die sie 2017 in Datacenter-Equipment stecken. Datengrundlage ist eine aktuelle Branchenbefragung durch das Berliner Borderstep-Institut für Innovation und Nachhaltigkeit. Dabei gibt es gute Beispiele im Großen wie im Kleinen: WestfalenWind IT baut derzeit ein verteiltes Colocation-Rechenzentrum direkt in die Türme seiner Windkraftanlagen (Seite 8), und der eChiller hat das saubere Flüssigkühlkonzept mit Wasser wieder ins Spiel gebracht (Seite 24).

Zur Energieeffizienz gehört auch eine Variante, von der wir bereits in der Ausgabe 1/2017 berichtet haben: Geothermie. Das Vorzeigeprojekt im Bremer Hochbunker Walle steht jetzt kurz vor der Eröffnung (Seite 10). Dieser Beitrag eröffnet zugleich das zweite Schwerpunktthema: Security. Schließlich hat die Location bereits bewiesen, dass sie bombensicher ist. Allerdings bereiten die virtualisierten und oft schon komplett softwaredefinierten Infrastrukturen RZ-Verantwortlichen zunehmend Schwierigkeiten. Der Security Development Lifecycle, sagt Dr. Markus Pleier, findet heute am besten auf Plattformebene statt (Seite 20). Für Containersysteme (Seite 12) wiederum gilt: Keep it gekapselt. Lieber ein Image mehr als ein Patch Level verschlafen. Der Zugriff auf die Images lässt sich mittlerweile gut steuern, und für CI/CD kann man entsprechend automatisierte Jobs einrichten. Automatisierung hören IT-Admins jederlei Geschlechts zwar gar nicht gerne, aber den Arbeitstag mit Routine-Resets zu vertun, ist wahrlich kein Vergnügen. Warum Automatisierungslösungen aus Unternehmensperspektive sinnvoll sind, setzt der Beitrag auf Seite 23 auseinander.

Wer es handfester mag, blättert direkt in die Heftmitte zur strukturierten Verkabelung. Dort gibt es zum einen praktische Lösungen für die Kreuzverbindungen in Spine-Leaf-Architekturen (Seite 16), zum anderen sauber vorkonfektionierte Verkabelungssysteme (Seite 14), die deutlich schnellere Installationen möglich machen und weniger Platz brauchen. Dieselben Vorteile ergeben sich aus Optical Distribution Frames für das Terminieren im Central Office (Seite 18). Wenigstens räumen damit sogar Männer am Ende auf.

Thomas Jannot

Inhalt

Stromsparen als Einkaufsgutschein

Rechenzentren holen sich Effizienztechnologien am liebsten mit neuer Hardware

Deutschland gefällt sich als Technologieführer, auch in Sachen Energieeffizienz. Die nötigen Technologien gibt es tatsächlich schon. Doch die deutschen Rechenzentren setzen sie erst zögerlich um. Woran das liegt, hat das Berliner Borderstep-Institut für Innovation und Nachhaltigkeit untersucht.

Wie effizient sind deutsche Rechenzentren? Welche Effizienztechnologien setzen sie ein, um die PUE (Power Usage Effectiveness) zu verbessern – und um vielleicht weitere Energieeinsparungen zu realisieren? Und was hat das alles mit dem RZ-Standort Deutschland zu tun? Um das herauszubekommen, hat das Borderstep-Institut zusammen mit dem Netzwerk energieeffiziente Rechenzentren (NeRZ) zwischen März und Juni 2017 eine umfangreiche Untersuchung durchgeführt: „Energieeffizienz und Rechenzentren in Deutschland. Weltweit führend oder längst abgehängt?“ Sie basiert auf einer Literaturrecherche, Modellierung der RZ-Landschaft in Deutschland mittels eines Strukturmodells, der Online-Befragung von Betreibern und strukturierten Interviews mit ausgewählten Experten.

An der Online-Befragung beteiligten sich 74 Personen, von denen 36 bei IT-Dienstleistern und 38 in sonstigen Rechenzentren tätig waren. Sie betreiben insgesamt 328 Rechenzentren mit einer Fläche von 475.000 m², was etwa einem Viertel der RZ-Kapazitäten in Deutschland entspricht. Rund 46 % der Befragten arbeiten für organisationseigene RZ, rund 24 % für Colocation-Rechenzentren, 23 % für Hoster, 14 % für Cloud-RZs, 15 % für Managed-Services-Provider, 12 % bei TK-RZs, 3 % bei Gebiets-RZ und 12 % bei Hochschul- oder Forschungseinrichtungen.

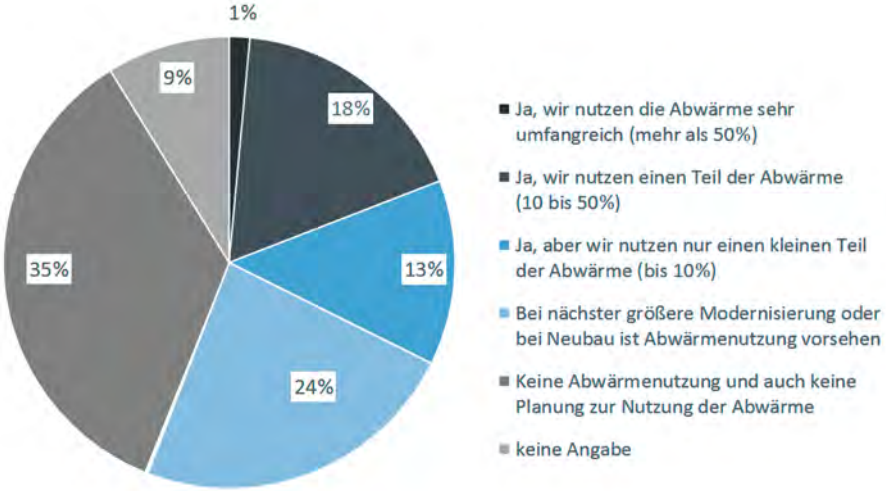
Leider sind die Daten der Studie nicht im strengen Sinne repräsentativ, sondern haben laut Borderstep „explorativen Charakter“. Dennoch dürften sie etwas über die besagten Themen aussagen. Bei vielen Fragen, die die IT-Infrastruktur betreffen, blieben die Antworten aus Kollokationsrechenzentren außer Betracht, da diese Aspekte von den Mietern entschieden werden und nicht vom RZ-Betreiber.

Investitionen legen zu

Eine gute Nachricht zumindest für die Hersteller von Datacenter-Equipment, aber auch für die Modernisierung der deutschen RZ-Landschaft ist, dass die Investitionen zuletzt gestiegen sind: 2016 legten sie um 10 % zu, 2017 werden sie etwa 1 Milliarde Euro erreichen. Dabei sind die Ausgaben für neue Informationstechnik noch nicht mitgerechnet. Sie lagen 2016 bei 7,3 Milliarden Euro. Bis 2019 wollen nur 4 % der Befragten nichts in die Informationstechnik stecken, 38 % planen lediglich Ersatzinvestitionen, und über die Hälfte wird entweder etwas oder sogar umfangreich erweitern.

Während die Fläche der übrigen Rechenzentren stagniert, legen Cloud-Einrichtungen mittlerweile kräftig zu, nach Borderstep-Analyse hauptsächlich wegen der Ansiedlung amerikanischer Cloud-Anbieter: Sie müssen mit eigenen RZ vor Ort sein, um den Anforderungen des deutschen Datenschutzrechts gerecht zu werden. Die Gesamt-IT-Fläche in deutschen RZ überschreitet mittlerweile 2 Millionen Quadratmeter, die der Cloud-Rechenzentren 0,5 Millionen Quadratmeter. Der Cloud-Markt macht also mittlerweile ein gutes Viertel der gesamten deutschen RZ-Fläche aus, Tendenz steigend.

NUTZEN SIE DIE ABWÄRME IHRES RECHENZENTRUMS/IHRER RECHENZENTREN?



Quelle: Borderstep Institut

Eine stärkere Nutzung der RZ-Abwärme ist den Befragten zufolge oft nicht realistisch umzusetzen oder schlicht unrentabel.

Insgesamt scheinen Rechenzentren flächenmäßig zu wachsen als zu schrumpfen: Während knapp 30 % der Befragten angeben, ihre RZ-Fläche sei in den vergangenen zwei Jahren um mehr als 20 % gewachsen und weitere rund 12 % sagen, sie habe bis 20 % zugelegt, nahm die RZ-Fläche nur bei 10 % der Befragten ab. Bei rund der Hälfte ist die RZ-Fläche gegenüber dem Stand von vor zwei Jahren allerdings gleich geblieben.

Mehr Energiebedarf, mehr Server

Zwischen 2010 und 2016 ist der Energiebedarf von Servern und Rechenzentren in Deutschland von 10,5 auf 12,4 Milliarden kWh/a und damit um rund 20 % angestiegen. Das geht auch in Zukunft so weiter: Nicht nur die Fläche wächst, auch die Zahl der physischen Server steigt trotz aller Virtualisierungsbemühungen weiter an, genau wie der Energieverbrauch. So geben allein knapp 30 % der Befragten an, die Serverzahl werde sich bis 2025 um mehr als ein Viertel erhöhen, weitere gut 20 % sehen eine Erhöhung um bis zu 25 % im selben Zeitraum. Auch der Energieverbrauch legt weiter tüchtig zu: Hier gehen gut 30 % von einer Steigerung bis 2025 um bis zu 25 % aus, etwa 16 % erwarten, dass der Energieverbrauch um weniger als 25 % steigt. Für Europa prognostiziert Borderstep für 2020 einen weltweiten RZ-Energiebedarf von etwa 375 Milliarden kWh/a.

Die IT-Dienstleister signalisieren übrigens besonders deutlich einen steigenden Strombedarf: Rund 30% von ihnen gehen davon aus, dass er um 25 % oder mehr zulegen wird, weitere 35 % prognostizieren ein Wachstum zwischen 5 und 25 %. Das spiegelt die zunehmende Nutzung von Dienstleistungsrechenzentren und Cloud Computing wieder.

Wie dem auch sei: Die höhere Effizienz von Servern wird augenscheinlich komplett von der Zunahme ihrer Menge infolge der Digitalisierung aufgefressen, und der Strombedarf der IT wächst unaufhörlich. Ob die Energieeinsparungen aus der Digitalisierung den Verbrauch der IT kompensieren, wie häufig versprochen wird, bleibt abzuwarten. Rechnet man weltweit, ist eher zu erwarten, dass der globale Energiebedarf – trotz oder wegen der IT – durch die unvermeidliche und berechtigte Aufholjagd sich entwickelnder Ökonomien und Rebound-Effekte weiter ansteigen wird.

Ausbaumarkt Cloud und Colocation

Der Trend zur (räumlichen) Größe ist bei deutschen Datacentern unübersehbar, insbesondere Cloud- und Colocation-Rechenzentren legen zu. Bei Dienstleistungsrechenzentren nennen 40 % der Befragten ein Wachstum von über 20 % in fünf Jahren. Zudem ist diese Gruppe besonders investitionsbereit – etwa 46 % geben an, dass sie sehr umfangreiche Erweiterungsinvestitionen planen, hinzu kommen noch einmal mehr als 20 %, die von etwas weniger umfangreichen Erweiterungsinvestitionen ausgehen. Aber kein Dienstleister plant überhaupt keine Investitionen. Das ist wenig verwunderlich, sondern entspricht den positiven Zukunftserwartungen der Dienstleister, die zu knapp 30 % in den nächsten fünf Jahren sogar Flächenerweiterungen über die Hälfte erwarten. Etwa 17 % gehen davon aus, dass sie mehr als 50 % mehr physische Server nutzen werden, weitere rund 40 % erwarten Zuwächse zwischen 5 und 25 %.

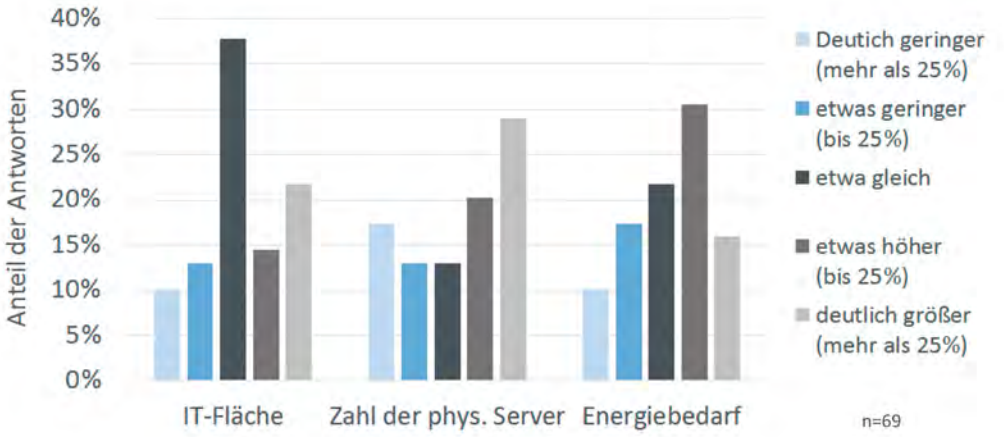
Dabei hat die Kollokation, bei der die Serverbetreiber ihre IT-Ressourcen bei einem Spezialisten unterbringen, der die Infrastruktur bereitstellt, einen Anteil von 40 % an der Gesamt-IT-Fläche in deutschen Rechenzentren. Allerdings gibt es immer noch rund 48.000 Rechenzentren in Deutschland mit einer Fläche unter 100 m^2. 93 % der IT-Verantwortlichen bei Mittelständlern halten den Betrieb eigener Rechenzentren weiterhin

BEFRAGUNG: RECHENZENTRUM IM JAHR 2025

Wachstumstendenz bei Fläche, Serverzahl und Energie

Wie sieht Ihr Rechenzentrum im Jahr 2025 aus?

Die Herausforderung: Bei einer steigenden Anzahl von Servern soll der Stromverbrauch allenfalls moderat mitwachsen.



Quelle: Borderstep Institut

für wichtig, was diese hohe Zahl kleiner RZ erklärt. Der Grund dürfte die verbreitete Sorge um die Sicherheit unternehmenskritischer Daten sein. Diese Zahl stammt aber nicht von Borderstep selbst, sondern aus einer Rittal-Untersuchung durch IDC aus dem Jahr 2014 – bei der rasanten Ausbreitung von Cloud kämen die Autoren vielleicht heute schon zu einem anderen Ergebnis. Als neuer Trend zeichnet sich die Errichtung sogenannter Edge-Rechenzentren ab, die als Konsolidierungsstufe der IT in IoT-Umgebungen zwischen der unmittelbar am Endgerät befindlichen IT und der Cloud-IT dienen.

Genutzte Effizienztechnologien

Angesichts der Wachstumstendenzen ist der gezielte (und hoffentlich erfolgreiche) Einsatz von Effizienztechnologien umso wichtiger, um die offenbar unaufhaltbaren Anstiege im Energieverbrauch wenigstens so gering wie möglich ausfallen zu lassen. Die wichtigsten Einsparfaktoren stecken in den Servern selbst – beim regelmäßigen Hardware-Austausch kommen in der Regel automatisch effizientere Technologien zum Zuge – sowie in der Kühl-/Klimatisierungs- und Lüftungstechnologie. In beiden Bereichen konnten über 80 % der Befragten in den vergangenen Jahren Einsparungen erzielen. Mit jeweils rund 50 % der Nennungen folgen USV/Stromverteilung und Datenspeichersysteme. Bei Netzwerken und Stromerzeugung dagegen sparten in den vergangenen Jahren nur 10 % der Befragten Strom – allerdings sind dies auch nicht die großen Verbraucher im RZ.

Bemerkenswert ist, dass die Abwärmenutzung erst bei 30 % der Anwender zu Energieeinsparungen beiträgt. Das bedeutet, dass hier möglicherweise noch viel ungenutztes Potenzial liegt, denn physikalisch gesehen setzen Rechner nur Strom in (Ab-)Wärme um – Nullen und Einsen sind kein Output in diesem Sinne.

Die wichtigste Maßnahme, um Energie einzusparen, ist die Servervirtualisierung, die flächendeckend eingesetzt wird. Im Zug der turnusmäßigen Hardware-Erneuerungen werden bei etwa 90 % der Befragten energieeffizientere Lösungen angeschafft, und effiziente Stromnutzung scheint sich mittlerweile zu einem selbstverständlichen Auswahlkriterium beim Serverkauf gemausert zu haben. Des Weiteren werden in Rechenzentren relativ häufig Kalt- und Warmgänge eingehaust (75 % Nennungen). Auch Mess-, Steuer- und Regeltechnik findet sich inzwischen in knapp 70 % der RZs. Rund 55 % haben auch ihre Speicher virtualisiert und stromfressende Überkapazitäten beseitigt. Hocheffiziente USV-Anlagen haben rund 60 % der Befragten beschafft, und etwa die Hälfte der Befragten verwendet indirekte freie Kühlung und/oder ein Energiemanagementsystem. Eher seltener werden die direkte freie Kühlung (etwas über 30 %) und die Netzwerkvirtualisierung (knapp unter 30 %) implementiert.

Diese Trends dürften sich fortsetzen. Knapp 55 % der Befragten planen die Beschaffung energieeffizienter IT-Hardware, etwa 46 % wollen künftig in ein Energiemanagementsystem für das RZ investieren. Servervirtualisierung und Kalt-/Warmgangeinhausung sind mit 36 % weitere beliebte Investitionsobjekte. Dann folgen Netzwerk- und Storage-Virtualisierung sowie hocheffiziente USV-Anlagen und MSR-Technik fürs RZ mit jeweils etwas über 30 % Nennungen. Indirekte freie Kühlung steht bei 18 % der Befragten auf dem Plan, in direkte Freikühlung wollen 14 % Geld stecken. Gezielte Investitionen in Wärmerückgewinnung gab keiner der Befragten an – allerdings ist nicht klar, ob diese Option überhaupt abgefragt wurde oder ob es sich um eine offene Frage handelte, auf die man selbst Antworten formulieren konnte.

Verschobene Prioritäten

Die Investitionspläne entsprechen nicht ganz den Einschätzungen, wo man am meisten Energie einsparen könnte. So gibt die Hälfte der Befragten an, man glaube, durch Wärmerückgewinnung hohe bis sehr hohe Einsparungen erzielen zu können – aber gezielte Investitionsvorhaben in dieser Richtung wurden entweder gar nicht abgefragt oder aber nicht genannt. Demgegenüber sind die Energiesparpotenziale bei neuer IT-Hardware mit 10 bis 25 % nicht mehr überwältigend, stehen aber bei den Invest-Plänen weit oben. Rund 45 % glauben, dass sich auch bei Kühlung, Klima und Lüftung mehr als 25 % sparen lassen. Fazit: Das, was ohnehin anfällt, wird auch gern gemacht (sprich: turnusmäßige Hardware-Erneuerungen); bei Sonderinvestitionen, die größere Einsparungen bringen könnten, hält man sich dagegen zurück. Immerhin 83 % der Befragten kennen ihren Jahresstromverbrauch, und 76 % wissen, welche PUE (Power Usage Effectiveness) ihr Rechenzentrum hat.

Hochschul- und Forschungsrechenzentren sind zumindest nach den Daten dieser Untersuchung keinesfalls die Vorreiter. Zwar haben sie

bei der Stromerzeugung rund doppelt so viel Energie eingespart wie der Durchschnitt, ansonsten liegen sie aber nur bei der Nutzung von IT-lastigen Einsparmaßnahmen geringfügig über dem Mittelwert der Befragten: bei Investitionen in energieeffiziente Datenspeichersysteme und Server. Viel seltener als im Durchschnitt der Rechenzentren wurden Kühl- und Klimatechnik, USV- und Stromverteilungstechnik sowie das Netzwerk als Themen für Energiesparinvestitionen genannt. Das könnte daran liegen, dass bei diesen Einrichtungen, die in der Regel von vielen Institutionen genutzt werden, der Fokus besonders stark auf höchster Verfügbarkeit und Leistung liegt. Immerhin gehen Hochschulrechenzentren davon aus, dass sie in Zukunft keine zusätzlichen oder weniger Flächen brauchen werden. So geben etwa 30 % an, der Flächenbedarf werde sich um 5 bis 25 % verringern, weitere etwa 8 % prognostizieren sogar einen Rückgang um mehr als 50 %. Es werden hier mehr Server benötigt, ohne dass deswegen der Strombedarf steigen soll.

Innovationen in der Nische

Dabei wären Technologien, die dazu beitragen, den Verbrauch zu drosseln, inzwischen durchaus verfügbar. Aber eine kombinierte Strom-Kältekopplung nutzen nur 15 % oder erwägen ihn kurzfristig, immerhin 22 % sind grundsätzlich daran interessiert. Hot Fluid Computing, also die Flüssigkühlung, indem man die IT-Komponenten in eine Inert-Flüssigkeit hängt, die durch Zirkulation und Wärmeentzug temperaturstabil gehalten wird, nutzen 17 % oder wollen das kurzfristig, weitere 14 % sind daran interessiert. Dass dies so ist, könnte nicht nur an der Umweltindolenz deutscher RZ-Betreiber liegen, sondern auch an der Situation des internationalen RZ-Markts, auf dem die Bedeutung deutscher und europäischer Rechenzentren tendenziell abnehmen soll. Das verwundert nicht, sinkt doch durch das Erstarken von Schwellenökonomien wie Indien und insbesondere China insgesamt die weltwirtschaftliche Bedeutung der alten Industrienationen. Etwas anderes wäre nur unter der Beibehaltung gravierender weltwirtschaftlicher Ungleichgewichte möglich. Der Anteil der EU am weltweiten RZ-Markt soll bis 2020 von 25 % im Jahr 2010 auf 21 % im Jahr 2020 abnehmen, der deutsche Anteil im selben Zeitraum von 4,9 % auf 3,9 %.

Wichtige Rahmenbedingungen

Nach positiven und negativen Standortfaktoren und gleichzeitig nach deren Qualität in Deutschland befragt, halten die Umfrageteilnehmer eine zuverlässige Stromversorgung, Anbindungen an Internet-Knoten, Datenschutz und Rechtssicherheit für die wichtigsten Faktoren, dicht gefolgt von der Verfügbarkeit von Fachkräften und der Qualität von Zulieferern und Dienstleistern. Nicht ganz so wichtig, aber immer noch in der oberen Hälfte der Skala rangieren Themen wie sonstige Versorgungsinfrastruktur (Straßen, Flughäfen etc.), Strompreise und schnelle Genehmigungsprozesse. Am unwichtigsten, aber immer noch oberhalb der Mitte der Skala ist die Nähe zum Kunden, die mit Cloud-Geschäftsmodellen eindeutig an Bedeutung verliert.

Annähernd Kongruenz zwischen Bedeutung und Situation am Standort Deutschland besteht bei Datenschutz und Rechtssicherheit sowie bei der Qualität von Zulieferern und Dienstleistern sowie bei der sonstigen Infrastruktur. Geringfügig größer als die Bedeutung des Faktors ist die Kundennähe in Deutschland, was durchaus mit der mittelständischen Struktur der RZ-Branche und damit zu tun haben dürfte, dass Deutschland breitflächig industrialisiert ist, sodass sich eben an vielen Orten Rechenzentren befinden. Geringfügig ins Negative tendiert die Verfügbarkeit von Fachkräften. Sehr viel besser könnte nach Meinung der Befragten die Situation bei Strompreisen und Genehmigungsprozessen sein. Dass die Mühlen im deutschen Baurecht langsam mahlen, ist ja sattsam bekannt, und genauso, dass Deutschland kein Strombilligland ist, zumal die meisten Datacenter keinen Industriestrom beziehen.

Inzwischen sind Rechenzentren übrigens ein wichtiger Arbeitsmarktfaktor – laut Borderstep haben sie in den vergangenen drei Jahren mehr als 10.000 neue Arbeitsplätze geschaffen. Insgesamt beschäftigen Rechenzentren 130.000 Menschen direkt, 80.000 Menschen sind bei Zulieferern wie Baufirmen, Systemhäusern, Sicherheitsdiensten oder im Handwerk beschäftigt. In beiden Bereichen – Rechenzentren und Zulieferer – herrscht akuter Fachkräftemangel.

Künftige Handlungsfelder

Schließlich fragte Borderstep nach Zukunftsthemen. Eines davon sind erneuerbare Energien. Wie hoch deren Anteil an ihrem Stromverbrauch ist, wusste immerhin ein Drittel der Befragten nicht. Weitere 29 % konnten aber angeben, dass ihre Einrichtungen den gesamten Strom erneuerbar beziehen – und sei es in Form von Zertifikaten. Nur 9 % der Befragten gaben einen Anteil von erneuerbaren Energien an, der im einstelligen Bereich liegt oder gar bei 0.

Hinsichtlich der Abwärmenutzung zeigt sich ein Hoffnungsschimmer am Horizont. Denn inzwischen planen – neben den etwa 30 %, die die Technologie umfangreicher nutzen und damit auch schon Einsparungen erreichen konnten – weitere 24 %, bei der nächsten Modernisierung oder einem Neubau diese Technologie zu implementieren. Andererseits nutzen 35 % derzeit keine Abwärme und haben es auch weiterhin nicht vor – verschenkte Energie, könnte man sagen. Das liegt laut der Mehrheit der Befragten vor allem (ca. 57 %) daran, dass im Einzelfall keine wirtschaftliche Nutzung möglich ist, warum auch immer. Rund 45 % geben an, keinen Abnehmer für die Abwärme zu haben, jeweils etwa 27 % beklagen die zu geringe Temperatur oder zu hohe Investitionen.

Mit dem in den kommenden Jahren zu erwartenden Zwang zum Umstieg auf HFKW-freie Kältemittel beschäftigen sich die RZ-Betreiber zu einem Drittel noch nicht, weitere 25 % sehen keinen akuten Handlungsbedarf, nur 3 % haben den Technologiewechsel schon vollzogen.

Flüssigkühlung wird vor allem von Hochschul- und Forschungsrechenzentren propagiert – obwohl Luft ein sehr schlechter Wärmeleiter ist und die IT-Dichte in den RZ immer weiter zunimmt. Doch 40 % der Befragten wollen trotzdem auf keinen Fall Wasser im RZ – eine Einstellung, die sich wohl nur durch erfolgreiche Nutzungsbeispiele ändern wird. Genauso viele Antworten (40 %) finden die kombinierte Produktion von Strom und Kälte in Blockheizkraftwerken interessant, allerdings gibt es noch Informationsdefizite. Eine aktive Teilnahme am Strommarkt, zum Beispiel als Bereitsteller von Reservestrom, halten 35 % der Befragten für ihre Organisation denkbar.

Energieeffizienz läuft nebenbei

Insgesamt scheint es unabweisbar, dass der Stromverbrauch von RZ weiter steigen wird – und dass die Investitionsbereitschaft gerade in neuartige Effizienztechnologien sich in Grenzen hält, sofern sie nicht im Rahmen der ohnehin fälligen IT-Investitionen „mitlaufen“. Eher fordern Datacenter niedrigere Strompreise und drohen wegen mangelnder internationaler Konkurrenzfähigkeit mit der Abwanderung der Branche ins Ausland, wo der Strom billiger ist – ob die durch geringere Preise verbesserten Renditen allerdings in Effizienztechnik investiert werden würden, ist keinesfalls sicher.

Ariane Rüdiger,
freie Autorin (München)

Frischer Wind fürs Rechenzentrum

Der Turm einer westfälischen Windkraftanlage ist Pilot für ein grünes Colocation-RZ

Energieeffiziente RZ-Technologien sind ein Weg, die Stromkosten im Griff zu behalten. Ein anderer ist eigenproduzierter Strom aus einem angeschlossenen Blockheizkraftwerk oder aus alternativen Energiequellen wie Sonne oder Wind. Der erste Windflügelturm mit integriertem Datacenter steht bereits.

Erneuerbare Energien für Rechenzentren zu nutzen, ist ein bekanntes Thema. Anlagen, die Biogase, Erdwärme oder Wasser nutzen, sind bereits in Betrieb. Neu ist dagegen die Idee von WestfalenWind. Der Stromanbieter nutzt seine eigene grüne Energie und hat ein Datacenter direkt in eine seiner Windkraftanlagen gebaut. Geplant und umgesetzt wurde das Projekt mit der dtm group.

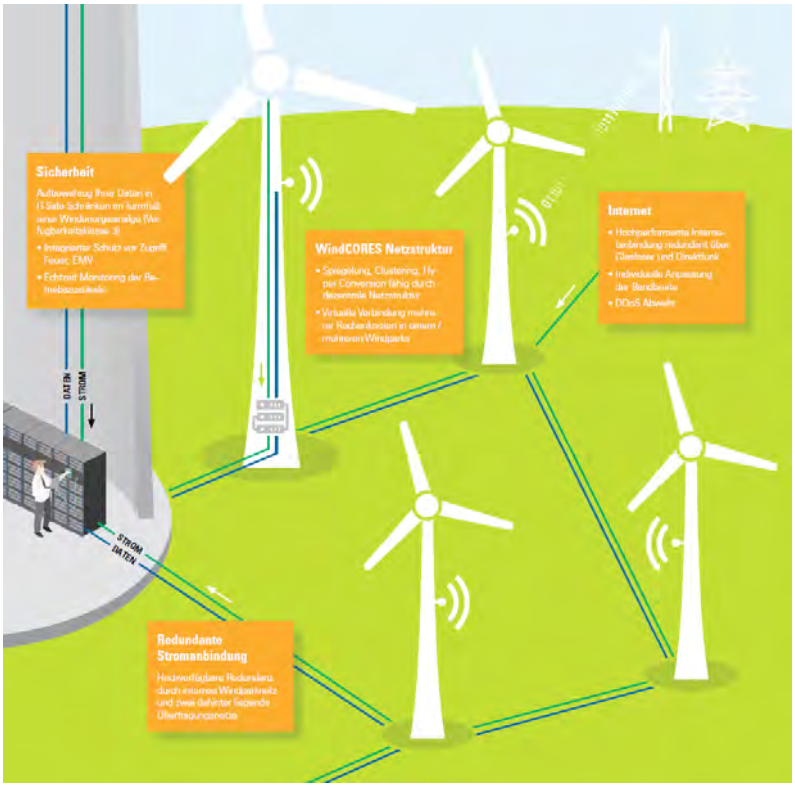
Die WestfalenWind GmbH hat sich die Erschließung und Nutzung der Windkraftenergie für ihre ostwestfälische Heimatregion zum Auftrag gemacht. Insgesamt sind dort bereits 260 Windkrafträder in Betrieb. Mit Blick auf seine zukünftige Geschäftsstrategie hat sich das Unternehmen entschieden, den Strom als Dienstleistung für Rechenzentren anzubieten. Strom ist bekanntlich der größte Kostenfaktor eines Datacenters. Die Kombination aus Windkraftanlage und RZ ergibt eine Win-win-Situation: Nutzer der künftigen Rechenzentren können günstigen Strom direkt von der Quelle beziehen und gleichzeitig kann das Unternehmen den Strom verwerten, der nicht ins Netz eingespeist werden kann.

Diese Strategie sollte gleich konsequent umgesetzt werden und nicht etwa durch ein Container-RZ neben dem Turm, das den Strom anzapft. Der Anspruch war vielmehr, den vorhandenen Raum des Turmes zu nutzen und dort das RZ einzubauen.

Das Eckige muss in das Runde

Dafür hat WestfalenWind mehrere Jahre einen IT-Dienstleister gesucht. Mit der dtm group aus Meckenbeuren am Bodensee war dann schließlich ein Partner gefunden, der als Einziger eine umsetzbare Lösung anbieten konnte. Die Herausforderung bestand darin, den Raum von den Höheneinheiten her bestmöglich auszunutzen, dabei aber die Servicewege für die Techniker nicht zu verbauen. Das heißt: Eine IT-Sicherheitszelle war von Anfang an ausgeschlossen. Gleichzeitig musste ein Konzept für die Stromversorgung erstellt werden. Zwar ist Energie im Überfluss vorhanden, sie musste jedoch kanalisiert und für Redundanzen genutzt werden. Die beiden Gewerke Windkraft und RZ sollten sich nicht untereinander beeinflussen, weder hinsichtlich der elektromagnetischen Verträglichkeit noch beim wesentlich komplizierteren Brandschutz.

Um die Klimatisierung, die Stromversorgung sowie den technischen und baulichen Brandschutz auf relativ kompaktem Raum zu realisieren, war eine sehr detaillierte Konzeptionsphase erforderlich. Die Datentechniker haben das RZ dabei gewerkeübergreifend geplant und die Besonderheiten der Örtlichkeit berücksichtigt. Beispielsweise wurden Rückkühler außerhalb des Turmes platziert, da der Turm oben gekapselt ist und ein Wärmekurzschluss gedroht hätte. Die Spezialisten übernahmen auch die Datenverkabelung und das Datennetz, ebenso wie das Monitoring durch den hauseigenen EnviMonitor. Energietechnik und RZ-Infrastrukturmanagement arbeiten dabei Hand in



Quelle: WestfalenWind IT

Die WindCores sind als verteiltes Colocation-RZ im Cluster konzipiert.

Hand: In Kooperation mit den Energietechnikfachleuten der ee technik GmbH, die den Windpark mithilfe der Siemens-Lösung WinCC überwachen, ist ein bidirektionaler Datenaustausch zwischen WinCC und EnviMonitor aufgesetzt, sodass man die Messwerte vergleichen und die Gesamtanlage auf größtmögliche Effizienz trimmen kann.

Hochverfügbarkeit im Custer

Die Realisierung verlief dann sehr schnell. „Wir haben Ende August damit begonnen, die erste IT-Infrastruktur zu installieren. Eine Woche später folgte die Datenverkabelung und Leitungsverlegung im Turm. Wieder eine Woche darauf wurde die Klimatisierung installiert. Seit Anfang Oktober ist das RZ betriebsbereit“, berichtet Frithjof Dubberke, Projektleiter und Geschäftsführer IT bei WestfalenWind. Um den begrenzten Raum optimal zu nutzen, entschieden sich die Planer dafür, vier einzeln stehende Racks zu verketten, von denen nur zwei Schränke fixiert sind. Die anderen beiden können, beispielsweise bei der Wartung eines Trafos, kurzfristig abgebaut werden. Um den Brandschutz entsprechend der DIN EN 1047-2 zu gewährleisten, wurden nebst einer Brandmeldeanlage sowie einer Brandfrüherkennung sogenannte DC-ITSafes der DC-Datacenter-Group GmbH sondergefertigt. Dabei handelt es sich um modulare RZ-Gehäuse, die absolut feuerbeständig sind.

Für die komplette RZ-Kapazität wurde eine gleichfalls modulare USV mit redundanten Kontrollern ausgelegt, die auch alle anderen Gewerke 15 bis 20 Minuten versorgen kann. Zusätzlich besteht die Möglichkeit, eine externe Netzersatzanlage an das RZ anzuschließen. Die sekundäre Anbindung des Datacenters wird indes über einen zweiten Netzbetreiber realisiert und ist damit deutschlandweit einzigartig. Die Zertifizierung durch den TÜV sieht eine Verfügbarkeitsklasse 3 des Turms vor. Da jedoch weitere Türme folgen sollen, die alle für sich die VK 3 vorweisen können, ist die Ausfallwahrscheinlichkeit durch das Cluster aus USVs, Stromanbindung, Klimatisierung und Datenanbindung gleich null. Der Windpark als RZ erreicht damit eine VK 4.

Distributed Hosting im Windpark

Das Turm-RZ ist nur das erste eines als verteiltes Colocation-RZ geplanten Windparks, der unter dem Namen WindCores vermarktet wird. Die Strategie sieht vor, eine Vielzahl von Türmen mit Rechenzentren auszustatten. Unternehmen mieten sich in den Windpark ein und hosten ihre Daten dann zum Beispiel in drei verschiedenen Türmen. Dafür wurden im kompletten Windpark Single-Mode-Fasern verlegt, um ein Datennetz mit einer sehr schnellen Infrastruktur abzubilden. „Die Uni Paderborn ist dabei unser erster Kunde und wird ungefähr ein halbes Jahr lang einen Testbetrieb durchführen“, sagt Dubberke. „Da sie stark im Bereich Big-Data-Analyse tätig ist, profitiert die Hochschule entsprechend von den Strompreisen. Wir profitieren natürlich von den Erfahrungswerten.“

Simon Federle,
freier Journalist

Nachweislich bombensicher

Im Bremer Hochbunker Walle eröffnet ein modernes Hochsicherheitsrechenzentrum

Eine Luftaufnahme der Royal Air Force aus dem Jahre 1944 zeigt eine Bombenwüste – die Stadt nur noch Schutt und Asche, die Häuser nurmehr Gerippe. Die einzige Ausnahme ist ein Hochbunker, der unbeschädigt inmitten der Trümmer steht. Dort ist in den vergangenen Jahren ein hochsicheres Datacenter eingezogen.

Der Bunker im Bremer Westend stand nie leer. Wegen seiner ungewöhnlich kompakten Bauweise wurde er bereits einige Jahre nach Kriegsende zum Atombunker umfunktioniert. In der digitalen Gegenwart soll er nun wichtige Unternehmensdaten schützen. Sicherheit, besonders Datensicherheit, ist hierzulande zu einem der drei wichtigsten digitalen Kriterien der Unternehmensentscheider geworden. Jedoch: Über zwei Drittel der deutschen Unternehmen (83 %) vertrauen ihre Daten nur dem eigenen Datacenter an. Obwohl Deutschland europaweit führend im Rechenzentrumsmarkt ist, belegt es beim Thema Datensicherheit in der Data Centre Risk Map 2016 von Cushman und Wakefield mit 73,75 von 100 Punkten gerade einmal Platz 16. Geht etwas schief, kann es teuer werden: Dem Global Data Protection Index 2016 von Dell EMC zufolge wirft ein Datenverlust in Deutschland durchschnittlich Kosten von rund 558.000 US-Dollar auf.

Hinzu kam noch eine weitere Beobachtung: Wie der BlitzAtlas von Siemens zeigt, ist die Blitzdichte in Bremen vergleichsweise gering. Aus diesen Erwägungen machte sich Andres Dickehut, geschäftsführender Gesellschafter der Bremer Consultix GmbH, im Jahr 2013 daran, ein Datacenter zu bauen, das einmalig sicher sein sollte. „Natürlich ist Bremen nicht der Nabel der deutschen Rechenzentren“, sagt er. „Hochburgen sind vor allem Frankfurt, das Ruhrgebiet, München, Hamburg, Berlin.“ Doch aus Sicht eines Ingenieurs war der Standort Bremen einzigartig. Zum Betrieb des Hochbunkers als Data Center gründete Dickehut ein eigenes Unternehmen: ColocationIX. Mit einer Gesamtfläche von über 2500 m^2 gehört ColocationIX zu den mittleren Rechenzentren in Deutschland.

Schichtweise RZ-Sicherheit

Mit dem Erwerb des Bremer Atombunkers begann ein mehrjähriger Umbau. Das Ziel: absolute physische und digitale Sicherheit aller Daten. Eine Konzeption nach dem „Zwiebelschalenprinzip“ nennt Andres Dickehut das. Zu den äußeren Schalen zählen ein Sicherheitszaun und der Bunker mit seinen 2 m dicken Außenwänden und -decken sowie den 5 m dicken Fundamenten. Ausgefeilte Sicherheitstechnik begleitet den Besucher auf Schritt und Tritt: gleich zu Beginn eine Detektorschleuse und Videoüberwachung, mehrere hundert Kameras im Ganzen; dann die Türen, Spezialtüren der höchsten Sicherheitsstufen, von außen nur mittels

Quelle: Consultix

Im Herbst 2017 ist es nun so weit: Das hochsichere ColocationIX-Rechenzentrum im Bremer Zwingli-Hochbunker nimmt den Betrieb auf.

Dreifaktorauthentifizierung über Code, Chip- und Biometrieerkennung zu öffnen. Zudem ist der Zutritt gestaffelt: Jeweils ein halbes Dutzend Türen muss man öffnen, um überhaupt in eines der fünf Data-Stockwerke zu gelangen. Diese sind hermetisch abgeschirmt – keine Fenster, kein Funk, keine elektromagnetischen Wellen. Ein modernes Brandschutzsystem mit systematischer Sauerstoffreduktion lässt keinerlei offenes Feuer in den IT-Räumen zu. Jedes Stockwerk ist ein eigenständiges Rechenzentrum mit gespiegelter Infrastruktur. Statt Energiekabeln, wie man sie häufig in Rechenzentren antrifft, wurden flexible, nicht brennbare Stromschienensysteme aus Metall verlegt.

Anbindung und Zertifizierung

Ebenfalls erstaunlich ist das geothermische Kühlkonzept, das 2014 bereits mit dem Deutschen Rechenzentrumspreis ausgezeichnet wurde. Die Abwärme wird mit über Erdsonden mit zusätzlicher adiabater Rückkühlung vierfach redundant in eine Tiefe von 100 bis 200 m abgeleitet. Dieses System liefert 200 KW Dauerleistung und erzielt Spitzen von bis zu 800 KW. Das System ist kaum wartungsanfällig, und die Verfügbarkeit der Erdkälte ist durchgehend und verlässlich zu 100 % gegeben, unabhängig von Wind und Wetter. Selbst länger anhaltende Hitzeperioden verändern die Temperaturen in diesen Tiefen nicht. Auch klimatechnisch ist der Hochbunker also nicht zu erschüttern. Auf dem Dach deutet Andres Dickehut auf die Blitzableiter und ist damit wieder beim Ausgangspunkt seiner Überlegungen: „Der Blitzschutz entspricht Klasse 0, diesen Standard haben sonst nur Krankenhäuser und sensible Infrastrukturen“, sagt er.

Zur physischen äußeren Sicherheit kommt die RZ-Sicherheit innerhalb des Bunkernetzwerks und auf Ebene der Racks. Via Glasfaser ist das Datacenter direkt und mit geringen Latenzzeiten mit den weltgrößten Internet-Exchange-Knoten DE-CIX, AMS-IX und LINX sowie nach China verbunden. Die direkten Wege erlauben es, Anwendungen hochperformant global zu betreiben. Sicherheitsservices wie Intrusion Prevention, DDoS Attack Mitigation oder RBTH (Remote Triggered Black Hole Filtering) sollen ColocationIX praktisch unangreifbar machen.

Die Eröffnung des RZ-Bunkers hat Dickehut auf der it-sa in Nürnberg für Mitte November angesetzt. Bis dahin wird das Rechenzentrum noch nach ISO 27001 auditiert. Der ehemalige Atombunker des Bundes ist für Tier 4/Class 4 gebaut und dürfte dann zu den sichersten Rechenzentren Deutschlands, wenn nicht sogar Europas gehören.

Vor allem bei deutschen Unternehmen dürfte das auf Interesse stoßen. Denn der Trend geht derzeit eindeutig in Richtung Hyprid-Clouds: Manche Dienste bezieht man aus der Public Cloud, geschäftskritische Anwendungen lässt man lieber in der Private Cloud laufen, entweder on premises oder eben im Hosting-Modell eines Colocation-RZs. Der typische deutsche Entscheider achtet bei der Wahl seines Cloud-Providers laut der IDG-Studie Cloud Security 2016 vor allem auf Vertrauen in den Anbieter, ein gutes Preis-Leistungs-Verhältnis sowie auf technologisches Know-how. Sicherheitsbedenken sind das mit Abstand größte Hemmnis. Somit dürfte der ehemalige Atombunker im Bremer Westend in Bälde seiner dritten Bestimmung erfolgreich nachgehen: Daten als Rohstoff der Digitalisierung mit Sicherheit zu bewahren.

Gerrit Reichert,
freier Autor (Bremen)

Jeden Tag ein sauberes Image

Containersysteme nehmen die Betreiber sicherheitstechnisch stärker in die Pflicht

Mit den Container-Nutzerzahlen wächst auch das Risiko von Missbrauch. Derzeit hält man sich vor allem an die Best Security Practices der Community. Am wichtigsten ist: das System so simpel wie möglich zu gestalten und im besten Fall für jeden einzelnen Prozess einen eigenen Container einzusetzen.

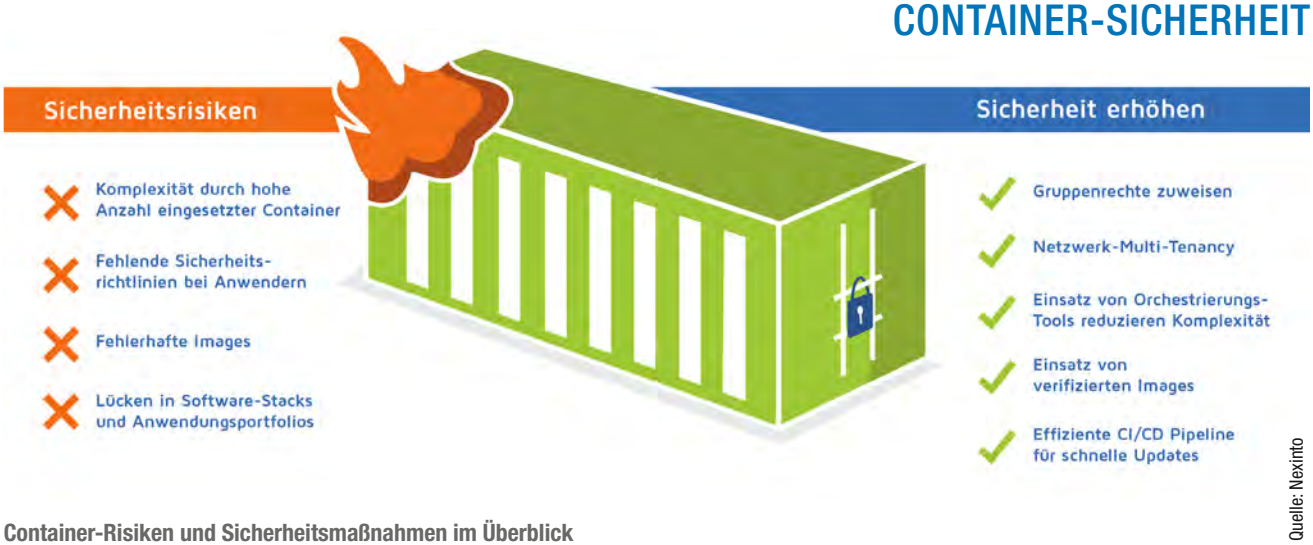
Fakt ist, dass moderne Containersysteme den klassischen virtuellen Maschinen (VM) zunehmend den Rang ablaufen. Unter dem Einfluss von Containern ändern sich die Zuständigkeiten der klassischen virtuellen Maschinen. Diese dienen in der Praxis immer häufiger als eine Art „schlanker Wirt“. Konkret stellen die VMs Compute-Ressourcen wie RAM, CPU oder Netzwerke zur Verfügung. Der Vorteil für den Nutzer liegt auf der Hand: VMs sind weniger sensibel für Angriffe von außen.

Als grundlegendes Container-Format fungiert noch immer das von Docker entwickelte System. Kernstücke sind der darin enthaltene Code der Laufzeitumgebung des Unternehmens sowie zusammenhängende Spezifikationen. Mit dem Docker Hub avancierte die Open-Source-Software schnell zu einem äußerst attraktiven Spielplatz für Tüftler und Entwickler. Der Online-Dienst beinhaltet eine Registry für Docker-Images und Repositories. In einem öffentlichen Bereich kann jeder Nutzer seine selbst erstellten Images hochladen und diese anderen Nutzern zur Verfügung stellen. Dazu gesellen sich immer mehr offizielle Images, etwa von Linux-Distributoren. In einem privaten Teil des Hubs können Nutzer ihre Images hochladen und firmenintern verteilen. Diese Images sind öffentlich nicht auffindbar – damit entfällt ein weiteres Sicherheitsrisiko.

Doch die Verwendung von Docker im Rechenzentrum wirft neue Fragen auf. Denn grundsätzlich steigt damit die Komplexität des gesamten Systems. Schließlich laufen in einem Rechenzentrum wesentlich mehr Container als klassische VMs, und es sind deutlich mehr Betriebssysteme vorhanden, die es zu patchen gilt. Aus diesem Grund werden ebenso mehr Services überwacht. Andererseits bietet ein Container auch weniger Angriffsfläche, da hier in einem geringeren Maße Software zum Einsatz kommt. Somit entsteht durch Container nicht nur ein besseres Lifecycle Management, sondern auch die Möglichkeit von automatisierten Updates im Rahmen von CI/CD-Pipelines und damit verbundenen Deployments.

Standards durchsetzen

In der jüngsten Vergangenheit hat Docker bereits Maßnahmen eingeleitet, um die Sicherheit der Container zu erhöhen. Die Plattform erlaubt heute daher das Zuweisen von Gruppenrechten und die Trennung zwischen routinemäßigen Container-Operationen und Root-Rechten auf dem Serverhost. Insgesamt überwiegen bei der Nutzung von Docker die Vorteile für den Container-Einsatz deutlich. So überzeugt das System durch eigene Security Features: Sämtliche Container erhalten einen eigenen Netzwerktrack. Zudem bedient sich das System Cgroups und Namespaces. Generell besticht Docker ebenso durch ein höheres Maß an Automatisierung, und das System ist schneller zu deployen. Außerdem bringen die Orchestrierungsfeatures von Docker Cluster weitere Security-Bausteine mit, etwa eine Netzwerk-Multi-Tenancy. Früher mussten Administratoren hier aufwendig Firewall-Zugriffe managen, heute macht das der Container-Orchestrator. Auch die automatische Konfiguration von Loadbalancern ist inzwischen eine gern genutzte Selbst-



Container-Risiken und Sicherheitsmaßnahmen im Überblick

verständlichkeit, ebenso die Verfügbarkeit von schnelleren Updates von Stateless Apps und Microservices in Bezug auf OS Security Patches.

Und doch gibt es noch einige Stolperfallen. Diese betreffen vor allem die aufwendige Etablierung von Security-Standards in den Unternehmen und die damit verbundene Bereitstellung von personellen, organisatorischen und auch finanziellen Ressourcen. Das ist ein Aufwand, den viele Unternehmen noch scheuen und dessen Notwendigkeit häufig erst erkannt wird, wenn es zu spät ist. Vor allem kleine und mittlere Unternehmen (KMU) haben hier noch Nachholbedarf. Das Thema Digitalisierung im Mittelstand ist zwar aktueller denn je. Doch schlussendlich gibt es zur Einrichtung bestimmter Sicherheitssysteme keine Alternative.

Problemfeld Images

Eine der häufigsten Fehlerquellen bei Containern ist die Nutzung öffentlicher Images. Damit verbunden ist eine Vielzahl von Applikationen. Experten raten daher, sämtliche Basis-Images von Containern, auf denen Applikationen laufen, täglich aufzuarbeiten und zu aktualisieren. Nur so wird das jeweils aktuellste (und damit sicherste) Patch Level erzeugt. Viele Unternehmen und IT-Verantwortliche bleiben aber schlicht und ergreifend untätig oder handeln zu spät. Dies betrifft insbesondere Sicherheitslücken in Software-Stacks und Anwendungsportfolios. Tun sich diese erst einmal auf, greifen auch alle übrigen Maßnahmen zu kurz. Der ursprüngliche Open-Source-Code muss konsequent kontrolliert werden, sonst wird lediglich sichergestellt, dass die im Image enthaltenen Bits genau diejenigen sind, welche die Entwickler ursprünglich dort eingestellt haben. Die eigentlichen und bekannten Schwachstellen der Open-Source-Komponenten bleiben.

Vor allem ein frei verfügbarer Zugriff auf Images bietet genug Ansatzpunkte für Sicherheitslücken. Natürlich, je barrierefreier der Zugang, desto mehr Images sind verfügbar. Doch je mehr Images vorhanden sind, desto größer ist auch die Anzahl potenziell fehlerhafter Dateien. Manchmal reicht schon ein einfacher Schreibfehler oder ein falscher Buchstabe innerhalb des Images, um Angreifern unbeabsichtigt Einlass zu gewähren. Eine Lösung wäre in diesem Fall die Bereitstellung eigener Basis-Images, welche so wenig Extrasoftware wie möglich enthalten. Doch die Entwicklung solcher Images erfordert ein höheres Maß an Automatisierung. Auch die erforderlichen Plattformen für CI/CD (Continuous Integration/Continuous Delivery) stehen in den meisten Fällen noch nicht zur Verfügung.

Sicherheitswerkzeuge nutzen

Um den Aufwand zu minimieren, empfiehlt es sich, in der CI/CD-Plattform Jenkins entsprechende Jobs einzurichten. Diese bringen sämtliche OS-Images sowie Images von Applikationen regelmäßig auf den neuesten Stand. Anfällige Container werden anschließend mithilfe von Deployments oder Update-Rollouts durch gepatchte Container ausgetauscht.

Das Secure Computing von Docker räumt den Nutzern mehr Kontrolle über die Applikationen innerhalb der Container ein. So sind auf spezielle Anforderungen zugeschnittene Systemaufrufe über ein Whitelisting abrufbar. Auch die Verbindung des Containers zum Host, zwischen einzelnen Containern oder nach außen über das Internet sollten Unternehmen streng reglementieren. Auf diese Weise können etwa DDoS-Angriffe (Distributed Denial of Service) verhindert werden. Eingerichtete Namespaces weisen Rollen und Rechte einzelnen Nutzern zu. So werden Zugriffe auf Informationen in anderen Hosts besser kontrolliert, sprich: reglementiert. Als Faustregel mag gelten: „So eng wie möglich!“

Derzeit gibt es bereits eine gute Bandbreite an hilfreichen Sicherheitstools. Es empfiehlt sich der Einsatz eines Docker-relevanten Hypervisors oder Basis-OS-Hosts wie CoreOS, Atomic Host, RancherOS oder PhotonOS. Diese Betriebssysteme sind abgespeckt und bieten dadurch weniger Angriffsfläche. Ebenso unterstützt Red Hat im Container-Betriebssystem Atomic Host Software für die Deep Container Inspection (DCI) sowie das Open Security Content Automation Protocol (OpenSCAP). Auch Rancher stellt bei Active Directory und LDAP die Multi-Tenancy sicher, indem das System Zugriffsrechte bestimmter Personengruppen und Environments einschränkt. Die Kommunikation zwischen Containern erfolgt über IPSec-Tunnel, die das System automatisch aufbaut.

Mehr Eigenverantwortung

Zumindest Docker hat seine Hausaufgaben gemacht. Die aktuellen Updates erlauben einen größeren Handlungsspielraum, um Nutzern Rechte zuzugestehen oder nicht. Was die einzelnen User (und IT-Verantwortlichen in den Unternehmen) damit machen, bleibt ihnen überlassen. Doch selbst die fundiertesten Sicherheitsupdates sind unbrauchbar, wenn sie von den zuständigen Mitarbeitern nicht adäquat umgesetzt und fortwährend kontrolliert werden.

Michael Vogeler,
Systemadministrator im Bereich Application and Database Services bei Nexinto

Das schnellere Licht

Mit vorkonfektionierten Verkabelungssystemen sind RZ rascher startklar

Statt dicken Kabelrollen, feldkonfektionierten Komponenten und einer Menge von Schnittresten am Ende kommen beim Aufbau eines modernen Datacenters meist anschlussfertige Verkabelungssysteme zum Zuge. Solche Systeme können viel Zeit sparen, erfordern aber eine sehr sorgfältige Planung im Vorfeld.

Zeit ist Geld. Benjamin Franklins Tipp ist nach über 250 Jahren so zutreffend wie eh und je. Der Wert der Zeit ist eher noch gestiegen, auch im Rechenzentrumsbau. Die Entwicklung hin zu technisch vorbereiteten Plug-and-play-Elementen ist von daher nur logisch. Man findet sie heute im Größten und im Kleinsten: vom modularen Gebäudebau selbst bis zu vorkonfektionierten Verkabelungssystemen für Hochgeschwindigkeitsnetze, wie sie mittlerweile fast jeder Anbieter im Portfolio hat. Diese Lösungen versprechen eine deutliche Kostenreduktion durch Platz- und Zeitersparnis, ermöglichen meist auch höhere Packungsdichten und sind in der Praxis die Basis einer vernünftig strukturierten Verkabelung.

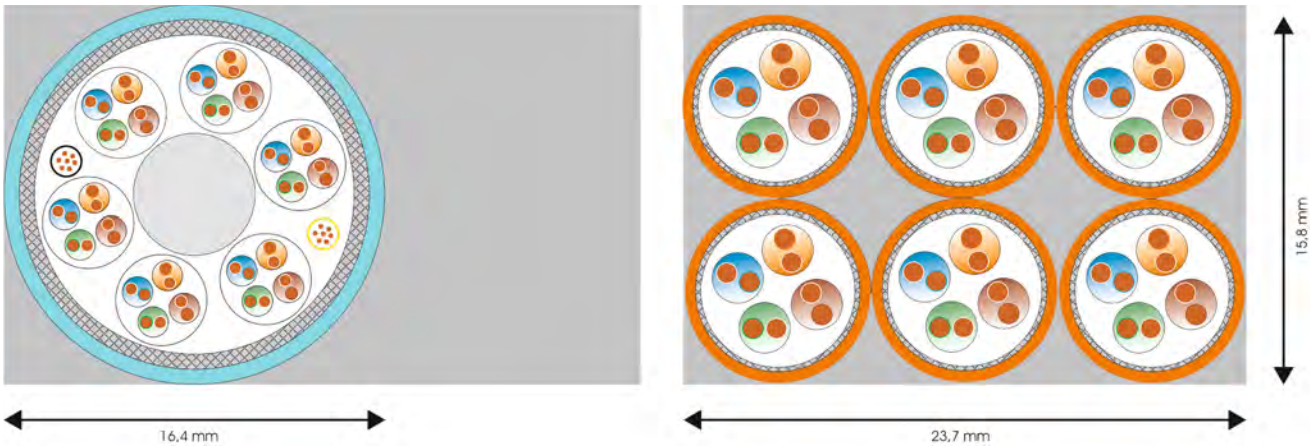
Wenig Platz und wenig Zeit

Ein Beispiel ist das H.D.S. (EasyLan High Density System) von ZVK. Der Anbieter packt hier sechs Datenkabel bei einem Außendurchmesser von < 16,4 bis 16,5 mm (AWG 24) unter einen Mantel, etwa für Schrank-zu-Schrank-Verbindungen. An den Kabelenden befinden sich die Gehäuseköpfe mit insgesamt sechs Jacks pro Kopf. Eine Aufschaltung von sechs einzelnen Keystones und sechs Modulen ist nicht mehr notwendig. Die Übertragungseigenschaften im Link sind hinsichtlich ihrer PoE+-Tauglichkeit durch eine GHMT-Zertifizierung nach DIN EN 60512-99-002 gewährleistet. Zusätzlich müssen sich Oberflächen und Material, Klima und Umwelt, Signalintegrität sowie Faseroptik laufend in akkreditierten Laboren Qualitätskontrollen unterziehen. Die H.D.S.-Panels ermöglichen eine maximale Packungsdichte von 168 LC-Duplex-Ports auf drei 19-Zoll-Höheneinheiten bzw. 48 LC-Duplex-Ports auf einer HE.

Die Vorteile vorkonfektionierter Systemlösungen zeigen sich spätestens dann, wenn im Rechenzentrum umgepatcht, erweitert oder geändert wird. Viele Konzepte haben für diese Zwecke außerdem bereits eine LED-Signalisierung integriert. Sie ermöglicht nicht nur eine schnelle und exakte Zuordnung, da die Ports eindeutig identifiziert sind, auch die Installationszeiten bei Umzügen etc. werden erheblich reduziert. Für die Leuchteinheit verlaufen beim H.D.S.-System innerhalb des Mantels zwei zusätzliche Drähte (AWG 28). Hier ist diese Commodity außerdem durchgehend ausgeführt, also unabhängig von den jeweiligen Ausführungen mit eigenen Spezifikationen, Klassifizierungen, Kerndurchmessern oder Standard-Steckverbindern und unabhängig davon, ob es sich um LWL- oder Kupfer-, Trunk- oder Patchkabel, Spleiße oder Panels handelt. Der größte Vorteil gegenüber konventionellen Verkabelungssystemen liegt indes in den Faktoren Platz und Zeit.

Obwohl ein solches Multikabel Durchsatz für sechs leistet, bleibt es dennoch gut beweglich. Tatsächlich ist der H.D.S.-Kabeldurchmesser laut

Quelle: ZVK GmbH



Zum Vergleich: Kabeldurchmesser H.D.S. (links) und gewöhnliche Trunkverbindung (rechts).

Anbieter sogar rund 60 % geringer als bei anderen Trunk-Verbindungen. Das erleichtert die Handhabung, macht die Installationen besser zugänglich, verbessert die Luftzirkulation im Schrank und reduziert die Brandlast. Weil die Luftkühlung dann effizienter funktioniert, reduziert man auf diese Weise sogar die Stromkosten. Die seitliche Schrankmontage ermöglicht zudem eine platzsparende Verkabelung.

Saubere LWL-Verbindungen

Durch die werkseitige Vorkonfektionierung erhalten Kunden geprüfte Kabel in exakter Lange, mit gelabelten Einzelteilen und Komponenten sowie eindeutig zuordenbaren Messprotokollen. Sie müssen dann lediglich Seite A und B aufschrauben und dazwischen das Kabel verlegen. Sonst benötigt ein Installateur über eine Stunde für das Aufschalten von 24 Ports, das Anlegen von 24 Keystones und das Aufschrauben der Panels. Die Zeitvorteile gelten auch für Um- oder Abbauten.

Der entscheidende Mehrwert gegenüber einer konventionellen Verkabelung liegt tatsächlich in der Zeitersparnis. Je schneller ein Rechenzentrum in Betrieb gehen kann, desto schneller können sich Unternehmen einmieten. Ganz nach dem Motto „Zeit ist Geld“ bedeutet jeder Arbeitsschritt, der schon vorher erledigt ist, eine höhere Gewinnspanne. Durch die Vorkonfektionierung im Werk kann man sich zum Beispiel die eigene Messung sparen. Auch Netzwerkausfälle durch unsachgemäße Installation vor Ort sind praktisch ausgeschlossen.

Auf der anderen Seite hat man sich mit Kabellängen und Spezifikationen bei solchen Systemen früh festgelegt; konventionelle Verkabelungssysteme sind da zunächst flexibler, weil man zum Zeitpunkt der Bestellung noch keine genauen Längenangaben benötigt. Zudem nimmt die Vorkonfektionierung selbst ein wenig Zeit in Anspruch. Unterm Strich sinkt jedoch der effektive Arbeitsaufwand dank des Plug-and-Play-Systems stark. Außerdem entfallen das Konfektionieren sowie die Messungen vor Ort. Nicht zu vergessen: Auch das Risiko von Verschmutzungen an den empfindlichen Glasfaserverbindungen entfällt weitgehend.

Simon Federle,
freier Journalist

Transparente Spine-Leaf-Architekturen

Kreuzverbindungsmodule erleichtern den Umstieg auf East-to-West-Routing

Die Virtualisierung treibt RZ-Planer zu neuen Routing-Strategien. An die Stelle traditioneller dreischichtiger Architekturen treten zunehmend zweischichtige Spine-Leaf-Topologien. Die Umsetzung der hochkomplexen Verbindungen im Mesh-Layer lässt sich durch Kreuzverbindungsmodule deutlich vereinfachen.

Im Rechenzentrumsbereich ist schon seit geraumer Zeit eine steigende Anzahl virtualisierter Applikationen zu verzeichnen. Vor allem Cloud Computing, SaaS und IP Storage treiben diese Entwicklung voran. Damit aber wächst in den Datacentern auch der Bedarf an hochperformanten Gigabit-Ethernet-Verbindungen. Lange sind extern und intern geroutete Verbindungen im Verhältnis 4:1 gestanden – nun kehrt sich dieses Verhältnis um: Bedingt durch die massive Nutzung von Plattformvirtualisierungen – zum Beispiel auf Basis von Docker – kommen auf eine externe mittlerweile vier interne Verbindungen. Ein Großteil des Datenverkehrs findet also zukünftig innerhalb der RZ-eigenen Infrastruktur zwischen virtuellen Servern statt. Das erfordert eine Anpassung der Routing-Strategien. Ziel der RZ-Planer muss künftig sein, die hochgradig parallelisierte Infrastruktur mit laufzeitoptimierten Datenverbindungen im Bereich von 10 bis 40GbE auszustatten.

East-to-west als Lösungsansatz

Gegenwärtig werden die Bottlenecks solcher Datenverbindungen unter anderem durch eine traditionelle dreischichtige Router-Architektur gebildet. Dieses vertikale Routing-Schema wurde ursprünglich für das externe Routing konzipiert und besteht aus den Ebenen der Core-, Aggregations- und Access-Router. Eine solche klassische Client-Server-Topologie wird auch als North-to-South-Routing bezeichnet.

Da angesichts der wachsenden Anzahl virtualisierter Server jedoch zunehmend horizontale Routing-Verbindungen notwendig werden, erfordert die Optimierung der Datenlaufzeit eine andere Router-Topologie. An die Stelle der klassischen dreischichtigen tritt deshalb eine zweischichtige Spine-Leaf-Architektur: Die Router werden direkt über eine voll vernetzte Kreuzverbindung angebunden, um Zwischenebenen in Form des klassischen Aggregation Layers zu vermeiden. Für diese Topologie hat sich der Name East-to-West-Routing etabliert.

Beim East-to-West-Routing sind die Router direkt über faseroptische GbE-Module in Form von SFP- und QSFP-Transceivern verbunden. Auf der Leaf-Seite sind derzeit Transceiver für Datenraten von 0,1 bis 25 GBit/s, auf der Spine-Seite Transceiver für Raten von 10 bis 100 GBit/s gängig. Aufgrund dieser speziellen Architektur sind die Router jeweils nur einen Hop voneinander entfernt – was die Datenlaufzeit deutlich verkürzt –, und es entsteht innerhalb des Routing-Schemas eine hohe Anzahl paralleler Pfade. Neuere Router-Protokolle wie TRILL (Transparent Interconnection of Lots of Links) oder SPB (Shortest Path Bridging) sollen diese Parallelpfade nutzbar machen und ältere Konzepte wie STP (Spanning Tree Protocol) ablösen. Gerade im Bereich IP Storage erwartet man sich hiervon signifikante Bandbreiten- und Latenzgewinne.

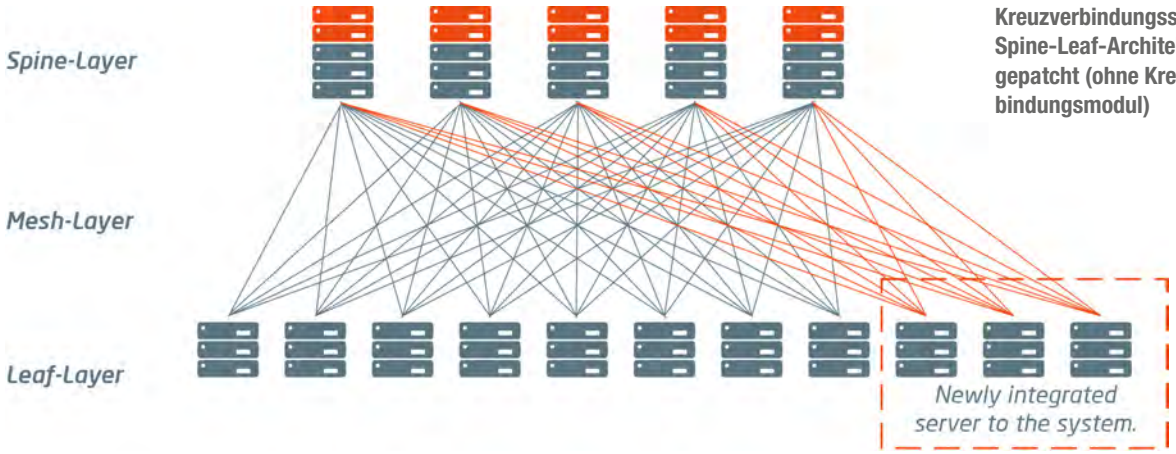
Module für Kreuzverbindungen

Bei Spine-Leaf-Architekturen besteht die besondere Herausforderung nun darin, diese hohe Anzahl paralleler optischer Verbindungen zwischen den einzelnen Routern – den sogenannten Mesh-Layer – lückenlos und zuverlässig zu realisieren. Eine East-to-West-Topologie setzt für n beteiligte Router bzw. Server genau n^2 faseroptische Verbindungen voraus. Das führt bei wachsender Anzahl von Routern zu immer komplexeren Leitungsverbindungen. Eine volle Kreuzverbindung von acht Routern auf acht Server erfordert genau $8^2 = 64$ Verbindungen – einschließlich der optischen Aktivkomponenten in Gestalt von SFP-Transceivern. Diese Kreuzverbindungen einzeln zu verlegen, ist äußerst aufwendig und kann insbesondere dann zu Schwierigkeiten führen, wenn eine rasche Skalierung der Datacenter-Infrastruktur erforderlich ist.

Einige Anbieter sind deshalb dazu übergegangen, die faseroptischen Kreuzverbindungen im Mesh-Layer in Form integrierter Kreuzverbindungsmodule bereitzustellen. Solche Module erleichtern die Erweiterung der Infrastruktur deutlich, da man nicht mehr jede Kreuzverbindung einzeln umsetzen muss, sondern zusätzliche Router bzw. Server lediglich per Trunkkabel an das Kreuzverbindungsmodul anschließt. Bei den von FiberCon entwickelten und von der euromicron-Tochter LWL-Sachsenkabel gefertigten CrossCon-Modulen etwa können beliebige Kreuzverbindungsbreiten erzeugt werden. Möglich wird das durch ein neuartiges dreidimensionales Steckschema der faseroptischen Verbindungen (mit

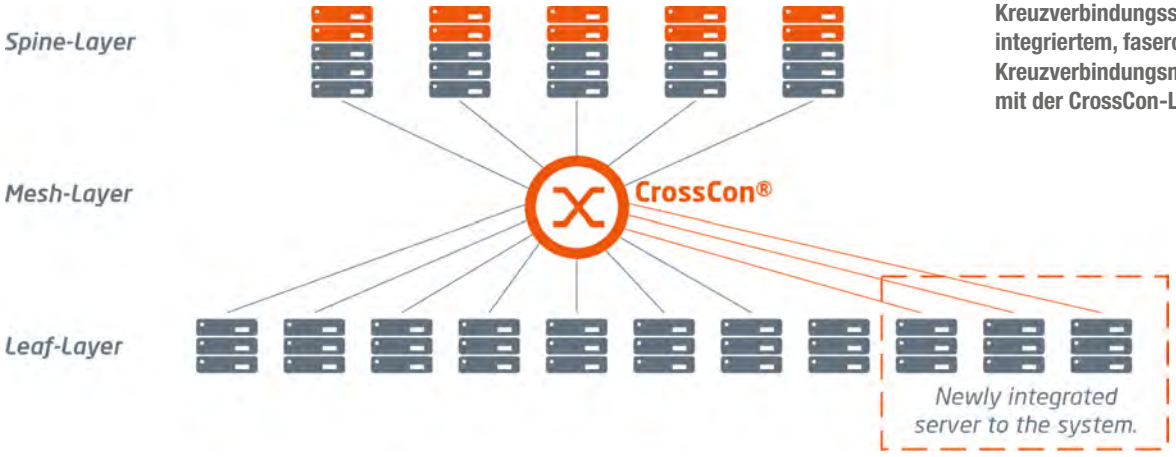
Quelle: FiberCon

Das Kreuzverbindungsmodul CrossCon mit 8 × 8 faseroptischen URM-Verbindungen (MMF).



Kreuzverbindungsschema der Spine-Leaf-Architektur, einzeln gepatcht (ohne Kreuzverbindungsmodul)

Quelle: FiberCon



Kreuzverbindungsschema mit integriertem, faseroptischem Kreuzverbindungsmodul (hier mit der CrossCon-Lösung)

Quelle: FiberCon

integrierten Spalten und Zeilentausch innerhalb des Kreuzverbindungsmoduls). Die zuvor zweidimensionale Kreuzverbindung wird durch die Erweiterung auf drei Dimensionen „entflochten“ und ermöglicht eine strukturierte Umsetzung des Spine-Leaf-Routing-Schemas. Das heißt konkret, dass ein sogenanntes Shuffling faseroptischer Datenleitungen stattfindet – etwa in Form von ein- und ausgehenden Faserbündchen (Ribbon Fibers). Auf diese Weise sind aktuell gekreuzte Kanalbreiten von bis zu 32 × 32 Fasern möglich.

Bye bye, Patchkabel!

Durch solche Module werden Kreuzverbindungen jedoch nicht nur entflochten und klar strukturiert, sondern es wird, wie ein Blick auf standardisierte Verkabelungsinfrastrukturen in Rechenzentren zeigt, auch die Verbindung der einzelnen Faserstrecken vereinfacht. Diese wurde bei Kreuzverbindungen von Spine-Leaf-Servern bisher über Patchfelder im Bereichs- oder Hauptverteiler realisiert. Spine- und Leaf-Geräte wurden dabei gleichermaßen am Patchfeld abgebildet und anschließend mit Patchkabeln verbunden.

Bei Modulsystemen erübrigt sich hingegen der Einsatz von Patchfeldern und Patchkabeln, da die Kreuzverbindungsmodule diese Aufgabe selbst übernehmen. Die Verbindung zum Spine- oder Leaf-Gerät wird dann einfach per Trunkkabel hergestellt. Das spart Zeit bei der Erstinstallation und erleichtert zudem – ein weiterer großer Vorteil – die Skalierung des Systems. So lassen sich beispielsweise Mesh-Layer-Bausteine definieren, die als Standard in die Topologie integrierbar sind und schnelle, transparente Erweiterungen ermöglichen.

Bei der Umsetzung von Spine-Leaf-Architekturen sind Kreuzverbindungsmodule eine enorm praktische Vereinfachung. Wo Verbindungen zwischen virtualisierten Servern hergestellt werden müssen, sind sie ein wichtiger Baustein bei der Realisierung einer strukturierten RZ-Verkabelung. Wer sie einsetzen will, muss sich allerdings von der Vorstellung verabschieden, dass Patchkabel universal notwendig seien. Das widerspricht zwar zunächst allen etablierten und standardisierten Verfahrensweisen, ermöglicht dafür aber den Aufbau einer enorm vereinfachten und dadurch leicht zu überblickenden Infrastruktur. Hinzu kommt, dass durch die klar definierten Verbindungswege eine klassische Fehlerquelle entfällt, was nicht zuletzt den Dokumentationsaufwand reduziert – ein Vorteil, dessen effizienzsteigernde Wirkung nicht unterschätzt werden sollte.

Philipp Nölle,
FiberCon GmbH
Kai Wirkus,
LWL-Sachsenkabel GmbH

Überschaubare 4032 Fasern

ODFs terminieren große Faserzahlen strukturiert und auf Dauer übersichtlich

Netzwerktechniker stehen unter enormem Druck: Mit dem Bedarf nach Bandbreite müssen sie die optische Dichte deutlich steigern. Zugleich soll das Fasermanagement investitionssicher und überschaubar bleiben. Dafür gibt es Optical Distribution Frames (ODFs). Sie sorgen für Ordnung im Verteilerschrank.

Optical Distribution Frames sind zentral bei der Campusverkabelung: Sie kommen zum Einsatz, wo Netzwerktechniker große Distanzen und die Strecken zwischen verteilten Gebäuden oder Orten überbrücken wollen. Kabel, die von außen in das Gebäude kommen, werden in einem speziellen ODF-Verteiler terminiert und lassen sich von dort aus weiter auf aktive Komponenten oder das nächste ODF patchen. Vor allem Carrier nutzen ODFs als Central-Office-Lösung für die Hochverfügbarkeit. Neben dieser Kernanwendung finden ODFs in großen Rechenzentren Anwendung. Auch hier laufen viele Fasern von außerhalb zusammen, sei es aufgrund von Internetanbindungen, sei es, weil das Rechenzentrum redundant ausgelegt ist und mit seinem Zwilling über die Campusverkabelung verbunden ist. Das ODF fungiert dabei als Übergabepunkt: Es sorgt für die Verteilung der Verbindungen über Spleiße zwischen den ankommenden Glasfasern, sichert den Anschluss der Lichtwellenleiter mit entsprechenden Steckern an den angeschlossenen optischen Kommunikationseinheiten und schützt die Fasern.

Spleiß oder Patch?

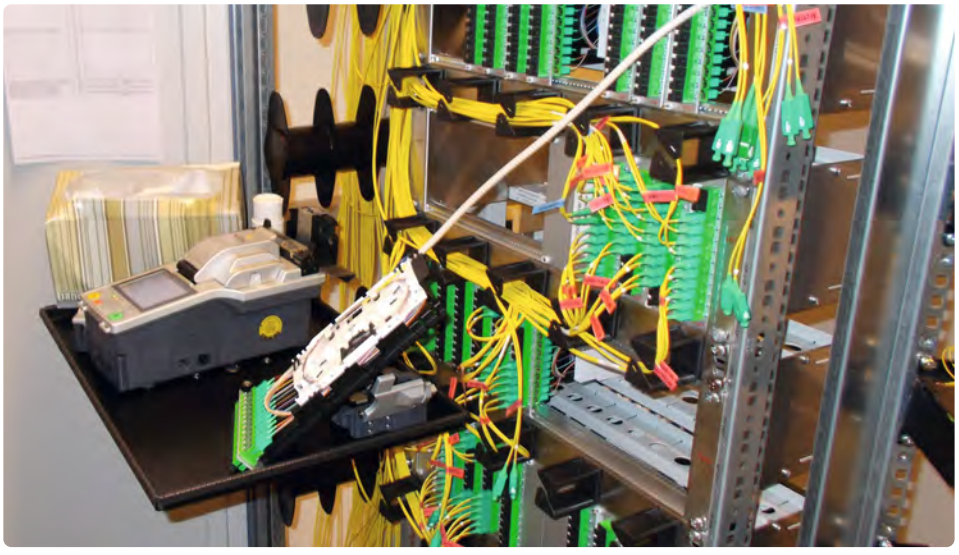
Ganz gleich, ob Carrier oder Rechenzentrum, ODFs erfüllen zwei wesentliche Funktionen für die Netzwerkinfrastruktur: Mithilfe des Verteilerschranks lassen sich möglichst viele Fasern auf geringem Raum terminieren. Zugleich bieten ODF-Verteiler dank ihrer Bauweise meistens auch eine Ebene, auf der sich die Überlängen der Patchkabel ablegen lassen. Dies ist nicht zu unterschätzen, denn es vermeidet Kabelchaos.

Je nach Anwendung lassen sich drei ODF-Lösungen unterscheiden: Die klassische, die Spleiß-to-Spleiß- und die Patch-to-Patch-Lösung. Die klassische Lösung ist eine Spleiß-to-Patch-Umsetzung, bei der Netzwerktechniker durch Anspleißen von Pigtails die Fasern terminieren. Die Anschlusstechnik befindet sich vorne, die Verbindung lässt sich über Patchkabel herstellen.

Eine andere Variante ist die Spleiß-to-Spleiß-Lösung. Hier kommen hochfaserige Kabel aus unterschiedlichen Gebäuden oder Orten im ODF-Verteiler an und werden dort zusammengespleißt. Möglich ist auch eine Aufteilung, wenn etwa Kabel von einem Hauptgebäude kommen und auf mehrere Fertigungshallen verteilt werden sollen. Hier lassen sich Leitungen mit einer extrem hohen Faserzahl mit mehreren Kabeln mit einer geringeren Faserzahl direkt zusammenspleißen. So spart man zusätzliche Übergänge (Steckverbindungen) und kann die Dämpfungen reduzieren. Andererseits lassen sich einmal gespleißte Verbindungen nachträglich nicht mehr ändern. Unternehmen sind somit nicht sonderlich flexibel, wenn sie Änderungen an ihrem Netzwerk vornehmen wollen.

Bei der Patch-to-Patch-Lösung entfällt das Spleißen. Diese Lösung kommt insbesondere innerhalb der Verteilerräume zur Vernetzung der Verteilerschränke zum Einsatz. Netzwerktechniker verwenden Patchkabel oder auch Trunkkabel und nutzen zunehmend auch die MPO-Anschlusstechnik als Plug-and-play-Lösung.

Auch wenn aktuell noch überwiegend über die klassische Spleiß-to-Patch-Lösung terminiert wird, sollten Unternehmen bereits jetzt über alternative Patch-to-Patch-Lösungen mit ODFs nachdenken. Welche der



Quelle: Westfalen Weser Netz

Besonders praktisch ist der tDF-Spleißtisch, auf dem Netztechniker das Spleißgerät abstellen und nahe an der Baugruppe betreiben können.

Ordnung im Verteilerschrank: Das tde-ODF ist gut zu handhaben und übersichtlich gestaltet – das sorgt für sauber verlegte Patchkabel.

Quelle: Westfalen Weser Netz

drei Varianten Unternehmen einsetzen, hängt von der jeweiligen Anwendung ab und ist letztlich eine Frage der Philosophie.

Ein Argument, das oft ins Feld geführt wird, ist die Kleinteiligkeit, die meist eine aufwendige Handhabung vieler ODF-Systeme bedeutet. Dass sich das aber gut in den Griff bekommen lässt, zeigt das Beispiel der Westfalen Weser Netz GmbH. Für sein umfangreiches Glasfaserkabelnetz benötigte der Energieversorger passende Endstellen in Form von ODFs.

Praxisbeispiel Westfalen Weser Netz

„Wichtig waren uns der modulare und montagefreundliche Aufbau des Systems mit einer leichten Bauweise aus möglichst wenigen Teilen sowie die Möglichkeit, den Schrank jederzeit einfach zerlegen zu können“, fasst Stefan Kenneweg zusammen – er ist bei WW Netz für die passive IKT-Infrastruktur zuständig. „Das ODF sollte benutzerfreundlich und übersichtlich gestaltet sein, um die Patchkabel sauber verlegen zu können.“ Die Dortmunder tde nahm diese Herausforderung an und entwickelte gemeinsam mit dem Anwender eine neue ODF-Lösung. In nur wenigen Monaten entstand ein zentraler Glasfaserverteiler, der im Design genau den Anforderungen entspricht, leicht zu montieren und einfach zu bedienen ist. Im Gegensatz zu anderen ODF-Systemen besteht die tDF-Lösung aus sehr wenigen Teilen, sodass die Netzwerktechniker umgehend mit dem Spleißen beginnen können.

Auf der linken Seite des Racks lassen sich die Überlängen der Patchkabel geordnet ablegen – dort ist noch reichlich Raum mit Biegeradienbegrenzern. Die Stammkabel finden auf der rechten Seite Platz. Das Rack hat abnehmbare Seitenwände und Türen, es lässt sich also relativ leicht montieren oder reihen; die Baugruppen kann man komplett von vorne bestücken. In die 19-Zoll-Rasterholme passen auch Switches und andere Komponenten, sodass Kunden unabhängig von proprietären Systemen und ETSI-Racks sind.

Grundsätzlich müssen ODF-Systeme auch künftigen Netzwerkanforderungen gewachsen sein; hier geht es vor allem um Fasererweiterungen und um die Implementierung neuer Splitter- oder WDM-Module etc. Deshalb ist die Packungsdichte das zentrale Merkmal von ODF-Systemen. Westfalen Weser Netz kann nun bis zu 4032 Fasern mit LC auf 46 Höheneinheiten terminieren. In ein Rack passen bis zu 14 Baugruppen mit jeweils drei Höheneinheiten. Eine 19-Zoll-Baugruppe belegt drei Höheneinheiten und kann bis zu zwölf Spleißmodule aufnehmen. So lassen sich bis zu 288 Fasern pro Baugruppe und bis zu 24 Fasern mit LC-Steckern pro Spleißmodul terminieren.

Vorausschauend aufgeräumt

Die Ablage der Spleiße erfolgt in Standardspleißkassetten. Während andere Lösungen eine zusätzliche Höheneinheit für das Überlängenfach benötigen, hat Westfalen Weser Netz dank des im Spleißmodul integrierten Bündelader-Überlängenmanagements zusätzlich Platz frei. Ein Flexschlauch schützt die Bündeladerüberlängen, sodass Netzwerktechniker sie sicher im Modul ablegen können. Zum Spleißen entnimmt man das Modul mit ca. 0,5 m Flexschlauch einfach aus der Baugruppe. Die Patchkabelführung erfolgt innerhalb der drei Höheneinheiten zur Seite. Hier fangen drei seitlich angebrachte Bügel die Patchkabel ab.

Auf Wunsch des Anwenders hat tde noch spezielle Aufteiler verbaut. Sie sind für unterschiedliche Kabeldurchmesser konzipiert, führen die Stammkabel bis seitlich an die Baugruppe heran und teilen diese erst dort auf. Als Folge ergeben sich sehr kurze Absetzlängen. Die Bündeladern lassen sich in Flexschläuchen ordnen und fixiert zu den Spleißmodulen führen.

Insgesamt zeigt dieses Beispiel, wie konstruktiv die enge Zusammenarbeit zwischen Anbieter und Kunde sein kann: Eine ganze Reihe von Lösungen entstand erst aus konkreten Vorschlägen des kommunalen Versorgers, vor allem was die Montagefreundlichkeit des ODFs betrifft: das Anbringen von Rangierbügeln, die Integration eines Kabelaufteilers und die Möglichkeit, die Montageplatte auch rechts zu befestigen, damit das Spleißgerät nahe an die Baugruppe rückt.

André Engel,
Geschäftsführer der tde – trans data elektronik GmbH

Hausrecht für die SecDL-Patrouille

Sicherheitskonzepte für virtualisierte Infrastrukturen setzen auf Plattformebene an

Im Zeitalter von Software-defined Everything hängt alles am Programmcode. Allerdings sind 10 bis 15 % allen Codes fehlerhaft, und Wirtschaftsspione nutzen Sicherheitslücken in virtualisierten Systemen gnadenlos aus. Wirksame RZ-Security-Konzepte beginnen am besten bereits beim Infrastrukturdesign.

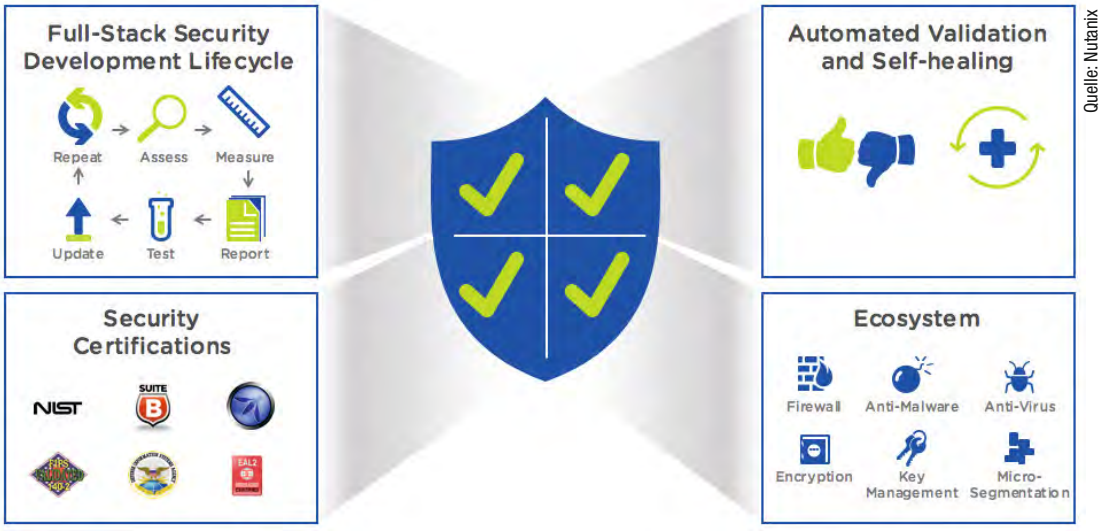
Es geht Angreifern heute nicht mehr darum, Systeme zum Absturz zu bringen, sondern darum, unbemerkt möglichst viel vom wertvollen geistigen Eigentum der Unternehmen zu entwenden oder Lösegeld zu erpressen. Die IT-Verantwortlichen in den Unternehmen müssen deshalb eventuelle Sicherheitslücken möglichst schnell aufspüren und beseitigen. Das ist insbesondere in virtualisierten IT-Umgebungen wichtig. Denn hier sind zusätzlich zu den Sicherheitslücken in den Gastbetriebssystemen der virtuellen Maschinen potenzielle Lecks im Hypervisor und den darunterliegenden Schichten – inklusive Storage und Networking – zu bedenken. Da in solchen Infrastrukturen weitaus mehr logische Systeme und Applikationen laufen als in nicht virtualisierten Umgebungen, gewinnt das Problem zusätzlich an Schärfe.

Die Unternehmen stehen also vor der Herausforderung, kontinuierlich Sicherheitslücken per Notfallmaßnahme schließen und Applikationen sowie Systemsoftware aktualisieren zu müssen. Das zeitnahe Einspielen von Updates ist aber nicht nur ein organisatorisches, sondern auch ein personelles und finanzielles Problem. Außerdem kann nur ausgiebig getestete Software nachträgliche Ausfallzeiten vermeiden. Aus diesen Gründen aktualisieren insbesondere große Unternehmen nur in bestimmten Zeitabständen – damit gehen sie das Risiko ein, dass sie über relativ lange Zeiträume angreifbar bleiben. Lösen lässt sich dieses Problem durch Automatisierung, allerdings müsste der Automatisierungsgrad in der Unternehmens-IT weit höher sein, als es heute üblich ist.

Der erste Ansatzpunkt ist folglich die RZ-Infrastruktur selbst: Ein sicheres Design trägt dazu bei, die Zahl der Sicherheitslücken zu senken. Ein schnelleres Einspielen von Security Updates verringert zusätzlich die Angreifbarkeit. Doch auch dann verbleibt ein Restrisiko, das mithilfe von spezialisierten Lösungen abgedeckt werden muss. Dies gelingt am einfachsten dann, wenn virtualisierte, softwaregesteuerte Infrastrukturen IT-Security-Anbietern vordefinierte Integrationsmöglichkeiten bereitstellen. Ein effektives Sicherheitskonzept setzt in virtualisierten Rechenzentrumsinfrastrukturen auf allen drei Ebenen an: bei der Plattform selbst, bei der Automatisierung und beim Ökosystem der Sicherheitslösungen Dritter.

SecDL auf Plattformebene

Sicherheitsmechanismen in einer herkömmlichen Dreischichtenarchitektur zu aktualisieren, dauert lange und ist teuer. Das liegt an der Vielzahl der involvierten Hersteller und der Unterschiedlichkeit ihrer Technologien. Ist eine IT-Infrastruktur hingegen komplett virtualisiert und wird sie ausschließlich von Software gesteuert, lassen sich diese Kosten deutlich reduzieren – ohne dass die Unternehmen Abstriche bei Sicherheit und Hochverfügbarkeit machen müssten. Dies setzt allerdings voraus, dass im Design dieser Infrastruktur die Sicherheit gleichsam eingebaut ist, in allen Phasen der Entwicklung und Weiterentwicklung.



Quelle: Nutanix

Bausteine einer sicheren Infrastruktursoftware für Unternehmen

Softwaregesteuerte Infrastrukturen haben den Vorteil, dass sie Security als eine gleichberechtigte Funktionalität neben allen anderen implementieren können. Sie bilden den gesamten Prozess einer auf Sicherheit ausgelegten Lösungsentwicklung ab: Entwurf, Einsatz, Test und zusätzliches Härten. In diesem Security Development Lifecycle (SecDL) wird der Programmcode systematisch auf Sicherheitslücken untersucht. Sobald die Entwickler eine Schwachstelle entdecken, nehmen sie sofort deren Beseitigung in Angriff. Dieses Vorgehen wiederholt sich ständig, zieht sich durch den kompletten Lebenszyklus in der Softwareentwicklung und besteht aus den Schritten Bewertung, Messung, Berichterstattung, Test, Aktualisierung und Wiederholung.

Sicherheitslücken ermitteln – in Tagen statt Monaten

Normkonform und regelgerecht

Ein SecDL zielt jedoch nicht nur darauf ab, Sicherheitslücken aufzuspüren, sondern berücksichtigt auch die einschlägigen Regelwerke. Die Lösung muss unter anderem Common Criteria Certified nach EAL2, FIPS 140-2 und NIST-SP800-131A sein, mit NSA Suite B Support sowie Section 508 VPAT und TAA Compliant. Eine RZ-Infrastruktur auf Softwarebasis, die diese Auflagen erfüllt, weist die folgenden Merkmale auf:

Wenn die Steuerungssoftware zur Verschlüsselung den Kernel-Enforced-FIPS-Modus nutzt, werden alle Hashwerte, Signaturalgorithmen und Message Authentication Codes standardmäßig durch den SHA512-Algorithmus gebildet. Für die Erstellung von Anwenderzertifikaten bieten sich drei Verfahren an: RSA (mit 2048-Bit-Schlüssel), der Elliptic Curve DSA (mit 256-Bit-Schlüsseln) und der Elliptic Curve DSA mit 384 Bit langem Schlüssel, um speziell den Vorgaben der NSA Suite B für „Streng geheim“ zu entsprechen. Des Weiteren ist das komplette Design auf TLS (Transport Layer Security) ausgelegt – mit Priorität auf TLS Version 1.2.

Selbstverschlüsselnde Laufwerke, idealerweise nach FIPS 140-2 validiert, bieten die Möglichkeit, Informationen auf den verschiedenen Speichermedien in der gesamten Infrastruktur gegen Diebstahl zu schützen: Wird ein selbstverschlüsselndes Laufwerk entnommen, aktiviert sich ein automatischer Sperrmechanismus, sodass sämtliche weitere Laufwerksoperationen fehlschlagen.

Um die Verschlüsselung auch in Zukunft wasserdicht zu halten, empfehlen sich offene Protokolle wie das Key Management Interoperability Protocol (KMIP) und die der Trusted Computing Group (TCG). Ferner darf es nicht mehr möglich sein, dass sich ein Administrator allein mit Benutzername und Kennwort am System ausweist. Eine durchgängige Zweifaktorauthentifizierung senkt das Risiko eines unautorisierten Zugriffs auf die Verwaltungsfunktionen der Infrastruktursoftware.

Automatisiert und reaktionsschnell

Da es keine hundertprozentige Sicherheit gibt, müssen sich allfällige Angriffe so gut wie möglich nachvollziehen lassen. Dokumentation ist ebenso in vielen Regelwerken eine zentrale Vorschrift, der die Infrastruktursoftware genügen muss, um Attacken nachvollziehbar zu machen und gegenüber den Behörden zu belegen. Cyberspione bemühen sich aber in der Regel, ihre Spuren zu verwischen. Deshalb muss die Protokollierung redundant und verteilt erfolgen. Nur so lässt sich die Integrität der Protokolldaten gewährleisten.

Ein weiterer Vorteil einer rein softwaregesteuerten Infrastruktur besteht darin, dass man Sicherheitslücken weitgehend automatisiert ermitteln und schließen kann. Dazu dienen insbesondere XCCDF-Sicherheitschecklisten (Extensible Configuration Checklist Description Format). Als maschinenlesbare Beschreibungssprache erlaubt XCCDF die einfache Implementierung von Sicherheitsleitfäden, sogenannten Security Technical Implementation Guides (STIGs). Werden die darin beschriebenen Aufgaben automatisch ausgeführt, ergeben sich die folgenden Vorteile:

Der maschinenlesbare STIG kann von automatisierten Assessment Tools zum Identifizieren von Sicherheitslücken genutzt werden. In der Praxis hat sich der dafür notwendige Zeitaufwand pro Fall von neun bis zwölf Monaten bis auf wenige Minuten reduziert. Enthält die Infrastruktursoftware Funktionen zur Autoreparatur, kann sie selbstständig den ordnungsgemäßen Zustand von Produktivsystemen wiederherstellen, wie von den verschiedenen Regelwerken verlangt.

Die bereits genannten selbstverschlüsselnden Laufwerke ermöglichen eine Verschlüsselung der Daten im Ruhezustand (Data at Rest Encryption), also von Daten, die nicht aktuell für die Verarbeitung durch Dienste und Applikationen gebraucht werden. Damit werden die Datenschutzvorgaben von FIPS 140-2 Level 2 erfüllt. Selbstverständlich dürfen die dazu verwendeten Schlüssel nicht auf der zu schützenden Infrastruktur selbst abgelegt sein. Vielmehr sollten die selbstverschlüsselnden Laufwerke die von ihnen erzeugten Schlüssel auf Key Management Server unter Verwendung von KMIP übertragen.

Vorbild Cloud-Sicherheit

Auch die beste Infrastruktursoftware kann keinen hundertprozentigen Schutz geben. Eine solche Software muss daher stets Kontakt zum Know-how der IT-Sicherheitsanbieter halten und dazu einfache Anbindungsmöglichkeiten mittels offener Programmierschnittstellen (APIs) bereitstellen. Dieses Zusammenspiel erfolgt idealerweise in puncto Datensicherheit über die Kooperation mit Anbietern von Key-Management-Servern sowie im Bereich der Endpunktsicherheit durch die Zusammenarbeit mit klassischen IT-Security-Anbietern. Außerdem reduzieren solche Systeme ihre Angriffsfläche mittels Mikrosegmentierung, um die verschiedenen Arbeitslasten in jeder einzelnen Applikation gleichsam mit einer Art Schutzmantel zu umhüllen.

Ein höherer Sicherheitsgrad im Rechenzentrum ist dank vollständig virtualisierter Infrastrukturen realistisch zu erreichen – wenn die Plattform selbst, die Automatisierung von Sicherheitsaufgaben und das Partnerökosystem perfekt zusammenspielen. Dieses Zusammenspiel muss bereits fest im Entwicklungszyklus der Infrastruktursoftware eingebettet sein. Dadurch lassen sich selbst neuartige Bedrohungen schneller als bisher abwehren. Das ist eine der Lehren aus dem Einsatz von Infrastrukturlösungen in der Public Cloud, von der die Unternehmen in ihren eigenen Rechenzentren durchaus profitieren können, wenn sie mittels geeigneter Softwarelösungen Enterprise Clouds implementieren.

Dr. Markus Pleier,
Director Deutschland und Österreich, Nutanix

Mit Printserver? Oder doch nicht?

Die Entscheidung im Output-Management hängt von ganz unterschiedlichen Faktoren ab

In großen Unternehmen kommen häufig dedizierte Druckserver zum Einsatz, die für alle Mitarbeiter Druckdienste zur Verfügung stellen. Direktes IP-Drucken hat jedoch ebenfalls Vorteile, die in bestimmten Umgebungen zum Zuge kommen.

Ob ein Druckserver wirklich erforderlich ist, hängt vom konkreten Einsatzszenario ab. In jedem Fall bietet diese Lösung den Vorteil, dass sich ein sehr umfangreiches Volumen besser abarbeiten lässt, was unter anderem auf die Parallelisierung der Jobs zurückzuführen ist. Es klemmt nichts, es kommt nicht zum Datenstau. Die Rechenlast, die beim Betrieb über einzelne PCs und Drucker anfällt, stellt ebenfalls kein Problem mehr dar. Wichtig ist allerdings, dass der Server ausreichend dimensioniert ist. So empfiehlt sich für Unternehmen, die ihre Anwendungen und Desktops mit einer geeigneten Software in einem Rechenzentrum in der Cloud zentralisieren wollen, ein zentraler Druckserver (besser noch: zwei Server), um Hochverfügbarkeit beim Drucken zu garantieren. Hierbei kann es sich auch um virtuelle Maschinen handeln. Sie zentralisieren das Druckmanagement und machen Server in den einzelnen Niederlassungen überflüssig.

Druckserver contra IP-Drucker

Vorteile bieten Druckserver vor allem Unternehmen mit einem recht großen Druckvolumen. Wer wann wo gedruckt hat, ist mit einem solchen Server sofort nachvollziehbar. Die Zugriffskontrolle ist gegeben und der Überblick über alle Druckausgaben bleibt gewahrt. Viele Unternehmen setzen hier sinnvollerweise auch auf eine systematische Erfassung der Druckkosten und der Auslastung der Druckerflotte. Richtig ist die Entscheidung für Druckserver außerdem, wenn die IT-Architektur – wie vom BSI empfohlen – gesichert werden soll, indem das Druckernetzwerk vom restlichen Firmennetz mit den PCs und Daten getrennt wird.

Auch das direkte IP-Drucken hat Kostenargumente auf seiner Seite. Bei der Anschaffung spielt diese Überlegung vor allem in sehr kleinen Unternehmen und Start-ups eine Rolle. Außerdem kann es für die Firma von Vorteil sein, dass beim direkten IP-Drucken der Offline-Druck möglich ist. Das bedeutet, dass keine Netzwerkverbindung zum Server bestehen muss. Das kann für Betreiber von kritischen Infrastrukturen je nach Art der Geschäftsprozesse sogar eine Anforderung sein, die sich aus dem IT-Sicherheitsgesetz ableitet. Die direkte Verbindung verkürzt nicht zuletzt die Druckwege und sorgt für eine schnelle Datenübertragung zum Drucker.

Geeignet ist diese Lösung auch, wenn es sich um Unternehmen handelt, die gar nicht über die Manpower verfügen, einen eigenen Druckserver zu verwalten. Allerdings ist es beim direkten IP-Drucken nicht möglich, die Druckjobs und Druckerwarteschlangen zu managen. Und ohne Einsatz einer geeigneten Cloud-Lösung zur Treiberverwaltung müssen die Druckertreiber manuell installiert und up to date gehalten werden.

Die Nachteile beim Druckserver liegen also hauptsächlich in den Kosten: im Betrieb des Servers sowie beim Kauf von Hardware und Software inklusive Wartung. Und gerade in Wide Area Networks (WAN), zum Teil mit Außenstellen, entsteht vor allem bei großen Druckaufträgen eine erhebliche Belastung des Netzwerks. Abhilfe können hier allerdings Drittanbieterlösungen schaffen, die die Druckjobs komprimieren und die Bandbreite begrenzen.

Die Nachteile beim serverlosen Drucken sind zunächst im Aufwand zu verorten: in der aufwendigen händischen Installation von Druckertreibern auf jedem PC. Dann kommt noch der Sicherheitsaspekt ins Spiel: Drucker und PCs hängen im selben Netzwerk. Hackerangriffe auf die PCs des Unternehmens über den Drucker werden so einfacher. Außerdem ist ein Management von größeren Druckaufkommen nicht möglich. Wer zuerst kommt, druckt zuerst – das kann ein Problem werden, wenn eilige Jobs gegen Reicht-morgen-auch-noch-Aufträge antreten.

Entscheidungskriterien nach Szenario

Der grundlegende Vorteil von Servern – die zentrale Verwaltung – ist auch beim Drucken einer der wichtigsten Pluspunkte: Große Unternehmen mit Mitarbeitern, deren Drucker im Tagesgeschäft ständig laufen, sind mit Druckservern oft besser beraten. Das Ergebnis ist nicht günstiger, schneller oder qualitativ besser – aber einfacher zu administrieren. Auch die Möglichkeit, den Druckserver zu zentralisieren und in einzelnen Niederlassungen abzuschaffen, sollte dabei evaluiert werden. Das verbesserte Management gleicht in vielen Fällen den Nachteil des erhöhten Kosten- und Wartungsbedarfs wieder aus.

Aus dem Umkehrschluss folgt, dass es vor allem für kleine Unternehmen sinnvoll sein kann, auf serverloses Drucken zu setzen, ebenso wie für Unternehmen, die ihre IT vorrangig aus der Cloud beziehen. Eine Cloud-Lösung zum Management der Druckertreiber für lokales IP-Drucken kann hier eine sinnvolle Ergänzung sein.

Am Ende heißt das Fazit also: Auf das Druckvolumen, die Standortverteilung und auf die Infrastruktur kommt es an. Doch nicht zwangsläufig ist eine Entscheidung für eines der beiden Modelle notwendig. Machbar ist auch ein Mischmodell: Direktes IP-Drucken für lokale Applikationen und Druckserver für die Anwendungen, die zentral zur Verfügung gestellt werden, wie es beispielsweise bei virtuellen Desktops der Fall ist.

Thorsten Hesse,
Chief Product Officer, ThinPrint GmbH

Aus dem Trott auf die Zielgerade

Die IT vieler Unternehmen steht sich mit allzu viel Handarbeit selbst im Wege

Routinearbeiten bei der Installation und Konfiguration von Servern, Speichersystemen, Netzwerkkomponenten und Applikationen sind ungeliebt, aufwendig und kostspielig. IT-Automation setzt diese Ressourcen frei und ist die Basis für effiziente und leistungsstarke Lösungen, die Innovationen antreiben.

Lange Jahre war die Unternehmens-IT auf ihre Rolle als interner Dienstleister fixiert. In der Vergangenheit waren Stabilität, Langlebigkeit und Kostenreduktion die Schlüsselwörter auf der IT-Agenda. Heute haben Agilität, Flexibilität und Geschwindigkeit Priorität. Im Ergebnis wird die IT zur Kernkompetenz für Unternehmen und zur treibenden Kraft in einer immer stärker digitalisierten Welt. Noch wird sie aber im Alltag der meisten mittelständischen ebenso wie großen Unternehmen durch zu viele manuelle Tätigkeiten bei der Einrichtung, Konfiguration und Anpassung von Rechnern und Applikationen ausgebremst.

Dagegen hilft eine Doppelstrategie aus Standardisierung und Automatisierung. Sie befreit die Fachleute von Routinetätigkeiten, und die IT kann als Folge davon die führende Rolle bei Innovationen einnehmen, die ihr zukommt. Standardisierung bedeutet hier vor allem, dass Prozesse transparent sind und immer zum gleichen Ergebnis führen, das heißt, sie sind idempotent. Eine standardisierte IT-Automation legt darüber hinaus ein leistungsstarkes Fundament für die digitale Transformation. Innovationen sind hier ein zentraler Aspekt, denn das Neugeschäft und die Digitalisierung erfordern, dass die IT stärker bei Geschäftsentscheidungen mitwirkt.

Innovation ohne Handbremse

Wenn Unternehmen nicht in der Lage sind, alle Software-Managementaufgaben zu automatisieren – angefangen von der Installation (heute Provisionierung genannt) über das Patchen, Upgraden und Updaten (was man heute als Software Lifecycle Management zusammenfasst) bis hin zur Ausmusterung (heute als Decommissioning oder Retirement bezeichnet) –, bleiben immer Schritte im Prozessfluss, die eine manuelle Ausführung oder Intervention erfordern. Das Ergebnis: Die Komplexität steigt und die Prozesse werden langsamer. Das ist schon insofern fatal, als wir mittlerweile unsere Serviceerwartungen aus dem Privaten ins Berufliche übertragen haben. Unsere Alltagserfahrung sagt uns beispielsweise, dass wir uns, wenn drei Stunden nach der Bestellung bei Amazon keine Bestätigungsmail eingegangen ist, einen anderen Onlineshop suchen sollten. Da das menschliche Gehirn bei der privaten und der Unternehmens-IT auf dieselbe Art funktioniert, erwarten wir eine sofortige Reaktion, und das erfordert eine vollständige Automation im Prozessfluss.

In nahezu allen Branchen stehen Unternehmen heute vor der Herausforderung, dass sie Produkt- und Serviceinnovationen aus all ihren Geschäftsbereichen schneller bereitstellen müssen. Sie spüren einen wachsenden Druck von etablierten Mitbewerbern und von neuen, disruptiven Start-ups – und nicht zuletzt von immer anspruchsvolleren Kunden. Um für die neuesten Technologien aufnahmefähig zu sein, die die Wettbewerbsfähigkeit verbessern, müssen IT-Architekturen angepasst und gleichzeitig Altsysteme weiterhin unterstützt werden. Die Ergebnisse sind häufig komplexe, isoliert voneinander arbeitende Systeme, die sich über Private Clouds, Public Clouds und das unternehmenseigene Rechenzentrum erstrecken. Diese Komplexität moderner IT-Umgebungen kann zu einer enormen Herausforderung werden. Ohne wirksame Automatisierung ist es oft unmöglich, innovationsfördernde Umgebungen, in denen neue und etablierte Systeme gleichzeitig eingesetzt werden, zu verwalten und zu betreiben. Mit anderen Worten: Ohne Automation ist es heute nahezu unmöglich, sehr umfangreiche Projekte zu managen.

Open-Source-Flexibilität

Bis dato wird Automatisierung in den Unternehmen aber eher punktuell eingesetzt. Getrennt arbeitende Teams nutzen proprietäre Tools für jede Installations- und Konfigurationsaufgabe und verwenden sie nur in eng begrenzten Anwendungsbereichen. Potenzial und Mehrwert der Automatisierung sind dadurch dramatisch eingeschränkt.

Es gibt auf dem Markt genügend Open-Source-basierte IT-Automatisierungslösungen, die genau die benötigten Tools zur deutlichen Vereinfachung von Routinetätigkeiten bieten. Im Vergleich zu Closed-Source-Lösungen, die an einen einzigen Hersteller bindet, kann quelloffene Software sogar helfen, neue Funktionen und Lösungen schneller bereitzustellen – unterstützt durch eine große Community, die immer mehr Legacy-Technologien einbezieht und damit die sie die in vielen Unternehmen vorhandenen Anforderungen aufgreift.

Tatsächlich geht es für Unternehmen mit Blick auf Innovationsfähigkeit und flexible Geschäftsprozesse genau darum: sich von starren Strukturen zu lösen, die Komplexität der IT-Infrastrukturen und Applikationen zu reduzieren und ihre IT-Umgebungen vom eigenen Rechenzentrum bis in die Cloud zu optimieren. IT-Automation ist der Schlüssel dazu. Sie schafft Freiräume für die digitale Transformation. Unternehmen sind damit in der Lage, mit Microservice-Architekturen und Container-Technologien neue agile IT-Modelle und -Prozesse zu etablieren. Ohne IT-Automation werden viele Organisationen Gefahr laufen, den Anschluss an die digitale Wettbewerbsfähigkeit zu verlieren.

Matthias Pfützner,
Senior Solution Architect Account & Cloud – DA(CH) bei Red Hat

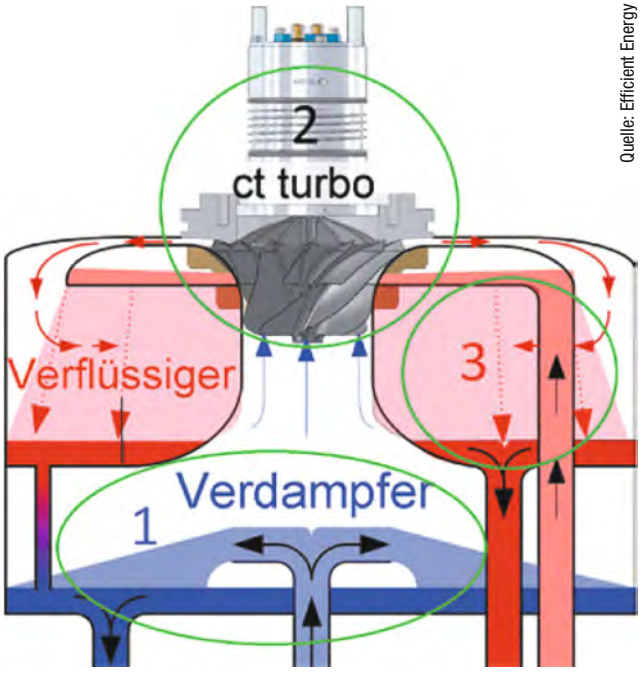
Die vakuumdichte H_2O-Kältemaschine

Wasser kühlt Serverschränke weitaus besser als Luft – und ist ebenso klimaneutral

Die Kältemittel für Flüssigkühlungen haben oft den Nachteil, dass sie in die Schusslinie der F-Gase-Verordnung geraten und daher alles andere als zukunftssicher sind. Deshalb wird derzeit eifrig an Lösungen gearbeitet, die R718 nutzen: reines Wasser. Der Vorreiter kommt aus Feldkirchen bei München.

Konventionelle Kältemaschinen werden in der Regel mit fluorierten Kältemitteln (FKW und HFKW) betrieben, die als Treibhausgase bekannt und reglementiert sind. Vor dem Hintergrund des weltweit wachsenden Kältebedarfs haben die europäischen Behörden mit verschärften Umweltanforderungen und der F-Gase-Verordnung Nr. 517/2014 reagiert. Dies führt dazu, dass die Kosten für konventionelle Kältemittel und die Wartung der Anlagen, die damit betrieben werden, weiter steigen. Dies bekommen die Betreiber von Serverräumen bei ihrer Betriebskostenabrechnung zu spüren.

Alternativen sind gefragt. Ein offensichtlicher Lösungsansatz sind Kältemaschinen, die ohne (teilweise) halogenierte Fluorkohlenwasserstoffe auskommen und stattdessen auf ein Kältemittel setzen, das ein niedriges Treibhauspotenzial aufweist: R718, also Wasser. Wasser ist aufgrund seiner chemischen und physikalischen Eigenschaften besonders klima- und umweltfreundlich, es hat einen GWP-Wert (Global Warming Potential) von 0, es ist nicht nur CO_2-neutral, sondern auch ungiftig, leicht zu handhaben, gut verfügbar und natürlich auch nicht brennbar.



Quelle: Efficient Energy

Funktionsschema des eChillers

Ausgezeichnete eChiller-Technologie

Auch aus Gründen der Energieeffizienz erlebt die Wasserkühlung derzeit eine regelrechte Renaissance in der RZ-Klimatisierung. Größere Hochleistungsrechner können das Warmwasser bereits als Heizenergiequelle für die Gebäude nutzen oder ins Fernwärmenetz einspeisen. Auch andere wassergekühlte Systeme, zum Beispiel von Cloud&Heat Technologies aus Dresden, verwenden die Abwärme der Server für Heizzwecke. Tatsächlich besteht eine der Hauptschwierigkeiten der Wasserkühlung derzeit darin, die Lösungen auch für überschaubare Rechenzentren praktikabel zu machen. So hat die niederbayerische Thomas-Krenn.AG hat einen Wasserkühlkreislauf für kleine bis mittlere RZ entwickelt (Hot Fluid Computing).

Bereits serienreif ist der Kaltwassersatz, den die Efficient Energy GmbH aus Feldkirchen bei München unter dem Namen eChiller anbietet. Der eChiller ist eine Kompressionskältemaschine für den Leistungsbereich 35 kW, die mit reinem Wasser als Kältemittel arbeitet – und noch dazu je nach Anwendung bis zu 80 % Energie spart. Die Lösung gewann im September den RAC Cooling Award 2017 in London, sie erhielt im Juni den Partslife-Umweltpreis 2017 und erreichte im April 2017 auf der Future Thinking in Darmstadt den ersten Platz des Deutschen Rechenzentrumspreises 2017 in der Kategorie RZ-Klimatisierung und Kühlung. Bereits 2016 wurde der eChiller vom Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) im Zuge der Nationalen Klimaschutzinitiative mit dem Deutschen Kältepreis 2016 ausgezeichnet. Derzeit ist die Anlage für den Bundespreis ecodesign 2017 nominiert.

Funktionsweise und Einsatzfelder

Der eChiller arbeitet mit der Direktverdampfung von Wasser in einem vakuumdichten, geschlossenen Kreislauf, der über Plattenwärmeübertrager hydraulisch vom externen Kühl- und Kaltwasserkreis getrennt ist. Besondere Bedeutung haben dabei zwei identisch aufgebaute Kältemodule, in denen jeweils der komplette thermodynamische Kreisprozess abgebildet ist. In jedem Modul befinden sich ein Verdichter, ein Verdampfer, ein Verflüssiger sowie das Expansionsorgan: Wasser tritt in den Verdampfer ein, ein Teil verdampft und entzieht dadurch dem restlichen Wasser Energie, wodurch es sich abkühlt. Der Wasserdampf wird

GEMEINSAM ENTWICKELTE INNOVATIONEN

Um Wasser als Kältemittel optimal einsetzen zu können, hat Efficient Energy den thermodynamischen Kreisprozess komplett neu umgesetzt. Nahezu alle Komponenten wurden hierfür neu entwickelt, da sie auf dem Markt nicht verfügbar waren. Ein Beispiel: die Frequenzumrichter für die Turboverdichter. Der Kreislauf von Direktverdampfung, Verdichtung, Kondensation und Entspannung erfolgt beim eChiller in einem Vakuum bei niedrigen Drücken zwischen 10 und 120 mbar absolut und damit in einem Temperaturbereich von ca. 5 °C bis 50 °C. Ein zentrales Element der Kältemaschine sind Turboverdichter mit 15 cm Raddurchmesser, die den bei der Verdampfung erzeugten Wasserdampf mit bis zu 90.000 Umdrehungen auf ein höheres Druck- und Temperaturniveau bringen. Der Antrieb der Turboverdichter erfolgt über Synchronmotoren, die ihren Strom von Frequenzumrichtern beziehen.

Seit dem ersten Prototyp kommt hierfür das Modell SD2S der Sieb & Meyer AG zum Einsatz. Die Turboverdichter hat Efficient Energy seitdem selbst weiterentwickelt, doch die Frequenzumrichter kommen nach wie vor aus Lüneburg. Derzeit arbeiten die beiden Unternehmen daran, das Seriengerät noch kompakter zu machen. Hintergrund dieser Entwicklung: Efficient Energy möchte den Frequenzumrichter langfristig direkt in die Anlage integrieren. Das würde die Kosten weiter senken, weil das Gerät somit nicht mehr in einem separaten Schaltschrank untergebracht werden müsste. „Die Voraussetzung dafür wäre eine modifizierte Bauform des SD2S mit einem neuen Platinenlayout“, erläutert Florian Mayer, Leiter Entwicklung Software und Elektronik bei Efficient Energy. Das ist Sieb & Meyer zufolge „durchaus zu bewältigen“.

Quelle: Efficient Energy

Blick in den eChiller. Als Kältemittel kommt reines Wasser zum Einsatz.

von dem Turboverdichter mit einer Drehzahl von bis zu 90.000 U/min verdichtet, wobei sich Druck und Temperatur des Dampfes erhöhen. Der komprimierte Wasserdampf kondensiert im Verflüssiger und erwärmt so den Kühlwasserstrom. Das kondensierte Wasser wird schließlich in den Verdampfer zurückexpandiert.

Die Verschaltung der Kältemodule bewirkt, dass die Anlage immer im optimalen Arbeitsbereich arbeitet, sodass die geforderte Kälteleistung mit minimalem Energieaufwand erzeugt werden kann. Der eChiller kann über eine integrierte SPS-Schnittstelle an alle externen Kommunikationssysteme angeschlossen werden. Die Maschinensteuerung enthält die komplette Regelungstechnik für die notwendigen Peripheriegeräte (Kalt-/Kühlwasserpumpen, Rückkühler, Ventile usw.). Dadurch wird erreicht, dass der eChiller im Verbund mit der Gesamtanlage immer am energetisch sinnvollsten Punkt betrieben wird. Da die Anlage bereits bei Kühlwassertemperaturen, die nur geringfügig unterhalb der geforderten Kaltwassertemperatur liegen, in den Freikühlmodus schaltet, erreicht die Maschine COP-Werte (Coefficient of Performance) von über 120. Das bedeutet, dass die Leistungsaufnahme weniger als 300 W beträgt, um die Nennkälteleistung von 35 kW zu erbringen.

Den Leistungsbereich von 35 kW kann man durch traditionelle modulare Zusammenschaltung der Maschinen beliebig erweitern. Anwendungsfälle mit einem kontinuierlichen Kühlbedarf bei gleichzeitig hohem Kaltwasserniveau sind der ideale Einsatzbereich dieses innovativen Kaltwassersatzes. Es können Kaltwasseraustrittstemperaturen von 16 °C bis

ENERGIEOPTIMIERTE SELBSTREGELUNG

Der eChiller kennt (außer Stand-by) vier Betriebszustände, die das System je nach Kühlwassertemperatur regelt:

Betriebszustand	Kühlwassertemperatur	Funktion
FreeCooling	< 18 °C*	Beide Module nehmen nicht aktiv am Prozess teil, maximaler COP.
FreeCooling PLUS	18–24 °C*	Ein Modul komplettiert die geforderte Kälteleistung.
Stage I	24–30 °C*	Ein Modul erzeugt den Temperaturhub und die geforderte Kälteleistung.
Stage II	30–45 °C*	Beide Module erzeugen den Temperaturhub und die geforderte Kälteleistung in Serie.

* Die Temperaturangaben beziehen sich alle auf den Nennarbeitspunkt sowie den Kaltwasserein- und -austritt von 28 °C auf 22 °C und eine Kälteleistung von 35 kW.

22 °C erzeugt werden – ideal zur Kühlung von Serverräumen und ein Bereich, den herkömmliche Kältemaschinen nur teilweise abdecken können.

Bewährung in der Praxis

In verschiedenen Referenzprojekten wird der eChiller bereits zur Kühlung von Serverräumen und Rechenzentren verwendet, etwa bei der DMK Deutsches Milchkontor GmbH und der Sparkassen IT Calw GmbH & Co. KG. Die Server werden hier mit 20 bis 26 °C kalter Luft gekühlt, die der eChiller erzeugt: Kaltluft wird mit Ventilatoren durch die Server transportiert und nimmt die Abwärme der Elektronik auf. Die erwärmte Abluft wird dann von einem Kühler, der mit dem eChiller verbunden ist, wieder auf die Zulufttemperatur gekühlt. Die Rückkühlung (Wärmeabgabe an die Umgebung) erfolgt über Trockenkühler und Solekreislauf. Für die erforderliche Redundanz ist ein herkömmlicher Kaltwassersatz mit HFKW als Kältemittel installiert worden. Das ist insofern interessant, als ein direkter Energieeffizienzvergleich möglich ist: Von Juni 2016 bis Februar 2017 erzeugte der eChiller etwa 80 MWh Kälte, wozu er etwa 4 MWh Strom benötigte – was unter anderem daran liegt, dass die Maschine ab Oktober überwiegend im Freikühlbetrieb arbeitete und in dieser Zeit eine Leistungsaufnahme von nur ca. 300 W hat. Damit ist der eChiller etwa sechsmal effizienter als die HFKW-Redundanzmaschine.

Die Klimatisierung des DMK-Rechenzentrums in Bremen erfolgt seit Dezember 2014 mit dem eChiller. Dort werden Server mit einer Leistung von 21 kW betrieben, wobei derzeit eine maximale Kühlleistung von ca. 30 kW, bei einer maximal zulässigen Kaltgangtemperatur von 26 °C, abgedeckt wird. Beim Milchkontor ist die Redundanz ebenfalls in Gestalt einer Standardkälteanlage (mit R410A) und Freikühlung installiert, sodass man auch hier beiden Maschinen, die über den gesamten Versuchszeitraum parallel betrieben wurden, direkt vergleichen konnte: Die über das gesamte Jahr gemittelte Kälteleistungszahl betrug ca 26 kWh Nutzen pro kWh Aufwand und lag damit um den Faktor 6 höher als die der Redundanzanlage .Neben der Kühlung von Serverräumen eignet sich der eChiller auch zur Kühlung von industriellen Anwendungen, zum Beispiel im Kunststoffspritzguss, in der chemischen Industrie oder bei Bioreaktoren. Bei der Gebäudekühlung kommt der eChiller insbesondere bei der Bauteilaktivierung oder bei Kühldecken zur Anwendung.

Effizient und zukunftsfähig

Ein wesentlicher Aspekt der Wasserkühlung sind die deutlich geringeren Kosten. Die Einsparung ergibt sich zum einen aus der Effizienz und dem reduzierten Stromverbrauch: Hochgerechnet hat sich in nunmehr 360 Betriebsmonaten eine Einsparung von 1120 t CO_2-Äquivalent ergeben, was Strom für ca. 390.000 Euro entspricht. Die Leistungsdaten sind zudem durch mehrere unabhängige Messungen, u. a. durch den TÜV in Anlehnung an die Norm DIN EN 14511-2 bestätigt. Zum anderen wirkt sich der minimale Wartungsaufwand positiv aus: Wasser als Kältemittel fällt nicht unter die F-Gase-Verordnung, und damit greift die gesetzliche Wartungs- und Meldepflicht nicht. Nach Außerbetriebnahme der Anlage kann das als Kältemittel verwendete Wasser problemlos der Abwasserentsorgung zugeführt werden. In der Regel werden die Anlagen mit Leitungswasser befüllt, das am Installationsort der Anlage aus dem Versorgungsnetz entnommen wird. Zudem ist die Anlage BAFA-förderfähig.

Florian Hanslik,
Leiter Entwicklung Anlage und Regelung, Efficient Energy GmbH

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.), Ralph Novak, Florian Eichberger (Lektorat)

Autoren dieser Ausgabe:
André Engel, Simon Federle, Florian Hanslik, Thorsten Hesse, Philipp Nölle, Matthias Pfützner, Dr. Markus Pleier, Gerrit Reichert, Ariane Rüdiger, Michael Vogeler, Kai Wirkus

DTP-Produktion:
Madlen Grunert, Matthias Timm, Hinstorff Media, Rostock

Korrektorat:
Ninett Wagner, Hinstorff Media, Rostock

Titelbild:
Hanns von Rein, Hinstorff Media, Rostock

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

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

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

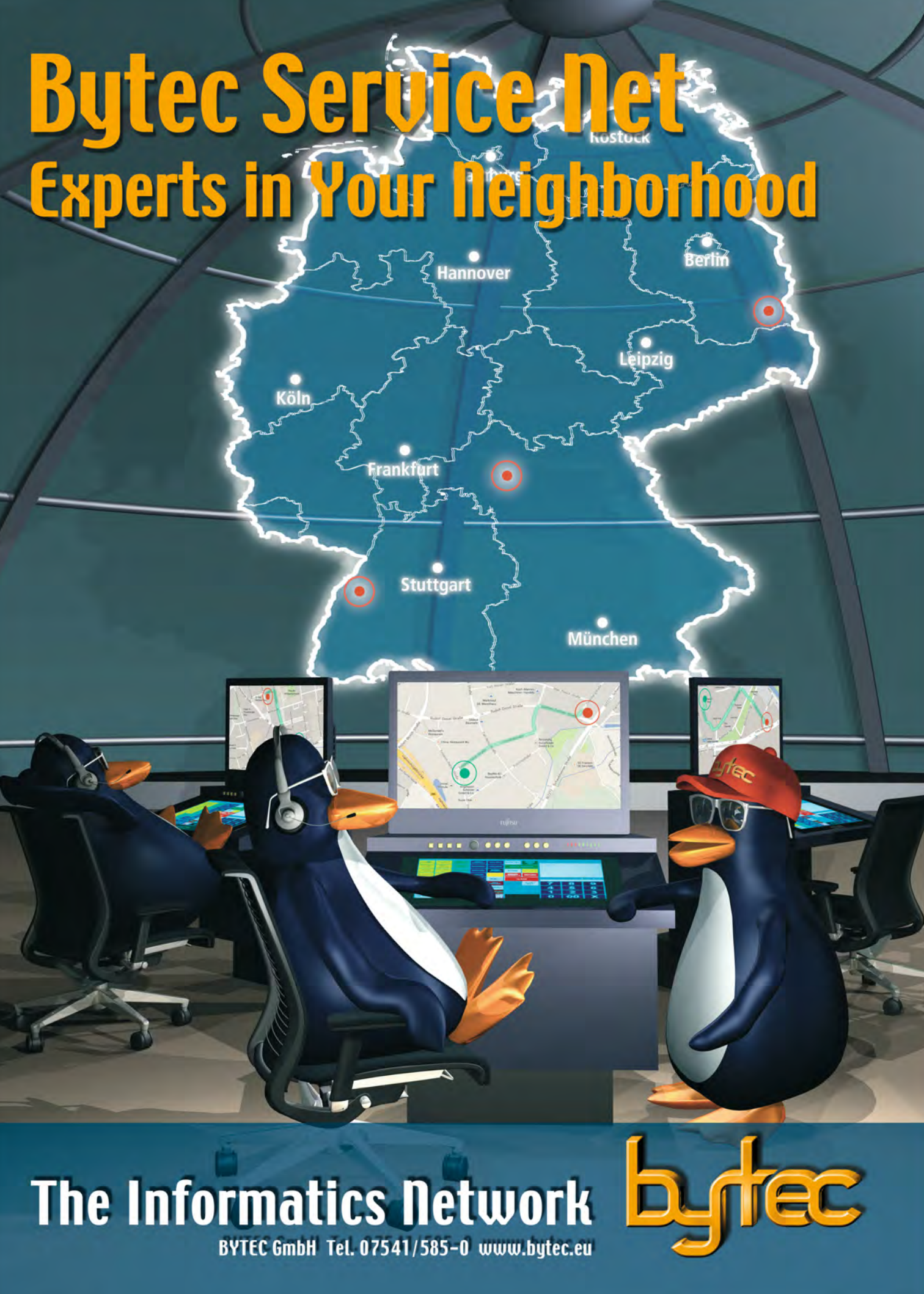
Die Inserenten

WIR TRINKEN DEN KAFFEE #000000.

iX. WIR VERSTEHEN UNS.

Jetzt Mini-Abo testen:
3 Hefte + iX-Kaffeebecher nur 13,50 €
www.iX.de/test

Sie mögen Ihren Kaffee wie Ihr IT-Magazin: stark, gehaltvoll und schwarz auf weiß!
Die iX liefert Ihnen die Informationen, die Sie brauchen: fundiert, praxisnah und unabhängig.
Testen Sie 3 Ausgaben iX im Mini-Abo + iX-Kaffeebecher für 13,50 Euro und erfahren Sie, wie es ist, der Entwicklung einen Schritt voraus zu sein.
Bestellen Sie online oder telefonisch unter +49 (0)541 800 09 120.


Bytec Service Net
Experts in Your Neighborhood
Rostock
Hannover
Berlin
Leipzig
Köln
Frankfurt
Stuttgart
München
The Informatics Network
BYTEC GmbH Tel. 07541/585-0 www.bytec.eu
bytec