Eine Themenbeilage der
Heise Medien GmbH & Co. KG

III
2016

RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Wie das Data Center der Dinge funktioniert

www.rechenzentren-infrastruktur.de

powered by:

Wie das Data Center der Dinge funktioniert

Ich kenne Systemtechniker, die morgens ihr Smart Home verlassen, während hinter ihnen die Heizung bis zum Abend herunterfährt. Am Arbeitsplatz legen sie dann zuerst seufzend den Lichtschalter um, damit die Neonröhren anknistern. Dabei ist die vernetzte Haustechnik nicht wirklich besser und sie besteht allzu oft aus Einzel- und Segmentlösungen mit Spielwarencharakter. Trotzdem wäre in den Rechenzentren bereits sehr viel mehr IP- und SNMP-basierte Steuerung möglich.

Doris Piepenbrink hat sich auf der diesjährigen Light + Building 2016 umgesehen, wie weit die intelligent automatisierte Zweckbausteuerung bereits geht (Seite 20). Das reicht von der LAN-basierten LED-Beleuchtung mit Präsenzmeldern bis zu digitalen Schnittstellen für Einbruchs- und Brandmeldeanlagen. Bei Feuer könnten die Prozesse sicher in redundante Systeme auswandern, und die Anlage würde kontrolliert herunterfahren. Ein solcher Notfall-Shutdown hält auch in virtualisierten Umgebungen, wenn man USV-System und Hypervisor richtig verknüpft (Seite 18). Überhaupt wird Strom mehr und mehr zur softwaregesteuerten Ressource – schließlich sind Energiekosten ein Argument, das das Controlling auf Anhieb versteht. Dazu erklärt Martin Reinert eingehend, wie der Eco-Modus bei einer Online-USV im Unterschied zur Line Interactive USV funktioniert (Seite 23).

Stromausfälle sind der Schrecken jedes Rechenzentrums, das ist schon richtig. Aber Urlaubsanträge und Krankmeldungen sind noch gefürchteter. Denn die Personaldecke ist vielerorts denkbar dünn, und die meisten RZ-Betreiber würden den letzten Serverschrank am liebsten zur Admin-Schlafkabine umbauen. Vor allem dass neue Kräfte so schwer zu gewinnen sind, gehört zu den drängendsten Problemen der Branche. Der jüngste Studienbericht aus der Optimized-Data-Center-Befragung (Seite 4) zeigt außerdem, dass Routineaufgaben im RZ-Management den größten Ärger machen. In Sachen Backup und Sicherheit sind die meisten Betreiber dagegen schon sehr weit. Allerdings möchte man DDoS-Attacken und massenhaft Bots gar nicht erst an die Server lassen. Was eine vorgelagerte Cloud-Lösung in diesem Punkt leisten kann, erklärt Ralf Gehrke ab Seite 6.

Außerdem klopfen wir in diesem Heft noch einmal die jüngsten Verkabelungsstandards ab, schließlich beruft sich die neue EN 50600-X ausdrücklich auf die EN 50173-5, die wiederum die Standards für eine strukturierte Verkabelung auf Patch-Ebenen setzt. Wie solche Topologien aussehen, was bei der Trassenführung zu beachten ist und wie ein kleines LED-Lämpchen für Durchblick bei Wartungsarbeiten sorgt, lesen Sie ab Seite 9. Anschlusstechnisch könnte unterdessen die IEEE 802.3bm einen Wechsel auslösen, vermutet Kai Wirkus (Seite 14). Denn für Base-8-Kabelsysteme bieten sich dann URM-Steckverbinder an, die deutlich sparsamer mit dem Dämpfungsbudget umgehen. Der Grund dafür liegt in der Physik der Herstellung, bei der jede einzelne Faser poliert werden kann.

André Engel ergänzt weitere wichtige Punkte, bei denen die Verarbeitung die Qualität der Netzwerkkomponenten entscheidend bestimmt: Goldauflage, Kontaktpresshöhen, Micro- und Macrobending und nicht zuletzt die Anzahl der Steckzyklen. Darum gehören fertige Installationen auch sauber durchgemessen, und zwar nicht nur stichprobenartig. Sparen können Sie an anderer Stelle besser und sinnvoller, zum Beispiel bei der Server-Beschaffung (Seite 19) oder mit einer trickreichen Kombination von Blockheizkraftwerk und RZ-Klimatisierung, wie sie die Stadtwerke Schönebeck an der Elbe gebaut haben (Seite 25). Im Sommer wandelt eine Adsorptionskältemaschine die Wärme in Kühlenergie für den IT-Kaltwasserkreis um. Für jetzt in der Übergangszeit ist das Nutzungsverhältnis bedarfsgenau regelbar, im Winter übernimmt dann der Freikühler die Server. So funktioniert Gebäudetechnik für Rechenzentren!

Thomas Jannot

Der Teufel steckt im Tagesgeschäft

Besonders bei Personal- und RZ-Management besteht Handlungsbedarf

Die Datenschutz- und Datensicherheitsdiskussion hat Rechenzentrumskunden wählerisch gemacht. Darum hat sich in diesem Punkt viel getan – zumindest im Serverraum selbst. Sehr viel effizienter könnten jedoch viele RZ-Routineabläufe sein, und neue Fachkräfte werden zu einem ernsthaften Problem.

Selbst das leistungsstärkste IT-Equipment macht noch kein erfolgreiches Rechenzentrum. Auch ein modernes Gebäude mit neuester Verkabelung, effizienter Klimatisierung und sicherer Stromversorgung ist noch kein Garant für Erfolg. Ebenso entscheidend – und vor allem nicht allein mit Geld zu lösen – ist die alltägliche Organisation und Kontrolle von Prozessen, Gebäude- und IT-Infrastrukturen sowie verkauften Leistungen, sprich: das Tagesgeschäft. Dass es sich hierbei nicht um banale Tätigkeiten, sondern um ein komplexes Aufgabenfeld handelt, spiegelt sich in der Selbstbewertung der Rechenzentrumsbetreiber wider, die im Rahmen einer repräsentativen Befragung ihre eigenen Prozesse bewertet haben.

Fasst man die Anforderungen – egal, ob von internen oder externen Anspruchstellern – an einen Rechenzentrumsbetreiber zusammen, ergeben sich als Aufgabenprofil die Sicherstellung des Betriebs von IT-gestützten Prozessen durch die Bereitstellung benötigter Ressourcen zur richtigen Zeit, in der richtigen Qualität, mit hoher Verfügbarkeit und ausreichender Sicherheit sowie die stetige Weiterentwicklung der Rechenzentrumsumgebung an die sich fortlaufend ändernden Rahmenbedingungen. Zugegeben: keine leichte, aber auch die wichtigste Aufgabe, wenn man sich dauerhaft gegen Konkurrenten durchsetzen will. Die besten Prozessoren im Server helfen wenig, wenn sie nicht gewinnbringend genutzt werden.

Effizienz in der Selbsteinschätzung

Um dieses anspruchsvolle Aufgabenprofil zu erfüllen, müssen die RZ-Verantwortlichen verschiedene Vorkehrungen treffen, die oft – und zum Teil auch zwingend – durch IT-Lösungen unterstützt werden müssen. Welche das sind, hat die Befragung ebenfalls eruiert, die sich nach den Maßnahmen in den Bereichen Rechenzentrumsbetrieb, externe Anbindung, IT-Infrastruktur und Gebäudeinfrastruktur erkundigte: Werden sie bereits eingesetzt und wenn ja, wie gut?

Das Gesamtergebnis fällt eher ernüchternd aus. Der Bereich Rechenzentrumsbetrieb schneidet mit 56 Indexpunkten am schlechtesten ab. Zum Vergleich: Die Gebäudeinfrastruktur, mit der die meisten Betreiber am zufriedensten sind, erreicht 62 Punkte. (Weitere Zahlen und Einzelheiten findet man in den vollständigen Studienberichten, die es kostenlos gegen Registrierung auf dem Optimized-Data-Center-Portal www.optimized-datacenter.de gibt. Die Studie und die Benchmark werden durch Sponsoren unterstützt, daher ist die Teilnahme kostenfrei.)

Von den sechs Aufgabenfeldern des Rechenzentrumsbetriebs fallen vor allem zwei negativ auf: sehr deutlich das Personalmanagement und, nur geringfügig besser, das RZ-Management. Was hingegen relativ gut funktioniert, sind die klarer definierten Bereiche Client-Management, Monitoring und Backup. Am besten schneidet der Bereich ab, auf den sich die größten Erwartungen von Kunden, Politik und Öffentlichkeit richten: die Datensicherheit, sowohl in rechtlicher als auch physischer Hinsicht.

Personal- und RZ-Management

Die Gewinnung neuer Fachkräfte ist der mit Abstand am schlechtesten bewertete Prozess im gesamten Rechenzentrumsbetrieb. Fast ein Drittel der Unternehmen benennt massive Probleme, weitere 51 % bewerten den eigenen Zustand nur als befriedigend oder ausreichend – also nahe der Erträglichkeitsgrenze. Das mag mit der Aus- und Weiterbildung zusammenhängen, die ebenfalls relativ schlecht bewertet wurde, Arbeitnehmern aber generell sehr wichtig ist – vor allem in der sich schnell und stetig verändernden IT-Branche. Leider bleibt dieser Punkt aber oft auf der Strecke, weil das Personal zu stark an operative Aufgaben gebunden ist.

Auch beim RZ-Management zeigen sich große Umsetzungslücken. Zu den besser umgesetzten Maßnahmen gehören solche, die mit der Automatisierung von wiederkehrenden Standardaufgaben zu tun haben, z.B. IMAC Workflows oder Selfservice-Plattformen zur Entlastung der IT-Abteilung. Allerdings beschränkt sich auch hier der Anteil der sehr zufriedenen Rechenzentrumsbetreiber auf etwa ein Drittel der Befragten.

Größere Probleme gibt es bei den weniger alltäglichen Aufgaben, wie einem umfassenden DCIM (Data Center Infrastructure Management) oder beim Change Management, das heißt der ordentlichen Planung und Durchführung von Änderungen an der IT-Infrastruktur. Hier hat nahezu jedes vierte Unternehmen massive Probleme.

Client-Management und Monitoring

Im Client-Management schneiden vor allem die Prozesse rund um die automatische Einrichtung einzelner Clients sehr gut ab, zum Beispiel die zentrale Patch-Verteilung, das automatisierte OS-Deployment und das zentrale Lizenzmanagement. In Relation dazu steht es um das übergreifende Management der Clients schlechter. So ist bei rund zwei Dritteln der Befragten sowohl die Inventarisierung als auch die Verwaltung der Gesamtheit aller IT Assets allenfalls befriedigend umgesetzt.

HYPERKONVERGENZ GEGEN FACHKRÄFTEMANGEL

Unter dem Schlagwort „Hyperkonvergenz“ bieten erste Hersteller IT-Komplettlösungen an, die das Rechenzentrum massiv verschlanken können. Bei dieser Art Systemarchitektur steht die Software im Mittelpunkt: Sie integriert Computing-, Storage-, Netzwerk- und Virtualisierungsressourcen etc. sehr eng miteinander. Das Konzept richtet sich vornehmlich an Unternehmen aus dem Mittelstand, die ein kosteneffizientes System brauchen und wenig Fachkräfte dafür abstellen können.

Der jüngste State of Hyperconverged Infrastructure Market Report von ActualTech Media und SimpliVity sieht die hoch automatisierten, kompakten Virtualisierungslösungen zwar noch ganz am Anfang, macht 2016 aber eine steigende Nachfrage aus. Im Fokus stehen dabei mittelständische Unternehmen, denn sie können damit einiges an Kostendruck aus der IT nehmen, nicht zuletzt deshalb, weil hyperkonvergente Systeme mit weitaus weniger Personalaufwand zu betreiben sind. Zudem leistet ein einzelner Anbieter Support für das gesamte Produkt.

SimpliVity wirbt momentan besonders aktiv. Das US-Start-up hat nach über drei Jahren Entwicklungszeit 2013 mit OmniCube eine hyperkonvergente Hard- und Software-Gesamtlösung präsentiert, die mittlerweile in deutschen Unternehmen angekommen ist (zum Beispiel beim Zementhersteller KHD aus Köln). SimpliVity setzt dabei vollständig auf Virtualisierung (derzeit VMware-Umgebungen, in Zukunft auch KVM und andere). Das Unternehmen hat für den Mittelstand sogar eigene Finanzierungsmodelle aufgelegt, die sowohl die Argumentation der Admins als auch die Entscheidung an der Spitze erleichtern sollen.

Bei vielen Betreibern konzentriert sich das Monitoring noch stark auf die Klimatisierung und weniger auf den gesamten Energieverbrauch. Dabei lässt sich schon durch verbrauchsoptimiertes IT-Equipment oder eine effiziente Stromversorgung viel einsparen, letztendlich sogar Wärme vermeiden, die sonst durch die Klimatisierung wieder abgeführt werden müsste. Das kontinuierliche Energiemonitoring wird derzeit aber noch von insgesamt einem Viertel aller Betreiber komplett vernachlässigt, das heißt sehr schlecht oder gar nicht durchgeführt. Am häufigsten wird die Klimatisierung regelmäßig auf den Energiebedarf überprüft. Erst mit Abstand folgen Hardware und Stromversorgungskomponenten.

Das Monitoring von IT-Leistungen und -Diensten wiederum variiert in seiner Umsetzung je nach Einsatzbereich. So steht die Netzwerkperformance im Vordergrund der Monitoring-Aktivitäten und wird von 40 % der Befragten auch gut oder sehr gut umgesetzt. Das Monitoring von Diensten, die auf den Servern betrieben werden, findet sich knapp dahinter. Die in Anspruch genommenen Cloud-Services überwacht allerdings nur ein Viertel der befragten Rechenzentrumsbetreiber auf einem ebenso hohen Niveau.

Quelle: techconsult GmbH

Der Kühlung gilt das Hauptaugenmerk, ein kontinuierliches Gesamtenergie-Monitoring findet dagegen so gut wie gar nicht statt.

Backup und Sicherheit

Auch das ganzheitliche Monitoring in einer zentralen Lösung wird noch weniger gut umgesetzt, und das, obwohl über die Hälfte der Betreiber angibt, mehr als fünf Stunden pro Woche für das Monitoring aufzuwenden. Bei 15 % liegt der Aufwand sogar bei mehr als zehn Stunden.

Einen sehr hohen Stellenwert genießen Backups. Der am besten umgesetzte Prozess im kompletten Rechenzentrumsbetrieb ist daher auch die Wiederherstellung von virtuellen Infrastrukturen: Mehr als die Hälfte aller Betreiber setzt diese elementare Aufgabe gut oder sehr gut um. Auch die Erarbeitung einer kompletten Backup-Strategie für alle IT-Infrastrukturen setzt fast die Hälfte der Befragten zufriedenstellend um.

Die besten Indexwerte erzielt der Bereich Sicherheit. Das heißt aber bei Weitem nicht, dass das angesichts seiner Bedeutung schon genügt. Informations- und Datensicherheit genießen in Deutschland höchsten Stellenwert und werden auch von Kunden bei der Anbieterauswahl sehr ernst genommen. So ist zum Beispiel ein ISMS (Information Security Management System) gerade im Kontext fortgeschrittener IT-Dienstleistungen, die ein RZ bereitstellt, sehr wichtig. Dass nur 41 % der Befragten ein solches Managementsystem gut oder sehr gut umgesetzt haben, ist genau genommen also zu wenig.

Darüber hinaus führt nur ein Drittel der Rechenzentrumsbetreiber Risikoanalysen gut oder sehr gut durch. Ein Teil der Unzufriedenheit lässt sich zum einen durch die fehlende Regelmäßigkeit – nur die Hälfte führt sie jährlich durch – und zum anderen durch den oft eingeschränkten Umfang erklären: Nur etwa 30 % analysieren auch das Gefahrenpotenzial der Gebäudeumgebung.

Marco Becker,
Analyst/Projektleiter ODC, techconsult GmbH

Die vorgelagerte Verteidigungslinie

Intelligente Cloud-Lösungen ziehen einen zusätzlichen Sicherheitsring

Lokale Firewalls und Load Balancer sind mit massiven DDoS-Attacken überfordert. Das wissen auch die Angreifer, die Rechenzentren und Webanwendungen ins Visier nehmen. Ein mehrstufiges Sicherheitskonzept erweitert die internen Lösungen um Cloud-basierte Dienste wie Bot-Management oder Client Reputation.

Die Zeiten sind vorbei, in denen rein präventive und lokal installierte Lösungen wie Firewalls oder Antivirenschutz ausreichten, um Netzwerke und Rechenzentren von Unternehmen effektiv zu schützen. Die IT-Sicherheitsmaßnahmen im eigenen Rechenzentrum sind bei massiven DDoS-Attacken mit Bandbreiten ab 10 GBit/s oder Angriffen auf Webanwendungen oft überfordert.

Dabei nehmen die Bedrohungen an Quantität und Qualität zu. Dem aktuellen State of the Internet Security Report von Akamai zufolge stieg im ersten Quartal 2016 die Zahl der Attacken auf Webanwendungen im Vergleich zum Vorquartal um 25,52 %, die der DDoS-Angriffe um 22,47 %. Im Vergleich zum ersten Quartal 2015 gab es gar einen DDoS-Anstieg um 125,36 %. Wiederholte Attacken auf das gleiche Ziel sind mittlerweile gang und gäbe. Der größte DDoS-Angriff im ersten Quartal 2016 erreichte einen Spitzenwert von 289 GBit/s.

Entlastung schon im Vorfeld

Die gestiegene Komplexität, die hohe Frequenz und die zunehmende Größe der Cyberattacken stellen Unternehmen vor große Herausforderungen. Da sie zudem selten IT-Spezialisten beschäftigen, die sich dezidiert mit dem Thema IT-Security befassen können, liegt es nahe, die traditionellen internen Sicherheitsmaßnahmen um Cloud-basierte Services zu erweitern. Damit erhalten Unternehmen einen gestaffelten und mehrstufigen Schutz ihrer IT-Infrastruktur und Webanwendungen.

Cloud-basierte Lösungen erfüllen mehrere Aufgaben: Da sie flexibel skalierbar sind, können sie bandbreitenintensive DDoS-Angriffe abwehren, denen interne Appliances oft nicht mehr gewachsen sind. Dann bleiben Webanwendungen trotz einer laufenden Attacke ohne Performance-Einbußen weiter verfügbar. Außerdem lassen Cloud-Lösungen, die als Reverse Proxy arbeiten, häufig nur Verbindungen zu bestimmten TCP-Ports zu (80: HTTP oder 443: HTTPS). Sie beenden diese Verbindungen auf der Client-Seite und können die gesendeten Befehle und Daten kontrollieren und filtern. Diese vorgelagerte Verteidigungslinie entlastet die Administratoren in den Unternehmen, da sie einen Großteil der Angriffe schon blockieren kann. Damit reduziert sich die Menge an lokalen (Firewall-)Logdateien.

Nicht zuletzt steht hinter einem Managed Service das umfangreiche Erfahrungswissen eines Dienstleisters, der viele Kunden schützt und somit auch viele unterschiedliche Angriffsvarianten sieht. Da beinahe täglich neue Angriffsvektoren entdeckt werden, muss eine Sicherheitslösung stets aktuell sein und in ihrer Konfiguration die veränderte Bedrohungslandschaft berücksichtigen.

Gute und böse Bots

Ein gutes Beispiel für Cloud-Security-Services ist das Bot-Management. Analysen haben ergeben, dass teilweise bis zu 40 % oder mehr des Webtraffics eines Unternehmens durch Bots erzeugt werden. Diese kleinen Programme arbeiten im Auftrag eines Nutzers oder eines anderen Programms sich wiederholende Aufgaben weitgehend automatisch ab oder simulieren Aktivitäten eines realen Benutzers auf einer Webseite. Es gibt „gute“ und „böse“ Bots.

Beispiele für nützliche und gutartige Bots sind die Webcrawler von Internet-Suchmaschinen. Bösartige Bots hingegen können Schaden anrichten, indem sie etwa Webinhalte unautorisiert kopieren, Werbeeinnahmen durch automatisierte Klicks auf betrügerische Weise erhöhen oder E-Mail-Adressen für Werbezwecke sammeln. Sehr gefährlich sind Bots als Teil von DDoS-Angriffen.

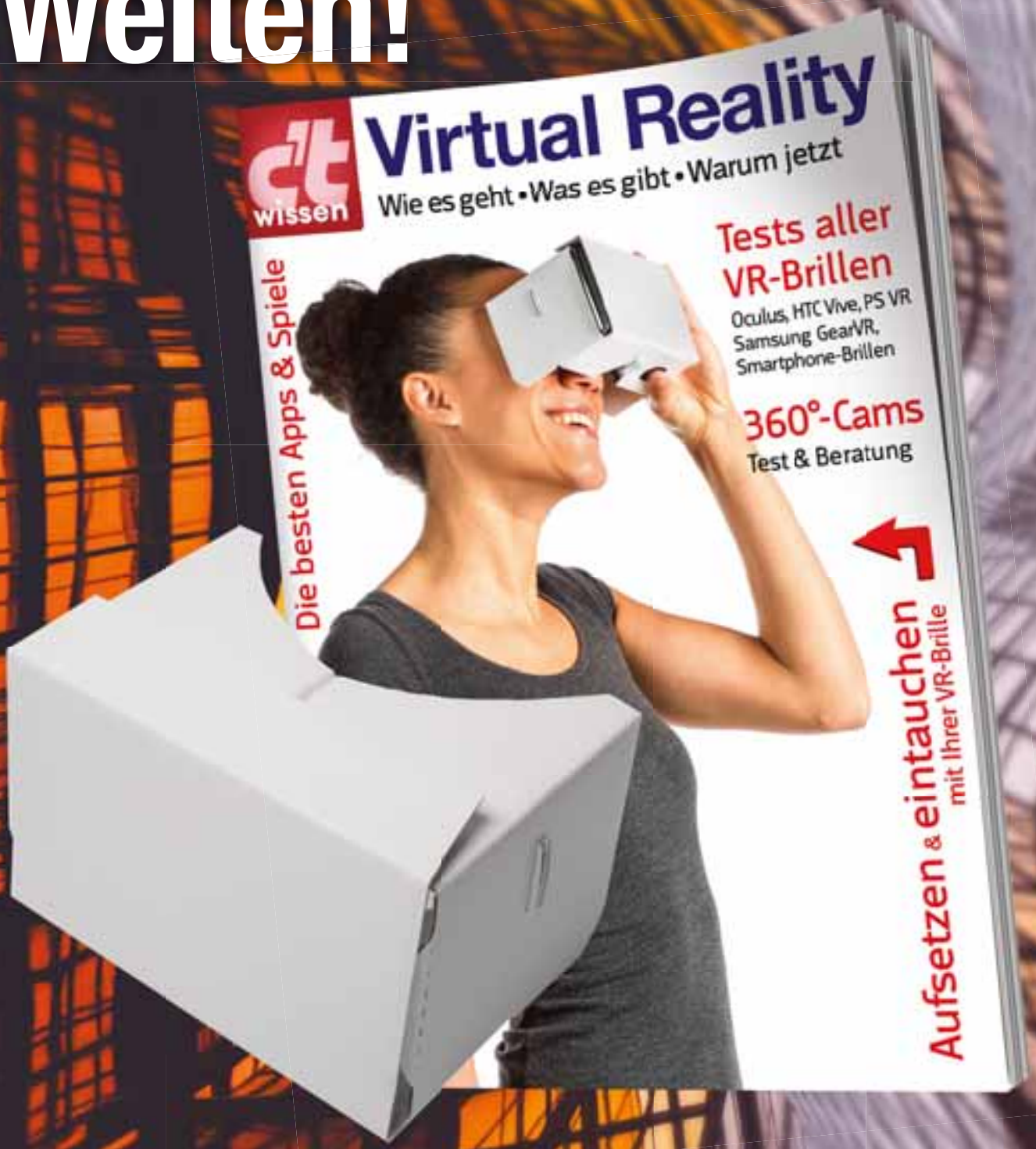
Im ersten Schritt geht es für ein Unternehmen also darum, den Bot-Datenverkehr auf seiner Website auszuwerten und die Guten von den Bösen zu unterscheiden. Ein fähiges Cloud-Bot-Management stellt dafür ein umfangreiches Verzeichnis mit bekannten Signaturen und legitimen Web- und Business-Services bereit, um den Bot-Datenverkehr schnell zu identifizieren. Darüber hinaus sollten Firmen etwa auf Basis von Header-Informationen oder Cookies individuell Bot-Signaturen und -Kategorien definieren können, mit denen sie neue oder einzigartige Bots auf ihrer Website besser erkennen. Der Cloud-Service sollte zudem über Funktionen für die Echtzeiterkennung bislang unbekannter Bots verfügen. Dazu nutzen die Dienstleister beispielsweise Informationen über Bots, die bereits auf den Webseiten anderer Kunden als Web Scraper tätig waren und unautorisiert Daten gesammelt haben.

Intelligentes Bot-Management

Im besten Fall kann das Unternehmen mit einem Bot-Manager flexible Richtlinien für den Umgang mit den verschiedenen Arten des Bot-Datenverkehrs erstellen. Denn eine pauschale Blockade aller Bots inklusive der Suchmaschinen-Bots ist wenig sinnvoll, da sich das negativ auf das Webseiten-Ranking auswirken kann. Anders sieht es bei schädlichen Bots aus. Ein einfaches Blocken ist jedoch auch nicht zielführend, da der Bot-Betreiber seinen Schnüffler anschließend so modifizieren kann, dass er nicht mehr erkannt wird. Daher müssen die Regeln für den Umgang mit Bots intelligent gestaltet und permanent aktualisiert werden.

Einen Sonderfall bilden Bots, von denen das Unternehmen profitiert, die aber wegen ihres Datenvolumens die Performance der Website be-

Hinein in andere Welten!



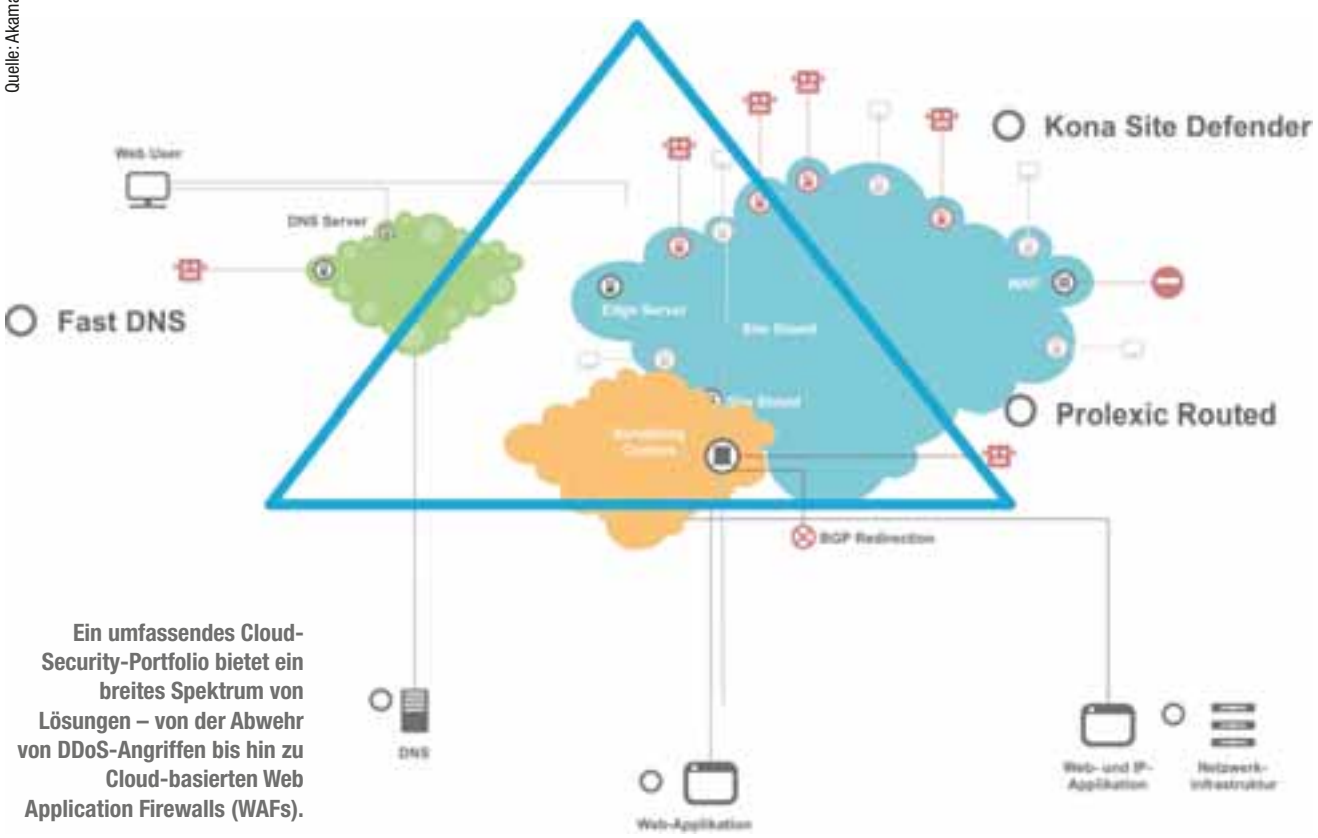
Jetzt für nur 12,90 € inklusive VR-Brille bis 18.9. portofrei bestellen.

shop.heise.de/ct-vr-2016 service@shop.heise.de
Auch als eMagazin erhältlich unter: shop.heise.de/ct-vr-2016-pdf

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

heise shop
shop.heise.de/ct-vr-2016 ›

Quelle: Akamai



Ein umfassendes Cloud-Security-Portfolio bietet ein breites Spektrum von Lösungen – von der Abwehr von DDoS-Angriffen bis hin zu Cloud-basierten Web Application Firewalls (WAFs).

einträchtigen können. Auch hier ergibt eine pauschale Blockade wenig Sinn. Ein Cloud-basierter Bot-Manager stellt dazu verschiedene Maßnahmen zur Verfügung. Er leitet beispielsweise die Anfrage des Bots an eine andere Website um, bietet alternative Inhalte an oder verzögert den Bot-Datenverkehr, sprich: Bots dürfen die Website erst nach einer Pause von einigen Sekunden wieder aufrufen.

Ein ordentlicher Bot-Manager stellt zudem über ein Dashboard ausführliche Berichtsfunktionen mit Visualisierungen bereit, damit das Unternehmen die Auswirkungen des Bot-Datenverkehrs auf seine Website besser versteht.

Risikobewertung mit Client Reputation

Etablierte Anbieter von Cloud-Security-Services analysieren täglich mehrere Terabytes an Webverkehr, den Hunderte Millionen IP-Adressen erzeugen. Damit gewinnen sie ein umfassendes Bild der sich ändernden Strategien und Vorgehensweisen von potenziellen Angreifern. Diese Erkenntnisse bilden schließlich die Basis für den Schutz der Webseiten und -Applikationen ihrer Kunden (etwa vor DDoS-Angriffen). Konkretes Beispiel dafür ist ein Client-Reputation-Service, der die Vertrauenswürdigkeit einzelner IP-Adressen bewertet.

Der Cloud-Anbieter analysiert dazu alle vergangenen Aktivitäten eines Clients und ermittelt, ob dieser bereits an einer Attacke beteiligt war. In die Risikobewertung fließen Faktoren wie die Lebensdauer des Clients, die Anzahl der angegriffenen Anwendungen oder der Schweregrad und der Umfang der Attacken ein. Potenziell gefährlicher Traffic wird anhand der damit verbundenen Gefahren gewichtet und in Kategorien wie klassische Webangriffe, DDoS-Attacken, Schwachstellenscanner oder Web Scraper eingeteilt.

Auf diese Weise ermitteln modernste Algorithmen und Heuristiken für jede IP-Adresse einen Reputationswert, der im Verlauf der Analysen weiter angepasst wird. So entsteht im Laufe der Zeit eine umfangreiche Client-Reputation-Datenbank mit verbotenen und erlaubten Websites sowie IP-Adressen, die ein Sicherheitsmodell auf Basis von Blacklists oder Whitelists etabliert und damit den Zugriff auf Websites oder Webanwendungen reguliert.

Da Client Reputation sich auf die Quelle der HTTP-Transaktion konzentriert und bösartige Aktivitäten vorhersagen kann, ergänzt der Service traditionelle Formen der Identifizierung von Attacken. In Kombination mit Web Application Firewalls, die mithilfe von Regeln geläufige Angriffsmuster wie SQL-Injection oder Cross-Site-Scripting (XSS) blockieren oder auf bestimmte Anomalien reagieren, erhöht Client Reputation die Sicherheit von Webanwendungen enorm.

Schutzmaßnahmen aktuell halten

Da sich die Bedrohungslandschaft und die Angriffsvektoren permanent ändern, passen die Cloud-Anbieter ihre Sicherheitsregeln und -methoden kontinuierlich an. Ein Beispiel ist das Anomaly Scoring. Hier bestimmen und gewichten sie die Risikowerte für verschiedene Angriffsarten und erstellen Risikogruppen für SQL-Datenbanken oder HTTP-Header. Dadurch können sie besser beurteilen, ob ein Request bösartig ist, Warnungen vor Attacken werden treffsicherer und genauer.

Nicht zuletzt bieten Cloud-Security-Services ergänzend zu ihren technischen Lösungen auch umfassende Beratung und Support rund um die Uhr an; gerade diese Expertise fehlt vielen Unternehmen intern. Auch deswegen sollten Firmen ihre bestehenden Maßnahmen im eigenen Rechenzentrum um eine Cloud-basierte Lösung ergänzen, um komplexe Angriffe mit mehrstufigen Sicherheitsmaßnahmen effizient abzuwehren.

Ralf Gehrke,
Senior Service Line Manager EMEA, Akamai

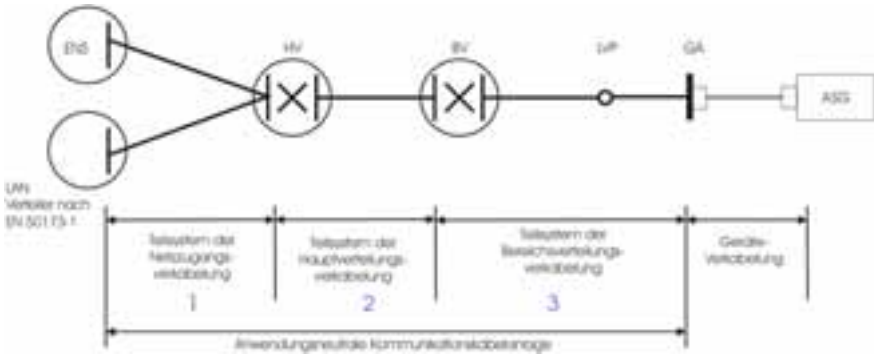
Übersichtlich und anpassungsfähig

Die Mittel für eine strukturierte RZ-Verbindung nach EN 50173-5 gibt es bereits

Obwohl die EN 50173-5 schon vor Jahren verabschiedet wurde, entsprechen noch längst nicht alle RZ-Infrastrukturen dieser Verkabelungsnorm. Die neue Normenreihe für Rechenzentren EN 50600-X verweist übrigens explizit auf die EN 50173-5. Es wird also höchste Zeit, das eigene Data Center daran anzupassen.

EN 50173-5 schafft die Basis für einen durchgängig übersichtlichen Aufbau von Verkabelungen im Rechenzentrum. Statt Server-to-Switch-Verbindungen per Anschlusskabel werden hier alle Geräte über eine gemeinsame Patch-Ebene angeschlossen. Das hat einen entscheidenden Vorteil: Die installierten Datenleitungen müssen nicht angetastet werden, wenn die IT-Abteilung einzelne Geräte tauscht oder zum Beispiel die Serverstruktur verändert.

Vor allem in überschaubaren IT-Umgebungen werden Server und Switches oft noch direkt per Anschlussleitung miteinander verbunden. Eine zusätzlich gespiegelte Patch-Ebene erscheint hier zunächst umständlich. Doch bei Punkt-zu-Punkt-Verbindungen lässt der IT-Betreuer den Wartungsaspekt außen vor. Sobald nämlich eine solche IT-Infrastruktur verändert wird, treten Probleme auf: Sollen beispielsweise neue Server oder Switches integriert werden, passen die Anschlüsse oft nicht mehr.



Quelle: ZVK

Die strukturierte Rechenzentrumsverkabelung gemäß EN 50173-5. ENS: Schnittstelle zum externen Netz; HV: Hauptverteiler; BV: Bereichsverteiler; LVP: lokaler Verteilerpunkt; GA: Geräteanschluss.

Solche Punkt-zu-Punkt-Verbindungen findet man auch in gewachsenen Infrastrukturen. Hier lassen sich die vorhandenen, oft dicht gepackten Kabel im Doppelboden kaum noch identifizieren. Ist dann die Netzwerkdokumentation nicht auf dem jüngsten Stand, steigt das Risiko, dass der Servicetechniker bei der Umschaltung einen aktiven Port unterbricht. Da sich das nicht mehr benötigte Kabel nicht eindeutig identifizieren und auch nur schwer bewegen lässt, verbleibt es meist im Doppelboden. So wird der Doppelboden mit jedem neuen Anschlusskabel voller, und die Brandlast steigt unaufhörlich. Hinzu kommt, dass mit zusätzlichen aktiven Komponenten auch der Kühlbedarf im Rechenzentrum zunimmt, die kalte Luft aber kaum noch ungehindert durch den vollgepackten Doppelboden strömen kann. Das Risiko von Hitzenestern steigt.

Flexibel und sauber auf Patch-Ebene

Die strukturierte Verkabelung nach EN 50173-5 vermeidet das. Die Norm basiert auf langjährigen Best-Practice-Erfahrungen von großen Rechenzentrumsbetreibern und ermöglicht Netzanpassungen ohne Störung des Betriebs. Sie stellt eine anwendungs- und herstellerneutrale Infrastruktur zur Verfügung, bei der die Verkabelungskomponenten und -systeme je nach Datendurchsatz und Umgebungsbedingungen bestimmten technischen Mindestanforderungen entsprechen müssen.

Bei einer Verkabelung nach EN 50173-5 werden die einzelnen Geräte und Systeme analog zur LAN-Verkabelung über Bereichsverteiler an den Hauptverteiler eines RZs angeschlossen. Der Hauptverteiler verbindet die Bereichsverkabelungen des RZs mit den Zugangsnetzen sowie mit dem LAN. Sowohl die Bereichs- als auch der Hauptverteiler müssen als Cross Connects also als echte Patch-Verteiler ausgeführt sein. Das gewährleistet ein sicheres, gut zu dokumentierendes und durch die gute Zugänglichkeit einfach und damit kosteneffizient durchführbares Patch-Management. Außerdem erlaubt diese Infrastruktur eine flexible Konfiguration von Redundanzen.

Topologien im Überblick

Die Norm erlaubt dabei verschiedene Verkabelungstopologien. Diese richten sich nach den Bedürfnissen des Betreibers und der vorhandenen Infrastruktur. Die Struktur sollte man jedoch einheitlich durchhalten, um Wartungsarbeiten und Erweiterungen zu vereinfachen und möglichst prozesssicher zu gestalten. Häufig findet man zum Beispiel Infrastrukturen mit zentralem Bereichsverteiler oder mit zusätzlichen lokalen Verteilerpunkten in den Schrankreihen.

Will der RZ-Betreiber alle IT-Komponenten einzelner Abteilungen eines Unternehmens oder einzelner Firmen in einem Bürogebäude jeweils in einem Schrank unterbringen, bietet sich eine Topologie mit einem zentralen Bereichsverteiler an. Dabei werden alle Schränke mit

GRUNDLAGE ZU EN 50600-X

Zusätzliche Anforderungen in Richtung Prozesssicherheit und vor allem Ausfallsicherheit ergeben sich aus der neuen Normenreihe EN 50600-X. Die zugehörigen Standards wurden seit Mitte 2013 sukzessive verabschiedet. Sie sollten bei der Planung oder Modernisierung einer RZ-Verkabelung unbedingt mit berücksichtigt werden: EN 50600-1 (Allgemeine Konzepte), EN 50600-2-1 (Gebäudekonstruktion), EN 50600-2-2 (Energieversorgung), EN 50600-2-3 (Klimatisierung), EN 50600-2-4 (Infrastruktur der Telekommunikationsverkabelung), EN 50600-2-5 (Sicherheitstechnik) und EN 50600-2-6 (Management und Betrieb).

Dabei umfasst die EN 50600-1 allgemeine Aspekte: Sie definiert die Teile eines Rechenzentrums, die Designform, Klasse, Typ und Größenordnung sowie die Verfügbarkeitsanforderungen. Außerdem können mit ihr Redundanzen normkonform festgelegt werden. Auf diesen Festlegungen basiert dann die Auslegung der einzelnen Gewerke, die über die EN 50600-2-X abgebildet sind. Für die Verkabelung ist die EN 50600-2-4 „Infrastruktur der Telekommunikationsverkabelung“ zuständig. Diese verweist explizit auf die EN 50173-X.

Quelle: ZVK

Die EasyLan-H.D.S.-Module bieten pro Anschlussmodul zwölf LC-Ports. Bei dieser Installation sind LED-Patch-Kabel im Einsatz: Rechts oben wurde außerdem ein LED-Detektor aktiviert, um bei Wartungsarbeiten den zugehörigen Port links unten sicher zu identifizieren.

ihren Netzwerk- und SAN-Servern sowie -Switches direkt an den zentralen Bereichsverteiler angeschlossen. Über diesen Bereichsverteiler erfolgt dann die Anbindung an Netzwerk-Core und SAN des Bereichs.

Ebenfalls eine gängige Umsetzung sind Rechenzentren, bei denen jede Serverschrankreihe mit einem Switch-Rack am Ende der Reihe ausgestattet ist. Diese Switch-Racks verfügen über einen großen Patch-Bereich und fungieren als lokale Verteilerpunkte. Sie binden die Server ihrer Schrankreihe an das Switch-Core und SAN dieses RZ-Bereichs. Bei dieser Topologie ist die Bereichsverteilung auf die lokalen Verteilpunkte und einen Verteiler am Core aufgeteilt, und die Verbindungen von den lokalen Verteilpunkten in den Reihen lassen sich besonders übersichtlich per Uplink mit dem Bereichsverteiler verbinden.

Trassen und Umgebungsbedingungen

Im RZ können die Kabel entweder im Doppelboden oder in Trassen über den Schränken geführt werden. Das Bundesamt für Sicherheit in der Informationstechnik bevorzugt in seinem IT-Grundschutzkatalog M1.69 „Verkabelung in Serverräumen“ jedoch eine Verlegung unter der Decke. Die Kabel lassen sich dort leichter austauschen und beeinträchtigen nicht den Luftstrom der Kühlung im Doppelboden. Außerdem sollen die Kabel „so weit als möglich umfassend fest“ verlegt sein. Das BSI schlägt vor, pro Serverschrank ein Kupfer- und ein LWL-Patchfeld vorzuhalten.

Die MICE-Klassifizierung (Mechanical, Ingress, Climatic, Electromagnetic) für Rechenzentren geht von einer mittleren mechanischen und einer hohen elektromagnetischen Belastung aus. Letzteres spricht zum Beispiel für Glasfaserlösungen. Darüber hinaus ist es sinnvoll, Glasfaserkabel wegen des Platzmangels biegeunempfindlich auszulegen. Solche Glasfasern können Daten selbst bei Biegeradien von 15 oder gar 7,5 mm nahezu verlustfrei übertragen. Ein reduzierter Brechungsindex mit einer Grabenstruktur im Mantel wirft das Licht zurück in den Kernbereich. Dennoch ist es wichtig, auch diese Fasern möglichst stressfrei zu verlegen. Denn auch biegeoptimierte Faser verhindert keine Faserbrüche.

Kupfertechnik-Komponenten

Die EN 50173-5 verweist für die Wahl der Komponenten auf den allgemeinen Teil 1 der Normenreihe (EN 50173-1). Darin sind die verschiedenen Kabel- und Steckertypen spezifiziert, die der Anwender für die ebenfalls darin normierten Übertragungsklassen und Komponentenkategorien benötigt.

Die Verkabelung in und zwischen den Schränken ist häufig mit Kupferverbindungen realisiert. Da im RZ hohe Datenraten vorherrschen, kommen in der Kupfertechnik derzeit nur genormte Komponenten der Kategorie 6A (500 MHz) oder 7A (1000 MHz) infrage. Eine Verbindung sollte mindestens der Klasse EA beziehungsweise FA entsprechen. Derzeit konträr diskutiert werden Kupferkomponenten für 25/40 GBit/s.

Sie müssen der künftigen Kategorie 8.1 und Channel-Klasse 1 (Weiterentwicklung der Kategorie 6A, Klasse EA über RJ45) oder Kategorie 8.2 mit Channel-Klasse 2 (Weiterentwicklung der Kategorie 7A, Klasse FA; der Steckertyp ist noch nicht abschließend festgelegt) entsprechen. ISO/IEC 11801 hat dafür jeweils eine maximale Übertragungsstrecke bis 30 m inklusive Patch-Kabel und eine Übertragungsfrequenz bis 2000 MHz spezifiziert. Erste Komponenten dazu soll es zumindest als Prototypen bereits geben. Wer sein Rechenzentrum dafür auslegen möchte, sollte diese Längenrestriktionen mit einplanen.

Doch derzeit setzen die meisten Rechenzentren in Deutschland Kupferkomponenten der Kategorie 6A ein. Sie eignen sich für 10-Gigabit-Ethernet-Verbindungen bis 100 m und basieren auf einem RJ45-Steckgesicht. Wichtig ist bei Datenraten von 1 und 10 GBit/s, dass alle Komponenten aufeinander abgestimmt sind. Das gilt nicht nur für die Datenleitung und die Anschlussmodule im Patch-Feld, sondern auch für die Patch-Kabel. Ein billiges Patch-Kabel, das nicht der installierten Komponentenkategorie entspricht, kann die Übertragung erheblich beeinträchtigen.

Glasfasertechnik-Komponenten

Die LWL-Verbindungen im Rechenzentrum sollten heute für Datenraten bis 40 oder gar 100 GBit/s ausgelegt sein. Manche RZ-Betreiber schwören auf Singlemode-Fasern (SM) und setzen diese durchgängig im Rechenzentrum ein. Das schafft zwar Bandbreitenreserven, ist aber erheblich teurer als Multimode-Lösungen. Allein der dafür nötige Fabry-Perot-Laser kostet um ein Vielfaches mehr als ein Vertical Cavity Surface Emitting Laser (VCSEL).

Bei Multimode-Faser-Verbindungen (MM) innerhalb des Rechenzentrums genügen für 10GBE direkte Short-Reach-Verbindungen mit OM3- beziehungsweise OM4-Fasern. Sie erlauben Distanzen von 300 m beziehungsweise 500 m. Bei 40-Gigabit-Ethernet ist ein Vierfachwellenlängenmultiplex nötig, um mit OM3-Fasern 100 m und mit OM4-Fasern 125 m zu überbrücken. Bei 100GBE sind zwei Multiplex-Varianten möglich: Mit einem 4-fach-Multiplex lassen sich Distanzen bis 100 m (OM3) beziehungsweise 125 m (OM4) überbrücken. Darüber hinaus ist mit 100GBASE-SR10 ein 10-fach-Multiplex definiert, das die gleichen Distanzen mit einem 10-fach-VCSEL-Array erreicht.

Bei Multiplex-Verbindungen bieten sich MPO-Steckverbinder (Multipath Push-On) an, die in einem Steckergehäuse parallel jeweils 4, 8, 12, 16 oder 24 Faserverbindungen bieten und kaum breiter sind als RJ45-Stecker. Ansonsten findet man im RZ heute fast nur noch LC- bzw. LC-Duplex-Steckverbindungen. Egal, ob MM- oder SM-Technologie zum Einsatz kommt, es muss immer darauf geachtet werden, dass LWL-Komponenten mit sehr hoher Güte (Premiumqualität) zum Einsatz kommen.

Spleißverteilung und Kabeltrunks

Moderne Rechenzentren sind heute durchgängig mit vorkonfektionierten Trunk-Kabellösungen und Mehrfachsteckern versorgt. Die dicken, starren, bis zu 144 Fasern fassenden Backbone-Kabel vom Provider oder Campus-Netz sollten möglichst direkt in einem zentralen Spleißverteiler auf dünne LWL-Trunk-Kabel mit Mehrfachstecker umgesetzt werden. Das erleichtert die Zuordnung und das Handling.

Darüber hinaus findet man für Schrank-zu-Schrank-Verbindungen meist komplett vorkonfektionierte Kabeltrunks im RZ. Die MPO-Verbindungen sind ein Beispiel für solch dünne Trunks. Es gibt außerdem noch LWL-Lösungen auf LC-Basis oder Trunks mit Kupferanschlussmodulen. Sie bilden die Verbindungen zwischen den einzelnen Patch-Ebenen im RZ. Allen gemein ist, dass mehrere Datenverbindungen in einem Kabel integriert sind. Das hat einen kleineren Gesamtquerschnitt, eine geringere Brandlast und zudem eine schnellere Installation zur Folge. Nicht zuletzt sind damit Packungsdichten von wesentlich mehr als 48 Ports pro Höheneinheit möglich. Da die Mehrfachstecker solcher Systeme meist in spezielle Einbaurahmen geschraubt werden, gibt es Lösungen, die auch einen senkrechten Einbau von schmalen Elementen seitlich neben der 19-Zoll-Ebene erlauben.

Patch-Kabel mit LED-Zuordnung

Bei der strukturierten RZ-Verkabelung wird die Patch-Ebene zum entscheidenden Betätigungsfeld für das Wartungspersonal. Da die Patch-Kabel im Verteiler direkt vom Port zur Seite geführt werden, treten gleich hinter dem Stecker Torsionskräfte auf. Diese Torsion beeinflusst bei vielen herkömmlichen Patch-Kabeln, die lediglich mit einer aufgesteckten Knickschutztülle ausgestattet sind, die elektrischen Übertragungswerte. Dabei kommt es vor, dass die Grenzwerte für Kategorie-6A-Komponenten nicht mehr eingehalten werden. Einen besseren Schutz bieten umspritzte Stecker. Hier sind die Adern für die Datenübertragung fest in ihrer Position fixiert. Zudem sollten sie mit einer aufgesteckten Tülle zur Zugentlastung ausgestattet sein.

Um Platz zu sparen, bieten mehrere Hersteller Patch-Panels an, bei denen die Ports in einem Winkel von etwa 30 Grad schräg zur Seite in der Frontplatte montiert sind. So laufen die daran angeschlossenen Patch-Kabel automatisch zur Seite, müssen nicht gebogen werden und benötigen nur eine Befestigung an den Holmen neben dem Patch-Bereich. Zusätzliche Rangierpanels sind unnötig. Damit können vorhandene Verteilerschränke mit doppelter Packungsdichte aufgebaut werden.

Prozesssicherheit ist in Rechenzentren und deshalb auch in der Normenreihe EN 50600-X ein wichtiger Aspekt. Bei jeder Netzveränderung müssen Anschlüsse im Verteilerschrank gepatcht werden, und das Netz ist einem ständigen Wandel unterworfen. Dabei hinkt die Dokumentation oft hinterher. Das führt dann dazu, dass eine Beschriftung nicht mehr mit dem zugeordneten Port übereinstimmt. Patch-Kabel mit LED-Signalisierung erhöhen hier die Prozesssicherheit: Sie leuchten auf, wenn der Anwender an einem Ende des Kabels einen Detektor einsteckt. Das erleichtert Wartungsmaßnahmen während des Betriebs beträchtlich. Ein unbeabsichtigtes Ziehen von Anschlussleitungen ist damit nahezu ausgeschlossen. Außerdem können diese Patch-Kabel als Bündel verlegt und später dank der LED-Signalisierung angeschlossen werden. Das wiederum beschleunigt die Installation.

Protokollneutrale Infrastruktur

Noch werden in Rechenzentren separate Infrastrukturen für Daten- und Storage-Netze betrieben. Schon jetzt aber kann man Data Center mit einer einfacheren, protokollneutralen Infrastruktur betreiben. Entsprechende Komponenten, die sowohl SAN- als auch Ethernet und InfiniBand-Protokolle unterstützen, sind bereits erhältlich. Somit muss nicht mehr zwischen SAN- und Netzwerk-Switch, SAN-Verbindung und Netzwerkkabel unterschieden werden. Damit ist sichergestellt, dass diese Komponenten zum Beispiel die für SANs notwendige verlustfreie Datenübertragung via Ethernet gewährleisten, sollten sie IEEE 802.1 Data Center Bridging DCB unterstützen. Darüber hinaus wird bei dieser durchgängig einheitlichen Verkabelung die exakte Dokumentation und sichere Zuordnung noch wichtiger für die Prozesssicherheit. Hier ist eine LED-Signalisierung auf jeden Fall anzuraten.

Andreas Klees,
Geschäftsführer und Leiter Business Unit EasyLan, ZVK GmbH

Vermutlich ein Wackelkontakt

Was Netzwerkkomponenten aushalten, hängt von der Verarbeitung ab

Mit den Übertragungsraten steigen auch die Ansprüche an das Datennetz. Dann zeigt sich, wie gründlich die Hersteller der Steckverbindungen gearbeitet haben. Systemausfälle durch Kabelprobleme können gravierende Folgen haben, und die Ursachenforschung treibt Admins regelmäßig zur Verzweiflung.

Fehlerhafte oder mangelhafte Verkabelung wirkt sich besonders tückisch aus, weil die Folgen meist nur schwer auf die Ursache zurückzuführen sind. Besonders heikel sind Störungen im Rechenzentrum, die nur sporadisch auftreten. Sie können klimatisch bedingt sein oder auf vorbeifahrende U-Bahnen oder Lkw zurückgehen, die Resonanzen erzeugen und Wackelkontakte verursachen.

Abgewetzte Steckkontakte

Hochwertige Komponenten sind nicht unbedingt auf den ersten Blick erkennbar. Die Unterschiede liegen oft im Detail. Das fängt bereits beim Rohmaterial an: Billigproduzenten verwenden für ihre Produkte oft Kunststoffe, die vorzeitig altern. Zudem fertigen sie unter Anwendung größerer Toleranzen und prüfen diese nicht zu 100 %.

Für die elektrische Anschlusstechnik sind solche Produkte in vielerlei Hinsicht problematisch: Das Kontaktmaterial hat meistens nur eine reduzierte Goldauflage, die zudem nicht ausreichend unternickelt ist, sodass die Verbindungsqualität schnell wieder sinkt. Negativ wirkt sich auch die oft sehr raue Kontaktoberfläche aus, die einen vorzeitigen Verschleiß der Kontakte auf der Gegenseite bewirkt und letztendlich zur Korrosion führt. Infolgedessen ist auf die Kontaktierung nicht dauerhaft Verlass. Da hilft auch die vorübergehende, aber nicht zuverlässig funktionierende Reaktivierung des Steckverbinders durch wiederholtes Stecken nicht weiter.

Besonders fatal sind RJ45-Patchkabel, die falsche Kontaktpresshöhen aufweisen und zur Überdehnung der Kontakte auf der Gegenseite führen. Hierdurch werden die RJ45-Ports dauerhaft geschädigt, da die Kontakte dieser Ports nicht mehr die Federkraft besitzen, die für eine dauerhafte Kontaktierung notwendig ist. Eine Datenübertragung in Echtzeit wie für VoIP ist dann nicht mehr gewährleistet. Besonders tückisch ist, dass derartige Probleme meist nur sporadisch auftreten und daher schwer lokalisierbar sind. Die falschen Presshöhen kommen durch schlechtes Verarbeitungsequipment zustande.

Quelle: tde – trans data elektronik

Höchste Präzision in allen Fertigungsschritten, hier beim Cable Preparing: Vor der eigentlichen Steckerkonfektionierung erfolgt die Vorbereitung des Kabelendes. Der Kabelmantel und der Buffer werden abgemantelt, und es wird das Kevlar beigeschnitten.

Verklemmte Glasfasern

Auch in der optischen Anschlusstechnik sind hochwertige Komponenten für ein sauberes Installationsergebnis entscheidend. Einfüge- und Rückflussdämpfung sind bei billigen Produkten meist deutlich schlechter als bei teuren. Ebenfalls eine Rolle spielt das Micro- und Macrobending der Fasern; dabei handelt es sich um eine Stressung der Fasern durch Druck, beispielsweise durch Übercrimpung oder einen schlechten Kabelaufbau. Insbesondere bei höheren Wellenlängen treten dann als Folge drastisch höhere Dämpfungen auf.

Bei qualitativ minderwertigen Steckverbindern ist zudem eine geringere Anzahl an Steckzyklen zu vermerken, die ein wichtiger Kennwert für Stecker und Steckverbinder ist. Ein Steckzyklus umfasst jeweils einen Einsteck- und einen Ziehvorgang. Bei häufigem Ein- und Ausstecken der Stecker ändern sich deren mechanische Toleranzen geringfügig, was zu einer Änderung der Übertragungsparameter führt. Das wirkt sich sowohl auf die Streckkräfte aus als auch auf die Einfüge- und Rückflussdämpfung. Besonders bei LWL-Steckverbindern sind die Steckzyklen genau zu beachten. Diese können bei Präzisionssteckern einige Hundert Zyklen betragen, bei LWL-Steckern liegen sie bei mindestens 500 bis 1000 und bei speziellen Linsensteckern bei mehreren Zehntausend Zyklen.

Qualitätsgarantie und Nachmessung

Eine Verkabelungsrichtlinie zu definieren, ist daher ebenso empfehlenswert wie die richtige Auswahl des Installationsunternehmens. Da auch die hochwertigsten Komponenten durch unsachgemäße Behandlung bei der Installation zerstört werden, zertifizieren sorgfältige Hersteller ihre Installationspartner und machen die Systemgarantie von Zertifizierung und Endabnahme der installierten Verkabelungslösung abhängig.

Nicht zuletzt ist entscheidend, dass Unternehmen alle installierten Strecken nachweislich messen und nicht nur stichprobenartig überprüfen. Bei TP-Anwendungen sollten entsprechende Link-Messungen vorgenommen werden. Bei LWL-Lösungen sind OTDR-Messungen hilfreich, um mögliche Probleme schon im Vorfeld zu identifizieren.

André Engel,
Geschäftsführer tde – trans data elektronik

Entscheidung am Patch-Punkt

Bei Base-8-Verkabelungen könnte URM dem MPO-Stecker Konkurrenz machen

Laut aktueller IEEE-Standardisierung sollen künftig sowohl 40GbE als auch 100GbE über Base-8-Verkabelungen realisiert werden. Das könnte das Ende der etablierten Base-12-Systeme einläuten. Wo bisher noch der Einsatz des MPO-12 üblich war, dürften dann auch Alternativen wie der URM in den Vordergrund rücken.

Strukturierte Verkabelungssysteme mit hoher Packungsdichte zu realisieren, gehört zu den zentralen infrastrukturellen Herausforderungen im Backbone-Bereich eines Rechenzentrums. Mit Base-2-Verkabelungen, die im RZ-Umfeld lange vorherrschend waren, lässt sich diese Aufgabe heute kaum noch erfüllen. Denn der Bedarf an LWL-Anschlüssen ist mittlerweile so hoch, dass ein durchgehender Base-2-Einsatz auf ein Kabelsystem hinausliefe, das nur aus Patch-Kabeln bestünde – und das wäre selbst für erfahrene Netzwerkspezialisten nicht mehr überschaubar.

Bewährtes Base-12

In vielen modernen Rechenzentren sind deshalb heute Base-12-Verkabelungen anzutreffen. Sie sind aus Inkrementen von 12 aufgebaut und werden mithilfe von Trunk-Kabeln mit 12, 24, 36, 48 oder mehr Fasern realisiert. Die Trunks werden dann erst auf der „letzten Meile“ vom Patch-Feld zum Server-Rack sowie in den Verteilbereichen in klassische 2-Faser-Kabel aufgefächert, die schließlich zu den einzelnen Ports führen. Diese übersichtliche und montagefreundliche Architektur hat sich vielfach bewährt: Selbst bei Servern sowie bei Speicher- und Netzwerkgeräten mit maximierter Port-Dichte lassen sich mit Base-12-Systemen problemlos strukturierte Verkabelungen verwirklichen.

Trotz der unstrittigen Vorteile von Base-12-Infrastrukturen spricht inzwischen jedoch einiges dafür, dass die Zukunft einem anderen Verkabelungssystem gehört. Grund dafür ist der Umstieg auf Highspeed-Datenübertragungen mit 40- oder 100-Gigabit-Ethernet. Diese Aussage mag manchen überraschen. Denn als beide Übertragungsmodi vor sechs Jahren erstmals durch das Institute of Electrical and Electronics Engineers standardisiert wurden, schien die Dominanz von Base-12 zunächst nicht gefährdet. Zwar sah die Norm IEEE 802.3ba-2010 für 40GbE eine Übertragung über 8 Fasern (4 Fasern pro Richtung) vor, sodass alternativ zu Base-12 auch die Möglichkeit von Base-8-Verkabelungen aus Trunks mit 8, 16, 24 oder 32 Fasern bestand. Da in IEEE 802.3ba jedoch für 100GbE eine Übertragung über 20 Fasern (10 Fasern pro Richtung) vorgesehen wurde, konnte sich diese Alternative nicht durchsetzen. Denn wer für 40GbE auf Base-8 umgestellt hätte, hätte im Falle einer Migration auf 100GbE zu Base-12 zurückkehren müssen, da ein Datentransfer über 10 Fasern pro Richtung nicht mit Base-8 realisiert werden kann und es keine 10- oder 20-Faser-Steckertechnik gibt. Da auch Trunks in aller Regel nicht aus Inkrementen von 10 oder 20 aufgebaut sind, sind für den Datentransfer über 10 Fa-

sern pro Richtung entweder zwei 12-Faser-Stecker oder ein 24-Faser-Stecker an entsprechenden Trunk-Kabeln erforderlich.

Umstieg auf Base-8

100GbE ließ sich also bislang nur über Base-12 realisieren. Und da auch 40GbE über Base-12 transportiert werden kann, gab es für RZ-Betreiber letztlich keinen Anlass, die entsprechenden Kabelinfrastrukturen im Backbone-Bereich zu verändern.

Doch inzwischen hat sich eine neue Situation ergeben. Denn in der Nachfolgenorm der IEEE 802.3ba-2010 wurde die Standardisierung der beiden Übertragungsmodi verändert: Die 2015 veröffentlichte Norm IEEE 802.3bm sieht nicht nur für 40GbE, sondern auch für 100GbE einen Datentransfer über insgesamt 8 Multimodefasern (4 pro Richtung) vor. Der 20-Faser-Standard für 100GbE ist damit hinfällig, was es prinzipiell möglich macht, beide Modi über Base-8-Verkabelungen laufen zu lassen.

Grundlage dieser Vereinheitlichung ist eine Änderung der Übertragungsraten: Bisher war sowohl bei 40GbE als auch bei 100GbE eine Rate von je 10 GBit/s pro Faser vorgesehen, sodass pro Richtung 4 (4 × 10 GBit/s) bzw. 10 Fasern (10 × 10 GBit/s) nötig waren. IEEE 802.3bm jedoch sieht für 100GbE eine Übertragungsrate von 25 GBit/s vor, während es für 40GbE bei 10 GBit/s bleibt. Dadurch genügen bei beiden Übertragungsmodi jeweils 4 Fasern pro Richtung (4 × 10 GBit/s bzw. 4 × 25 GBit/s). Der Umstieg auf Base-8 wird dadurch erstmals vertretbar. Denn eine Migration von 40GbE auf 100GbE ist jetzt nicht nur bei Base-12, sondern auch bei Base-8 problemlos möglich.

Vier Fasern ungenutzt

Tatsächlich haben Base-8-Kabelsysteme gute Chancen, sich in Zukunft auf breiter Front durchzusetzen. Denn auch wenn Base-12-Systeme etabliert sind und sowohl 40GbE als auch 100GbE transportieren können, haben sie einen Nachteil: Überträgt man 40GbE über 12-Faser-Trunks, bleiben 4 Fasern ungenutzt, da lediglich 8 benötigt werden. Dasselbe gilt bei 100GbE: Ob für die Übertragung über insgesamt 20 Fasern nun zwei 12-Faser-Trunks oder ein 24-Faser-Trunk eingesetzt werden – in jedem Fall bleiben auch hier 4 Fasern ungenutzt. Das ist wirtschaftlich unsinnig. Bei 100GbE bliebe ein Sechstel, bei 40GbE sogar ein Drittel der Faserinfrastruktur ohne Nutzwert und würde somit streng genommen überhöhte Investitionskosten verursachen.

Da die technische Notwendigkeit von Base-12-Systemen seit IEEE 802.3bm obsolet ist, kann dieser Nachteil künftig spätestens bei Neuverkabelungen beseitigt werden. Denn verwirklicht man Highspeed-Datenübertragungen über Base-8-Architekturen, ist eine vollumfängliche Ausnutzung der vorhandenen Infrastruktur gewährleistet, und es muss nicht in eigentlich überflüssige Infrastrukturbestandteile investiert werden. Für Gigabit-Ethernet ist Base-8 also eine in jeder Hinsicht logische Lösung. Und nicht nur dort: Denn da grundsätzlich auch im übrigen RZ-Bereich jede Anwendung über Base-8 realisiert werden könnte, ist es nicht unwahrscheinlich, dass die RZ-Backbone-Verkabelung der Zukunft vollständig aus Base-8-Kabelsystemen bestehen wird.

Multipath Push-On

Die Umstellung auf Base-8-Kabelstrecken hat auch Folgen aufseiten der Infrastrukturkomponenten. Das betrifft nicht allein die Trunk-Kabel, bei denen künftig statt 12- oder 24-Faser-Trunks die schmaleren und günstigeren 8- oder 16-Faser-Trunks dominieren werden. Es drängt sich auch die Frage auf, welche LWL-Stecker auf Base-8-Kabelstrecken eingesetzt werden sollten. Auf der „letzten Meile“, auf der die Trunks in 2-Faser-Kabel aufgefächert werden, spricht alles für den lange bewährten LC-Stecker. Nicht ganz so eindeutig ist die Sachlage hingegen an den Patch-Punkten des RZ-Backbones.

Für Base-12-Kabelsysteme wurde bislang zumeist der mit 12 Steckerkanälen ausgestattete MPO-12 (Multipath Push-On) genutzt, der in DIN EN 50173-5 und IEC 11801 als RZ-Mehrfaserstecker standardisiert ist. Dieser Stecker kann grundsätzlich auch für Base-8-Strecken verwendet werden; allerdings bleiben dann zwangsläufig 4 Steckerkanäle ungenutzt. Der MPO-12 ist für Base-8-Systeme also nur bedingt geeignet. Als Alternative scheint sich spontan der verwandte, speziell für 8-Faser-Strecken entwickelte MPO-8 anzubieten. Doch dieser Eindruck täuscht. Denn da bei 40GbE und 100GbE die MPO-Steckerkanäle 1 bis 4 sowie

9 bis 12 genutzt werden, der MPO-8 jedoch die Kanäle 1 und 2 sowie 11 und 12 nicht aufweist, ist dieser kleinere MPO-Verbinder für die Highspeed-Datenübertragung ungeeignet. Der MPO-12 ist deshalb trotz seiner Überdimensionierung der einzige MPO-Stecker, der bisher in der Breite für die Verbindung von GbE-Strecken genutzt und genormt wurde.

Gleichwohl bleibt die Frage, ob die MPO-Technologie unter den Voraussetzungen einer Base-8-Verkabelung konkurrenzlos bleiben wird. Grund ist die hohe MPO-12-Einfügedämpfung von meist 0,3 bis 0,5 dB. Sie gab Anwendern schon immer Anlass zu Kritik, da GbE-Strecken ein niedriges Dämpfungsbudget aufweisen (etwa 1,5 bis 1,9 dB) und somit bei Einsatz des MPO-12 nur Kabelstrecken mit wenigen Patch-Punkten realisierbar sind. In manchen Fällen ist das Budget schon nach zwei Patchungen so weit strapaziert, dass man keine weiteren Patchungen mehr plant. Hinzu kommt, dass die MPO-Technik das Dämpfungsbudget auch auf der letzten Meile belastet. Denn die Umsetzung von MPO auf LC wird mithilfe von Kassetten realisiert, die auf der Rückseite eine MPO-MPO- und auf der Frontseite eine LC-LC-Steckverbindung aufweisen und damit die Dämpfung noch einmal erhöhen.

URM-Steckverbinder

Vor allem bei 100GbE werden sich diese Schwachpunkte des MPO-12 in Zukunft noch gravierender auswirken. Denn die Übertragung von 25 GBit/s je Faser zieht eine weitere Reduzierung der (schon bisher nicht üppigen) maximalen Link-Länge nach sich: Während bei der älteren Übertragungsrate von 10 GBit/s noch maximale Link-Strecken von 150 (OM4) bzw. 100 m (OM3) einkalkuliert waren, liegt die größtmögliche Strecke künftig nur noch bei 100 (OM4) bzw. 70 m (OM3). Die Maximallänge MPO-12-basierter 100GbE-Strecken wird also um rund ein Drittel sinken. Nicht anders werden sich die Dinge bei Gigabit Fibre Channel verhalten, da bei steigenden Bandbreiten auch dort mit kleineren Dämpfungsbudgets zu rechnen ist.

Angesichts dieser eher unerfreulichen Fakten scheint es ratsam, sich nach Alternativen zum MPO-12-Steckverbinder umzusehen. Eine zukunftsfähige Komponentenlösung stellt beispielsweise der URM-Stecker dar, der aktuell durch die IEC standardisiert wird (IEC 61754-34). Er ist für die Datenübertragung über wahlweise 2 oder 8 Multimode- oder Singlemode-Fasern konzipiert (URM-2 bzw. URM-8) und lässt sich nahtlos sowohl in Base-2- als auch in Base-8-Verkabelungen einpassen. Seine Einfügedämpfung liegt für Multimode unter 0,2 dB (OFL). Der URM ermöglicht so beispielsweise bei einem Dämpfungsbudget von 1,6 dB insgesamt fünf bis sechs Patchungen pro Link und damit zwei- bis dreimal so viele Patchungen bei gleich langen oder sogar längeren Kabelstrecken wie der MPO-12.

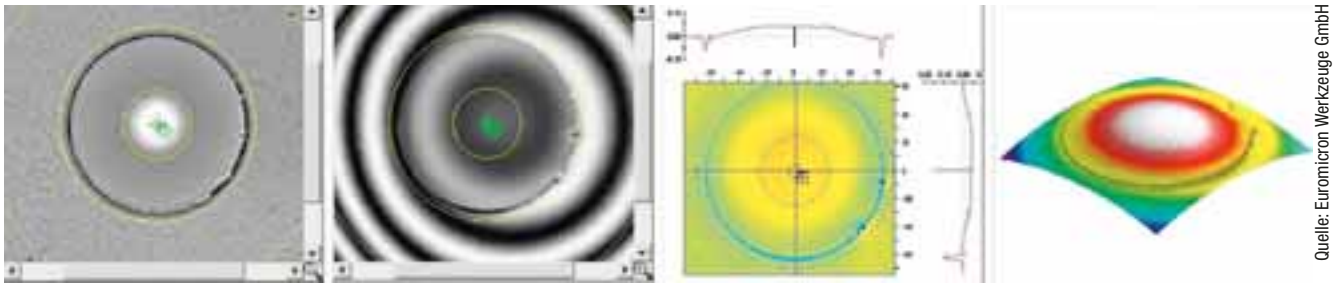
Dieser Vorsprung liegt an einer Ferrulentechnik, die sich deutlich von der MPO-Technik abhebt: Während die Fasern dort in einer einzigen Kunststoffferrule zusammengefasst sind, wird beim URM jede Faser für sich in einer einzeln gefederten Keramikferrule geführt. Damit ist es möglich, jede einzelne Faser gleichmäßig konvex zu polieren und so eine maximal dämpfungsreduzierende Stirnflächengeometrie zu realisieren. Beim MPO hingegen muss bei der Endpolitur die ganze Fasergruppe auf einmal bearbeitet werden. Das führt dazu, dass sich selbst mit überdurchschnittlichen Polierkenntnissen keine gleichmäßig konvexen Faserendflächen verwirklichen lassen – mit entsprechend negativen Folgen für die Einfügedämpfung und die Anzahl möglicher Patchungen bei niedrigen Dämpfungsbudgets. Da diese Schwachstelle des MPO-12 in der speziellen Bauart dieses Steckertypus begründet ist, sind künftige Nachbesserungen kaum denkbar. Der URM wird daher auch langfristig die besseren Dämpfungswerte aufweisen.

Weniger Verluste, weniger Kosten

Die Vorteile der URM-Technologie kommen freilich nicht nur bei den Mehrfaserpatchungen einer GbE-Faserstrecke zum Tragen. Vielmehr lässt sich damit auch der für die letzte Meile typische Übergang zu Base-2 unter deutlich niedrigeren Dämpfungsverlusten und zudem zu geringeren Kosten realisieren. Denn während der Einsatz von MPO-LC-Kassetten zwei Patchungen pro Link bedeutet (eine am MPO- und eine am LC-Port), kann man den URM-8 über eine einfache Kupplung mit vier URM-2-Steckern verbinden. Für den Übergang von Base-8 auf Base-2 ist damit nur noch eine Patchung erforderlich. Deren Handhabung wird überdies dadurch vereinfacht, dass es beim URM keine Male- und Female-Stecker und nur einen einzigen Typ von Kupplungen gibt; die Polarität des Systems ist somit immer klar. Für den Anschluss der finalen Base-2-Kabelstrecke an Server, Switches oder Router können Anwender auf vorkonfektionierte Patch-Kabel mit einem URM-P2- und einem LC-Stecker zurückgreifen.

Insgesamt erscheint es nicht mehr zwingend, Base-8-Verkabelungen für 40GbE und 100GbE mithilfe von MPO-12-Steckern zu realisieren. Lediglich dort, wo Aktivgeräte einen Mehrfachstecker-Port aufweisen, ist der MPO-12 gegenwärtig noch unverzichtbar, da solche Ports derzeit standardmäßig als MPO-Ports ausgeführt sind. Doch selbst in diesen eher seltenen Fällen – die meisten Ports sind als LC-Ports ausgeführt – müssen die Anwender nicht auf die Vorteile des URM verzichten. Denn vorkonfektionierte Kabel mit einem URM-8 und einem MPO-12 bieten heute selbst unter der Voraussetzung von MPO-Aktivgeräteanschlüssen die Möglichkeit, an den Patch-Panels auf URM zu setzen. Darüber hinaus ist es durchaus vorstellbar, dass Mehrfachstecker-Ports in Zukunft nicht mehr automatisch als MPO-Ports ausgeführt werden. Es könnten durchaus auch einmal URM-Ports sein.

Kai Wirkus,
LWL-Sachsenkabel GmbH (Euromicron-Gruppe)



Quelle: Euromicron Werkzeuge GmbH

URM führt jede Faser einzeln in einer Keramikferrule. Dadurch wird eine optimal dämpfungsreduzierende Stirnflächengeometrie möglich, weil man jede einzelne Faser gleichmäßig konvex polieren kann.

INTERNET SECURITY DAYS 2016

22.-23. September 2016
Phantasialand, Brühl

JETZT ANMELDEN!

FACHMESSE.KONFERENZ.NETWORKING

DIE PLATTFORM FÜR INTERNATIONALE SECURITY-EXPERTEN

Digitale Identitäten | Kryptographie für alle | Cyber-Angriffe

- » Lernen Sie von Experten, wie Sie ihr Unternehmen vor Hackern schützen
- » Erweitern Sie Ihr Netzwerk
- » Tauschen Sie sich mit Kollegen aus
- » Nehmen Sie an spannenden/impulsgebenden Keynotes und themenzentrierten Vortragssessions teil
- » Besuchen Sie die Ausstellung namhafter Security-Spezialisten
- » Ergründen Sie die Internet-Sicherheit in Workshops
- » Lassen Sie die Veranstaltung im Phantasialand unterhaltsam ausklingen

heise Events
Conferences, Seminars, Workshops

Sichern Sie sich Ihre Teilnahme!

Mehr Informationen unter: isd.eco.de

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

20 JAHRE eco

eco VERBAND DER INTERNETWIRTSCHAFT

WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.

Bei Blackout Ruhe bewahren

Hypervisor-Umgebungen könnten bereits sehr viel resilienter sein

Im Zusammenspiel von moderner USV-Technik, Power-Management und Virtualisierung lässt sich die Stromversorgung situationsgerecht organisieren. Intelligente Software zieht eine ergänzende Sicherheitsebene ein und ermöglicht zum Beispiel den kontrollierten Notfall-Shutdown virtualisierter Datacenter.

Virtualisierung spielt in IT-Umgebungen jeglicher Couleur eine entscheidende Rolle. Doch virtuelle Maschinen können schnell Schaden nehmen, wenn der Betrieb des physikalischen Host-Systems bei einem Stromausfall plötzlich unterbrochen wird. Zwar nimmt der Virtualisierungsgrad in deutschen Rechenzentren stetig zu, viele Betreiber setzen jedoch nach wie vor in erster Linie auf physikalische Systeme zum Schutz vor Stromschwankungen. Was bisher noch leicht mittels herkömmlicher USV-Technik umgesetzt werden konnte, stellt in Zeiten von Virtualisierung und Software-defined Data Centern (SDDC) eine ganz neue Herausforderung dar.

VM-Instanzen bei Stromausfall

Klassischerweise werden kurzfristige Blackouts oder Netzschwankungen im Rechenzentrumsumfeld heute durch zentrale Doppelwandler-USV kompensiert. Sie versorgen Serversysteme mit sauberem Strom und können den Rechenzentrumsbetrieb bis zu einer Stunde lang aus eigener Kraft aufrechterhalten. Zeichnet sich ab, dass die Dauer eines Stromausfalls die USV-Stützzeit überschreitet, ist ein Herunterfahren der IT-Umgebung unvermeidlich. Sofern keine Netzersatzanlage (NEA) vorhanden ist, wird die Batteriekapazität dann genutzt, um die Serverinfrastruktur sicher herunterzufahren.

Beim Notfall-Shutdown einer Hypervisor-Umgebung kommt jedoch ein weiterer Aspekt hinzu: Bevor der physikalische Host selbst seinen Betrieb einstellen kann, muss zunächst ein sequenzielles Beenden einzelner VM-Instanzen eingeleitet werden. Dabei spielt die betriebliche Hierarchie der VM-Instanzen eine entscheidende Rolle. Bleiben gegenseitige Abhängigkeiten unberücksichtigt, drohen Inkonsistenzen oder sogar Datenverluste. Schlimmstenfalls kann die Hypervisor-Umgebung dann nur noch mithilfe einer Datensicherung wiederhergestellt werden.

Um solche Szenarien zu vermeiden, gewinnt neben Flexibilisierungs- und Kostenaspekten ein weiterer Punkt zunehmend an Bedeutung: die Resilienz. Der Begriff Resilienz meint im Zusammenhang mit Virtualisierungstechnologien vor allem den Aufbau von Fehlertoleranz durch intelligente Softwarefunktionen wie Echtzeitreplikation oder Live-Migration. Wird in diese Prozesse auch der aktuelle Status der Stromversorgung miteinbezogen, entsteht eine ergänzende, logische Sicherheitsschicht im Rechenzentrum, die das USV-System entlastet und eine effizientere Energieverteilung unterstützt. Darüber hinaus wird auch das künftig für den normgerechten Betrieb von Rechenzentren geforderte Verfügbarkeitsmanagement gemäß EN 50600 maßgeblich vereinfacht.

Manuell sind solche Prozesse jedoch kaum umsetzbar, denn die für eine ordnungsgemäße Replizierung notwendigen Abhängigkeiten umfassen mitunter Hunderte von virtuellen Instanzen. Intelligente Power-Management-Lösungen schaffen hier Abhilfe, indem sie Stromversorgung und Virtualisierungsebene miteinander verbinden und dem Hypervisor so relevante Betriebsdaten aus der Stromversorgung zur Verfügung stellen. Wichtige Parameter sind etwa die verbleibende USV-Stützzeit, der Status verschiedener Rack-PDU-Gruppen und die Verfügbarkeit des externen Stromnetzes. Ein integriertes Alert-System ermöglicht darüber hinaus die Ausführung vordefinierter Aktionen. Der Einsatzbereich reicht vom punktuellen Stromausfall bis hin zum Infrastructure Shutdown – also dem geordneten Herunterfahren der kompletten virtuellen Infrastruktur.

Kommt es etwa aufgrund von langfristigen Stromversorgungsengpässen zu einer Notfallsituation, können anhand der hinterlegten Regeln besonders kritische virtuelle Instanzen, wie Domain-Controller oder DNS-Server, via Live-Migration auf einem zentralen physikalischen Host zusammengeführt werden. Weniger wichtige Server lassen sich in diesem Zuge mittels Lastabwurf automatisiert herunterfahren, um die verbleibende USV-Stützzeit für kritische Dienste zu erhöhen. In einem weiteren Schritt werden alle betriebswichtigen VM-Instanzen, die zentrale Hypervisor-Management-Konsole (zum Beispiel VMware vCenter, Citrix XenCenter) und die Power-Management-Software selbst auf einem einzelnen, noch verbleibenden physikalischen Server zusammengeführt: dem sogenannten Ultimate Host. Jetzt versetzt die Software den für die optimale Verteilung der VM-Workloads verantwortlichen DRS-Dienst (Distributed Resource Scheduler) in den manuellen Modus, um alle verbleibenden virtuellen Maschinen kontrolliert beenden zu können. Dann erfolgt der Shutdown der eigentlichen VM-Operationskonsole und zum Schluss wird der physikalische Host selbst heruntergefahren.

Kehrt dann die Stromversorgung zurück, erfolgt ein automatischer Neustart, bei dem die sequenziellen Abhängigkeiten innerhalb der Serverhierarchie erhalten bleiben, sodass die komplette virtuelle Infrastruktur nach einer minimalen Downtime wieder ihren Betrieb aufnehmen kann.

Mehr Ausfallsicherheit und Verfügbarkeit

Derartige Power-Management-Lösungen können weder ein fachgerecht dimensioniertes USV-System noch eine vernünftige Disaster-Recovery-Strategie ersetzen. Durch die Verknüpfung von Hypervisor und USV-System leisten sie jedoch einen wichtigen Beitrag zur Ausfallsicherheit. Sie etablieren eine ergänzende Sicherheitsebene zwischen USV-System und der Datensicherung, die die Resilienz gegenüber Stromausfällen deutlich erhöht, ohne dass in zusätzliche USV-Kapazitäten investiert werden müsste. Im Rahmen des Software-defined Data Centers wird damit auch Strom zu einer Ressource, die sich letztlich beliebig zuweisen lässt. Dann lassen sich die Auswirkungen von Störungen schon auf einer möglichst hohen Funktionsebene eindämmen, außerdem werden momentan noch brachliegende Energieeinsparpotenziale, etwa auf Ebene einzelner VM-Instanzen, besser sichtbar.

Ralf Enderlin,
Leiter Service Power Quality, Eaton Electric GmbH

Benchmarks für die Server-Beschaffung

Beim (Ersatz-)Kauf braucht man realistische Daten zu den Folgekosten

So gut wie jeder Server-Beschaffungsleitfaden legt Wert darauf, dass das „wirtschaftlich günstigste“ nicht das billigste Angebot ist. In der Praxis gibt aber meist der Anschaffungspreis den Ausschlag – ohne Rücksicht auf die Folgekosten. Und die sind vor allem durch den Stromverbrauch bedingt.

Voraussetzungen für die Planung sind die möglichst zuverlässige Kenntnis der geplanten Nutzungsdauer und des Verwendungszwecks sowie eine hinreichend genaue Abschätzung der zu erwartenden Auslastung. Denn am wichtigsten ist es, Überkapazitäten zu vermeiden. Ein zu groß dimensionierter Server ist nicht nur in der Anschaffung teuer, sondern zieht auch höhere Betriebskosten mit sich. Bei einer Ersatzanschaffung liefern Log- und Monitoring-Daten bereits brauchbare Anhaltspunkte zur Dimensionierung; bei einem neuen Projekt kann es sinnvoll sein, auf Hilfsmittel wie das Intel IT Server Sizing Tool zurückzugreifen.

Viele Leitfäden für das IT-Procurement betrachten den Server als unteilbare Einheit. Aber um eine Investitionsentscheidung technisch vorzubereiten, ist es sinnvoll, sowohl das Gesamtsystem als auch die Kernkomponenten der Hardware getrennt zu betrachten.

Energieeffizienz im Detail

Für das Gesamtsystem kann man die Kenngröße Performance per Watt heranziehen. Sie berechnet sich einfach: I × Auslastung/Leistungsaufnahme. I ist dabei ein Indikatorwert, der prinzipiell aus einer beliebigen, für den Anwendungszweck sinnvollen Benchmark ermittelt wird. Das kann eine etablierte Anwendungsbenchmark sein, wenn beispielsweise ein Web- oder Datenbankserver ersetzt werden soll; in anderen Fällen sind eventuell synthetische Benchmarks sinnvoller. Darüber hinaus gibt es energiespezifische Benchmarks der SPEC, namentlich der SPEC Power Benchmark aus dem Jahr 2008 (mit Schwerpunkt auf Java), sowie der TPC-Energy, um Einsparpotenziale genauer zu bestimmen. Im besten Fall können mit einer Teststellung des Herstellers entsprechende Vergleiche durchgeführt werden.

Die CPU gehört zu den Großverbrauchern in einem Server. Entsprechend wichtig ist ihre Energieeffizienz. Für aktuelle Prozessoren veröffentlicht Passmark Benchmarklisten nach Thermal Design Power (TDP). TDP ist zwar als Kriterium für den Stromverbrauch umstritten, aber es ist fast immer der einzige Wert zum Energieverbrauch, den die CPU-Hersteller ins Datenblatt schreiben.

Energieeffizienz ist auch das wichtigste Kriterium bei der Netzteilwahl. Hier genügt es in der Regel, auf eine 80-PLUS-Zertifizierung zu achten und Netzteile mit „80 PLUS Gold“ oder „Platinum“ zu kaufen. Deren Wirkungsgrad liegt bei 92 bzw. 94 %; das Level „Bronze“ bringt es auf 85 %, jeweils bei einer fünfzigprozentigen Auslastung. Ältere Netzteile ohne Label haben oft nur einen Wirkungsgrad von 70 % und weniger. Die optimale Effizienz liegt in der Regel bei 50 % Auslastung; darunter und darüber sinkt sie um wenige Prozentpunkte ab. Typischerweise liegt die Verlustleistung eines modernen Netzteils etwa in der gleichen Größenordnung wie der Stromverbrauch der CPU. Da leistungsfähige und trotzdem stromsparende CPUs teuer sind, sollte man also zuerst in ein energieeffizientes Netzteil investieren.

Den RAM-Energieverbrauch abzuschätzen, ist komplex und hängt unter anderem stark vom Einsatzzweck, der Bestückung, der Taktrate und der Spannung ab. Eine der umfassendsten Betrachtungen zu diesem Thema (für DDR3) stammt von der Firma Micron (TN-41-01: „Calculating Memory System Power for DDR3“). Als ganz grobe Abschätzung kann man derzeit etwa 5 bis 6 Watt pro 16-GByte-RDIMM im Betrieb annehmen, bei DDR4 um wenige Prozent weniger als bei DDR3.

Der Speicher trägt bei vielen Servern nur etwa 10 % zum Gesamtverbrauch bei, bei Storage-lastigen Systemen natürlich erheblich mehr. 2,5-Zoll-Platten brauchen bei gleicher Leistung rund 40 % weniger Strom als 3,5-Zoll-HDDs. Damit können sie durchaus auch gleichauf mit SSDs liegen.

Ausfallraten und Maintenance

Rein Hardware-bezogen beschränkt sich die Wartung des Servers auf den Austausch ausgefallener oder bald ausfallender Teile. Die Mean Time Between Failures (MBTF) als Kriterium für Ausfallwahrscheinlichkeiten von Komponenten hat an Relevanz verloren. Lediglich für Speichermedien ist sie noch von praktischer Bedeutung.

Im Vergleich zu HDDs ist die Lebensdauer von SSDs rein physikalisch durch die Anzahl der Schreibvorgänge auf eine Zelle beschränkt. Ersatz von SSDs sollte also immer dann eingeplant werden, wenn überwiegend flüchtige Daten in hoher Frequenz verarbeitet werden. Alternativ dazu ist auch der Einsatz von Enterprise-SSDs zu erwägen. Netzteile als preiswerte, aber wegen des Lüfters fehleranfällige Komponenten können mit wenig Aufpreis redundant ausgelegt werden.

Verfügbarkeit und Support

Selbst wenn nur eine dreijährige Nutzungsdauer geplant ist, sollte man darauf achten, Hardware zu kaufen, für die der Hersteller längeren Support anbietet (etwa fünf Jahre), denn dann ist es sehr wahrscheinlich, dass auch nach Ablauf der drei Jahre noch Komponenten zur Verfügung stehen.

Ulrich Wolf,
Manager Communications, Thomas-Krenn.AG

Das Internet der Rechenzentrumsdinge

Moderne DCIM-Systeme verbinden Haustechnik und RZ-Monitoring

Das Internet of Things ist im Rechenzentrum bereits Stand der Technik: Schranküberwachungen, Zutrittskontrollen und IP-Kameras werden webbasiert konfiguriert und übertragen die Informationen per SNMP. Nun ist es auch möglich, Beleuchtung, Klima und Stromversorgung aus der Gebäudetechnik einzubinden.

Digital Building ist im Rechenzentrum bereits Realität: Moderne Rechenzentrumsschränke sind mit einer IP-basierten Management-Lösung zur Klimatisierung, zum Schutz vor unbefugtem Zugriff sowie zur Optimierung des Stromverbrauchs ausgestattet. Integrierte Sensoren messen Temperatur, Luftfeuchte, CO_2-Werte und Stromverbrauch und geben diese Werte an das Monitoring-System weiter. Das alarmiert bei Über-/Unterschreitung von Toleranzgrenzen oder bei auffälligen Ereignissen den Administrator und löst je nach Konfiguration gleichzeitig eine Aktion aus. Es fährt zum Beispiel die Schrankkühlung hoch, wenn ein Temperaturfühler auf Überhitzung deutet. Oder: Bei korrekter Authentifizierung gibt es dem Schließsystem das Signal, die Schranktür zu entriegeln. Diese Lösungen arbeiten meist mit einer Weboberfläche und SNMP-basiert.

Ein vergleichbares Monitoring und Management ist auch für die rechenzentrumsweite Gebäudetechnik möglich und für einige Rechenzentren sogar gefordert. Mit der neuen europäischen Normenreihe DIN EN 50600 kommen einige Rechenzentrumsbetreiber gar nicht mehr ohne ein Monitoring-System für die Gebäudetechnik aus.

DCIM nach DIN EN 50600

Die DIN EN 50600 gibt Unternehmen einen Leitfaden an die Hand, wie sie ihr Rechenzentrum für ihre individuellen Anforderungen auslegen sollten. Dabei legen Geschäfts- und IT-Leitung im ersten Schritt fest, wie verfügbar, ausfallsicher und energieeffizient das eigene RZ sein soll. Daraus ergibt sich eine Einordnung in eine der vier Rechenzentrumsklassen und daraus wiederum die Auslegung mit Geräten, Komponenten und Management-Systemen. Ein Data Center der höchsten Klasse 4 benötigt zum Beispiel ein umfassendes Monitoring-System, das auch die Gebäudetechnik mit einschließt. Solche DCIM-Systeme (Data Center Infrastructure Management) arbeiten in der Regel IP- und SNMP-basiert. Sie sammeln die Informationen der verteilten Sensoren und Aktoren und verarbeiten diese wie das die Management-Systeme der Schrankhersteller schon seit Jahren tun, binden dabei aber möglichst viele Bussysteme der Gebäudetechnik ein.

Die Regelungen für die Gebäudetechnik finden sich in jeweils spezifischen Teilnormen der DIN EN 50600: Die Aspekte der Energieversorgung und -verteilung sowie deren mehr oder weniger ausfallsichere und energieeffiziente Auslegung ist in DIN EN 50600-2-2 geregelt. Die Regelung von Temperatur, Flüssigkeitsströmen, Luftfeuchte, Schwebeteilchen, Schwingungen, Verfahren zur Energieeinsparung sowie die Dokumentation der Standorte von Geräten im Rechenzentrum sind mit der DIN EN 506000-2-3 abgedeckt. Die DIN EN 50600-2-5 wiederum spezifiziert Anforderungen und gibt Empfehlungen, wie ein Rechenzentrum und dessen Bestandteile vor unautorisiertem Zugang, Feuer und anderen umgebungsbedingten Ereignissen geschützt werden soll. Damit sind zum Beispiel elektromagnetische Beeinflussung, Vibration, Überflutung, Gas und Staub gemeint. Und in der DIN EN 50600-3-1 (bisher DIN EN 50600-2-6) sind die Prozesse für das Management und den Betrieb spezifiziert. Hauptkriterien sind hier wieder: Ausfallsicherheit, Verfügbarkeit, Sicherheit und Energieeffizienz.

Lösungen im Vorführmodell

Es gibt für fast alle Bussysteme der Gebäudeautomation bereits IP-Gateways, die die Daten aus BACnet (Gebäudemanagement), KNX (Raumautomation), Dali (Beleuchtung), Modbus (Heizung/Klima) und anderen in SNMP und HTTP umsetzen, sodass sie übers LAN in eine zentrale Management-Lösung integriert werden können. Dabei binden die angeschlossenen dezentralen Bussysteme mit nur einer Datenleitung die Anlagen der Feldebene direkt in die übergeordnete Steuerung ein. Die einzelnen Komponenten können jederzeit ausfallsicher überwacht und zentral gesteuert werden.

Auch für Funksensoren sind solche Gateways verfügbar, zum Beispiel für die batterielos betriebenen Enocean- oder Zigbee-Sensoren. Darüber hinaus arbeiten viele Systeme der Gebäudetechnik bereits von Haus aus auf LAN-Basis, zum Beispiel Zutrittskontrollsysteme oder Überwachungskameras.

Auf der diesjährigen Light + Building in Frankfurt wurde in der Sonderschau „Digital Building“ die Gebäudetechnik eines Zweckbaus weitgehend IP- und SNMP-basiert angesteuert. Das LAN diente dabei als zentrale Infrastruktur. Es wurden neben hochmodernen Lösungen auch handelsübliche Systeme über verbreitete Bussysteme mit entsprechen-

BITKOM-LEITFADEN ZUM DOWNLOAD

Der Branchenverband Bitkom hat 2015 einen Leitfaden „Energieeffizienz in Rechenzentren“ herausgebracht, der sich auch mit DCIM-Lösungen befasst, mit denen die Anforderungen der DIN EN 50600 erfüllt werden. Er steht auf www.bitkom.org kostenlos zum Download bereit.

den Gateways an das Management-System angeschlossen. Natürlich befand sich in diesem Raum auch ein umfassend überwachter IT-Schrank.

Das Zusammenspiel der verschiedensten Systeme wurde in mehreren Szenarien demonstriert. Konzept und Umsetzung dieser Installationen stammen von den beiden Ingenieurbüros Canzler (Projektsteuerung, Heizung, Lüftung, Sanitär mit Prozess- und Regeltechnik) und Groben Ingenieure (Elektrotechnik und Sicherheitstechnik) in enger Kooperation mit dem Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI). Ein Szenario war zum Beispiel „Feuer".

Zweckbauszenario Feuer

Sobald das Szenario Feuer in dem Zweckbau startete, ging eine laute Sirene los und es blinkte eine große Warnleuchte. Außerdem fuhr die Gangbeleuchtung herunter, während die Fluchtwegmarkierungen hell aufleuchteten. Die Türverriegelung am Hinterausgang wurde entriegelt, damit dieser als Fluchtweg nutzbar war. Außerdem wurden innerhalb von Millisekunden die motorisch angesteuerten Brandschutzklappen betätigt. – Ein Brand im Rechenzentrum sollte ähnliche Aktionen auslösen. Es kämen aber sicher noch eine Reihe weiterer Maßnahmen hinzu, die vorab definiert sein sollten.

Da Einbruchs- und Brandmeldeanlagen aufgrund gesetzlicher Regelungen analog ausgeführt werden müssen, haben die Ingenieure im Digital Building beide Anlagen mit einer zusätzlichen digitalen Schnittstelle ausgestattet. So konnte die Brandmeldung per SNMP für zahlreiche Alarme und Aktionen genutzt werden. Das System könnte automatisch die Entrauchungsanlage einschalten (oder dies zumindest vorschlagen), sobald Präsenzmelder oder eine Kamera Personen in der Brandzone erkennt. Außerdem sollte das Management-System verhindern, dass die hohen Temperaturen automatisch eine stärkere Kühlung in Gang setzen, die womöglich Frischluft in den Brandherd bläst. Eine sinnvolle Aktion wäre zum Beispiel, dass die Systeme in den betroffenen Bereichen geregelt herunterfahren, nachdem der Betrieb auf redundante Systeme außerhalb der Brandzone umgestellt wurde.

Praxisbeispiel Beleuchtung

Die Steuerung von Beleuchtungssystemen erfolgt in der Regel über Bussysteme wie KNX oder DALI. Lässt sich eine der Leuchten als Master über SNMP ansteuern, sind nach Einschätzung von Markus Groben, Geschäftsführer von Groben Ingenieure, spezifische Beleuchtungsszenarien realisierbar. Es gibt bereits LED-Leuchten, die wie Netzwerkkameras als LAN-Komponenten angeschlossen und geschaltet werden.

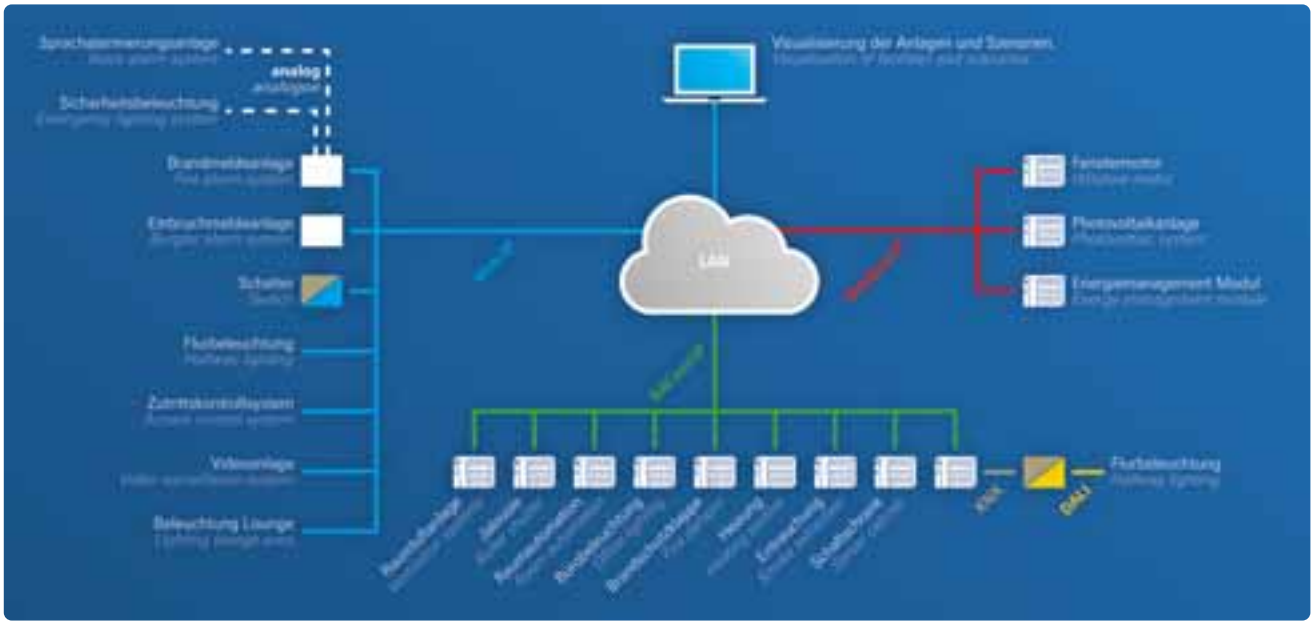
Mit so einer LAN-basierten LED-Beleuchtung und verteilten Präsenzmeldern kann man zum Beispiel mit wenig Aufwand eine Nachführbeleuchtung realisieren. Oder: Nach Freigabe der Zutrittskontrolle werden nur die Bereiche beleuchtet, für die der Besucher Zutrittsberechtigung hat; betritt er andere Bereiche, erhält der Administrator eine Meldung, und die entsprechende Netzwerkkamera wird aktiviert. Und wenn das Rechenzentrum mit LAN-Leuchten ausgestattet wird, können dort auch die Arbeitsplätze ebenso bestückt werden. Dann gehen Licht und Heizung an, sobald der Administrator sich auf diesen Arbeitsplatz zubewegt. Die Lichtstärke wird zum Beispiel bei der Lösung von Microsens per App konfiguriert.

Bedienung per App

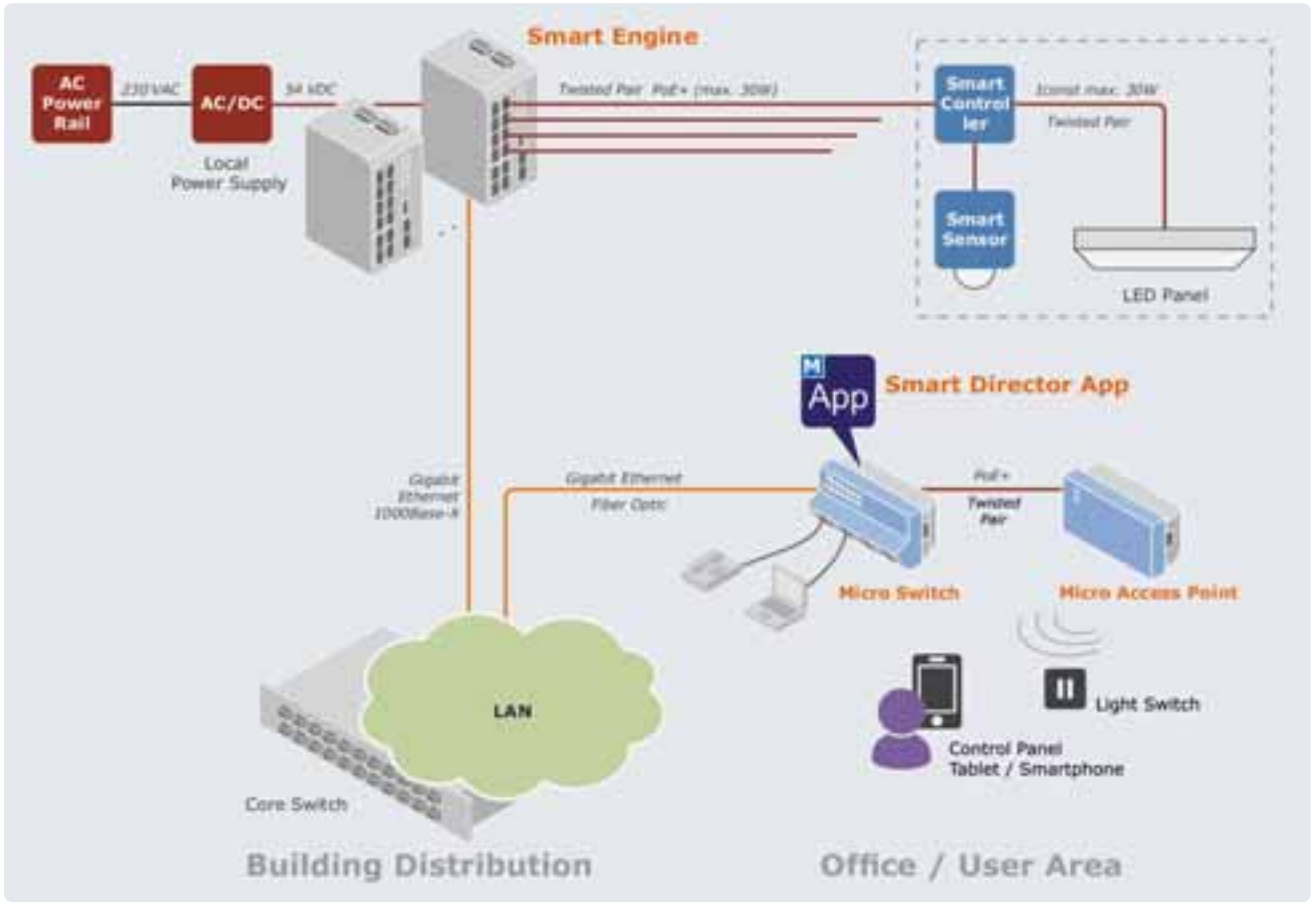
Die Installationen im Digital Building konnten zum großen Teil über eine passwortgesicherte App abgefragt und auch konfiguriert werden. Als Programmierschnittstelle kann laut Groben ein webbasiertes IT-Management mit API genutzt werden. Speziell für kleine und mittlere Rechenzentren bietet zum Beispiel dtm eine IP-basierte DCIM-Lösung an, die laut Hersteller alle SNMP-basierten Sensoren einbinden kann. Auch diese Variante kann über eine App per Smartphone oder Tablet bedient werden und arbeitet ebenfalls nur mit Passwortschutz.

Passwortschutz ist das Minimum an Schutzvorkehrungen vor unbefugtem Zugriff. Für größere Rechenzentren reicht das nicht aus. Es sollte vorher abgeklärt sein, wer auf welche RZ-Daten zugreifen darf, damit entsprechende Rechte vergeben werden können (Autorisierung). Außerdem sollten Sicherheitsmaßnahmen, wie sie sonst beim Fernzu-

Quelle: Messe Frankfurt



Das Netz des Digital Buildings bindet unterschiedlichste Anlagen und Bussysteme in das LAN-basierte DCIM-System ein und ermöglicht Interaktionen.



Quelle: Microsens

Smart Lighting: Lösung zur Beleuchtung eines Arbeitsplatzes mit LAN-basierten LED-Lampen

griff aufs Netz üblich sind, integriert sein. In einem gut geschirmten Rechenzentrum funkt ja kein Sensor wichtige Daten in eine externe Cloud, sondern nur an ein internes System.

Systemintegration und Gateways

In der Praxis kommt in der Industrie- und Gebäudeautomation eine große Anzahl an Feldbussystemen zum Einsatz. Damit die Elemente der Feldbussegmente und das LAN-basierte Management-System miteinander kommunizieren können, bedarf es Gateways als Schnittstellen. Auch verfügbare IP-Gateways müssen an die Anforderungen der Management-Lösung angepasst werden. Auf diese Weise lassen sich verschiedenste Anwendungen unterschiedlicher Hersteller in ein Gesamtsystem integrieren.

Laut Markus Gruben muss die Steuerebene nicht unbedingt auf einer Webanwendung basieren. Es ginge genauso gut über BACnet und SPS. Doch dann müsste man für diese Anwendung eine spezielle Lösung entwickeln. Auch für die Wartung wäre dann ein BACnet-Spezialist nötig. Außerdem könne man nur die Komponenten verwenden, die BACnet unterstützen. Groben weiter: „Und nur weil ein System proprietär ist, ist es nicht sicherer. Denn jemand mit BACnet-Kenntnissen könnte auf dieses System mindestens genauso gut unbefugt zugreifen wie ein IT-Hacker auf ein webbasiertes.“ Offene Systeme, basierend auf den LAN-Standards, können mit den gängigen Techniken abgesichert werden und lassen sich problemlos anpassen.

Quelle: Rittal

Beispiel eines SNMP-basierten Schranküberwachungssystems

Asynchrone Innovationszyklen

Rechenzentren sind in der IP-basierten Gebäudeautomation die Early Adopters. Denn hier besteht eine besonders große Affinität zur IT. Gebäudetechnik ist allerdings für Standzeiten von mehr als 40 Jahren ausgelegt. Da ist es verständlich, dass neue Techniken sich nur langsam umsetzen lassen. Dennoch wird das LAN langfristig proprietäre Strukturen verdrängen. Gateways sind dabei eine gute Möglichkeit, vorhandene Technik in die LAN-Infrastruktur einzubinden.

Doris Piepenbrink,
freie Journalistin, München

Energieversorgung über Bypass

Online-USV im Stromsparmodus umgehen die Spannungsregulierung am Ausgang

Maßnahmen zur Effizienzsteigerung sind mittlerweile zu festen Bestandteilen in Nachhaltigkeitskonzepten von Unternehmen geworden, auch bei unterbrechungsfreien Stromversorgungen. Der „Eco-Modus“ gilt inzwischen als gefragtes Merkmal und wird speziell im Bereich der einphasigen Online-USV viel diskutiert.

Die Online-USV, auch Doppelwandler genannt, ist derzeit das gängigste USV-Modell zur sicheren Stromversorgung von Rechenzentren: Sie bietet spannungs- und frequenzunabhängigen VFI-Betrieb (Voltage and Frequency Independent) und gewährleistet zu jeder Zeit ein höchstes Maß an Stromqualität. Aufgrund der zweistufigen Umwandlung hat diese USV aber den höchsten Energieverbrauch. Deswegen haben die meisten Online-USV-Produkte einen Betriebsmodus, der effizienter mit Energie umgeht. So kann der Energieverbrauch der USV-Anlage herabgesetzt und der Wirkungsgrad noch weiter gesteigert werden. „Eco-Modus“, „Energiesparmodus“ oder „Hocheffizienzmodus“ – die Bezeichnungen variieren je nach Hersteller.

Line Interactive: Eco als Standard

Der größte Unterschied zwischen Online-USV und USV der VI-Kategorie (Voltage Independent, auch Line Interactive oder Single Conversion genannt) besteht darin, dass bei letzteren der Eco-Modus kein zusätzliches Feature darstellt. Sie arbeiten von Grund auf mit einem bereits implizierten Sparmodus: Der Strom fließt vom Eingang durch verschiedene Schutzfilter – beispielsweise gegen Überspannung – sowie zusätzlich durch einen Transformator zur automatischen Spannungsregulierung (AVR). Aufgrund des sehr hohen Wirkungsgrads der AVR (rund 98–99 %) und der Schutzfilter sowie durch die geringe Anzahl elektronischer Komponenten bei diesem USV-Typ kann eine Line-Interactive-USV bei Volllast einen Wirkungsgrad von mehr als 96 % erreichen.

Online-USV arbeiten im Eco-Modus wie eine Line-Interactive-USV. Das heißt: Die Doppelwandlung wird umgangen und die Netzspannung wird vom Eingang zum Ausgang durchgeleitet. Line-Interactive-USV sind durch ihren quasi inhärenten Eco-Modus in der Lage, mit einem hohen Wirkungsgrad auch bei Schwankungen der Eingangsspannung zu arbeiten und gleichzeitig die Ausgangsspannung zu regulieren. Bei einer Online-USV hingegen funktioniert der Eco-Modus lediglich in einem niedrigen Eingangsspannungsbereich.

Online: Eco via Bypass

Charakteristisch für Online-USV ist ein automatischer Bypass, zusätzlich zur Doppelwandlerfunktion, bei der die ankommende Wechselspannung in eine Gleichspannung und anschließend über den Wechselrichter wieder in eine saubere, sinusförmige Wechselspannung umgewandelt wird. Erst der Bypass macht den Eco-Betriebsmodus bei diesem USV-Typ möglich. Er kommt bei Überlastung, falschem Betrieb oder im Fall einer Wartung zum Einsatz und verbindet Eingang und Ausgang miteinander. Beim Bypass-Modus handelt es sich um einen vorübergehenden Zustand, der aufgehoben wird, sobald die besonderen Umstände nicht mehr gegeben sind. Netzfehler, die während des Bypass-Modus auftreten, können einen Lastabfall zur Folge haben.

Online-USV machen sich im Eco-Modus den automatischen Bypass wie folgt zunutze: Die Spannung fließt über die Bypass-Linie vom Eingang zum Ausgang. Dieser Zustand bleibt bestehen, solange die Bedingungen am Eingang stabil sind. Treten im Eco-Modus ernsthafte Störungen auf, beispielsweise Spannungsschwankungen, schaltet die USV automatisch vom Bypass in den Online-Modus, um weiterhin qualitativ hochwertige Spannung liefern zu können. Obwohl die Spannung im Bypass-Modus und im Eco-Modus denselben Weg geht, sind Betrieb und Lastschutz also in unterschiedlicher Form gegeben.

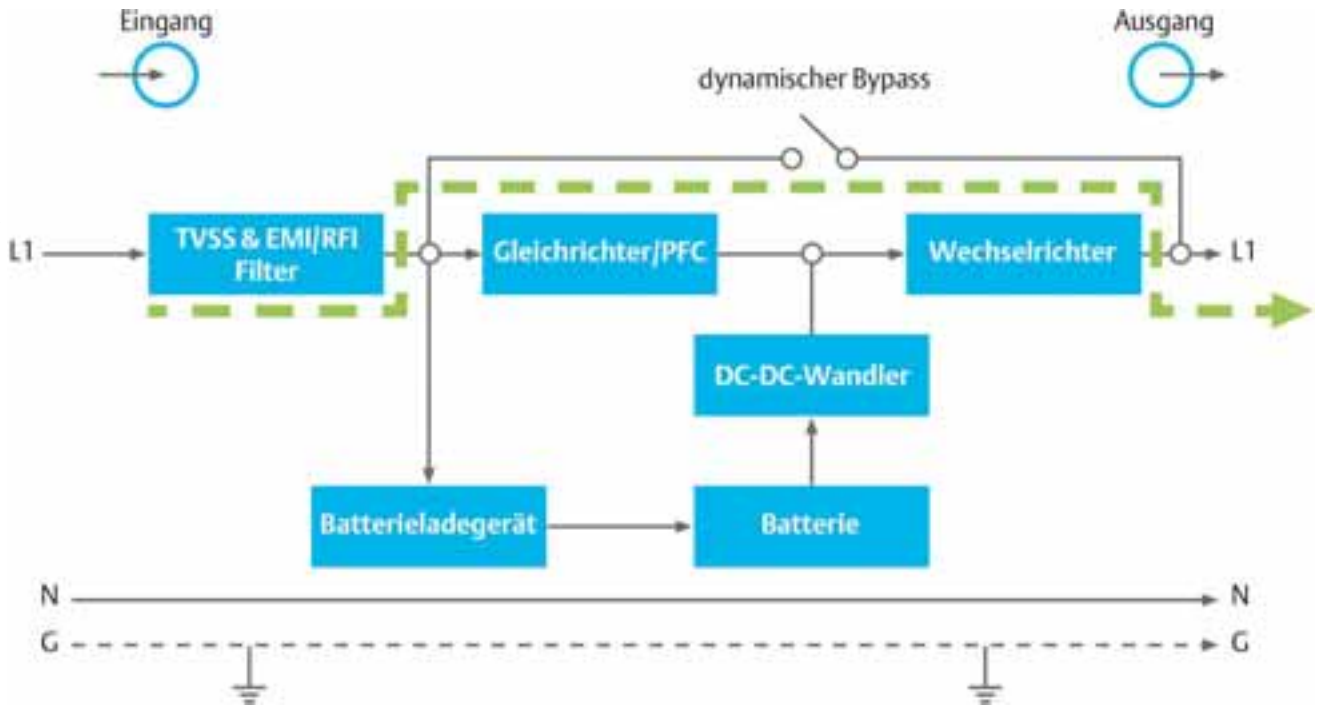
Der entscheidende Vorteil des Eco-Modus bei Online-USV ist der sehr hohe Wirkungsgrad. Dieser liegt bei voller Auslastung in diesem Betriebsmodus bei 94–98 %, und selbst bei niedriger Auslastung lassen sich hohe Werte erzielen.

Vor der Entscheidung für oder gegen eine Online-USV mit Eco-Modus steht die zentrale Abwägung, wie hoch auf der einen Seite die Kosten für die Implementierung sind und welche konkreten finanziellen Vorteile sich auf der anderen Seite durch Energiekosteneinsparungen ergeben. Zu berücksichtigen sind außerdem die Anzeige des Signal- und USV-Status für den Nutzer (LCD oder Software), der Wirkungsgrad, der durch den Eco-Modus erzielt wird, der Eingangsbetriebsbereich im Bypass-Modus, die Umschaltzeit und die Möglichkeit, zu bestimmen, ob die USV im Bypass- oder Eco-Modus betrieben wird, außerdem (vom Nutzer) konfigurierbare Parameter, die den Betrieb in den Eco-Modus versetzen, ferner die Möglichkeit, den Betriebsmodus aus der Ferne zu überwachen oder zu steuern, und die Möglichkeit, interne Batterietests während des Eco-Modus durchzuführen, sowie der Schutz der USV im Eco-Modus am Eingang und Ausgang (Trennschalter oder Überspannungsschutz).

Einphasige Online-USV

Darüber hinaus sind speziell bei einphasigen Online-USV einige spezifische Eigenschaften des Eco-Modus zu berücksichtigen. So ist der Bypass-Pfad zwar nicht direkt an den Ein- und Ausgang gekoppelt, aber indirekt über einige Schutzmechanismen, die über TVSS- (Transient Voltage Surge Suppressor) und EMI/RFI-Filter (Electromagnetic

Quelle: Emerson Network Power



Im Eco-Modus einer Online-USV fließt die Spannung über die Bypass-Linie vom Eingang zum Ausgang.

Interference/Radio-Frequency Interference) mit dem Eingang verbunden sind. Diese Art der Anbindung hat Konsequenzen für Schutz und Wirkungsgrad.

Spannungsregulierung am Ausgang

Wenn die Online-USV im Eco-Modus arbeitet, ist parallel zur kontinuierlichen Messung und Überwachung der Ausgangsspannung ein Überspannungsschutz gegeben. Dafür sorgen einige Vorrichtungen am Spannungseingang, die etwa vor Spannungsspitzen oder Überstrom schützen. So ist sichergestellt, dass Spannungs- und Stromzufuhr laufend über den Hauptmikroprozessor der USV kontrolliert werden und sich in einem akzeptablen Bereich bewegen – auch im Fall einer Überlast oder in anderen außergewöhnlichen Situationen. Im schlimmsten Fall eines internen Fehlers, beispielsweise am Wechselrichter oder Mikroprozessor, ist somit immer noch ein Schutz am Eingang gegeben, der Störungen filtert oder zumindest limitiert, sodass der Fehler nicht automatisch durchgereicht wird..

Im Eco-Modus bleiben sowohl die Leistungsumwandler am Eingangsgleichrichter als auch am Wechselrichter operativ und befinden sich im Standby-Modus. Beide Blöcke anzuschalten, würde zwar ein paar Watt einsparen und den Wirkungsgrad erhöhen, es hätte allerdings auch einen negativen Effekt: Das Umschalten von Eco- auf Online-Modus würde beträchtlich länger dauern, je nach Modell zwischen 4 und 10 ms – eine Zeitspanne, die die kontinuierliche Stromversorgung und Lastsicherheit beeinträchtigen könnte.

Während des Eco-Modus findet keine Spannungsregulierung am Ausgang der USV statt. Hierin unterscheidet sich eine Online-USV maßgeblich vom Line-Interactive-Typ. Dieser ist dank der bereits erwähnten automatischen Spannungsregelung in der Lage, im weiten Rahmen einer gewissen Eingangsspannung jederzeit einen hohen Wirkungsgrad zu erzielen.

Bei der Frage, wann man den Eco-Modus bei einer Online-USV in Betracht ziehen sollte, sind noch die Oberschwingungen im Eingang zu berücksichtigen und zu bewerten. Denn wie auch immer die Ausgangslast im Online-Modus aussieht – ob widerstandsfähig oder mit starken Oberschwingungen: Der Gleichrichter am Eingang ist verantwortlich für eine perfekte Sinuswelle des Eingangsstroms – ein entscheidender Vorteil einer Online-USV. Arbeitet die USV allerdings im Eco-Modus, sind die Oberschwingungen am Eingang ein Spiegel der Oberschwingungen, die die Last verursacht.

Oberschwingungen stellen bei modernen Stromversorgungen mit aktiver PFC (Power Factor Correction) am Eingang zwar kein ernsthaftes Problem dar. Doch sollten sich Nutzer des Verhältnisses bewusst sein und es verstehen, damit sie die richtige Entscheidung bei der Wahl des Betriebsmodus – Eco oder Online – treffen und den maximalen Nutzen daraus ziehen können.

Eco-Effizienz nach Szenario

Vor der Entscheidung für eine USV sollte grundsätzlich die Frage nach der richtigen USV gestellt werden. Denn nicht jede USV ist für jede Umgebung geeignet. Das gilt auch für den Eco-Betriebsmodus. Er gilt zwar oft als vielversprechendes Feature zur Steigerung des Wirkungsgrades, ist aber längst nicht für jedes Vorhaben sinnvoll: Wie kritisch ist die zu schützende Anwendung? Wie viel Energie benötigt die USV, um gegen Störungen und Unterbrechungen abzusichern?

Als Nutzer informiert man sich am besten genau über die konkrete Funktionsweise des Eco-Modus, seine Merkmale und die Rahmenbedingungen, unter denen er sinnvoll ist. Nur so lässt sich der volle Nutzen aus ihm ziehen und nur so sind tatsächliche Verbesserungen in der Effizienz und beim Stromverbrauch möglich.

Martin Reinert,
Sales Director Germany, Emerson Network Power

Trickreich temperierte Schaltschränke

Ein Blockheizkraftwerk kühlt die Serverracks in Schönebeck an der Elbe

Die Techniker der Stadtwerke Schönebeck haben ihr Rechenzentrum modernisiert: IT-Racks, Klimatisierungslösung und Überwachungstechnik helfen, die Ausfallsicherheit der IT zu gewährleisten und den Energieverbrauch zu senken. Ein Blockheizkraftwerk mit Kraft-Wärme-Kopplung trägt zur IT-Klimatisierung bei.

Die Stadtwerke Schönebeck versorgen die 32 000 Bürger sowie das Umland mit Strom, Gas, Wasser und Wärme. Hierfür betreibt die GmbH mit ihren mehr als 100 Mitarbeitern ein umfangreiches Leitungsnetz sowie mehrere moderne Blockheizkraftwerke. Insgesamt verwaltet der Versorger rund 40 000 Zähler und erbringt ergänzende Dienstleistungen wie die Betriebskostenabrechnung für 8500 Wohneinheiten.

Rechenzentrum für Versorger

In den vergangenen Jahren hat die Bedeutung der IT-Systeme für die Stadtwerke immer mehr zugenommen. Beispielsweise erlaubt das im EEG (Erneuerbare-Energien-Gesetz) geregelte Einspeisemanagement, dass Erzeuger ihren Strom variabel dem Netz zuführen können. Dies verlangt jedoch permanent verfügbare IT-Systeme. Auch künftige Lösungen wie Smart Metering und die fortschreitende Digitalisierung von Geschäftsabläufen machen einen ausfallsicheren IT-Betrieb notwendig. Darüber hinaus wird im hauseigenen Rechenzentrum der Stadtwerke das Prozessleitsystem betrieben, das die Versorgungsnetze sowie die Eigenerzeugungsanlagen überwacht.

Die IT-Umgebung hat daher eine große Bedeutung für die Versorgungssicherheit der etwa 17 000 angeschlossenen Haushalte sowie der Gewerbe- und Industriekunden. Wie wichtig die IT für das Tagesgeschäft ist, betont Thomas Heinemann, Leiter IT der Stadtwerke Schönebeck: „Wenn unsere IT-Systeme stillstehen, können wir die Mitarbeiter im Grunde nach Hause schicken, weil die meisten administrativen und operativen Prozesse dann nicht mehr funktionieren."

Quelle: Rittal

Eine Adsorptionskältemaschine wandelt im Sommer die Wärmenergie des Blockheizkraftwerks in Kühlenergie um, die in den Kaltwasserkreis der IT-Klimageräte eingeht.

Die Gebäudeinfrastruktur des Rechenzentrums wurde um das Jahr 2000 installiert. Ein 2014 gestartetes Modernisierungsprojekt sollte helfen, die Klimatechnik und Energieversorgung zu verbessern und damit die Ausfallsicherheit zu erhöhen und Kosten zu senken. „In der Energiewirtschaft wird der Einsatz von IT-Systemen weiter zunehmen. Wir müssen daher die Ausfallsicherheit der Systeme weiter steigern und gleichzeitig den laufenden Betrieb günstiger gestalten", erklärt Thomas Heinemann. „Die Energiewende mit ihren technischen Veränderungen beim Betrieb der Stromnetze war einer der Gründe, dass wir unsere IT-Landschaft ausbauen mussten", ergänzt Thomas Bolz, Bereichsleiter Technik der Stadtwerke Schönebeck. „Denn nur mit modernen IT-Systemen können wir die Versorgungsnetze effizient steuern."

Blockheizkraftwerk mit KWK

Zu den Besonderheiten der Stadtwerke Schönebeck zählt die eigene Energieerzeugung über Blockheizkraftwerke (BHKW) sowie die Nutzung von Kraft-Wärme-Kopplung (KWK), beispielsweise für Fernwärme. Bei der KWK werden in einem Kraftwerk gleichzeitig elektrischer Strom und thermische Energie gewonnen. Die primär erzeugte mechanische Energie, zum Beispiel von Gasmotoren, wird durch Generatoren unmittelbar in elektrische Energie umgewandelt. Die so entstehende Wärme wird für Heizzwecke (Nah- und Fernwärme) oder für Produktionsprozesse genutzt. „Der Vorteil der Kraft-Wärme-Kopplung besteht neben einer signifikanten CO_2-Minderung in der hocheffizienten Erzeugung von Strom und Wärme. Wir erreichen Brennstoffnutzungsgrade im Bereich von 90 %. Zum Vergleich dazu erreichen sehr gute Kraftwerke mit reiner Stromerzeugung etwas über 40 %", betont Thomas Bolz.

Den Stadtwerken ist es gelungen, die thermische Energie aus der Kraft-Wärme-Kopplung eines eigens zu diesem Zweck errichteten Blockheizkraftwerks ganzjährig zur Kühlung der IT und zur Erwärmung der Gebäude zu verwenden. Die thermische Energie des BHKW wird im Sommerbetrieb in der Adsorptionskältemaschine über einen chemischen Prozess zur Kühlung des Kaltwasserkreises der IT-Klimageräte genutzt. Die Leistung der Kältemaschine ist regelbar, sodass man in der Übergangszeit das Verhältnis von genutzter Wärme oder

Kälte dem Bedarf anpassen kann. Bei ausreichend niedrigen Außentemperaturen von weniger als 10° C erfolgt die Kühlung über den ohnehin notwendigen Freikühler. Im Winterbetrieb wird die im BHKW erzeugte Wärme für die Gebäudeheizung und zur Warmwasserbereitung eingesetzt.

Wasserkühlung aus BHKW-Wärme

Zur direkten Kühlung der Racks werden im Rechenzentrum integrierte Luft-/Wasser-Wärmetauscher genutzt. Diese Klimatisierungsgeräte lassen sich innerhalb der Serverrack-Reihen montieren und liefern eine maximale Kühlleistung von bis zu 30 kW. Hierbei wird die warme Luft der IT-Komponenten an der Geräterückseite angesaugt, gekühlt und nach vorne wieder in den Kaltgang ausgeblasen, wo sie den Geräten erneut zugeführt wird. Als Kühlmittel kommt Wasser zum Einsatz, das über einen Freikühler oder eine Kältemaschine gekühlt wird.

Im Sommer benötigt das Rechenzentrum bis zu 23 kW an Kälte. Um diese Kühlleistung zu erreichen, benötigt die Adsorptionskältemaschine etwa 45 kW an Wärme. Die Wärme stammt aus dem zugehörigen Blockheizkraftwerk, das eine thermische Leistung von 48 kW liefert. Die Anlage ist nahezu ganzjährig für Wärme- oder Kälteerzeugung nutzbar, wobei überschüssige Wärme in Wärmespeichern gelagert wird.

Die ursprüngliche Idee zur Nutzung der Kraft-Wärme-Kopplung entwickelten die Energiespezialisten der Stadtwerke, die anschließend gemeinsam mit Fachleuten aus der RZ-Branche weitere Berechnungen rund um das Klimakonzept durchführten. Hierbei wurden alternative Lösungsansätze berechnet und schließlich erfolgte die finale Validierung des Konzepts mit der Netzwerk Kommunikationssysteme GmbH aus dem 40 km entfernten Barleben als Generalunternehmer.

Um die Sicherheit der Anlage zu steigern, wurde eine Brandmelde- und Löschanlage in den Racks verbaut. Diese Lösung erkennt austretende Dämpfe und erste Rauchentwicklung sehr frühzeitig und kann so Alarm geben, lange bevor die Rauchmelder der Haustechnik reagieren.

Kosteneffizient neu aufgestellt

Entstanden ist eine hocheffiziente Gesamtlösung, die den Energieeinsatz im Rechenzentrum für Klimatisierung und Strom optimiert und hierbei auch den Bedarf an Gebäudewärme berücksichtigt. Nach Schätzungen der Stadtwerke ergeben sich Einsparungen an den Betriebskosten für Gebäude und Rechenzentrum von 5000 Euro im Jahr. Die neue Klimatechnik, die erneuerte Energieverteilung in den Racks sowie zusätzliche Sicherheitstechnik und das Monitoring sind wichtige Komponenten, mit denen die Stadtwerke ihre Ziele erreicht haben, die Ausfallssicherheit zu erhöhen und die IT-Betriebskosten zu senken.

Bernd Hanstein,
Hauptabteilungsleiter Produktmanagement IT, Rittal
Olaf Barth,
IT-Systemberater, Rittal

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:
Olaf Barth, Marco Becker, Ralf Enderlin, André Engel, Ralf Gehrke, Bernd Hanstein, Andreas Klees, Doris Piepenbrink, Martin Reinert, Kai Wirkus, Ulrich Wolf

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

Korrektorat:
Kathleen Tiede, Hinstorff Media, Rostock

Technische Beratung:
Uli Ries

Titelbild:
vladimircaribb, fotolia

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

Technology Review

2016
INNOVATORS SUMMIT

02. – 03. 11. 2016
OBERHAUSEN
www.heise-events.de/tr_energy2016

ENERGY

DER TRENDKONGRESS FÜR DIE ENERGIEWIRTSCHAFT

Drei Megatrends treiben die Entwicklung: Dezentralisierung, Dekarbonisierung, Digitalisierung. Auf dem „Innovators Summit – Energy" erfahren Sie, was das für Ihre Strategie bedeutet.

- IT Security – Sicherheit im Smart Grid
- Dezentralisierung – Lernen von den neuen Playern im Energiesektor
- Von Big Data zu Smart Data – neue Geschäftsmodelle bei strengem Datenschutz
- Lastmanagement – Zukunftsmodelle oder Übergangslösungen
- Energie 2030 – Welche Technologien erwarten uns

Tauschen Sie sich aus mit führenden Branchenvertretern, renommierten Wissenschaftlern und Start-ups.

Zusätzlich zu Panelvorträgen vertiefen wir Themen in Roundtables und Sie haben ausreichend Zeit zum Networken.

REFERENTEN u.a.:

Dr. Reinhold Achatz,
Leiter Corporate Technology
thyssenkrupp

Andreas Kuhlmann,
Vorsitzender der Geschäftsführung Deutsche Energie-Agentur dena

Prof. Dr. André Thess,
Leiter Institut für Technische Thermodynamik, Deutsches Zentrum für Luft- und Raumfahrt

Goldsponsor: iwo Institut für Wärme und Oeltechnik

Partner: agentur con energy

Organisiert von: heise Events Conferences, Seminars, Workshops

WIE GESCHMIERT.

iX. MEHR WISSEN.

Jetzt für 12,90 € bestellen.

shop.heise.de/ix-dev-effektiv ✉ service@shop.heise.de

Auch als digitale Ausgabe erhältlich unter: shop.heise.de/ix-dev-effektiv-pdf

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

heise shop

shop.heise.de/ix-dev-effektiv