Eine Themenbeilage der
Heise Zeitschriften Verlag GmbH & Co. KG

III
2013

RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Was Big Data zur Folge hat

www.rechenzentren-infrastruktur.de

powered by:

heise Events
Conferences, Seminars, Workshops

Worauf Rechenzentren gefasst sein müssen

Auf den ersten Blick nur eine Marketingvokabel mit sehr viel Potenzial zum Wahlkampfgetöse um die wahrscheinlich größte Selbstverständlichkeit der Welt, seit es digitale Speicher gibt – das ist Big Data. Egal, welche Regierungen, Unternehmen und Menschen künftig das Sagen haben, sie alle werden ständig sammeln, auswerten und benutzen, was Datenträger zu bieten haben. Weil es technisch möglich ist.

Die eigentliche Herausforderung hinter Big Data liegt weniger in der politischen Brisanz vermeintlich spektakulärer Spionage, sondern in der unfassbaren Kleinteiligkeit, die immer und überall abgreifbar und sicherheitshalber mehrfach redundant in maximal verfügbaren Rechenzentren gespeichert wird.

Für die Betreiber von Rechenzentren und Infrastrukturen bedeutet das vor allem eins: Ständig steigende Anforderungen, die mit herkömmlicher Technik kaum zu bewältigen sind. Das bedeutet so sicher wie das Amen in der Kirche: Nach dem Hype ist vor dem Hype. Denn der nächste kommt bestimmt. Ein möglicher Kandidat sind so genannte Effizienztechnologien. Dahinter verbirgt sich die aus Marketingsicht noch nicht ganz perfekt, weil zu sperrig, aber immerhin euphemistisch formulierte Lösung für ein altes – nun aber exponentiell ausuferndes – Problem, das alle Anwender von buchstäblich ausgelagerten Ressourcen schon immer hatten und ständig haben werden, wie mein Kollege, Gerald Strömer vom MittelstandsWiki, bei Recherchen zum Thema Big Data herausgefunden hat.

Eine im September 2012 veröffentlichte aktuelle Version von Symantecs State of the Data Center – eine Befragung unter 2453 IT-Profis aus 34 Ländern – hat schwarz auf weiß ergeben, dass Rechenzentren weltweit tatsächlich immer komplexer werden. Als Gründe dafür werden aktuelle Trends wie Mobile Computing, Cloud-Technik und Virtualisierung genannt. Das Problem: Immer vielschichtigere Infrastrukturen sind grundsätzlich fehleranfälliger und wartungsaufwendiger. Das ist gar nicht gut.

Laut Ciscos Global Cloud Index vom Oktober 2012 wächst der Cloud-basierte Datenverkehr im Rechenzentrum schneller als jeder andere Bereich; er soll bis 2016 das Sechsfache (4,3 Zettabyte) des heutigen Werts erreichen. Der gesamte weltweite Datenverkehr in Rechenzentren soll sich auf 6,6 Zettabyte vervierfachen. In drei Jahren wird der Cloud-Traffic Cisco zufolge rund zwei Drittel (64 Prozent) des gesamten Datenverkehrs ausmachen – 2011 waren es nur 39 Prozent. Der Großteil (76 Prozent) dieses Cloud-Traffics wird laut Cisco 2016 innerhalb des Datacenters selbst entstehen und überwiegend durch Storage sowie Produktions- und Entwicklungsdaten erzeugt werden. Das ist eine gewaltige Menge.

Im Februar dieses Jahres veröffentlichte Oracle seinen Next Generation Data Center Index 2013, der ein recht überraschendes Fazit hatte: Europäische Unternehmen, die ihre Daten im letzten Jahr zu externen Dienstleistern ausgelagert hatten, holten sie wieder in die eigenen Rechenzentren zurück. Laut Oracle wurden viele Unternehmen 2011 vom rasanten Datenwachstum überrascht und lagerten Daten aus. Dieser Trend schien sich 2012 wieder umzukehren. „Dies lässt den Schluss zu, dass der Wert, den die Unternehmen ihren Daten zumessen, gestiegen ist“, so Oracle im NGDCI. Allein an diesen beiden gegenläufigen Trends zeigt sich, dass die Fähigkeit, umfangreiche Datenmengen nahtlos zwischen Private und Public Clouds zu verschieben, ganz normal ist.

Ganz aktuell hat nun IDC seine Studie Storage in Deutschland 2013 vorgestellt. Ihr Fazit: Stark steigende Datenmengen sind Treiber für die Anforderungen an Speichertechnologien in Rechenzentren. Die Ausrichtung der Speichertechnologien auf wachsende Datenmengen hat oberste Priorität. Die Mehrheit der Befragten habe das auch erkannt; es sollen verstärkt Investitionen in zukunftsorientierte Lösungen wie Storage-Virtualisierung, Cloud-Storage, SSD-/Flash-Speicher und konvergente Systeme erfolgen.

IT-Verantwortliche stehen zunehmend unter Druck. Einerseits müssen sie dafür sorgen, dass die Storage-Technik den kontinuierlich und rapide steigenden Anforderungen an Performance, Kapazität und Effizienz genügt. Andererseits erwartet man von ihnen umgekehrt proportionale Einsparungen. Die Quellenlage lässt momentan nur einen Schluss zu: Diese beiden entgegengesetzten Vorgaben lassen sich nur dann unter einen Hut bringen, wenn Big-Data-freundlich kalkulierte Investitionen in zukunftsfähige Speichersysteme erfolgen.

Thomas Jannot

RZ-VERKABELUNG

Kategorie-8-Datenkabel für Datacenter schon jetzt erhältlich

Dätwyler hat ein erstes kompaktes S/FTP-AWG23-Kabel „CU 8203 4P“ entwickelt, das die voraussichtlichen Anforderungen der neuen Kategorie 8.2 gemäß ISO/IEC-Standard (Entwurf) laut Hersteller in vollem Umfang erfüllt. Dätwyler zufolge wurde besonderes Augenmerk darauf gelegt, dass die Kabel hinsichtlich der Dämpfung (NEXT, PS-NEXT) große Reserven zu den diskutierten beziehungsweise definierten Grenzwerten bieten.

Mit den Normentwürfen IEC 46C/976/NP und ISO/IEC TR 11801-99-1 sind zurzeit die neuen internationalen Standards für Kategorie-8-Kupferkabel sowie für symmetrische Verkabelungssysteme für 40 Gbit/s in der Entwicklung. Entgegen den noch vor einigen Jahren diskutierten Normvorschlägen für symmetrische Datenkabel der Kategorie 8 – damals für die strukturierte Gebäudeverkabelung und mit einer Grenzfrequenz von maximal 1,2 Gigahertz (GHz) – ist in den internationalen Standardisierungsgremien heute die ausschließliche Verwendung im Datacenter und eine Grenzfrequenz von maximal 2 GHz vorgesehen.

Der Standard ISO/IEC TR 11801-99-1 definiert eine Punkt-zu-Punkt-Verbindung zwischen aktiven Geräten mit einer maximalen Distanz von 30 Metern, die aus 26 Metern Installationskabel und jeweils 2 Metern Patchkabel auf beiden Seiten besteht. Eine solche Verbindung kann im Datacenter die kostspieligeren Fiberoptik- und Twinax-Verkabelungen ersetzen.

Die genauen Parameter für die Channel-Spezifikationen sollen in den nächsten Monaten erarbeitet werden. Insbesondere hinsichtlich der zukünftigen Anschlusstechnik und dem Übertragungsverfahren sind noch viele Fragen offen.

TE ICM MOBILE APP

iPhone App erleichtert das Netzwerk-Management

TE Connectivity hat die Infrastructure Configuration Manager (ICM) Mobile App für Apples iOS nach eigener Auskunft für die straffere Kontrolle von physischen Netzwerken entwickelt. Die ICM Mobile App arbeitet zusammen mit einer aktiven ICM-Software. Um geplante Arbeitsanweisungen zu koordinieren, ist die App direkt mit dem ICM-Server verbunden. Außerdem können Nachrichten mit den betroffenen Technikern direkt ausgetauscht werden.

Laut Hersteller soll die App eine sofortige Echtzeitansicht des Netzwerks bieten und es damit transparenter machen für die RZ-Spezialisten im Unternehmen. Zum Zeitpunkt der Produktion dieser Ausgabe stand die App noch gratis im iTunes-Store zum Download. Wann diese Testphase ausläuft, ist nicht bekannt.

In Verbindung mit einem ICM-System soll die App unter anderem folgende Funktionen bieten:

- Selektiertes Auflisten der Arbeitsanweisungen
- Synchronisation von Arbeitsanweisungen
- Kontrolle von Arbeitsanweisungen und LED-Aktivierung
- Arbeitsanweisungen schrittweise selektieren und managen
- Handhaben von Rückmeldungen
- Protokollieren von Incidents.

NEUES ENERGIEKONZEPT

Strom aus Algen

Die in Nordrhein-Westfalen angesiedelte PRIOR1 GmbH hat ein bisher einmaliges Konzept eines algenativen Rechenzentrums entwickelt, bei dem Algen für die Stromerzeugung verwendet werden. In Zusammenarbeit mit dem Frankfurter Architekten Bernd Schenk wurde die Idee entwickelt, das Rechenzentrum vom Konsumenten zum Erzeuger von Energie und Biomasse zu machen. Durch einen neuen Denkansatz entsteht ein effizientes Gesamtsystem, das an natürliche Prozesse angepasst ist und entstehendes Methan zum Erzeugen von Strom nutzt. RZ-Ausrüster Schneider Electric hat PRIOR1 für das Konzept mit dem Best Innovator Award ausgezeichnet.

Im algenativen Rechenzentrum sind in den sonnenzugewandten Teilen der Fassade Paneele eingebaut, in denen eine mit Algen gesättigte Flüssigkeit kreist. Denn Algen binden unter anderem Kohlenstoffdioxid (CO_2), das sie für ihr Wachstum benötigen. Dafür geben sie Methan ab. Die so über Gärprozesse erzeugte Biomasse dient als gasförmiger Brennstoff, der stromerzeugende Generatoren (BHKW) antreibt. Diese liefern Strom für das Rechenzentrum. Die daraus entstehende Prozesswärme kann als Heizung in das System zurückgespeist oder verkauft werden (Fernwärme).

Die über die Algenproduktion entstehende Biomasse wird zu Biokunststoffen veredelt, die biologisch abbaubar sind. Die Abwärme des Data Centers wird nicht energieaufwendig weggelüftet, sondern genutzt, um in gut temperierten Gewächshäusern Lebensmittel zu erzeugen.

Erleben Sie das entspannte Gefühl eines erfolgreichen Rechenzentrumsmanagement

FNT
IT SERVICE SOLUTIONS

Mit der DCIM Lösung von FNT organisieren und optimieren Sie die Ressourceneffizienz Ihres Rechenzentrums.

Facility, Netzwerke, IT Equipment, Software und Business Services in einem durchgängigen Datenmodell bilden die Grundlage für die Bereitstellung hochwertiger IT Services und ein energieeffizientes Data Center.

Erfahren Sie mehr unter:
www.fnt.de/DCIM

Network Packet Broker – Trend oder Renaissance?

Funktion und Unterschiede verschiedener Network Packet Broker

In den USA taucht bei Marktanalysten verstärkt das Thema Network Packet Broker auf. Es wird auch Intelligent Data Access oder Traffic Visibility genannt. Gemeint ist intelligentes Aggregieren und Filtern von Netzwerkdatenströmen zu Überwachungs- und Optimierungszwecken. Versteckt sich dahinter wirklich eine technische Neuerung, die auch in Europa zunehmend Einfluss gewinnen wird?

Die Themen Big Data, Bring Your Own Device (BYOD), Cloudbestrebungen, Outsourcing und Virtualisierung haben die Netzwerkagenda vieler Unternehmen in den letzten Jahren im Wesentlichen bestimmt. Kaum verwunderlich, da immer größer werdende Datenmengen in immer leistungsfähigeren Netzwerktopologien transportiert und benutzerorientiert bereitgestellt werden sollen. Idealerweise soll sich die gesamte Infrastruktur möglichst flexibel den sich permanent ändernden Geschäftsfeldern und Kundenbedürfnissen anpassen.

Wie so oft bei rasanten Weiterentwicklungen von Basistechniken bleiben dabei sicherheitstechnische und administrative Aspekte auf der Strecke. Ein permanentes Überwachen und Optimieren der Netzwerke und Rechenzentren wird bei den heutigen virtuellen und dynamischen Strukturen immer komplexer. Zudem können manche Anbieter kaum mit dieser rasanten Weiterentwicklung im Infrastrukturumfeld Schritt halten und bieten lediglich performanceoptimierte und keine dynamischen Lösungen für die Netzwerküberwachung und Optimierung an.

Ergebnis: Für eine Gesamtüberwachung wäre eine Vielzahl von Lösungen für verschiedenste Überwachungsproblematiken zu implementieren. In Zeiten sinkender IT-Budgets eher eine Wunschvorstellung statt Realität. Entsprechend sind in der Praxis nur Insellösungen zu beobachten, die lediglich eine Teilüberwachung und Optimierung bestimmter Bereiche ermöglichen. Der Gesamtüberblick geht in der Regel schnell verloren oder ist schlichtweg nicht vorhanden.

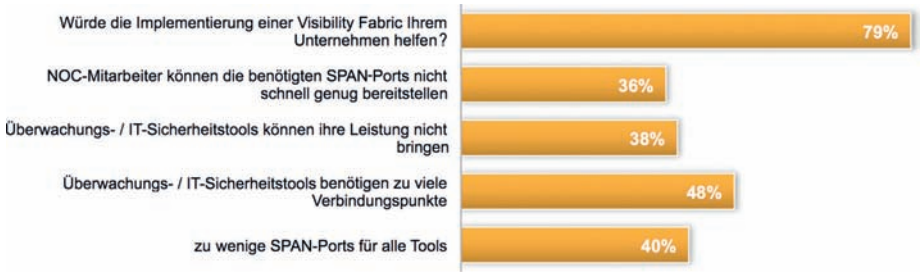
Genauer Blick aufs und ins Netz

Genau mit dieser Problematik haben sich Anbieter aus dem noch relativ jungen IT-Bereich „Network Packet Broker“ oder „Traffic Visibility“ auseinandergesetzt. Der Grundgedanke liegt im Aufbau einer unabhängigen, jederzeit verfügbaren Überwachungsebene. In diese werden alle relevanten Netzwerkdatenströme vom Produktivnetzwerk unabhängig, in voller Leitungsstärke und ohne Paketverlust gespiegelt. Hierbei liegt das Hauptaugenmerk auf dem Aufbau eines möglichst ganzheitlichen Überblicks über alle Netzwerkdatenströme ohne negative Beeinflussung der Produktivumgebung. Die gespiegelten Datenströme können dann bearbeitet und optimiert aufbereitet, beispielsweise an Überwachungs-, Optimierungs-, Audit-, Compliance-, Help-Desk-, Troubleshooting-, IT-Sicherheits-, Speicher- und forensische Lösungen oder Abteilungen, weitergeleitet werden. Durch das Aufbereiten der Datenströme sollen die Leistung, die Genauigkeit und die Einsatzdauer vorhandener Tools optimiert und zentralisierte Ansätze leichter umgesetzt werden können.

Wie sieht nun eine solche „Network Packet Broker“- beziehungsweise „Traffic Visibility“-Lösung in der Praxis aus? Zunächst einmal müssen die Datenströme aus den Netzwerken und Rechenzentren gespiegelt werden. Hierfür kann auf vorhandene Span-/Mirror-Ports von Switches oder auch virtuelle Span-/Mirror-Ports von virtuellen Systemen zugegriffen werden. Der Nachteil an dieser Zugriffsmöglichkeit besteht neben der begrenzten Anzahl dieser Ports vor allem in der nicht garantierten Weiterleitung (Paketverluste) aller zu überwachenden Daten, wenn die Geräte, die diese Ports bereitstellen, bestimmte interne Auslastungsgrenzen überschreiten.

Wider den Paketverlust

Um diese potenziellen Paketverluste zu umgehen, wird der Einsatz von TAP-(Traffic Access Point)-Lösungen empfohlen. TAPs sind physische Lösungen, die direkt den Datenverkehr von Kupfer- und/oder optischen Leitungen spiegeln und an ein System in voller Leitungsstärke ohne Paketverlust weiterleiten können. Die meisten Anbieter von Network Packet Brokern oder Traffic-Visibility-Lösungen haben entsprechende TAPs für verschiedene Leitungsstärken und Leistungsarten in ihrem Portfolio.



Quelle: NetDescribe GmbH

Eine Untersuchung der Enterprise Strategy Group (Dez. 2011) zum Thema Intelligent Management Aggreation Networks untermauert den Bedarf nach entsprechenden Lösungen (Abb. 1).

STULZ

IT Cooling Solutions

CyberCool 2 – der High-End-Chiller für Rechenzentren

- In Deutschland entwickelt, konstruiert und produziert
- Maximale Energieeffizienz (gemäß Eurovent Klasse A)
- Integriertes Freikühlsystem
- Geräuschoptimierter Anlagenbetrieb
- Optimiert für die Nutzung in Rechenzentren
- Hohe branchenspezifische Optionenvielfalt

www.stulz.com/cybercool2

Neben den Zugriffsmöglichkeiten mittels Span-/Mirror-Ports und TAPs bieten einige Anbieter mittlerweile auch Zugriffslösungen auf virtuelle Serverfarmen mit eigenen virtuellen TAPs an. Einige Anbieter haben zudem noch sogenannte Vor-Aggregationslösungen in ihrem Portfolio. Diese können den Datenverkehr einer Vielzahl nicht ausgelasteter Leitungen, wie sie beispielsweise in der Anfangsphase nach einer Netzwerkmigration von 1 auf 10 GB oft anzutreffen sind, zusammenfassen und komprimiert mit deutlich weniger Verbindungen an die zentrale Sammellösung weiterleiten. Der Vorteil dieser Vor-Aggregation liegt in der geringen Schnittstellenanzahl, die für die zentrale Sammellösung benötigt wird.

Wenn alle Datenstrom-Sammelpunkte definiert und fixiert sind, können diese Datenströme in speziell hierfür optimierten Lösungen gesammelt werden. Die Geräte der verschiedenen Anbieter unterscheiden sich hierbei sowohl hinsichtlich der Hardwareausstattung, wie auch hinsichtlich der installierten Software für zusätzliche Funktionalitäten.

Harte Ware zum Sammeln von Paketen

Bei der Hardware stehen die Anzahl und Art der unterstützten Schnittstellen, die modulare Ausbaufähigkeit und die Durchsatzleistung im Vordergrund. Zukunftsfähige Systeme sollten Schnittstellen von 1 GB, 10 GB, 40 GB und im Idealfall bereits 100 GB unterstützen. Diese Schnittstellen dienen für die Verbindung mit den zuvor definierten Knotenpunkten des Netzwerkes, zum Verbindungsaufbau der Geräte untereinander (Stacking, Clusterbildung) und natürlich für das Anbinden der vorhandenen und zukünftig geplanten Überwachungs-, Optimierungs- und IT-Sicherheitslösungen.

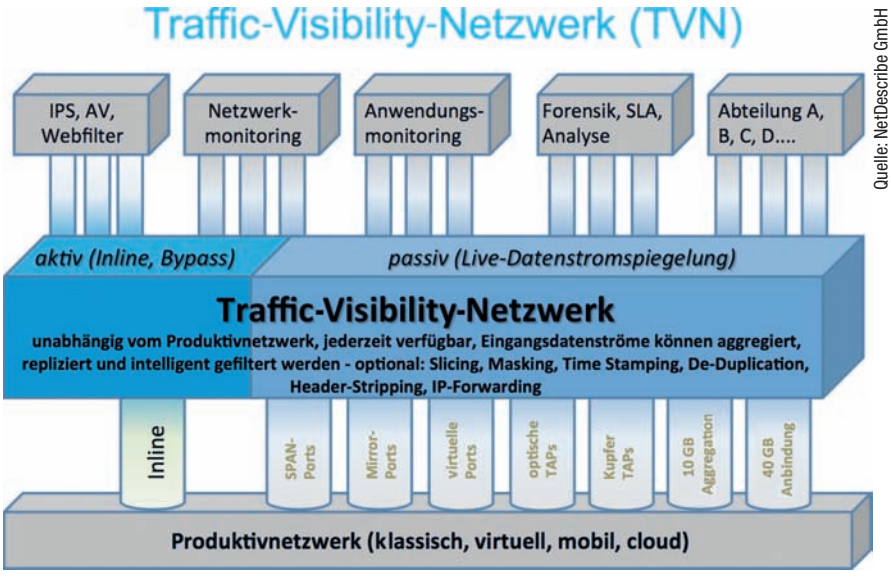
Entsprechend ist die Art, Anzahl und Erweiterbarkeit dieser Schnittstellen von grundlegender Bedeutung. Meist sind bereits verschiedene Schnittstellen fest in ein Gerät integriert und können durch Module und Blade-Einsätze bedarfsgerecht erweitert werden. Einige Anbieter bieten zudem noch aktive und passive TAP-Module für die direkte Integration von TAPs in die eigenen Lösungen an. Dies ist bei wenigen passiv und vor allem bei aktiv zu „tappenden" Verbindungen durchaus sinnvoll, wenn auch in der Regel teurer. Bei einer hohen Anzahl von zu „tappenden" Verbindungen sind aber separate TAPs (wie oben beschrieben) mit einem eigenen Management zu bevorzugen. Bedenkt man diese flexiblen Leitungsaggregationsmöglichkeiten, dann sollte bei der Auswahl einer solchen Lösung auf eine entsprechende ausbaufähige Durchsatzleistung geachtet werden, um auch zukünftige höhere Netzwerklasten oder Netzwerkmigrationen auf höhere Geschwindigkeiten mit derselben Lösung verarbeiten zu können. Redundante Netzteile und Lüfter sollten auch selbstverständlich sein.

Neben den verschiedenen Hardware-Konfigurationsmöglichkeiten unterscheiden sich die Lösungen vor allem hinsichtlich ihrer Zusatzfunktionalitäten. Alle Lösungen können in der Regel Datenströme aggregieren, replizieren und filtern. Dies sollte sowohl die Aggregation von mehreren Eingangs-Datenströmen zu einem Ausgangs-Datenstrom (N:1), die Replikation eines Eingangs-Datenstroms auf mehrere Ausgangsdatenströme (1:M) wie auch die kombinierte Aggregation/Replikation von mehreren Eingangs-Datenströmen an mehrere Ausgangsdatenströme (N:M) umfassen. Mit dieser Funktionalität erhält der Anwender mehrere Optionen zur Weiterleitung der Daten:

- Eingangs-Datenströme mehrerer Netzwerksegmente konzentriert und zentralisiert (via eines Ausgangsdatenstroms) an eine Netzwerküberwachungslösung
- dedizierter Eingangs-Datenstrom in voller Leitungsstärke repliziert an mehrere verschiedene Überwachungs- und Optimierungslösungen (Ausgangsdatenströme)
- mehrere Eingangsdatenströme kombiniert und in voller Leitungsstärke repliziert an verschiedene Überwachungs-, Optimierungs- und IT-Sicherheitslösungen (Ausgangsdatenströme)

Auf die Filter kommt es an

Dies ist aber nur die Basisfunktionalität. Die maßgebliche Intelligenz dieser Lösungen liegt in den Filtermöglichkeiten – meist hinsichtlich der OSI-Ebenen 2 – 4. So können sehr einfach aus den empfangenen Netzwerkdatenströmen bestimmte IP-Adressbereiche, VLANs oder beispielsweise Datenmuster vorgefiltert und gezielt an einen oder mehrere Ausgangsports weitergeleitet werden. Somit lässt sich unter anderem eine intelligente Datenreduktion und/oder gezielte Aggregation der Datenströme verschiedener Netzwerksegmente bewerkstelligen.



Quelle: NetDescribe GmbH

Ein Traffic-Visibility-Netzwerk dient zum Überwachen des Produktivnetzwerks und wird unabhängig von diesem oder anderen Schutztechniken betrieben (Abb. 2).

Denkt man hier beispielsweise an ein Troubleshooting, eine zentrale Netzwerkanalyse oder eine VoIP-Optimierung im gesamten Netzwerk, dann werden die Vorteile dieser Lösung sehr schnell klar. Auch seitens der an das System angeschlossenen Überwachungs-, Optimierungs-, Analyse- und IT-Sicherheitslösungen können deutliche Optimierungen vorgenommen werden. Traditionell werden beim Optimieren eines Netzwerkes die notwendigen Tools mit jedem relevanten Knotenpunkt im Netzwerk verbunden. Die Tools müssen dann selbst zuerst den Datenverkehr ausfiltern, den sie überhaupt analysieren können. Dies führt oft zu einer Performanceüberlastung der Tools, Paketverlusten bei der Analyse und möglicherweise fehlerbehafteten Berichten.

Mit einem Network Packet Broker können die gesammelten Datenströme derart vorgefiltert werden, dass die an die Lösung angeschlossenen Tools nur noch die

datacenter.de
Eine Marke der noris network AG

datacenter.de – Der beste Platz für Ihre IT

Premium Produkte rund um Europas modernstes Rechenzentrum

- höchste Verfügbarkeit
- höchste Leistungsfähigkeit
- höchste Energieeffizienz durch KyotoCooling®
- Green IT
- zertifiziert und ausgezeichnet nach strengsten Richtlinien

noris network

noris network AG • Thomas-Mann-Straße 16 - 20 • 90471 Nürnberg • T +49 911 9352-160 • F +49 911 9352-100 • vertrieb@noris.de • www.noris.de

Daten empfangen, die sie auch verarbeiten können. Entsprechend sinkt die Performanceauslastung bei gleichzeitigem Anstieg der Analysegenauigkeit der Tools. Als Nebeneffekt schrumpft zudem meist die Anzahl oder die Lizenzgröße der benötigten Analyselösungen. Ebenso können in der Regel bei einem Netzwerkupgrade beispielsweise von 1 GB auf 10 GB vorhandene 1-GB-Analyselösungen durch ein intelligentes Setzen von Filtern und einer Tool-Clusterbildung noch lange Zeit eingesetzt werden.

Filtervariationen

Es gibt drei grundlegende Filtermöglichkeiten: Eingangsfilter für die Ports, an denen die Datenströme aus den Netzwerken empfangen werden, Ausgangsfilter für die Ports, an denen Daten weitergeleitet werden, sowie zentrale Regelwerke. Hier sind massive Unterschiede hinsichtlich der maximalen Regelanzahl und der Zählweise der Regeln bei den Lösungen festzustellen. Es gibt Lösungen, die jeden Filter auf jedem Eingangs- und Ausgangsport separat anwenden und zählen. Eine einfache Kombination verschiedenster Filter kann so bereits Hunderte Regeln in der Zählweise der Systeme verbrauchen.

Zudem bedingt auch jede Eingangs- oder Ausgangsportänderung ein Anpassen der jeweiligen Filter und Regeln. Andere Lösungen wählen hier ein zentrales Design, in der in „Regelcontainern“ bestimmte Filter für beispielsweise ein bestimmtes Analysetool definiert werden und diese Sammelregel dann automatisch auf alle eingehenden Datenströme angewendet wird. Solche zentralen Regelwerke wirken auf den ersten Blick etwas komplexer, werden aber von den Lösungen nur einmalig gezählt und passen sich auch bei Änderungen der Eingangsports automatisch an. Eine generelle Aussage zur Vorteilhaftigkeit dieser unterschiedlichen Filterzählweisen und Ausprägungen zu treffen ist schwierig und kommt immer auf den spezifischen Anwendungsfall an. Entsprechend ist ein Test unterschiedlicher Lösungen ratsam.

Die verschiedenen Anbieter der Network Packet Broker bieten dazu noch Modifikationsmöglichkeiten für ihre Lösungen an. Hierunter fallen beispielsweise:

- De-Duplizierung: Ausfiltern doppelter Datenpakete
- Masking zum Überschreiben sensibler Daten
- Slicing: Abschneiden überflüssiger Daten
- Time-Stamping: Empfangszeitpunkt der Pakete
- Port-Stamping: Erfassung des Ursprungsortes der Datenpakete
- Header-Stripping: Ausblenden unwichtiger Informationen
- En-/Decapsulation: Entfernen nicht standardkonformer Paketinformationen
- Tunneling: Einpacken und Versenden der lokalen Paketinformationen für eine genaue Analyse verteilter Standorte vor einer Weiterleitung an die Ausgangsports.

Diese Zusatzfunktionalitäten verlangen in der Regel nach reichlich Performance, da die Datenströme detailliert untersucht und bearbeitet werden. Daher werden sie entweder als zusätzliche Blades mit eigenen CPUs angeboten oder kommen mit fest im Gerät verbauten Zusatzprozessoren. Je nach Anzahl und Umfang der aktivierten Zusatzfunktionalitäten sind hier bei den Lösungen erhebliche Leistungsunterschiede festzustellen. Entsprechend ist auch hier ein Test anzuraten.

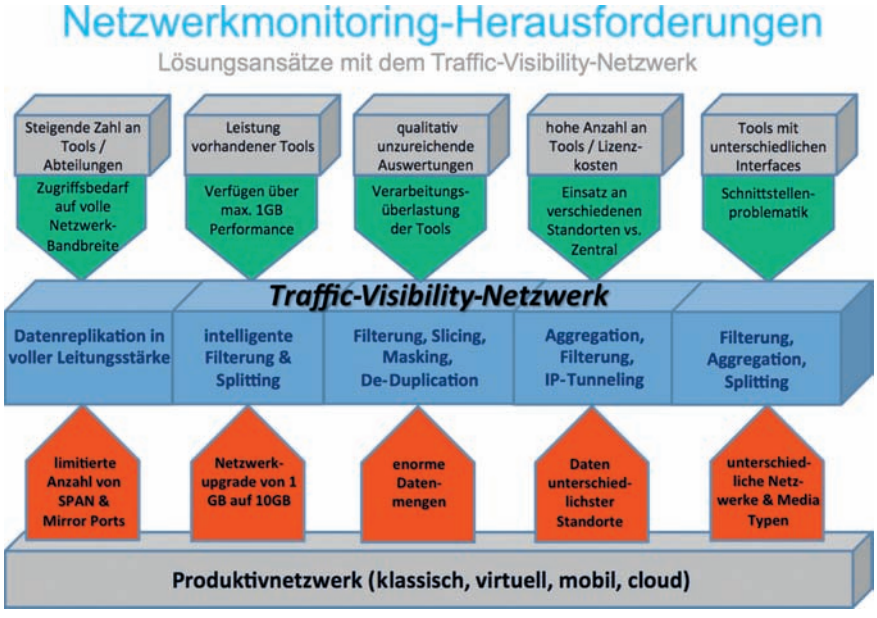
Neben der Hardwareausstattung, den Filtern und den Zusatzfunktionalitäten unterscheiden sich die Lösungen auch hinsichtlich der Verwaltung. Generell sollte für die Administration neben einer webbasierten Benutzerschnittstelle auch die klassische Kommandozeile zur Verfügung stehen. Je nach Leistungsumfang der Lösung, der Möglichkeit zum Schaffen von Clustern und der zentralen Verwaltbarkeit der Lösungen über verschiedene Standorte hinweg steigt die Komplexität und entsprechend groß werden die jeweiligen Unterschiede beim Verwalten der Systeme. Auch hier kann keine generelle Empfehlung gegeben werden – es kommt auf den individuellen Einsatzzweck an.

Die Lösung für verteilte Netzwerke

Network Packet Broker, Intelligent-Data-Access- oder Traffic-Visibility-Lösungen als neuen Trend zu bezeichnen ist übertrieben. Genauso wenig stellen die Produkte aber eine Renaissance der klassischen Netzwerküberwachung dar. Da es heute kaum noch klassische, abgeschlossene Netzwerke gibt, ist die bekannte Art Netzwerküberwachung nicht mehr sinnvoll anwendbar.

Die Lösungen sind durch ihre zentrale Datenstromaggregation selbst in verteilten Netzwerken die Antwort auf sich ständig ändernde Netzwerktopologien. Sie ermöglichen überhaupt erst wieder eine dauerhafte und dynamische Netzwerküberwachung sowie Optimierung. Die Produkte sind das Bindeglied zwischen den meist noch sehr klassisch konzipierten punktuellen Überwachungslösungen und den dynamischen Strukturen heutiger Netzwerke und Rechenzentren. Die flexiblen Lösungen können nahezu jedem Unternehmen helfen, das rechtliche Vorgaben zum Überwachen seiner Netzwerke umsetzen muss. Gleichzeitig können die Lösungen auch den Einsatz von Netzwerk-Überwachungs- und Analyselösungen optimieren und deren Nutzungsdauer vor allem bei Netzwerkmigrationen wesentlich verlängern.

Gregory Blepp
Geschäftsführer, NetDescribe GmbH



Quelle: NetDescribe GmbH

Ein leistungsfähiges Werkzeug zur Traffic Visibility leitet nur die Daten an Analysetools, die diese auch benötigen, und senkt so unter anderem Lizenzkosten (Abb. 3).

transtec Cloud:
flexibel. sicher. einfach.

make-it-cloud: Virtuelle Systeme von transtec

33 JAHRE PROFESIONELLE IT-SYSTEME UND LÖSUNGEN „MADE IN GERMANY“

Erhöhen Sie die Flexibilität Ihrer IT-Infrastruktur

Sparen Sie sich Pflege und Wartung Ihrer Hardware

Bezahlen Sie nur das, was Sie wirklich benötigen

Profitieren Sie von einem hochverfügbaren, ausfallsicheren Rechenzentrum

intel inside™ XEON®

Intel® Xeon ® Prozessor

transtec
accelerate productivity

Globale Cloud-Infrastrukturen im Griff behalten

Daten rechtskonform in weltweit verteilten Cloud-Rechenzentren speichern

Cloud-Services sollen einerseits international flexibel verfügbar sein, andererseits müssen manche Daten nach strengen Datenschutzregeln verarbeitet werden. Viele Entscheider stehen immer noch in einem Dilemma zwischen diesen beiden Möglichkeiten. Wer beides in Einklang bringen will, sollte sich auf den Weg in die Cloud gründlich vorbereiten und das Cloud-Management seines Anbieters unter die Lupe nehmen.

Cloud Computing ist ein Wachstumsmarkt. Laut der Marktforschungsgesellschaft Experton Group entfallen 2013 mehr als fünf Prozent der deutschen IT-Ausgaben (4,6 Milliarden Euro) im Business-to-Business-Segment auf Cloud-Computing-Angebote. Bis 2017 soll das Umsatzvolumen gar auf mehr als 18 Milliarden Euro steigen.

Dennoch ist das Cloud Computing nach wie vor kritischen Fragen ausgesetzt. Unter anderem geht es darum, ob das Speichern und Verarbeiten von Daten in Cloud-Data-Centern außerhalb Deutschlands oder der EU mit den deutschen Datenschutzbestimmungen vereinbar ist. Der Hintergrund: Deutsche Unternehmen, die Cloud-Computing-Dienste nutzen, müssen gemäß dem Bundesdatenschutzgesetz sicherstellen, dass die Verarbeitung personenbezogener Daten in Rechenzentren in der EU erfolgt oder in Ländern, die vergleichbare Rahmenbedingungen bieten, etwa durch das „Safe Harbour"-Abkommen.

Wo seine Daten lagern, ist für den Nutzer von Cloud-Services jedoch häufig nicht nachvollziehbar. Die großen Anbieter unterhalten eine Vielzahl von Rechenzentren in allen Regionen der Welt. Der Nutzer kann häufig nicht festlegen, dass bestimmte Daten nur in Data-Centern auf EU-Territorium bearbeitet werden. Bei Backups weichen viele Cloud-Anbieter beispielsweise gerne auf Data Center im Nicht-EU-Ausland zurück.

Quelle: BT

Fachleute sind der Meinung, dass sich EU-Datenschutzrichtlinien und internationale Cloud-Angebote durchaus vertragen (Abb. 1).

„Made in Germany" reicht nicht

Einige Provider, etwa T-Systems, Fujitsu, ProfitBricks und Host Europe, werben gezielt damit, dass ihre Cloud-Dienste ausschließlich über Data Center in Deutschland bereitgestellt werden. Allerdings geben sie damit wichtige Vorteile des Cloud-Computing auf. Betroffen hiervon sind insbesondere Kunden, die Standorte in mehreren Ländern unterhalten, egal ob multinational tätige Großunternehmen oder Firmen aus dem gehobenen Mittelstand mit verteilten Fertigungsstätten oder Vertriebsniederlassungen.

Wenn beispielsweise ein Vertriebsbüro in Asien oder Südamerika häufig Multimediadaten in Form von Marketingvideos aus der Cloud lädt, führt das bei Beschränkung auf ein Rechenzentrum in Deutschland zu höheren Latenzzeiten und eingeschränktem Benutzererlebnis. Ruckelbilder in einer Verkaufspräsentation sind kontraproduktiv. Das Gleiche gilt für den Servicetechniker eines deutschen Maschinenbauers, der bei der Reparatur einer Maschine in der Mongolei eine Videoanleitung benötigt. Und auch viele geschäftskritische Applikationen wie SAP reagieren empfindlich auf lange Latenzzeiten. Nicht zuletzt ist es möglich, dass international tätige Unternehmen auf anderen Kontinenten wiederum regulatorisch verpflichtet sind, bestimmte Daten vor Ort zu speichern.

In Szenarien wie diesen ist „Made in Germany" allein keine Option. Die Lösung des Dilemmas liegt vielmehr in einer global angelegten Cloud, die der Anwender mit Hilfe von Virtualisierung zentral steuert.

Verteilte Ressourcen intelligent steuern

Ein solches globales Cloud-Szenario kombiniert das Einhalten der Datenschutzregeln mit dem Einsatz regional verteilter Cloud-Data-Center. Technisch lässt sich das so realisieren, dass der Systemverwalter in verschiede-

icyteas
simply intelligent ICT

Wollen Sie auch, dass NSA und MI6 die Finger von Ihren Daten lassen?*

* Dann nutzen Sie die Vorteile einer icyteas-Lösung:
Virtual Datacenter Services – Made in Germany

- Deutsche Standards
- Deutsche RZ-Flächen
- Deutsche Compliance

www.icyteas.de

Maßgeschneidert. Einfach. Sicher.

Made in Germany

nen Data-Centern des Providers Virtual Machines (VM) implementiert, die jeweils für eine spezielle Aufgabe ausgelegt sind. „Das Anbinden der Cloud-Infrastruktur an das Firmennetz des Kunden kann dabei aus Sicherheits- und Performancegründen direkt per MPLS oder Ethernet-Anbindung erfolgen, also vollständig getrennt vom Internet“, sagt Jörg Keller, Senior Product Manager Cloud Compute bei BT Global Services.

In diesem Szenario verwalten die Anwender ihre Unternehmensdaten dann rechtskonform entsprechend ihrer Eigenschaften:

– Personenbezogene Daten, wie etwa Personalinformationen und deutsche Kundendaten, lagern in einem deutschen Rechenzentrum des Service-Providers. Damit erfüllt das Anwenderunternehmen die Vorgaben des Bundesdatenschutzgesetzes.
– Marketing-Materialien oder Dokumente für den technischen Support in den USA stellen beispielsweise Cloud-Ressourcen in einem amerikanischen Rechenzentrum bereit.
– Zeitkritische IT-Services, etwa OLTP-Datenbanken oder Kommunikationsdienste für Unified Communications und Collaboration, laufen in global verteilten Data-Centern, die in der Nähe der jeweiligen Unternehmensstandorte liegen.

Für eine solche Cloud-Infrastruktur sind auf Seiten des Anbieters neben den physischen Ressourcen in Form von IT- und Kommunikationshardware vor allem zwei Hauptkomponenten erforderlich:

– Ein Cloud Management System, mit dem der Systemverwalter die gebuchten Cloud-Computing-Dienste über ein Web-Portal ordert und verwaltet. Darüber legt er fest, in welchem Data-Center der Cloud-Service-Provider die aufgabenspezifischen VM implementiert werden.
– Eine Cloud-Topographie, die den Überblick über die unterschiedlichen Bereiche der physischen Infrastruktur erlaubt.

Als Front-end für den Anwender zum Verwalten der verteilten Ressourcen bietet sich ein Web-basiertes Dashboard an. „Hier steuert der Administrator die verteilten Ressourcen wie Speicherplatz, Anwendungen, Zugriffsrechte oder Bandbreiten“, so Keller. Wichtig fürs Automatisieren von Verwaltungsvorgängen sind die Application Programming Interfaces (APIs) zum Anbinden eigener Management-Lösungen und firmeninterner Ressourcen. Denn einer Umfrage des BITKOM zufolge ist die Integrationsfähigkeit der eigenen IT in das Cloud-Angebot des Service-Providers für drei Viertel der Unternehmen die wichtigste Anforderung. Der Cloud-Anbieter sollte daher auch möglichst viele verschiedene Hypervisor-Modelle unterstützen.

Cloud-Management per Dashboard

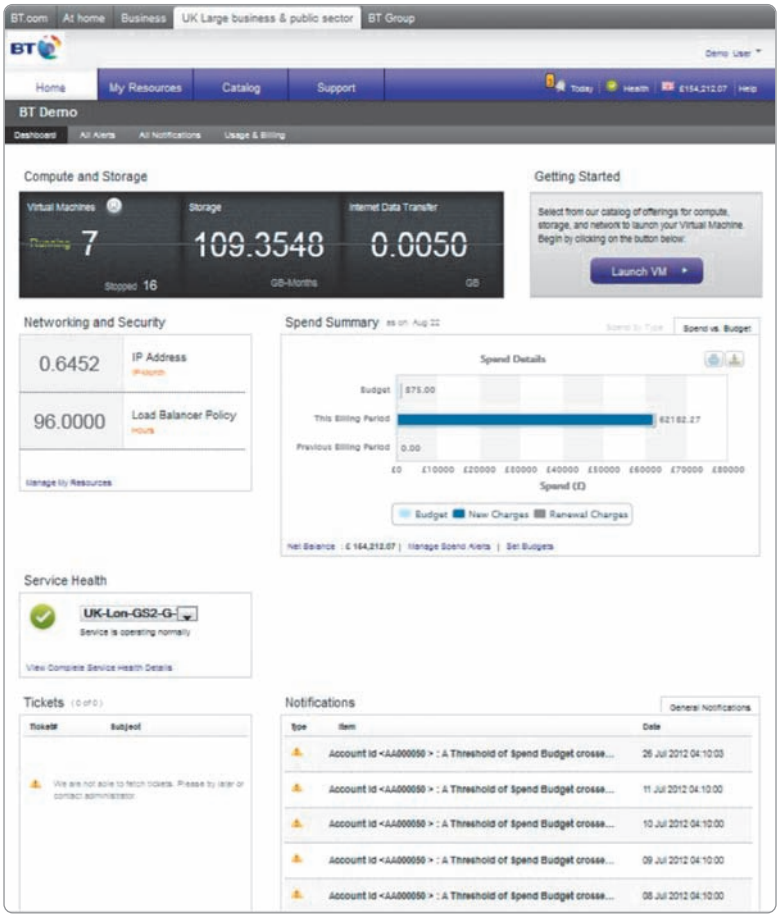
Um sicherzustellen, dass Kundeninformationen wie im oben skizzierten globalen Cloud-Szenario beispielsweise in einem Rechenzentrum in Frankfurt gespeichert werden, richtet der Administrator mit dem Cloud Management System eine Virtuelle Maschine im gewünschten Cloud-Data-Center ein. Dabei definiert er unter anderem den geographischen Standort des Rechenzentrums, den Hypervisor und die Art der Netzwerkanbindung.

Um Ressourcen in der verteilten Cloud-Infrastruktur besser verwalten zu können, bietet es sich an, die System-Topographie in logische Einheiten oder Bereiche zu gliedern. Die Definition der verschiedenen Bereiche sollte auf Basis der unterschiedlichen Anforderungen an Verfügbarkeit und Sicherheit der Daten erfolgen.

Der allgemeine Cloud-Bereich ist als Public Cloud Service in jeder Region verfügbar, die der Provider abdeckt. Die Nutzer teilen sich physische Ressourcen wie Rechenleistung, Storage und Netzwerkkapazitäten. Der gemeinsam genutzte Cloud-Bereich adressiert Gruppen von Anwendern, die gleiche Anforderungen an einen Cloud-Service haben, etwa in Bezug auf die Sicherheit. Die Mitglieder einer Gruppe teilen sich spezielle Netzwerk- und Rechenkapazitäten. Speicherplatz wird über den allgemeinen Cloud-Bereich bereitgestellt.

Der private Cloud-Bereich richtet sich an Anwender, die dedizierte Netzwerkdienste, Sicherheitssysteme und Blade-Server nutzen wollen. Diese Ressourcen stehen jeweils ausschließlich einem Unternehmen zur Verfügung.

Unternehmen und öffentliche Einrichtungen, die Cloud-Computing weltweit einsetzen wollen, können also durchaus von der internationalen Reichweite großer Cloud-Anbieter profitieren. Dadurch haben sie die Möglichkeit, unkompliziert zu definieren, dass zum Beispiel bestimmte Daten in Deutschland, andere auf anderen Kontinenten verarbeitet und gespeichert werden sollen – abgestimmt auf die jeweiligen technischen, organisatorischen und regulatorischen Anforderungen.



Quelle: BT

Per Dashboard steuert der Administrator unter anderem, in welchem lokalen Rechenzentrum er eine Virtual Machine einrichtet (Abb. 2).

Bernd Reder
Freier Journalist

20 JAHRE

MCL

HP. Günstig. Kompetent.

DIE MCL SPAR-HOTLINE
0800 - 11 99 151
Viele HP-Renew Produkte ab Lager verfügbar

HP c7000 Blade Enclosure

- bis zu 16 High-Performance Blade-Server in einem Enclosure
- bis zu 8 Interconnect Module zur redundanten & flexiblen Anbindung an Ihre vorhandene Infrastruktur
- redundante Auslegung der Komponenten sowie einfache zentrale Verwaltung

1x c7000 Blade Enclosure:
» **Versorgung:** 6x Netzteile | 10x Lüfter
» **Lizenzen:** 16x Insight Control Suite
Renew | volle HP Garantie

mit Interconnect-Modul:
» **HP FlexFabric 10Gb 24-Port VC**
SFP+ Ports für FibreChannel & Ethernet

ERWEITERN SIE DIE GRUNDLAGE IHRER CONVERGED INFRASTRUCTURE MIT HP

&

HP BL460c Gen8 Blade-Server

- bis zu zwei Intel Xeon 8-Core Prozessoren der neusten Generation!
- Agentenlose Hardware-Überwachung und Warnfunktionen mit iLO 4
- HP SmartMemory bietet unübertroffene Leistung und Qualität (bis 512GB pro Blade)

4x HP BL460c Gen8 mit je:
» **Prozessor:** 2x Intel Xeon E5-2670 8-Core 2.6GHz
» **Memory:** 64GB (8x 8GB) PC3-12800R RDIMMs
» **Adapter:** FlexLOM 554FLB FlexFabric 10Gb 2-Port
» **Controller:** Smart Array P220i/512MB FBWC
Renew | volle HP Garantie

-57%

€ 19.999
HP-Listpreis: €47.452

Art.-Nummer: BL460-8C-B2

&

MCL Services

Converged Infrastructure Gold Specialist 2013

» inkl. Factory Service
Hardwareumrüstung, Testing, Updates & Systemkonfigurationen nach Wunsch.

» mit rasantem Versand
Ihre fertig konfigurierten Systeme erhalten Sie auf Wunsch innerhalb von 24 Std.

» optionaler Start-Up Service
Installation & Abstimmung mit der vorhandenen Hardware vor Ort!

Informationswerte schützen

Wie und wovor Rechenzentren umfassend zu schützen sind

Um ein Rechenzentrum umfassend zu schützen, müssen drei Schutzziele erreicht werden: Versorgungssicherheit (Energieversorgung und Kühlung der IT-Systemtechnik), Desaster-Toleranz und Objektschutz. Insbesondere Letzteres ist ein oftmals vernachlässigter Bereich – Zeit, sich darum zu kümmern.

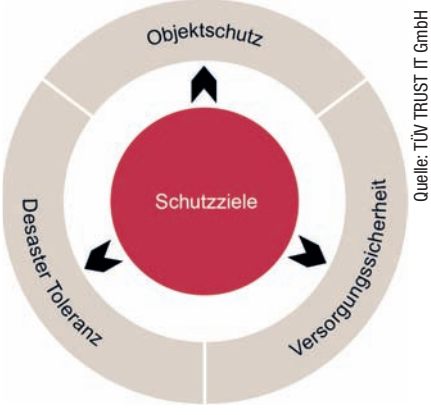
Punkte wie die Desaster-Toleranz sind hinlänglich bekannt. Hierzu werden in der Regel mehrere Rechenzentren mit großen Abständen von fünf bis mehr als 5000 Kilometer benötigt, damit ein Schadenereignis (Desaster) wie Überschwemmungen, Erdbeben, Chemieunfälle, Großbrand nicht beide RZ-Standorte beeinträchtigt.

Weniger geläufig ist vielen RZ-Verantwortlichen hingegen der Objektschutz. Unter Objektschutz wird im Allgemeinen der Schutz von Objekten (Liegenschaften) durch Bewachung verstanden. Bezogen auf die Sicherheit eines Rechenzentrums muss der Begriff jedoch weiter gefasst werden. Das zu schützende Objekt ist nicht die Liegenschaft allein, sondern die Informationswerte auf den IT-Infrastrukturen im Rechenzentrum. Wobei das Rechenzentrum selbst wieder aus den IT-Räumen (Serverräume und Netzwerkknoten) und den Technikräumen (Energieversorgung, Kühltechnik und Sicherheitstechnik) besteht.

Unter den Objektschutz des Rechenzentrums fallen der Schutz gegen unautorisierten Zugriff oder Manipulation von IT-Infrastrukturen beziehungsweise der darauf befindlichen Daten durch technische und organisatorische Maßnahmen, die außerhalb der IT-Systemtechnik selbst liegen. Die technischen und organisatorischen Maßnahmen richten sich im Allgemeinen gegen Umgebungsgefahren wie Feuer, Wasser, Rauch, Einbruch, Vandalismus, Erschütterung oder elektromagnetische Felder.

Risikoanalyse als Basis

Im Vordergrund des Objektschutzes sollte immer eine Risikoanalyse bezogen auf die Gefahren, deren Erwartungswert und das Schadenspotential stehen. Nur so kann eine wirtschaftlich angemessene Auswahl der Maßnahmen vorgenommen werden. Um einen geeigneten Objektschutz zu gewährleisten, ist eine Umfeld-Analyse für das Rechenzentrum notwendig. Hierbei ist sowohl das nähere Umfeld (umliegende Räume) der IT- und Technikräume als auch das weitere Umfeld des Standortes des Rechenzentrums zu betrachten.



Quelle: TÜV TRUST IT GmbH

Für den umfassenden Schutz eines Rechenzentrums gilt es neben den beiden gängigen Schutzzielen auch den Objektschutz zu beachten.

Ziel der Umfeld-Analyse ist es, eine optimale Lage für den Komplex „Rechenzentrum“ beziehungsweise seiner einzelnen IT- und Technikräume zu bestimmen. Erst im zweiten Schritt werden die verbleibenden Risiken auf ein akzeptables Maß reduziert. Im Rahmen des weiteren Umfelds sind Faktoren wie Verkehrswege, Gefahrguttransporte, Funkstrecken, Chemie-/Schwerindustrie, Grund- und Oberflächenwasser oder Veranstaltungsorte zu betrachten. Im Bereich des näheren Umfelds sind zu beachten: Lösch-, Stadt- und Abwasser, Gefahrstoffe, Betriebsstoffe oder sonstige Brandlasten, Blitz/Überspannung, interne Verkehrswege (Anlieferung, Flure, Treppenhäuser), Besucher und Lieferanten.

Unterschiedliche Maßnahmen verzahnen

Sofern die akzeptablen Standorte für die Räume des Rechenzentrums definiert sind, kann im Rahmen der Risikoanalyse eine geeignete Behandlungsoption ausgewählt werden, um das Risiko auf ein akzeptables Maß zu mindern. Alle Objektschutzmaßnahmen sollten in ein integriertes Gefahrenmanagement übernommen werden. Grob lassen sich die Objektschutzmaßnahmen den folgenden Bereichen zuordnen: Intrusionsschutz, Brandschutz, Wasserschutz, Überspannungsschutz und elektromagnetischer Schutz.

Intrusionsschutz ist der Schutz von Anlagen, Gelände, Gebäuden und Räumen vor unberechtigtem Zutritt von Personen. Maßnahmen bestehen beispielsweise in Form von Einbruchmeldeanlagen, Zutrittskontrollanlagen, Widerstandsklassen von Bauteilen oder Videoüberwachung.

Wichtig ist ein strukturiertes Vorgehen, das mit der Definition der Schutzziele über eine Analyse der Tätergruppen und des Täterverhaltens in ein integriertes Schutzkonzept mündet. Basis ist ein Sicherheitszonenkonzept, das nach dem Zwiebelschalenprinzip aufgebaut werden sollte. Das heißt, um in die höchste Sicherheitszone zu gelangen, muss eine Person alle vorgelagerten Sicherheitszonen durchqueren. Die sensibelsten Bereiche sollten daher möglichst im Innersten des Gebäudes platziert werden.

Es ist wichtig, die Zonenübergänge und Zonengrenzen möglichst homogen zu sichern. An den vorgesehenen Zonenübergängen wird mit geeigneten Zutrittskontrollanlagen nur berechtigten Personen der Zutritt gewährt. Die Zonen sind je nach Sicherheitsstufe durch Einbruchmeldetechnik und Videoaufzeichnung an den Grenzen und/oder in der Fläche gesichert.

Unter Brandschutz sind Maßnahmen zu verstehen, die Personen und Unternehmenswerte vor Feuer und Rauch schützen. Dabei wird das Schadenspotenzial von Rauch meist unterschätzt, obwohl dieser

in der Regel das weitaus höhere Schadenspotenzial für Personen und auch die IT-Systemtechnik aufweist.

Im Gegensatz zum baurechtlichen Brandschutz, bei dem allein der Personenschutz im Mittelpunkt steht, ist beim Brandschutz eines Rechenzentrums auch der Sachschutz zu beachten. In der Regel bedeutet dies, dass die baurechtlichen Maßnahmen für ein Rechenzentrum nicht ausreichen. Das oberste Ziel des Brandschutzes ist die Brandvermeidung, gefolgt von der Branderkennung und Brandbekämpfung. Das bedeutet, es sollte auf nicht brennbare oder schwer entflammbare, halogenfreie Baustoffe in IT- und Technikräumen geachtet werden. Auch in der Umgebung der IT- und Technikräume sollten sich keine beziehungsweise nur sehr geringe Brandlasten befinden. Zum Vermeiden von Bränden dienen auch Sauerstoffreduktionsanlagen (siehe Seite 20). Wichtig ist der Schutz vor Kaltrauchübertragung. Damit sind Schmelzlot gesteuerte Brandklappen ungeeignet. Auch die Lüftungsanlage darf keinen Kaltrauch verteilen.

Wasserschutz ist der Schutz der IT-Systemtechnik und des Gebäudes vor Wasser. Dabei kann Wasser in Form von Oberflächenwasser, Löschwasser, Brauchwasser, Frischwasser, Kondenswasser oder auch Kühlwasser auftreten. Wichtig ist auch hier das Vermeiden. Es sollten also keine wasserführenden Leitungen in IT- und Technikräumen verlegt werden, die nicht zum Betrieb des Rechenzentrums notwendig sind. Falls Wasser auftritt, muss dieses möglichst schnell lokalisiert werden. Hierzu existieren auf dem Markt eine Vielzahl an Sensoren. In einem weiteren Schritt sollte auch die Wassermenge begrenzt werden. Dies kann zum Beispiel über automatische Ventile und Wärmetauscher geschehen. Zudem sollte dennoch auftretendes Wasser schnellstmöglich beseitigt werden können.

Überspannungsschutz

Hierbei geht es um den Schutz der technischen Einrichtungen vor zu hohen elektrischen Spannungen. Überspannungen können durch Blitz, kapazitive oder induktive Einkopplungen wie auch elektrostatische Entladungen (ESD) hervorgerufen werden. Gemäß DIN EN 62305-4 VDE 0185-305-4:2011-10 ist eine energetische Koordination durchzuführen. Damit ist sicherzustellen, dass alle ableitenden Einrichtungen bis zum Endgerät aufeinander abgestimmt sind.

Zum elektromagnetischen Schutz stellt das BSI mit der Technischen Richtlinie „BSI TR-03209 Elektromagnetische Schirmung von Gebäuden“ einen Leitfaden zur Verfügung, der zeigt, wie mit handelsüblichen Baumaterialien eine ausreichende Gebäudeschirmung erzielt werden kann.

Die Auflistung macht deutlich, dass auch Objektschutz mit vertretbarem Aufwand zu gewährleisten ist. Mindestens ebenso wichtig wie die technischen Komponenten, die für den Schutz des Rechenzentrums sorgen, ist eine sorgfältige Planung und vor allem Analyse der eventuell drohenden Gefahren.

Joachim Stephan
CTO, TÜV TRUST IT GmbH / Unternehmensgruppe TÜV Austria

Rack und Raum im Fadenkreuz

IT-Grundschutz in kritischen Infrastruktureinheiten

In Serverräumen wird es nur selten zu heiß, da fast in jedem Rechenzentrum Brandmelder sind. Aber vor Wasser, Spannungsausfall, Fehlbedienung, technischen Schäden und Sabotage schützt die empfindlichen Einrichtungen kaum jemand. Nur 20 Prozent der Unternehmen besitzen einen ausreichenden Grundschutz in ihren kritischen Infrastruktureinheiten. Ein Missstand, dem Abhilfe geschaffen werden kann.

Nahezu jedes Unternehmen hat Security Software in unterschiedlichster Ausprägung immer im Einsatz, das Überwachen des firmeneigenen Netzwerks ist fast schon Usus. Da wirken Bedrohungen wie Brände, Wassereinbruch, Überspannung oder schlicht Sabotage oder Diebstahl fast schon altmodisch.

Doch gerade diese physischen Gefahren werden häufig unterschätzt. Dabei gibt es strikte Regelungen, was die entsprechende Absicherung betrifft: Gemäß dem Standard BSI (Bundesamt für Sicherheit und Informationstechnik) 100-1 des IT-Grundschutzes und entsprechend der Standardfamilie ISO 2700x müssen Unternehmen und Behörden ihre Serverräume sowie Betreiber von Rechenzentren ihre IT gegen die häufigsten physischen Risiken schützen.

Umso erstaunlicher ist die Tatsache, dass dem ganzheitlichen Schutz von Serverräumen und Infrastrukturen in vielen Betrieben so wenig Bedeutung zuteil kommt: Studien belegen, dass 80 Prozent aller Serverräume und Racks physisch nicht adäquat abgesichert sind. Das sind rund eine Million Unternehmen allein in Deutschland. Zu den Bedrohungen zählen in diesem Zusammenhang beispielsweise Temperaturprobleme, ein Ausfall der Spannungsversorgung, Zutritt von Unbefugten, Manipulationen, Brände und Leckagen. Diebstahl, technische Schäden oder die Störung der Betriebsumgebung sind die größten physischen Risiken, die die Daten und die IT-Infrastruktur in Serverräumen täglich bedrohen. Teilweise überwachen bereits vorhandene Systeme diese Risiken schon.

Wie Zahnräder im Sicherheitsuhrwerk

Um Schutz zu garantieren, müssen jedoch mehrere physische Schutzmechanismen sinnvoll ineinandergreifen – im Prinzip wie Zahnräder in einem Sicherheitsuhrwerk: Ein Bewegungsmelder im Serverraum beispielsweise sichert diesen vor Diebstahl, Sabotage und unbefugtem Zutritt. Wichtig hierbei ist der Einsatz eines spezialisierten Bewegungsmelders, der die verschiedenen Temperaturzonen und Gerätetemperaturen in einem IT-Raum berücksichtigt und keine Fehlalarme provoziert. Ideal sind Melder, die auf Radartechnik basieren, oder Passiv-Infrarotmelder (PIR) mit Temperaturkompensation.

Wird der Raum zu heiß, steigt die Temperatur zu schnell oder sind die Temperaturschwankungen zu hoch, verkürzt sich die Lebensdauer des technischen Equipments, sogar ein Ausfall der Server ist möglich. Hier schützt ein Temperatursensor, der die Raumtemperatur und auch die Funktion von Kühl- oder Heizanlagen überwacht. Um technische Schäden und Serverausfälle durch Kondenswasser zu vermeiden,

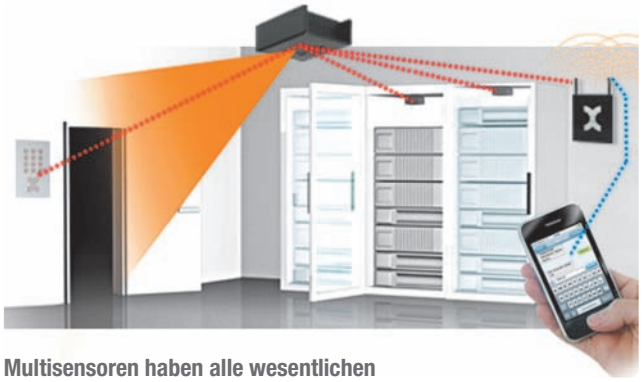
lässt sich die Luftfeuchte ebenso überwachen wie der Taupunkt. Wasser, das auf dem Boden des Serverraumes steht, erkennt ein sogenannter Leckage-Sensor. Feuer detektiert ein Brandmelder – im Idealfall ein Kohlenmonoxid-Sensor, mit einer sensiblen Auslöseschwelle im Bereich zwischen 20 und 200 ppm. Je empfindlicher die Einstellung, desto eher wird die Gefahr erkannt.

Ebenfalls überwacht werden sollte die externe Netzspannung. Spannungsausfälle müssen gemeldet und im Idealfall gleich überbrückt werden. Bei einem Stromausfall sollte das System eine Notspannungsversorgung haben, sodass in jedem Fall noch die Alarmierung per GSM funktioniert. Denn ganz ohne Strom gibt es auch kein LAN und keine E-Mail-Benachrichtigung. Diese Redundanz der Übertragungswege erhöht die Sicherheit erheblich. Um Störungen in der Betriebsumgebung frühzeitig zu erkennen, sollten neben der reinen Überwachung auch noch Klimadaten wie Luftfeuchtigkeit, Raumtemperatur oder Spannungsschwankungen erfasst und ausgewertet werden. Durch ein Echtzeit-Monitoring der Betriebsparameter im Serverraum lassen sich manche Gefahrenpotenziale bereits im Vorfeld erkennen und abwenden.

Viele Köche verderben den Brei

Die obige Aufzählung zeigt, dass prinzipiell durchaus ganzheitlich abgesichert werden kann. In der Praxis beschränken sich die Mechanismen aber in aller Regel auf eine Brandmeldezentrale, das Messen der Stromqualität per USV-System sowie das Überprüfen der Ein- und Austrittstemperatur über die Klimaanlagen. Insofern ist eine gewisse Grundabsicherung in den meisten sensiblen Räumen gegeben – mehr aber auch nicht.

Natürlich gibt es auch Betriebe, die besser gegen physische Bedrohungen abgesichert sind. Allerdings kommen hier meist mehrere Insellösungen diverser Hersteller zum Einsatz. In diesem Fall fehlt es dann an der Abstimmung der Geräte untereinander. Zudem treiben einzelne Lösungen die Kosten in die Höhe. Eine Alternative sind All-in-One-Monitoring-Lösungen, die sämtliche Bedrohungen im Blick haben. Sie arbeiten mit den oben beschriebenen Sensoren – integriert



Quelle: Kentix GmbH

Multisensoren haben alle wesentlichen Gefahren für Serverräume im Blick.

in einem Gerät –, die auf unterschiedliche Parameter reagieren und im Notfall den Verantwortlichen alarmieren.

Überwachungslösungen sind vernetzt

Bei vernetzten Überwachungslösungen laufen alle Informationen der Sensoren zusammen und werden ausgewertet. Diese Vernetzung erfolgt in Serverräumen per LAN oder Funk, da die zu sichernden Räume in der Praxis meist komplett eingerichtet sind und die Möglichkeit der Signalübertragung per Draht entfällt (schließlich müssten hier Wände aufgeklopft und Leitungen gelegt werden). Wird ein Diebstahl oder ein technischer Schaden von einem Sensor erkannt, gelangt die Information in Echtzeit an den verantwortlichen Mitarbeiter, der daraufhin, je nach Alarmquelle, entsprechend reagiert.

Zusätzlich sollte eine stille Alarmierung eingerichtet werden, die zuvor festgelegte Personen gezielt benachrichtigt. Die stille Alarmierung erfolgt dabei wahlweise per SMS, E-Mail, SNMP oder Telefonanruf und lässt sich individuell einstellen. Ferner ist es möglich, über Schaltausgänge weitere Verbraucher zu aktivieren, zum Beispiel eine externe Beleuchtung, was die Sicherheit ebenfalls erhöht.

Marius Schenkelberg
Freier Autor

Verfügbarkeit der IT im Brandfall sichern

Wie wäre es mit einem Update für den Brandschutz?

Was passiert eigentlich, wenn es im Rechenzentrum einmal brennt? Können die althergebrachten, konventionellen Brandschutzlösungen ein IT-Zentrum wirklich noch zeitgemäß schützen? Oder sollten sich RZ-Betreiber alsbald nach modernen Schutzalternativen umschauen?

Weder unsere Gesellschaft noch die Wirtschaft kommen heute ohne komplexe IT-Infrastrukturen aus. Ganz gleich, ob mittelständisches Unternehmen oder IT-Dienstleister – der Erfolg eines Unternehmens steht und fällt auch mit der Erreichbarkeit und Zuverlässigkeit seiner IT. Steht die IT still, sind alle firmeninternen und -externen Abläufe gleichermaßen betroffen. Das ist eine Binsenweisheit. Und dennoch wird in der Praxis oftmals übersehen, wie wichtig es ist, ein Rechenzentrum so zu gestalten, dass auch im Brandfall die Verfügbarkeit der IT nicht unnötig gestört wird. Typischerweise geht beispielsweise nach dem Stromlosschalten des RZ erst einmal gar nichts.

IT-Verantwortliche unternehmen und investieren viel, um ihr Rechenzentrum auf die unterschiedlichsten Störfälle vorzubereiten. Zutrittskontrollsysteme, Antivirenschutz und eine doppelte Notstromversorgung werden eingerichtet. Der Brandschutz wird dabei jedoch allzu oft vernachlässigt. Vorhandene Lösungen sind oftmals veraltet oder technisch nicht hinreichend durchdacht. Die Auswirkungen im Brandfall können verheerend sein, denn gerade im IT-Bereich ist durch die Vielzahl elektrischer Anlagen das Brandrisiko besonders hoch. Laut einer VdS-Mängelstatistik entstehen 20 bis 25 Prozent aller Brände durch Mängel an Betriebsmitteln, Leiteranschlüssen und Verbindungen, Überlast- und Kurzschlussorganen und bei Kabelleitungen.

Viele Rechenzentren wurden bei ihrer Errichtung vollkommen normenkonform mit einer Gaslöschanlage ausgestattet. Dass eine Gaslöschanlage jedoch bei ihrer Projektierung einmalig auf die zu diesem Zeitpunkt vorliegenden Anforderungen ausgelegt wird und danach oftmals über Jahre oder gar Jahrzehnte hinweg unverändert bleibt, machen sich viele IT-Verantwortliche nicht bewusst.

Quelle: Wagner Group GmbH

Brandvermeidungsanlagen schützen die IT vor den Auswirkungen eines Feuers und lassen ein Betreten des RZ weiterhin zu (Abb. 1).

Risiken von Gaslöschanlagen

Ein Rechenzentrum ist in aller Regel hingegen bekanntermaßen sehr dynamisch: Neue Racks, leistungsstärkere Server, stärkere Klimatechnik, Kalt- und Warmgänge und zusätzliche Netzwerkverbindungen halten Einzug und verändern somit auch die Bedingungen, die beim Auslegen der Gaslöschanlage noch galten. Die Folge: Die Löschanlage passt nicht mehr zum Rechenzentrum, kann für die neuen vorherrschenden Bedingungen über- oder unterdimensioniert sein und im Brandfall unter Umständen keinen Löscherfolg mehr gewährleisten. Ein zweites, nicht außer Acht zu lassendes Risiko bringen erweiterte Netzwerkverbindungen mit sich. Durch neue Installationskanäle oder nicht abgeschottete Durchlässe in Wänden oder im Doppelboden können Raumundichtigkeiten entstehen, die im Brandfall gravierende Auswirkungen haben können. So führt eine Undichtigkeit unter Umständen dazu, dass die erforderliche Löschgaskonzentration nicht erreicht oder nicht lange genug gehalten werden kann. Eine Brandbekämpfung ist somit nicht optimal möglich. Zudem besteht die Gefahr, dass das Rauch-Löschgas-Gemisch durch die Öffnungen in den Wänden oder im Unterboden in angrenzende Räume gelangt und dort anwesende Personen gefährdet.

Stromlosigkeit ist Pflicht

Die Sachversicherer empfehlen zudem, bei einer Gaslöschung im Brandfall sämtliche IT-Anlagen und die gesamte Klimatechnik stromlos zu schalten, um dem Brand die Stützenergie zu entziehen. Dies soll den Löscherfolg sicherstellen und eine Rückzündung nach dem Löschen vermeiden. Würde nach dem Löschvorgang eine verbliebene Entzündungsquelle den Brand erneut entfachen, hätte eine Gaslöschanlage diesem nichts entgegenzusetzen, da das Löschmittel bereits verbraucht wurde.

Zusätzlich kann die IT-Hardware nicht nur durch das Brandereignis selbst, sondern auch durch das Auslösen der Gaslöschanlage gefährdet werden: Löst eine Anlage aus, entweicht das Löschgas über die Düsen unter hohem Druck innerhalb kürzester Zeit. Der dabei entstehende Schalldruckpegel kann eine Lautstärke von bis zu 130 dB(A) erreichen, was beispielsweise die Köpfe von Festplatten zum Schwingen bringen kann. Werden keine geeigneten Schutzmaßnahmen in Form von spe-

ziellen Schalldämpfern getroffen, können die Zerstörung der Festplatte und damit der Verlust von Daten die Folge sein.

Um die oft fatalen Auswirkungen eines kleinen technischen Defekts zu vermeiden, empfiehlt sich der Einsatz einer vorausschauenden, auf die Anforderungen eines Rechenzentrums abgestimmten Brandschutzlösung. Speziell in den sensiblen IT-Bereichen hat sich eine aktive Brandvermeidung mittels Sauerstoffreduktion bewährt. Dabei erfolgt mittels Stickstoffzufuhr üblicherweise ein dauerhaftes Absenken des Normalsauerstoffgehaltes der Luft von 20,9 Vol.-% auf ein reduziertes Sauerstoffniveau von zirka 15 Vol.-%. Durch das Absenken wird einem möglichen Feuer der notwendige Sauerstoff entzogen und die IT-Hardware gleichzeitig vor den Auswirkungen eines Brandes geschützt. Zudem bleibt der so geschützte Gebäudeteil weiterhin für autorisiertes Personal begehbar.

Aktives Vermeiden von Bränden als Alternative

Ein alternatives Brandschutzkonzept für IT-Räume ist die Kombination des Brandvermeidungssystems OxyReduct mit einer N2-Schnellabsenkung. Bei dieser Kombination wird das Sauerstoffniveau nach einer Detektion durch ein Brandfrühesterkennungssystem von einem bereits reduzierten Grundniveau von 17 Vol.-% innerhalb weniger Minuten auf ein sicheres Niveau von 13,6 Vol.-% abgesenkt. Dies entzieht dem Feuer den notwendigen Sauerstoff und erstickt es damit.

Ein weiterer Vorteil der Schnellabsenkung ist der niedrigere Energiebedarf der Anlage: Durch das höhere Grundniveau von 17 Vol.-% verringern sich die Laufzeiten des Stickstoffgenerators. Ein Absenken auf 13,6 Vol.-% erfolgt ausschließlich im Fall einer Branddetektion. Der hierfür notwendige Stickstoff wird aus wiederbefüllbaren Flaschen zur Verfügung gestellt, nach der Absenkung auf 13,6 Vol.-% wird über die Sauerstoffreduktionsanlage das Niveau gehalten.

Nach der Schnellabsenkung übernimmt das Aufrechterhalten des reduzierten Sauerstoffniveaus bei 13,6 Vol.-% erneut die Sauerstoffreduktionsanlage. Die reduzierte Sauerstoffkonzentration kann somit theoretisch unendlich lange gehalten werden, was auch etwaige Raumundichtigkeiten ausgleicht. Der Vorteil: Weder im Dauerbetrieb des Brandvermeidungssystems noch während der Schnellabsenkung ist ein Stromlosschalten der IT notwendig. Auch im Brandfall ist somit eine Verfügbarkeit der IT weiterhin gesichert.

Brandvermeidung und freie Kühlung

Ein ganzheitliches und mehrstufiges Brandschutzkonzept kann auch in Kombination mit neuartigen Klimakonzepten wie der freien Kühlung oder der von noris network verwendeten Kyoto-Kühlung (siehe Rechenzentren & Infrastruktur, Ausgabe IV/2012, Seite 17) angewendet werden. Der Brandfrühesterkennung kommt dabei ein besonderer Stellenwert zu: Sensible Rauchansaugsysteme können bereits ab zwei Gramm stoffliche Brandzersetzung einen Brand erkennen. Dies funktioniert selbst bei hohen Luftgeschwindigkeiten durch die Klimatisierung. Beim Auslösen des Hauptalarms wird dann beispielsweise das Kyoto-Kühlsystem abgeschaltet. Die Kühlung des IT-Zentrums übernimmt dann ein geschlossenes Ersatzkühlsystem.

Im Rechenzentrum der noris network AG wird beispielsweise sofort die Schnellabsenkung durch das Einleiten von Stickstoff aus Gasflaschen gestartet und der Sauerstoffgehalt des Raumes innerhalb weniger Minuten von den üblichen 20,9 Vol.-% auf 16 Vol.-% reduziert. In der Folge wird dieses Niveau durch das Brandvermeidungssystem kontinuierlich gehalten. Sollte im Laufe dieses Prozesses über die Brandfrühesterkennung weiterer oder erneuter Rauch detektiert werden, kann durch das Auslösen einer zweiten Stufe die Zielkonzentration auf einen Wert von 13,6 Vol.-% Sauerstoff im Raum weiter abgesenkt und dort ebenfalls kontinuierlich gehalten werden.

Quelle: Wagner Group GmbH

Ein aktives Vermeiden von Bränden kommt auch beim Auslösen der Anlage ohne Stromlosschalten der IT-Komponenten aus und sorgt so für durchgängigen Betrieb (Abb. 2).

Neben noris network haben noch zahlreiche weitere Kunden eine Anlage zur aktiven Brandvermeidung mittels Sauerstoffreduktion im Einsatz. Das Prinzip hat sich in der Praxis also bereits bewährt.

Katrin Strübe,
Kommunikation, WAGNER Group GmbH

Planung, Bau und Umzug aus einer Hand

Neues Rechenzentrum der WISAG mit Infrastruktur und LAN-Konzept

Die WISAG ist mit mehreren zehntausend Mitarbeitern eines der führenden deutschen Dienstleistungsunternehmen. Aufgrund ihres dynamischen Wachstums wurde ein Umzug der Frankfurter Unternehmenszentrale in eine neue Immobilie nötig. Hierfür mussten Rechenzentrums-Infrastruktur und Switch-Architektur neu aufgesetzt und der Umzug des Rechenzentrums in kürzester Zeit durchgeführt werden.

Das Netzwerk am angestammten Standort der WISAG in der Kennedyallee 76 in Frankfurt am Main basierte auf einem HP5000er-Coreswitch, ist aber in wenigen Jahren stark gewachsen. Besonders im Hinblick auf Betriebssicherheit, Redundanz, Skalierbarkeit und Performance war das Netzwerk zuletzt nicht mehr zeitgemäß. „Durch das historische Wachstum hatte unser altes Netzwerk gewisse architektonische Defizite entwickelt, beispielsweise gab es immer wieder Probleme mit Loops“, erinnert sich Michael Futterer, Leiter Informationssysteme und Prokurist bei der WISAG. Als die WISAG Flächen im ehemaligen IBM-Gebäude in der Herriotstraße 3 erwarb, bot sich die Chance, eine komplett neue LAN-Architektur aufzubauen.

Anforderungen ans Netzwerk

Kernziele des Redesigns waren das Beseitigen von Leistungsengpässen, der Einsatz moderner Designansätze und neuer Produkt-Leistungsmerkmale für ein zukunftsorientiertes Design, das Schaffen eines hohen Verfügbarkeitsniveaus, die Unterstützung von Sicherheitsmechanismen bereits auf Netzwerkebene sowie Voice-Readiness für den anstehenden, flächendeckenden IP-Telefonie-Rollout bei der WISAG.

Das Rechenzentrums-LAN in der Herriotstraße 3 wurde aufgrund der hohen Anforderungen an Performance und Verfügbarkeit mit Datacenter-Komponenten aus der „Nexus“-Familie von Cisco Systems aufgebaut. Die hohe Verfügbarkeit wird in diesem Falle über das redundante Anbinden der Server- und Storage-Komponenten an zwei

Quelle: Cancom physical infrastructure

Das neue Rechenzentrum der WISAG mit Warmgangeinhausung (links) und Klimageräten (rechts) (Abb. 1).

unterschiedliche Nexus 22xx erreicht, die wiederum zwei unterschiedlichen Nexus 5596UP zugeordnet sind. Der Access-Layer auf den Stockwerken hingegen wurde mit HP-Switches ausgebaut. Sie waren nicht nur preisgünstiger, sondern bieten auch den Vorteil, dass die Administratoren vor Ort auf ihrem Know-how bezüglich HP-Komponenten aus dem alten Rechenzentrum aufbauen können.

„Wir hatten für das Rechenzentrum sowohl HP- als auch Cisco-Switches in der Diskussion", erinnert sich Michael Futterer. „Da wir den Neubau für eine mindestens zehnjährige Nutzung planten, waren die stabilen Produktlebenszyklen von Cisco ein wichtiges Argument für uns. Zudem konnte uns HP im Corebereich mangels eigener Produkte, aber auch preislich nicht überzeugen."

Moderne Infrastruktur

Im Zusammenhang mit der Planung des neuen LAN diskutierte Futterer mit dem gewählten Dienstleister, der Cancom physical infrastructure GmbH, auch über den erforderlichen Neubau der Rechenzentrumsinfrastruktur in der Herriotstraße 3. Cancom physical infrastructure ist ein zertifizierter Meisterbetrieb des Elektrohandwerks und der Klimatechnik und verfügt außerdem über die Große Bauvorlageberechtigung. Damit kann der Dienstleister alle baulichen Leistungen rund um die physische Infrastruktur aus einer Hand erbringen.

Bei den intensiven Beratungsgesprächen standen für IT-Leiter Futterer zwei Ziele klar im Vordergrund: Die Brandvermeidung durch Sauerstoffreduktion und eine energieeffiziente Klimatisierung mit Leistungsreserven im Hinblick auf einen weiteren Ausbau. „Das neue Rechenzentrum führt Aufgaben zusammen, die bislang auf mehrere Standorte verteilt waren. Hier wird nicht nur die IT für die rund 7000 Anwender in unserem Unternehmen bereitgestellt, sondern auch alle Private-Cloud-Services, die wir für unsere Kunden erbringen. Höchste Verfügbarkeit, Kosteneffizienz und Ausbaufähigkeit sind somit unternehmenskritisch", betont Michael Futterer.

Bei den Konzeptionsgesprächen waren auch neue Techniken im Gespräch wie der Einsatz eines Kyoto-Rades für die Klimatisierung. Letztlich stellte sich jedoch eine Kaltwasserrückkühlung in Kombination mit einer indirekten Freikühlung als Optimum heraus. Dabei wird in den kühlen Zeiten des Jahres die Außenluft zur Kühlung der Server nutzbar gemacht. Tragfähig ist ein solches Konzept nur, wenn die Umluftkühlgeräte, die die Kälte in die Rackreihen mit den Servern bringen, einen höchstmöglichen Wirkungsgrad erreichen.

Dies erreichte Cancom physical infrastructure im neuen WISAG-Rechenzentrum durch eine Warmgangeinhausung. Dabei werden Racks und Umluftkühlgeräte in zwei Reihen aufgebaut. Die Racks stehen mit den Rückseiten zueinander, der so entstehende Gang ist der sogenannte Warmgang. Die Umluftkühlgeräte werden in diese Reihen integriert, um die Distanz zwischen Wärmequelle – im Warmgang grenzen in jeder Rackzeile die Rückseiten der Racks und die Vorderseiten der Umluftkühlgeräte aneinander – und der Klimageräte so gering wie möglich zu halten. Die volle Kälteleistung steht somit dem IT-Equipment zur Verfügung. Die integrierten Umluftkühlgeräte nehmen die im Warmgang geschottete erwärmte Server-Abluft auf und geben sie gekühlt in die Kaltgangzone ab. Ergebnis: Der Raum bleibt kühl.

Der Warmgang wird durch Türen und Dachpaneele versiegelt, um eine Vermischung der warmen Abluft mit der kalten Raumluft zu vermeiden. Dieses Abschotten führt zu einer Leistungssteigerung der Umluftkühlgeräte, da der latente Anteil der Luftwärme innerhalb des Warmgangs signifikant verringert und somit der kühlbare, sensible Anteil erhöht wird. Durch dieses Prinzip der Warmgangeinhausung kann auch anderes, nicht eingehaustes Equipment im selben Raum platziert werden, da die Raumtemperatur durch die offenen Kaltgangbereiche kühl gehalten wird.

Modular erweiterbar

Für das Warmgangkonzept entschieden sich die Verantwortlichen der WISAG auch deshalb, weil es ihren Wunsch nach modularer Ausbaufähigkeit in besonders hohem Maß erfüllte. Die gesamte Infrastruktur des Rechenzentrums wurde nach dem Bausteinprinzip in standardisierten Data Cubes angelegt. Ein Data Cube besteht dabei aus zwei Warmgangeinhausungen mit je 16 Racks, vier Reihenklimageräten und 80 kW Gesamtlast. „Sobald die ursprünglichen 16 Racks eines Cube voll bestückt sind, wird der Cube durch 16 weitere Racks erweitert. Diese haben bezüglich Stromversorgung, Klimatisierung, Rack-Aufteilung, Verkabelungs- und LAN-Infrastruktur den gleichen Aufbau wie die ersten 16 Racks. Dadurch reduziert sich der Planungsaufwand für Er-

Quelle: Cancom physical infrastructure

Detailansicht der Stromversorgung an der Oberseite der Racks (Abb. 2).

Quelle: Cancom physical infrastructure

Racks mit Servern und Switches im neuen Rechenzentrum der WISAG (Abb. 3).

weiterungen erheblich“, erklärt Christian Steininger. Dasselbe gilt analog, wenn weitere Cubes dazukommen.

Planung und Ausstattung aller weiteren Gewerke im Datacenter übernahm ebenfalls Cancom. Oliver Baake, Projektleiter IT bei der WISAG, hebt besonders die Bedeutung der Verkabelung hervor. „Bei der gewachsenen Sternverkabelung im alten Rechenzentrum mussten wir die Leitungen teilweise mehrere Meter über den Boden ziehen. Deshalb schwebte uns für den Neubau eine Top-of-Rack-Verkabelung vor“, erläutert Baake. Diese stellte sich jedoch als zu teuer heraus. Der Dienstleister habe dafür jedoch eine elegante Alternative gefunden, so Futterer: „Wir haben jetzt eine Kombination aus Top-of-Rack- und Sternverkabelung, die wir ‘Top-of-Rack in einem Rack’ nennen. Damit können wir vom Top-of-Rack-Switch direkt auf das Panel patchen, was uns eine flexible und übersichtliche Verkabelung innerhalb des Schranks ermöglicht.“

Zeitplan und Umzug

Die ersten Gespräche zwischen der WISAG und Cancom fanden im November 2011 statt. Im Februar 2012 wurde der Auftrag für den Rechenzentrumsbau erteilt. Seit November 2011 arbeitet der Dienstleister schon daran, die IT-Systeme des Kunden auf den Umzug vorzubereiten. Denn als Cancom physical infrastructure im Sommer 2012 mit dem Bau des Rechenzentrums begann, stand der Umzugstermin bereits fest. Spätestens am 8. Dezember 2012 musste es so weit sein, da der Mietvertrag der alten Räume zum Jahresende gekündigt werden sollte.

Quelle: Cancom physical infrastructure

Michael Futterer, Leiter Informationssysteme und Prokurist, WISAG (Abb. 4)

Aufgrund von baulichen Verzögerungen bei der Sanierung des Gebäudes musste das Team von Christian Steininger den EN-1047-2-zertifizierten IT-Sicherheitsraum, der das neue Datacenter aufnehmen sollte, in der entkernten Fläche des Stockwerks errichten. „Dadurch musste während der Arbeiten immer wieder der Staub abgesaugt werden, der durch die gleichzeitigen Trockenbauarbeiten entstand“, beschreibt Jörg Rummel die besondere Herausforderung.

Die langfristige Vorbereitung des Umzugs mit Beschriftung und Dokumentation aller Server erwies sich als richtige Strategie, denn aufgrund der starken Dynamik des Dienstleistungsunternehmens WISAG kam es auch in der vorher definierten „Frozen Zone“ vor dem Umzug noch zu Veränderungen der Systeme. Der Servicegedanke der WISAG machte es auch unmöglich, für den Umzug einen zusätzlichen Werktag als Downtime vorzusehen: Alles musste zwischen Freitagabend und Sonntagabend über die Bühne gehen.

Um das zu schaffen, waren rund 60 Cancom-Mitarbeiter im Dreischichtbetrieb im Einsatz. „Wir mussten Fachleute aus laufenden Projekten in ganz Deutschland holen, und das sehr kurzfristig, weil das definitive Go der WISAG für den Umzug erst kurz vor dem Start erfolgte“, erklärt Jörg Rummel.

Tatsächlich ging es dann am Freitag, den 17. November los. Am Abend wurden sämtliche Systeme der WISAG heruntergefahren, Cancom-Berater bauten die Systeme in der Kennedyallee ab, der beauftragte Logistiker fuhr sie in die Herriotstraße. Der Aufbau durch das Team am Zielort ging so schnell vonstatten, dass bereits am Samstag um 13 Uhr die ersten Server hochgefahren werden konnten. Nach Lasttests durch den Dienstleister und Key-User-Tests durch die WISAG war der Umzug bereits am Samstag um 17 Uhr erfolgreich erledigt.

„Der generalstabsmäßig geplante Umzug des Rechenzentrums in einer Nacht war eine Wahnsinnsleistung“, betont Michael Futterer. Technische Probleme seien praktisch keine aufgetreten, lediglich die belegten Brötchen seien irgendwann ausgegangen. „Daraufhin hat Herr Wisser kurzerhand mitten in der Nacht für das Team gekocht“, erinnert er sich schmunzelnd. Michael Wisser, der die WISAG-Gruppe führt, war von der professionellen und partnerschaftlichen Zusammenarbeit sichtlich beeindruckt.

Gerald Fiebig
Fachjournalist, Augsburg

Category 8 gibt Rätsel auf

Neuer Verkabelungsstandard verwirrt durch seine Bezeichnung

Kürzlich wurde ‘Category 8’ als Bezeichnung für das symmetrische Twisted-Pair-Kupferverkabelungssystem der nächsten Generation gewählt. Cat 8 soll Datenraten von 40 Gbit/s im Rechenzentrum (RZ) über eine Distanz von bis zu 30 Metern unterstützen. Was steckt hinter der Category 8 und Kategorie 7/7A und warum droht eine Verwechslung mit den traditionellen Bezeichnungen der ISO/IEC Gremien?

Verantwortlich für den Standard ist der Unterausschuss für Kupferverkabelung TR-42.7 der TIA. Category 8 weicht hinsichtlich der Topologie vom gängigen 4-Connector Channel-Modell ab, welches für Ethernet-Anwendungen bis 100 Meter geeignet ist. Mit den Anpassungen soll ein Kompromiss zwischen dem Stromverbrauch der Transceiverchips in den neuen Anwendungen und der Übertragungsreichweite im RZ gefunden werden.

Das ANSI/TIA-568-C.2-1-Projekt zur Ausarbeitung der Spezifikationen für ein Verkabelungssystem, das Datenraten von 40 Gbit/s unterstützt, wurde bereits Anfang 2011 in Angriff genommen. Dennoch hat sich der Unterausschuss für die Kupferverkabelung TR-42.7 der TIA bei der Namensvergabe erst Ende 2012 für ‘Category 8’ entschieden.

Bislang bauten die Verkabelungskategorien stets aufeinander auf, was bedeutet, dass die nächsthöhere Kategorie/Klasse alle elektrischen und mechanischen Anforderungen der vorangehenden erfüllt beziehungsweise übertrifft und zur leistungsschwächeren Kategorie/Klasse abwärtskompatibel ist. TIA spezifizierte Verkabelungssysteme bis zur Kategorie 6A/Klasse EA und beschloss dann, die Kategorie 7/Klasse F beziehungsweise 7A/Klasse FA, wie sie von der ISO/IEC verabschiedet wurde, nicht zu übernehmen.

Stattdessen entschied sich die TIA, ihr Verkabelungssystem der nächsten Generation mit ‘Category 8’ zu bezeichnen, um einer Verwechslung mit den von ISO/IEC herausgebrachten Kategorie 7 und Kategorie 7A Standards, die vollständig aufeinander aufbauen und wirkliche Obermengen voneinander und der Kategorie 6A sind, aus dem Wege zu gehen.

Keine Obermenge von Cat 7A

Zwar beschreiben die Spezifikationen der Category 8 recht vorsichtig eine Grenzfrequenz bis 2 GHz, während ISO/IEC für die Kategorie 7A Anforderungen bis 1 GHz definiert. Fakt jedoch ist, dass die gegenwärtig vorgeschlagenen Leistungsgrenzen der Category 8 weder an die Anforderungen der Kategorie 7A bis 1 GHz herankommen noch diese übertreffen.

Genau hier liegt das Rätsel begründet: Die Category 8 soll eine andere Channeltopologie aufweisen und wird keine Obermenge der Kategorie 7A sein. In der Tat sind die Grenzwerte der ISO/IEC für den Kategorie-7A-Channel und den Permanent Link bei jedem Kennwert für die Übertragungsleistung, mit Ausnahme der Rückflussdämpfung, strenger als bei den vom TIA-Unterausschuss TR-42.7 vorgesehenen Grenzwerten für die Category 8 bis 1 GHz. Insbesondere in Hinblick auf die Crosstalk-Werte des Kabels sind signifikante Unterschiede vorhanden. Die Kategorie 7A übertrifft die Category 8 hier um den stolzen Wert von mehr als 20 dB.

Wie sieht es nun mit der Bandbreite aus? Während die Kategorie 7A gegenwärtig bis 1 GHz spezifiziert ist, wird die Grenzfrequenz und damit die Bandbreite mit den neuen Ausarbeitungen (wie der fast finalisierten dritten Ausgabe des Standards IEC 61076-3-104 für die Stecksysteme der Kategorie 7A) auf 2 GHz erweitert. Die Situation, die dann entsteht – zwei Verkabelungsspezifikationen sind bis 2 GHz definiert und Category 8 bietet eine weitaus geringere Performance als Kategorie 7A –, wird mit Sicherheit so einige Verwirrung stiften.

Das Problem mit der Namensvergabe für das Verkabelungssystem der nächsten Generation hat nicht nur die TIA. Auch ISO/IEC stand vor der gleichen Herausforderung bei ihrem neuen Projekt, zwei neue Übertragungsstreckenklassen mit unterschiedlicher Schirmung der Verkabelung (geschirmt und voll geschirmt) zur Unterstützung von 40 Gbit/s zu definieren. ISO/IEC entschied sich kürzlich für Klasse I, um eine Verkabelung zu bezeichnen, die aus geschirmten modularen Kategorie-8.1-Komponenten im RJ45-Format besteht, und Klasse II für eine Verkabelung mit voll geschirmten Kategorie-8.2-Komponenten.

Quelle: Siemon

Nach wie vor die derzeit leistungsfähigsten Twisted-Pair-Verkabelungssysteme: voll geschirmte Kupferkabel der Kategorie 7A

Zur Verteidigung der TIA sei gesagt, dass es bei einer alternativen Namensvergabe mit Sicherheit zu einer Abweichung von der gewohnten Nummerierungskonvention der Kategorien gekommen wäre. Die Folge: ein ebenso unangenehmer Beigeschmack. Die Entscheidung der TIA wurde nicht von heute auf morgen gefällt, und man kann sagen, dass aus einer Handvoll höchst unattraktiver Varianten noch die beste herausgesucht wurde.

Wichtig zu verstehen ist, dass die einstige goldene Regel „höhere Kategorien sind Obermengen der niedrigeren Kategorien“ durchbrochen wurde. Bevor allerdings die Übertragungskapazität einer 40-Gigabit- Ethernet-(40GBASE-T)-Anwendung endgültig feststeht, ist es verfrüht, eine bestimmte Reichweite bei 40GBASE-T-Anwendungen für irgendein Medium zu garantieren. In jedem Fall bleiben voll geschirmte Kategorie-7A-Lösungen die derzeit leistungsfähigsten Twisted-Pair-Verkabelungssysteme. Dabei bieten diese Lösungen nicht nur eine bessere Abschirmung gegen EMI/RFI und flexiblere Möglichkeiten für das Cable Sharing als Lösungen mit RJ45-Steckverbinder, sondern ISO/IEC arbeitet auch beflissen an einem Projekt, das die Kapazität der bestehenden Kategorie-7A-Verkabelung in Hinblick auf eine Datenübertragung mit 40 Gbit/s auslotet.

Valerie Maguire
Director of Standards and Technology, Siemon

Höchste Kühlleistung auf geringer Fläche

Klimatisierung anspruchsvoller Rechenzentren

Hochleistungsrechner tragen erheblich zur Sicherung des Wissenschaftsstandortes Deutschland bei. In Rheinland-Pfalz wurde Ende 2012 ein neuer Supercomputer an der Technischen Universität Kaiserslautern in Betrieb genommen, mit einer für diesen Leistungsbereich speziell entwickelten Kühllösung.

SuperMUC, JuQueen, Hermit, Mogon, Elwetritsch: Hochleistungsrechnen ist aus Wissenschaft und Forschung nicht wegzudenken. In der Grundlagenforschung und in der Entwicklung neuer Stoffe und Verfahren werden Vorgänge, beispielsweise die Ausbreitung von Wellen, mittels leistungsstarker Rechner simuliert und modelliert. In der Biologie werden Proteine analysiert, in der Klimaforschung die Auswirkungen von Veränderungen bei Niederschlagsmengen oder Temperatur durchgespielt.

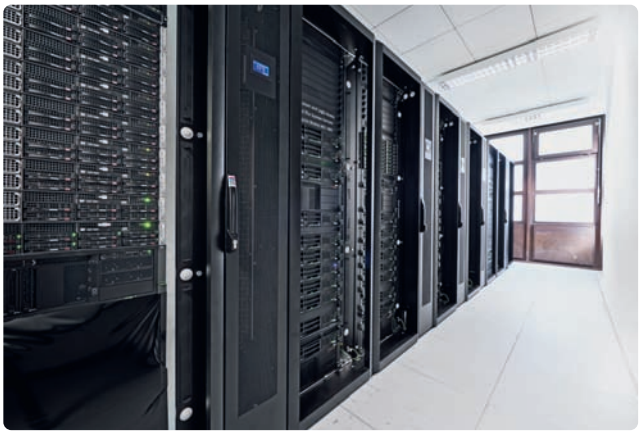
Um Deutschland als Standort für Spitzenforschung zu stärken, entstehen bundesweit an Forschungseinrichtungen und Hochschulen Rechenzentren für High Performance Computing (HPC). In Rheinland-Pfalz koordinieren über die Allianz für Hochleistungsrechnen Rheinland-Pfalz (AHRP) die Universitäten Kaiserslautern und Mainz das Schaffen und Bereitstellen dieser Ressourcen. Ihr Beitrag zur Superrechner-Landschaft sind die Zwillingscomputer Mogon an der Johannes Gutenberg-Universität Mainz und Elwetritsch an der Technischen Universität Kaiserslautern, die über eine 13×10-GBit-Glasfaserverbindung ihre Rechenleistung bündeln können.

Nach dem Fertigstellen von Mogon im Sommer 2012 sollte mit Elwetritsch, benannt nach dem in der Pfalz beheimateten Fabelwesen, die Rechenkapazität für die Hochschulen und Forschungseinrichtungen in Rheinland-Pfalz aufgestockt werden. Ziel war es, die kleinen Einheiten von ein bis drei Racks in den jeweiligen Arbeitsgruppen des Standortes zusammenzuführen beziehungsweise abzulösen.

Beim Aufbau der neuen HPC-Infrastruktur an der TU Kaiserslautern lag zunächst der Gedanke nahe, die schnellen Rechner in das bestehende Rechenzentrum zu integrieren. „Dafür reichte jedoch zum damaligen Zeitpunkt der Platz nicht aus“, sagt Heiko Krupp, Wissenschaftlicher Mitarbeiter am RHRK der TU Kaiserslautern und verantwortlich für die Infrastruktur im Bereich Rechenzentrum. „Außerdem benötigen Hochleistungsrechner sehr viel Kühlung. Dafür hätte das Rechenzentrum unter laufendem Betrieb umgebaut werden müssen, was nachteilig für dessen Betriebssicherheit gewesen wäre.“

Höchste Kühlleistung auf 65 Quadratmetern

Die TU Kaiserslautern entschied sich daher, einen größeren Infrastrukturraum in der Nähe des bestehenden Rechenzentrums zu benutzen und umzubauen. Mit rund 65 Quadratmetern war er gerade groß genug, dass er Racks mit insgesamt 650 Höheneinheiten aufnehmen konnte. Bei der dichten Packung der Rechner auf dem begrenzten Raum sollte die Kühlleistung 200 bis 250 kW betragen, und damit genauso viel wie für das bestehende Rechenzentrum auf einer mehr als fünfmal so großen Fläche. Damit keine Verzögerungen entstehen, weil



Quelle: Rittal

Mit rund 65 Quadratmetern war der ehemalige Infrastrukturraum gerade groß genug, dass er Racks mit insgesamt 650 Höheneinheiten aufnehmen konnte (Abb. 1).

Quelle: Rittal

Elwetritsch schafft aktuell 53 Billionen Rechenoperationen pro Sekunde auf 240 Rechnern und hat einen Energiebedarf von 110 kW (Abb. 2).

Quelle: Rittal

Jedes LCP ist an eine Leitung für Kalt- und für Warmwasser angeschlossen. Die Wasserleitungen verlaufen im Doppelboden des Rechenzentrums und sind an die Klimatechnik der TU Kaiserslautern angeschlossen (Abb. 3).

DER SUPERRECHNER ELWETRITSCH

Der Hochleistungsrechner „Elwetritsch“ an der TU Kaiserslautern bildet zusammen mit „Mogon“ an der Universität Mainz das Supercomputer-Cluster für die Hochschulen und Forschungsinstitute in Rheinland-Pfalz. Die Landesregierung von Rheinland-Pfalz, die Deutsche Forschungsgemeinschaft (DFG) und die TU Kaiserslautern investierten knapp zwei Millionen Euro in die erste Ausbaustufe von Elwetritsch.

Das Cluster ist in die Allianz für Hochleistungsrechnen Rheinland-Pfalz (AHRP) eingebunden und wird vorwiegend von naturwissenschaftlichen Fachbereichen und Arbeitsgruppen für Simulations-Aufgaben genutzt. Elwetritsch schafft aktuell 53 Billionen Rechenoperationen pro Sekunde auf 240 Rechnern und hat einen Energiebedarf von 110 kW. Eine zweite Ausbaustufe wird voraussichtlich bis Ende 2013 in Betrieb gehen.

Komponenten unterschiedlicher Hersteller aufeinander abgestimmt werden müssen, war der TU Kaiserslautern außerdem wichtig, dass die neue HPC-Infrastruktur als Systemlösung umgesetzt wird.

Mehr Höheneinheiten nutzbar

Rittal beteiligte sich an der Ausschreibung und erhielt den Auftrag. Nach Mogon in Mainz, für den Rittal kurz zuvor die Hochleistungs-Klimatisierung realisiert hatte, waren die Lösungen des Anbieters auch für den Zwillingsrechner gefragt. Das liegt zum einen daran, dass Rittal alle geforderten Komponenten aus einer Hand anbieten kann, von Klimalösung und Doppelboden über Gangeinhausung und Racks im Sonderformat bis zum Monitoring-System. „Zum anderen“, so Krupp, „hat uns Rittal eine High-Performance-Kühlung vorgeschlagen, die unserem Rechenzentrum die erforderliche Leistung und Redundanz auf geringer Fläche zur Verfügung stellt.“ Bei der Kühllösung handelt es sich um Klimageräte der Baureihe Liquid Cooling Package (LCP) mit Luft/Wasser-Wärmetauscher, die kaum mehr als einen Drittel Quadratmeter Stellplatz brauchen.

Innerhalb von drei Monaten erfolgte der Umbau des Raumes und die Installation der Racks und Klimainfrastruktur. Zunächst mussten die bisherige Infrastruktur des Raumes entfernt und dann neue Versorgungssysteme für Strom und Wasser eingebaut werden. Die Führung der Kaltluft erfolgt nicht über den Doppelboden zu den Server-Schränken, sondern wird von den LCPs, die in den Rack-Reihen zwischen den Server-Schränken aufgestellt sind, über die gesamte Höhe ausgeblasen. „Die Kaltluft verteilt sich gleichmäßig nach rechts und links über die Fronten der benachbarten Racks mit dem Ergebnis, dass wir alle Höheneinheiten ohne Gefahr der Bildung von Hotspots nutzen können“, sagt Krupp. „Auf diese Weise ermöglicht uns die Lösung, dass wir eine größere Anzahl von Rechnern unterbringen, als wir ursprünglich veranschlagt hatten.“

Die 16 Racks wurden in zwei Reihen à acht Racks angeordnet, dazwischen in jeder Reihe fünf Klimaschränke. Für höchste Verfügbarkeit legte Rittal die Anzahl, Leistung und die Verteilung der LCPs auf die Rack-Reihen in einer „n+1“-Konfiguration fest. Beim Aufstellen der Racks war zu berücksichtigen, dass sich in dem neuen Rechenzentrum nicht nur Server und Klimageräte befinden, sondern auch die USV-Anlagen und die Elektroverteilung. „Wir mussten verhindern, dass die Raumtemperatur über 22 Grad Celsius steigt und die Funktionsfähigkeit der anderen Rechenzentrumskomponenten beeinträchtigt oder ihre Lebenszeit verkürzt“, erläutert Krupp. Rittal ordnete die Racks in Warmgang-Aufstellung an und schottete den Gang ab, in dem die Lufttemperatur bis auf 50 Grad Celsius steigen kann.

Trennung von Elektronik und Wasser

Um solche hohen Temperaturen abzuführen, gibt es keine effizientere Lösung, als die physikalischen Eigenschaften von Wasser zur Wärmeabfuhr zu nutzen. Die an der Server-Rückseite abgegebene Warmluft wird von den LCPs angesaugt und über den Luft/Wasser-Wärmetauscher abgekühlt. Die gekühlte Luft wird dann auf der Vorderseite in Racks abgegeben. Dabei sind Wasserkreislauf und Elektronik durch die Unterbringung in unterschiedlichen Schränken vollständig voneinander getrennt. Komponenten im Rack können nicht mit austretendem Wasser in Berührung kommen. Leckage-Sensoren in den LCPs erkennen einen Defekt im Wasserkreislauf sofort und melden ihn über ein Sicherheitssystem an einen Techniker.

Jedes LCP ist über die im Doppelboden verlaufende Verrohrung an die zentrale Kühlwasserversorgung der Klimatechnik der TU Kaiserslautern angeschlossen. Die Vorlauftemperatur beträgt zirka 10 Grad Celsius und erwärmt sich in den LCPs auf zirka 17 bis 23 Grad Celsius. Durch den sehr gezielten Einsatz der Kaltluft in LCPs könnten die Vorlauftemperaturen im Wasserkreislauf sogar bis auf 21 Grad Celsius erhöht und so eine effizientere Klimatisierung durch Ausdehnen der Freikühlzeit erreicht werden. „Energieeinsparungen durch höhere Vorlauftemperaturen spielen für uns noch keine Rolle“, sagt Krupp. „An einer technischen Universität wird sehr viel Kälte benötigt, beispiels-

Quelle: Rittal

Innerhalb von drei Monaten erfolgte der Umbau des Raumes und der Installation des Rechenzentrums bei der TU Kaiserslautern (Abb. 4).

Quelle: Rittal

Die Racks sind in Warmgang-Aufstellung angeordnet, so dass der Gang abgeschottet ist, in dem die Lufttemperatur bis auf 50 Grad Celsius steigen kann (Abb. 5).

weise um in der Chemie spezielle Laborräume zu klimatisieren. Das Rechenzentrum ist dabei nur ein Verbraucher unter vielen.“ Um den Stromverbrauch für den gesamten Bereich der Klimatisierung zu senken, soll ab Ende 2013 die Kälteversorgung auf freie Kühlung umgestellt werden.

Rechenreserven für das Bundesland

Nach der Installation aller anderen Komponenten und den Tests für Server, Dateisysteme und Software hat Elwetritsch im Dezember 2012 den Betrieb aufgenommen und steht der TU Kaiserslautern und den anderen Hochschulen und den Forschungseinrichtungen des Landes Rheinland-Pfalz offen. „Aus den Fachbereichen, die ihre Systeme zugunsten der Clusterlösung aufgegeben haben, kamen prompt positive Rückmeldungen“, sagt Krupp. „So ein hochmodernes Linux-Cluster mit mehr als 200 Rechenknoten erledigt die Großaufträge spürbar schneller als die bisherigen Einzelsysteme.“

Auch Reserven für weiteres Wachstum sind vorhanden: Aktuell sind fünf der 16 Racks nicht belegt. Krupp zufolge reicht der Platz in jedem Fall bis Ende des Jahres 2013. Bis dahin wird voraussichtlich die zweite Ausbaustufe des Clusters fertiggestellt. Auch hinsichtlich der Kühlleistung gibt es noch Spielraum. Von den 250 kW, die die Rittal-Lösung abfahren kann, werden derzeit 95 kW, bei voller Auslastung der Rechner 115 kW in Anspruch genommen. Wenn die verbleibenden fünf Racks ebenfalls gefüllt sind, rechnet Krupp mit einer Steigerung auf 150 kW, immer noch deutlich unterhalb der Leistungsgrenze. Ein Monitoring-System hält ihn über alle Werte der Klimalösung auf dem Laufenden. „Um Hotspots oder Serverausfälle infolge von Überhitzung muss ich mir absolut keine Gedanken machen“, fasst Krupp seine Erfahrungen mit der Klimalösung zusammen.

Michael Nicolai
Abteilungsleiter Technischer Projektvertrieb, Rittal, Herborn,
Patricia Späth
PR-Referentin IT, Rittal, Herborn

(R)Evolution im Rechenzentrum

Goethe-Universität implementiert QFabric-Architektur

Die Goethe-Universität in Frankfurt am Main geht beim Aufrüsten der Computing- und Speicherelemente einen Schritt weiter, als es bei herkömmlichen Upgrades üblich ist: Als erstes Rechenzentrum in Deutschland setzt sie das QFabric-System ein, revolutioniert damit gleich die gesamte Netzwerktopologie ihres Rechenzentrums und verbessert die Performance um ein Vielfaches. Ein Blick hinter die Kulissen.

An der Frankfurter Universität sind derzeit mehr als 41.000 Studenten eingeschrieben und über 4.500 Mitarbeiter beschäftigt. Damit ist sie die drittgrößte Hochschule in Deutschland. Aufgrund der stetigen Zunahme der Studentenzahlen bezog die Universität vor kurzem einen größeren Campus. Dies nahm die IT-Abteilung zum Anlass, das Hochschulrechenzentrum nicht nur räumlich vom alten Standort Bockenheim zum neuen im Westend umziehen zu lassen, sondern auch strukturell von der klassischen hierarchischen Architektur in eine Fabric-Topologie zu wandeln. „Das war Herausforderung und Chance zugleich“, erinnert sich Ast. „Einerseits hat die QFabric unsere Anforderungen am besten erfüllt, andererseits erfordert ein so komplexes Projekt immer einen sehr hohen Aufwand. Ohne die Unterstützung durch den Service Integrator Xantaro, in dessen Frankfurter XT3Lab wir Komponenten und Netzdesigns testen konnten, hätten wir die Migration nur schwer geschafft.“

Die Virtualisierung von Servern und Speichern hat die Effizienz von Rechenzentren gesteigert. Die QFabric-Technik von Juniper Networks hingegen bietet Anwendern noch mehr als nur Effizienzsteigerungen. Sie behandelt Computing-, Speicher-, Service- und Netzwerkressourcen des Datacenters als austauschbare Pools, die dynamisch untergliedert werden können, ohne Infrastruktur oder Anwendungen zu beeinflussen. Zudem lassen sich die Ressourcen mit hohen Geschwindigkeiten und gleichzeitig geringer Latenz miteinander verbinden.

Diese Vorteile hat die Goethe-Universität in Frankfurt am Main erkannt und die Lösung als erster QFabric-Kunde in Deutschland gemeinsam mit dem Service Integrator Xantaro implementiert. „Die QFabric bietet uns ein klares Wachstumskonzept und eine gute Zukunftsperspektive für unser Datacenter“, sagt Dr. Hansjörg Ast, stellvertretender Leiter des Hochschulrechenzentrums. „Dank QFabric stoßen wir auf absehbare Zeit bei der Bereitstellung neuer Dienste oder höherer Kapazitäten an keine Grenzen mehr. Alle drei bis vier Jahre können wir nun eine Verdoppelung der Bandbreite und Anzahl der Services stemmen.“

Warum Junipers QFabric?

Die IT-Experten der Universität wollten im neuen Rechenzentrum eine möglichst schnelle, skalierbare und sichere Infrastruktur realisieren. Dies gewährleistet derzeit nur das Single-Hop-Konzept, bei dem zwischen Absender und Empfänger genau eine Zwischenstation liegt. Zudem sollte es ein technisch in sich geschlossenes System sein, das hochskalierbar ist und Kapazitäten beliebig an-

Foto: Mathias Brandstetter, Goethe-Universität Frankfurt

Die Universität Frankfurt hat als erster Anwender in Deutschland das komplette Netzwerk auf QFabric umgestellt (Abb. 1).

Foto: Jürgen Lecher

Mehr als 45.000 Studenten werden an der Universität Frankfurt ausgebildet (Abb. 2).

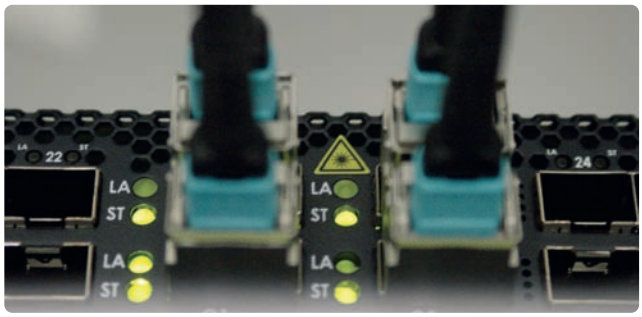


Foto: Mathias Brandstetter

QFabric-Nodes lassen sich als Einzel-Switches einsetzen (Abb. 3).

passbar macht. Nur zwei Hersteller hatten Lösungsangebote, die diese Anforderungen erfüllten – darunter Juniper Networks.

Die Entscheidung für die QFabric fiel schließlich aufgrund mehrerer Faktoren: Erstens sind die QFabric-Nodes – die sich am Rand des Systems befinden, um Zugang zur Fabric zu bieten – bi-funktionale Geräte, die auch als Einzel-Switches eingesetzt werden können. Dadurch lassen sich auch Gruppen, die ursprünglich eine andere Aufgabe hatten, nach Bedarf später in die größere Fabric integrieren. Außerdem bieten die dualen Persönlichkeitsmerkmale der Geräte Investitionsschutz, denn sie sorgen für eine Wiederverwendbarkeit der QFabric-Nodes als Einzel-Switch, wenn in der Fabric Geräte mit höherer Kapazität eingesetzt werden.

Tests in Amsterdam

Die QFabric ist eine neuartige Lösung – daher legte die Hochschule vor dem Einsatz in ihrem Rechenzentrum großen Wert auf umfangreiche Tests. Schließlich hängen tausende Studenten und Mitarbeiter mit ihren rund 40.000 PCs, Telefonen und mobilen Geräten von der einwandfrei funktionierenden Infrastruktur ab. Ohne Prüfung hätte niemand vorhersagen können, ob ein derart komplexes Netzwerk fehlerfrei läuft.

Ein Machbarkeitsnachweis der QFabric-Implementierung erfolgte im Juniper Networks Proof-of-Concept-Lab in Amsterdam. Entgegen kam der Universität darüber hinaus, dass im Frankfurter Xantaro-Labor ein QFabric-System und entsprechende Lastgeneratoren stehen. Hier spielten die Spezialisten der Universität in Zusammenarbeit mit den Experten von Xantaro zusätzlich diverse Szenarien durch, darunter das zur externen Netzwerkanbindung auf Basis verschiedener Router- und Firewall-Konfigurationen. Im Rahmen eines Beta-Testprogramms des QFX3000-M QFabric Systems, die kleinere der beiden QFabric-Lösungen, konnte das Hochschulrechenzentrum erste eigene Betriebserfahrungen sammeln und wertvolle Hinweise für die Weiterentwicklung geben.

Risiko und Chance

Die Tests haben sich gelohnt: Die Server-Systeme und ihre redundanten Anbindungen an die QFabric funktionieren. „Wir sind uns bewusst, dass wir sehr früh in die Fabric-Technik eingestiegen sind, aber wir sind zuversichtlich, die richtige Entscheidung getroffen zu haben“, sagt Hansjörg Ast. Eine Infrastruktur im Rechenzentrum, die komplett auf QFabric basiert, erfordert einen signifikanten Aufwand bei Planung, Installation und Verwaltung, weshalb umfangreiche Netzwerkkenntnisse nötig sind.

Da die gesamte QFabric-Installation sich wie ein einzelnes Gerät verhält, bestehen die Verbindungen zwischen den Servern aus einem Single-Hop. Dadurch ist deutlich weniger Absprache erforderlich und es gibt auch weniger Missverständnisse und Übertragungsfehler. Zudem zeigen sich die Services robust gegen Abbrüche in Fail-Over-Szenarien. Ein weiterer Vorteil von QFabric ist, dass VLANs systemweit eingerichtet werden können. Beispielsweise beim Umzug eines physischen oder virtuellen Servers wird eine neue Anbindung dann einfach auf den Ports konfiguriert anstatt auf allen Trunks zwischen den einzelnen Geräten des VLANs.

Nutzen für den Alltag

„Durch die QFabric erhalten wir eine hohe intrinsische Redundanz der Hardware und stellen damit die Hochverfügbarkeit vieler Services sicher“, sagt Hansjörg Ast. „Alle Netzwerk- und Steuergeräte sowie Daten- und Kontrollebenen sind doppelt vorhanden. Es müssten also jeweils mehrere identische Komponenten ausfallen, damit das System nicht mehr funktioniert.“

Da Dienste nicht von der Netzwerktopologie abhängen, liefert die QFabric immer die gleiche Dienstgüte – auch wenn diese innerhalb der virtualisierten Umgebung verschoben werden. Die Fehleranfälligkeit im täglichen Betrieb sinkt zudem, weil das Gerät Spanning-Tree-frei ist und vor fehlerhafter Verkabelung schützt.

Nach der vollständigen Umstellung vom alten auf das neue Rechenzentrum wird die Universität die Virtualisierung und Mandantenfähigkeit weiter ausbauen. So sollen in Zukunft einer Arbeitsgruppe bestimmte Portgruppen zugeordnet werden, inklusive eigenständiger Verwaltung. Damit kann sie beispielsweise Bandbreiten begrenzen oder die Auslastung der Ports kontrollieren. „Obwohl die QFabric hochentwickelt ist, kann sie dennoch von der internen IT-Abteilung bewältigt werden“, sagt Hansjörg Ast. „Wir haben im Prinzip einen Sack voll Switching-Hardware und Linux-basierter Serversysteme eingekauft, die als Gesamtsystem einwandfrei funktionieren. In Eigenregie hätten wir ein vergleichbares System nur schwer hinbekommen.“

Günter Unterholzner
Freier Autor

Kontrolle ist besser

Rack-Management-Systeme als Security-Tool

Wenn die Server im Rechenzentrum das Herz der Unternehmens-IT sind, dann sind die Racks der Brustkorb. Als unmittelbare Hülle der empfindlichen Geräte schützen sie diese sowohl vor schädlichen Umwelteinflüssen als auch vor unbefugtem Zugriff. Moderne Rack-Management-Systeme bieten für die IT-Security aber noch Möglichkeiten, die weit über die simple Mechanik des IT-Schranks hinausgehen.

Längst vorbei sind die Zeiten, in denen ein 19-Zoll-Rack einfach ein Schrank war, in dem man IT-Komponenten ordentlich verstaute: Mit dem Anwachsen der erforderlichen Rechenleistung ist auch in kleineren Unternehmen das Einzelrack mit einem einzigen Server zur Ausnahme geworden, der Trend geht zum Rechenzentrum. Aufgrund der wachsenden Packungsdichte, etwa durch moderne Bladeserver, werden aber Energiebedarf und Wärmemanagement auch in kleineren Serverräumen ein Thema. Fragen der betriebswirtschaftlichen Effizienz und Sicherheitsthemen sind hier eng verzahnt. Stromsparen (und zwar bei den Servern wie auch bei deren Infrastruktur, also beispielsweise der Klimatisierung) ist in Zeiten steigender Strompreise ein Gebot der wirtschaftlichen Vernunft. Das Vermeiden von Wärmeentwicklung durch Geräte mit geringer Leistungsaufnahme sowie die sinnvolle Abführung von heißer Luft ist aber auch eine wichtige Voraussetzung für den ausfallsicheren Betrieb der Server. Umgekehrt betrachtet fallen überhitzte Rechner nicht nur irgendwann aus, sondern stellen auch eine potenzielle Brandgefahr dar.

Überwachung physikalischer Parameter

Effiziente Klimatisierungskonzepte sind durchaus vorhanden, nicht nur für Großrechenzentren („Serverfarmen“) à la Google und Facebook, sondern inzwischen durchaus auch für den mittelständischen Serverraum. Doch jedes Konzept ist nur so gut wie seine praktische Umsetzung. Diese gilt es also lückenlos, aber zugleich mit möglichst begrenztem Aufwand zu überwachen. Hier überschneidet sich das Thema physische IT-Sicherheit mit dem Thema „Security“ im engeren Sinne: Der Zugang von Personen zum Rechenzentrum muss genauso überwacht werden wie die Temperatur in den Racks. Moderne Rack-Management-Systeme ermöglichen beides.

Quelle: Schäfer IT-Systems

Die gängige Bauform von Rack-Management-Hardware sind 19-Zoll-Geräte für den Einbau ins Rack, hier abgebildet sind die Vorderseite (oben) und die Rückseite eines typischen Geräts (Abb. 1).

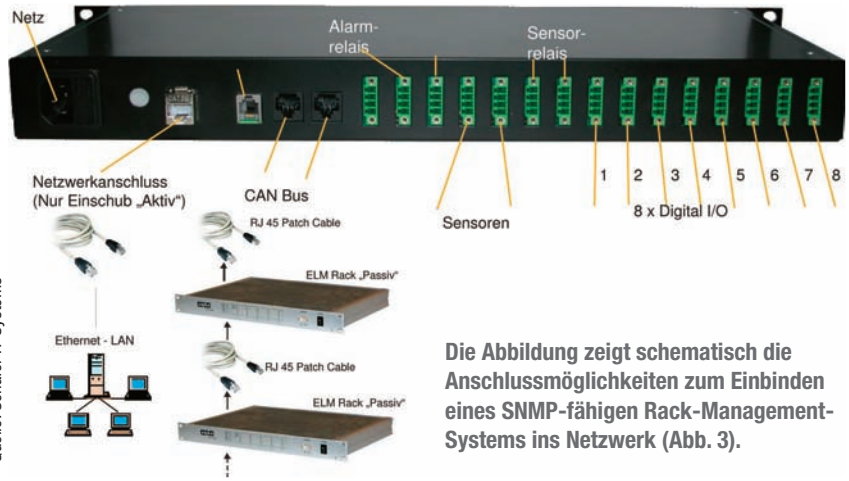
Quelle: Schäfer IT-Systems

Ein GSM-Modul im Rack ermöglicht die Alarmierung des verantwortlichen Administrators über Mobilfunk (Abb. 2).

Die zentrale Komponente eines Rack-Management-Systems (RMS) ist typischerweise ein 19-Zoll-Gerät, das selbst in den entsprechend genormten Serverschrank eingebaut werden kann. Hier laufen die Informationen zusammen, die von Sensoren unterschiedlichster Art innerhalb des Racks gesammelt werden. Für die Überwachung der physikalischen Parameter sind Temperaturfühler, Klimasensoren für die Überprüfung der Luftfeuchtigkeit und Rauchmelder unverzichtbar. Sie sollten zum Standardumfang jedes RMS gehören.

Durch das strategische Verteilen der Sensoren im Rack lässt sich ein differenziertes Gesamtbild der Bedingungen erstellen, unter denen die Server arbeiten. So sollten an allen bekannten „Hot Spots“, an denen beispielsweise die Heißluft aus den Servern austritt, Temperaturfühler installiert werden, um ein Überschreiten der Normaltemperatur möglichst früh zu erkennen. Zu hohe Luftfeuchtigkeit, die unter Umständen die Hardware schädigt, kann etwa auf ein Problem mit der Klimaanlage hindeuten, die unzureichend gefilterte Luft von außen zuführt. Rauchmelder im Rack wiederum sind für eine Brandfrühesterkennung wesentlich besser geeignet als deckenmontierte Geräte. Denn bis der Rauch aus dem Rack an die Decke des Serverraums aufgestiegen ist, dürften im Fall eines Brandes bereits gravierende Schäden aufgetreten sein. Bei modernen Kalt- oder Warmgangeinhausungen, in denen Server zwecks effizienterer Kühlung in einer separaten überdachten Zelle im Raum untergebracht werden, sind Rauchmelder an der Zimmerdecke sogar praktisch wirkungslos.

Damit ein RMS zukunftssicher bleibt, sollte es modular erweiterbar sein und analoge Eingänge zum Einbinden weiterer Sensoren bereitstellen. Um den Betrieb der gesamten IT-Anlage sicherstellen zu können, muss das RMS auch bei einem Stromausfall funktionsfähig sein. Seine Notstromversorgung sollte



Quelle: Schäfer IT-Systems

Die Abbildung zeigt schematisch die Anschlussmöglichkeiten zum Einbinden eines SNMP-fähigen Rack-Management-Systems ins Netzwerk (Abb. 3).

dabei auch die interne Spannungsversorgung für alle Sensoren gewährleisten, weil das System sonst im Fall eines Blackouts blind und taub wäre. Da auch das Betriebssystem des RMS besonders stabil und hochverfügbar sein muss, wird Linux in diesem Bereich immer populärer.

Kommunikation ist alles

Von entscheidender Bedeutung für die Wirksamkeit der Überwachung ist die Kommunikationsfähigkeit im Alarmfall. Wird ein vorher definierter Messwert über- oder unterschritten, muss der IT-Administrator schnellstmöglich informiert werden, um Gegenmaßnahmen ergreifen zu können. Neben einer lokalen Alarmierung am Rack, etwa über LEDs, besteht die Möglichkeit, über Schaltausgänge ein GSM-Modul anzubinden, das den zuständigen Rechenzentrumsverantwortlichen per SMS alarmiert.

Bei Einsatz von SNMP-(Simple Network Management Protocol)-fähigen Rack-Management-Systemen wird die Alarmierung zudem an die Netzwerkmanagement-Software übertragen. Diese steuert die Racks zentral, also beispielsweise das Abschalten von überhitzten Servern durch eine remote schaltbare Steckdosenleiste. Auch der Schaltvorgang selbst kann als automatisierte Reaktion auf den Alarmfall hinterlegt werden. Im genannten Beispiel erfolt das Abschalten dann zeitgleich mit dem Alarmieren des Personals. So werden Schäden vermieden, und der Administrator gewinnt Zeit für eine gründliche Fehlersuche.

SNMP hat sich als Standard für Rack-Management-Systeme weitgehend durchgesetzt. Ein RMS-Gerät, das dieses Protokoll nutzt, kann in alle gängigen Netzwerkmanagement-Plattformen eingebunden werden. Um die Fernüberwachung von mobilen Geräten zu vereinfachen, ist bei der Auswahl des RMS auf http-Unterstützung zu achten. So kann der Administrator auch außerhalb üblicher Bürozeiten von zu Hause oder unterwegs per Webbrowser auf die Systeme zugreifen.

Das Überwachen der physischen IT-Sicherheit ist die Kernaufgabe eines Rack-Management-Systems. Durchdachte Systeme unterstützen auch die IT-Security im engeren Sinne: Sie tragen dazu bei, unbefugte Zugriffe auf die Hardware zu verhindern. Damit folgen sie der Philosophie, dass die Sicherheit von Rechenzentren nur durch ganzheitliches Betrachten aller beteiligten Gewerke nachhaltig gewährleistet werden kann.

RMS warnt vor Eindringlingen

Prinzipiell setzt die Zugangskontrolle zu Rechenzentren bereits auf der Ebene des Serverraums ein. Nur Personen mit speziellen Befugnissen dürfen das Datacenter überhaupt betreten. In der Regel ist eine Identifizierung erforderlich, um Zugang zu den Räumlichkeiten zu erhalten, die meist videoüberwacht werden. Sollte sich ein Unbefugter, beispielsweise mit einer entwendeten Transponderkarte, jedoch tatsächlich Zugang zum Rechenzentrum verschaffen, hilft eine Videoüberwachung freilich nur dann, wenn sie auch permanent von jemandem kontrolliert wird. Das bedeutet einen erheblichen personellen Aufwand, der nicht in jedem Rechenzentrum betrieben werden kann. Zwar kann eine Videoaufnahme als Beweismittel vor Gericht genutzt werden, wichtiger aber wäre es, den Schaden bereits im Vorfeld zu verhindern.

Auch hier kann die Alarmierungsfunktion eines Rack-Management-Systems hilfreich sein. Türkontakt- und Erschütterungssensoren können ins Rack montiert und mit dem

RMS verbunden werden. Dabei sollte das RMS unterschiedliche Arten der Türkontaktsicherung unterstützen, also beispielsweise Profilhalbzylinder, aber auch Transponderkarten, die tastaturbasierte Eingabe von Zugangscodes oder die Verifizierung über ein Mobilgerät per GSM. Andernfalls müsste im Fall einer Änderung im Sicherheitskonzept, typischerweise wäre dies die Umstellung von Zylinderschlössern auf modernere, fälschungssichere Systeme, womöglich das RMS ausgetauscht werden.

Wird eine Racktür geöffnet, ist dies ein sicheres Anzeichen, dass sich jemand im Rechenzentrum aufhält und sich an den Schränken zu schaffen macht. Auch für diesen Fall kann eine Alarmfunktion definiert werden, die den zuständigen Administrator auf den Plan ruft oder eine Alarmanlage im Gebäude auslöst. Durch eine umgehende Kontrolle vor Ort kann eine Manipulation von Geräten durch Unbefugte womöglich verhindert werden. Müssen die Serverschränke hingegen für Wartungsarbeiten beziehungsweise Ein- oder Ausbau von Geräten geöffnet werden, kann der Administrator mit seinen Zugriffsrechten auf der Netzwerkmanagement-Plattform die Alarmierung vorübergehend außer Kraft setzen. Nach Abschluss der Arbeiten wird sie dann wieder aktiviert.

Ein professionelles Rack-Management-System bietet jedoch noch eine zweite Ebene der Sicherung. Die Geräte sollten über eine integrierte Benutzerverwaltung verfügen, bei der man sich mit einem Passwort anmelden muss. Ohne ein solches Passwort kann ein Unbefugter, auch wenn er bis zum Rack vorgedrungen ist, keine Einstellungen an dem System verändern.

Mit der Security-Funktion der Türkontaktksensoren schließt sich der Kreis zu den Kernfunktionen des RMS beim Überwachen der physikalischen Parameter. Denn offen stehende Racktüren sind auch dann unerwünscht, wenn sie nicht von einem Eindringling verursacht werden, sondern „nur“ von einem defekten Kontakt. Weil das Abdichten der Racks für den effizienten Kreislauf von warmer und kalter Luft in den Schränken von zentraler Bedeutung ist, hilft ein Alarm auch in einem solchen Fall, das Problem schnellstmöglich zu beheben.

Moderne Rack-Management-Systeme bieten vielfältige Unterstützung für den ausfall- und zugriffssicheren Betrieb von Rechenzentren. Je nach Größe und Lage des Rechenzentrums wird der Anwender unterschiedliche Gewichtungen auf die unterschiedlichen Features legen. Ihr volles Potenzial realisieren die Systeme aber nur, wenn man sie im Rahmen einer ganzheitlichen Planung des Datacenters betrachtet. Es ist daher empfehlenswert, sich bei der Auswahl eines RMS von Anbietern mit umfassendem Know-how im Rechenzentrumsbereich beraten zu lassen.

Peter Wäsch
Vertriebsleiter, Schäfer IT-Systems

Impressum
Themenbeilage Rechenzentren & Infrastruktur

Redaktion just 4 business GmbH
Telefon: 080 61/348 96 90, Fax: 080 61/348 96 99,
E-Mail: tj@just4business.de

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

Autoren dieser Ausgabe:
Gregory Blepp, Gerald Fiebig, Dave Greenfield, Valerie Maguire, Michael Nicolai, Bernd Reder, Marius Schenkelberg, Joachim Stephan, Kathrin Strübe, Günter Unterholzner, Peter Wäsch

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

Korrektorat:
Silke Peters

Technische Beratung:
Uli Ries

Titelbild:
© Michael Osterrieder – Shotshop.com

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

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung:
Beate Gerold

Verlagsleiter:
Dr. Alfons Schräder

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

Assistenz:
Stefanie Frank -205, E-Mail: stefanie.frank@heise.de

Anzeigendisposition und Betreuung Sonderprojekte:
Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf:
PLZ-Gebiete 0 – 3, Ausland: Tarik El-Badaoui -395, E-Mail: tarik.el-badaoui@heise.de,
PLZ-Gebiete 7 – 9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de

Anzeigen-Inlandsvertretung:
PLZ-Gebiete 4 – 6: Karl-Heinz Kremer GmbH, Sonnenstraße 2,
D-66957 Hilst, Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22,
E-Mail: karlheinz.kremer@heise.de

Teamleitung Herstellung:
Bianca Nagel

Druck:
Dierichs Druck + Media GmbH & Co. KG, Kassel

Die Inserenten

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

clouD – der Clou ist das D.

clouD

SAFE IN GERMANY

Dürfen wir Ihnen clouD vorstellen?

clouD ist unsere neue Hosting-Innovation. Erweitern Sie ab sofort flexibel Ihre Ressourcen mit der sicheren **clouD** von Thomas Krenn.
Ihre Daten werden ausschließlich in Deutschland gehosted. Die Leistung ist sofort verfügbar, dabei flexibel zuschaltbar und stundengenau abrechenbar. Die Qualität ist auf unserem gewohnten Premium Niveau – durch VMware Software auf Basis von VMware Enterprise Plus. Das ist unsere **clouD** – safe in Germany.

clouD – mehr Platz für Ihre Bedürfnisse.

- Sicheres Hosting in Deutschland
- Einfach Leistung zuschalten
- Keine Kapitalbindung
- Sofort verfügbar
- Premiumqualität
- Hohe Performance
- Professionell, geschützt und kosteneffizient
- Keine Einrichtungsgebühr
- VMware Software auf Basis von VMware Enterprise Plus

QR Code mit Smartphone scannen oder
www.thomas-krenn.com/clou_d

hosting@thomas-krenn.com

Thomas-Krenn.AG®
Die Server-Experten

ERLEBEN SIE UNS LIVE:

it-sa 2013
IT-Security Messe,
08.-10.10.2013, Nürnberg,
www.it-sa.de

SNW – Powering the cloud
29.-30.10.2013, Frankfurt,
www.poweringthecloud.com

DER BESTE GRUND, ENTSPANNT ZU BLEIBEN.

ROSENBERGER OSI CABLING COMPETENCE.

Verkabelungssysteme bilden das Rückgrat jedes Rechenzentrums. Rosenberger OSI steht für effiziente und maßgeschneiderte Cabling-Lösungen aus einer Hand: von der Beratung über die Installation bis hin zur Wartung und Dokumentation. Mit umfassendem Know-how und High-Quality-Komponenten – für eine sichere Infrastruktur und den reibungslosen Ablauf aller Prozesse.

www.rosenberger-osi.de

Rosenberger OSI®