Eine Themenbeilage der
Heise Zeitschriften Verlag GmbH & Co. KG

III
2014

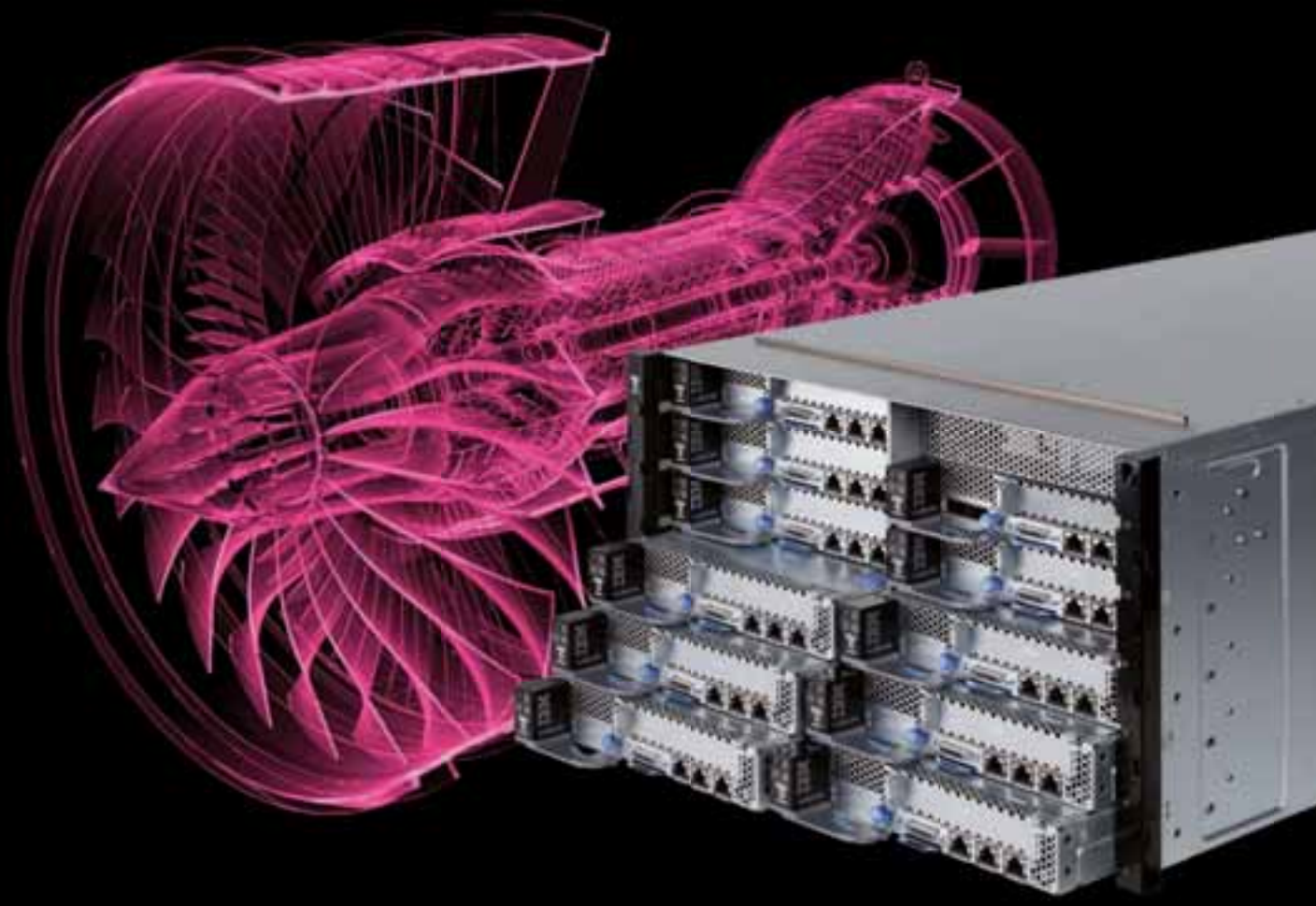
RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Warum Rechenzentren nie sicher genug sind

www.rechenzentren-infrastruktur.de

powered by: iX



Remote zum Konstruktionserfolg

Konstruieren Sie auch als Remote-User flexibel & sicher im Team.

- Performanter Remote-Zugriff mit Citrix HDX-Technologie auf GPUs im Datacenter
- Hohe Leistungsdichte und flexible Erweiterbarkeit des IBM NeXtScale-Systems
- Sicherheit der Konstruktionsdaten durch Verbleib der Daten im Rechenzentrum

Alle Informationen zu Remote-Visualisierung unter:
www.transtec.de/go/3d

intel inside XEON

Intel® Xeon® Prozessor

transtec

Warum Rechenzentren nicht sicher genug sein können

Hand auf's Herz: Hätten Sie es gewusst? Einer uralten Studie zufolge gehen 93 Prozent der Firmen, deren Server für mehr als zehn Tage ausfällt, innerhalb eines Jahres Konkurs. Zugegeben, diese Zahl betraf im Wesentlichen die Festplatten eines Servers, die i.d.R. noch zu retten wären, wenn man sie einem professionellen Datenretter überlässt. An der brutalen Tendenz dieser Zahl dürfte sich jedoch bist heute kaum etwas geändert haben.

Wer seine Daten so gut wie komplett einem Rechenzentrum überlässt, hat gute Gründe, ihre Sicherheit gegenüber Angriffen, Unfällen und Störungen von außen und innen zu hinterfragen. Das fängt beim vermeintlich simplen Brandschutz an und endet bei Denial-of-service-Attacken – womit wir beim Fahrplan dieser Ausgabe wären: Das Rechenzentrum des Niedersächsischen Landtags schützt sich zum Beispiel durch aktive Sauerstoffreduzierung vor Bränden, schreibt Katharina Bengsch auf Seite 6. Durch Brandvermeidung soll die Datenverfügbarkeit eben auch im Brandfall sicher gestellt sein. Doch was tun, wenn's brennt? Ein automatisiertes Notfallhandbuch soll optimale Unterstützung in Ausnahmesituationen bieten, wissen Wilfried Cleres und Klaus Pfeiffer (Seite 10).

Ein großes Problem – nicht nur im Störfall – ist die Gewährleistung der Energieversorgung. Deshalb ist es wichtig, die passenden Stromverteilungsleisten zu finden. Welche Arten es gibt, fasst Carrie Higbie auf Seite 13 zusammen.

Kommen wir zur Remote-Überwachung von überall und zu jeder Zeit, die wesentlich zur Entstörung beitragen kann. Jan Moll beschreibt ab Seite 15, wie man das komplette Rechenzentrum aufs Smartphone bringt. Mit rund 800 Servern steht in Bodensee-Oberschwaben einer der größten Private-Cloud-Dienstleister der Region. Eine Software überwacht sämtliche Umgebungsparameter im Datacenter von jedem mobilen Endgerät aus.

Um Sicherheit von der Spannungsversorgung bis zum Serverrack geht es im Beitrag von Michael Schell, Bernd Hanstein und Kerstin Ginsberg ab Seite 18. In Hannovers Süden ist in den vergangenen Monaten eines der modernsten Rechenzentren Deutschlands entstanden: Die TÜV Nord Group konzentriert hier zukünftig alle EDV-Aktivitäten der nationalen und internationalen Tochtergesellschaften. Neben hoher Verfügbarkeit und Sicherheit stand bei der Planung auch die Energieeffizienz ganz oben auf der Prioritätenliste.

Dass Datenverschlüsselung kein Hexenwerk ist, bringt Peter Rost auf Seite 21 auf den Punkt. Unzureichend geschützte Datentransportleitungen bergen die Gefahr massiver wirtschaftlicher Schäden für Unternehmen. Warum jedoch nur knapp ein Drittel aller Unternehmen auf Sicherheitslösungen zum Verschlüsseln der Verbindungen setzt, ist uns ein Rätsel. Dabei ist das Absichern von Übertragungen durchaus machbar.

Wir nähern uns dem Ende dieser Ausgabe: Clouds für definierte Gruppen, sogenannte Community Clouds, schützen gespeicherte Inhalte durch definierte Eintrittsbarrieren. Ein funktionierender Datenschutz bleibt der wunde Punkt. Verantwortliche, die größere Datenmengen auslagern oder Möglichkeiten zum Austausch mit anderen Unternehmen schaffen wollen, sollten daher auf größtmögliche Sicherheit achten. Eine Lösung können Community Clouds sein, fasst Josef Glöckl-Frohnholzer ab Seite 22 zusammen.

Welch geballter Angriffskraft Rechenzentren heutzutage ausgesetzt sind, hinterfragt Uli Ries in seinem ausführlichen Beitrag ab Seite 24. Lokale Lösungen helfen kaum. Denial-of-Service-Attacken wachsen sich zum katastrophalen Problem aus, da bei DDoS-Angriffen aus zehntausenden oder mehr Rohren gleichzeitig gefeuert wird – und so selbst leistungsstarke Rechenzentren de facto nicht mehr erreichbar sind. Herkömmliche Infrastrukturen haben solchen verteilten Attacken nichts entgegen zu setzen. Hilfe winkt – einmal mehr – aus der Cloud.

Hand auf's Herz: Hätten Sie wirklich gewusst, wie vielschichtig das Problem Sicherheit in Rechenzentren tatsächlich ist? Deshalb sind wir der Meinung, dass eine nahezu vollständige Ausgabe von Rechenzentren und Infrastruktur sich dieses Themas gar nicht oft und gründlich genug annehmen kann.

Thomas Jannot

NEUE HP-SWITCHES WOLLEN SDN-UMSTIEG ERLEICHTERN

HP stellt mit der Produktserie HP 5400R zl2 eine neue Switch-Generation vor, die Kunden unter anderem den Umstieg auf Software Defined Networking (SDN) erleichtern soll. Laut Hersteller soll die Serie sowohl kleinen und mittleren Unternehmen als auch Großkonzernen dabei helfen, Campus- und Zweigstellennetzwerke aufzubauen – vom mittelgroßen Kernnetz bis hin zur Netzzugangsschicht. Zugleich senken die Geräte laut Hersteller die Gesamtbetriebskosten um bis zu 43 Prozent. Die Switches der neuen Serie unterstützen auch die Bandbreitenanforderungen anspruchsvoller Anwendungen.

Der Umstieg auf SDN soll mit den neuen Switches gelingen, ohne dass Anwender ihre komplette IT-Infrastruktur austauschen müssen, so HP.

Die Switch-Serie HP 5400R zl2 sei gut geeignet für bandbreitenhungrige Anwendungen. Ausgestattet mit ProVision Fabric ASICs der fünften Generation, erreichen sie laut Hersteller eine drei Mal schnellere Datendurchsatzrate als Konkurrenzprodukte; die Angaben beruhen laut HP auf einem HP-internen Vergleich mit öffentlich zugänglichen Daten wichtiger Mitbewerber. Die Switche sollen zudem über eine um 58 Prozent geringere Latenzzeit und eine Switching-Kapazität

Quelle: HP

Sollen den schrittweisen Umstieg auf SDN möglich machen: Switche der HP-Serie 5400R

von bis zu zwei Terabits pro Sekunde verfügen. Anwender in den Unternehmen, in denen die neuen Switche zum Einsatz kommen, sollen daher dem Hersteller zufolge vom unterbrechungsfreien Betrieb neuer Anwendungen und verbesserten Umgang bei bestehenden Anwendungen profitieren, wie etwa Videokonferenzlösungen.

Laut HP sind die neuen Switches HP 5406R zl2 und HP 5412R zl2 weltweit erhältlich. Preise beginnen bei 1.859 Euro (HP 5406 R zl2) und 3.549 Euro (HP 5412R zl2).

GRATIS-TOOL ZUR ANALYSE VON IT-RESSOURCEN IM RZ

American Megatrends International (AMI) bietet Betreibern von Rechenzentren das Software-Tool StorTrends iDATA (Intelligent Data Analysis Tracking Application) zum kostenlosen Download unter www.stortrends.com/resources/stortrends-idata-tool. Laut Hersteller soll die Anwendung Administratoren und IT-Verantwortlichen in Unternehmen und großen Organisationen bei der Analyse ihrer IT-Architektur helfen.

Die Software läuft über einen Zeitraum von sieben Tagen im Hintergrund des regulären IT-Betriebs und zeichnet laut Hersteller den Datendurchsatz aller wichtigen Komponenten auf. Am Ende gibt Stor-

Quelle: AMI

Auslastung im Blick: das Gratis-Tool von AMI analysiert die Auslastung aller wichtigen Komponenten im Rechenzentrum

Trends iDATA einen Analysereport aus, der dem Hersteller zufolge Kennzahlen angibt wie Kapazitätsauslastung und prognostiziertes Wachstum, IOPS (Vergleich von Schreib- und Lesezugriffen), Netzwerkauslastung, Vergleich von aktiven und inaktiven Datenbeständen, Systemperformance, Auslastung einzelner Anwendungen, Latenzzeit in Millisekunden und Warteschlangentiefe (Queue depths, siehe Abbildung unten).

Laut AMI sollen IT-Verantwortliche so auf mögliche Engpässe in Bezug auf Rechen- und Speicherkapazitäten aufmerksam werden und besser den Bedarf an neuer Storage-Hardware und Virtualisierungs-Software ermitteln. Ziel sei es, wirtschaftliche Kaufentscheidungen zu ermöglichen, mit denen sich zugleich die Leistungsfähigkeit der IT-Systeme sicherstellen und eine kostspielige Überdimensionierung der Speicherressourcen vermeiden lasse.

Hauptzielgruppe für StorTrends iDATA seien laut AMI Betreiber von Rechenzentren, die ihre bestehende Storage-Infrastruktur im Hinblick auf mögliche Neuanschaffungen überprüfen möchten. Das Tool ermittle die Leistung des Gesamtsystems in Bezug auf Schreib- und Lesezugriffe, die Gesamtmenge der IOPS und den Datendurchsatz sowie die tägliche Wachstumsrate der Daten. Dadurch lasse sich laut Anbieter sicherstellen, dass die Anschaffung neuer Storage-Komponenten im Einklang mit dem tatsächlichen Wachstum der Datenmenge steht.

Das Verhältnis zwischen aktiven und inaktiven Daten sei ein zentraler Faktor bei der Auswahl einer adäquaten Storage-Architektur. StorTrends iDATA biete dem Nutzer somit auch eine solide Grundlage für die Entscheidung, ob er mit Plattenspeichern, Hybridlösungen aus SSD und HDD oder reinen Flash-Speichern arbeiten sollte. In Virtual-Desktop-Infrastrukturen (VDIs) komme es laut AMI zudem immer wieder zu Problemen, weil die tatsächlichen Anforderungen der einzelnen Nutzerprofile unterschätzt werden.

StorTrends iDATA ermittle aufgrund des realen Nutzungsverhaltens, ob ein Nutzer der Kategorie Light, Medium, Power Standard oder Power Heavy User zuzurechnen ist. Auf Basis dieser Erkenntnisse könne der Administrator den Nutzern die entsprechenden Systemressourcen zuweisen oder diese im Bedarfsfall erweitern.

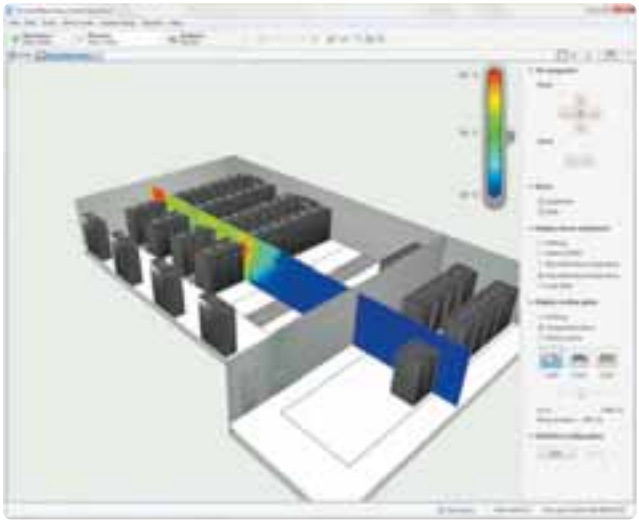
NEUE DCIM-SOFTWAREVERSION FÜR VERBESSERTES MONITORING

Schneider Electric hat nach eigener Auskunft seine Software StruxureWare for Data Centers überarbeitet. Die Version 7.4 soll neue Funktionen für das Management von Colocation-Datacentern, die Überwachung der Stromversorgung und Netzwerkverwaltung mitbringen. So sollen IT und Facility Manager die Kapazitäten besser verwalten, die Infrastruktur optimal ausnutzen und daher die Betriebskosten senken können.

Ein wesentliches Merkmal der Optimierung sind laut Anbieter doppelte Anschlussbuchsen, um einen Überblick über die komplette Stromredundanz auf Cage- oder Rack-Ebene zu erlauben. Nur so seien IT-Manager in der Lage, die Auswirkungen einer Störung zu simulieren und die Lastverteilung für jeden Anschluss zu erkennen. StruxureWare for Data Centers 7.4 biete zudem eine überarbeitete Cage- und Rack-basierte Leistungsübersicht. Dank verbesserter Daten und detailgenauer Zeichnungen, werde die Abrechnung der einzelnen Mieter erleichtert.

Die Software will die Lücke zwischen IT und Facility weiter schließen, indem sie Einblicke bis auf Leistungsschalterebene biete. Dies verschaffe RZ-Betreibern Informationen über den Stromkreis. Weitere neue Features seien die Überwachung der Lichtleitungen sowie die Möglichkeit, Verteilerpläne zu drucken. Durch grafische Netzwerkverbindungen, visuelles Port-Mapping und Kabelweg- sowie -Typ-Visualisierung lassen sich laut Hersteller potenzielle Netzwerkprobleme besser ermitteln.

Quelle: Schneider Electric



Die RZ-Managementsoftware von Schneider Electric stellt auch die Temperaturverteilung im RZ dar.

(SDN)-PLATTFORM AUF OPEN-SOURCE-BASIS

Extreme Networks stellte eine Software Defined Networking (SDN)-Plattform vor, die auf dem Open-Source-Projekt „OpenDaylight“ (ODL) basiert. RZ-Betreiber sollten ihre vorhandenen Netzwerke laut Hersteller ohne kostspielige und aufwändige Updates auf eine SDN-Plattform migrieren können. Eine nahtlose SDN-Migration erfordere jedoch einen übergreifenden, offenen und auf Standards basierenden Ansatz, der Überlegungen der Entwicklercommunity berücksichtigt und Partner sowie Kunden unterstützt.

Die Extreme Networks SDN-Plattform basiere auf dem OpenDaylight (ODL)-Controller, der Netzwerkmanagement, Netzwerkzugangskontrolle, Anwendungsanalyse und Wireless-Controller-Technologie beinhaltet. Der Anbieter bewahrt nach eigener Auskunft die durch den ODL geschaffene Integrität der offenen API, will aber gleichzeitig das Orchestrieren, Automatisieren und Bereitstellen des Rechenzentrums einheitlich auf das gesamte Netzwerk ausdehnen.

Die SDN-Plattform soll sich in die bestehenden Hard- und Software-Netzwerkumgebungen verschiedenster Anbieter integrieren und so Abhängigkeit von nur einem Anbieter verhindern. Die Abwärtskompatibilität mit den Infrastrukturkomponenten und die Konformität zu OpenFlow sowie zu weiteren offenen APIs seien ebenfalls sichergestellt.

PDU-PRODUKTE FÜR OPTIMIERTES KAPAZITÄTSMANAGEMENT

Emerson Network Power hat mit der MPH2 Managed Rack-PDU und dem RPC2-Kommunikationsmodul neue RZ-Komponenten im Angebot. Die MPH2 Rack-PDU biete sehr hohe Temperaturtoleranzen. In Kombination mit dem RPC2-Kommunikationsmodul sollen Fernverwaltungsfunktionen, Echtzeitüberwachung und Kontrolle der angeschlossenen Verbraucher möglich sein. Die Management- und Authentifizierungsprotokolle sollen laut Hersteller Branchenstandards entsprechen und die neuen Komponenten so kompatibel machen zu vorhandenen IT-Netzwerken und Kommunikationsnetzwerken.

Laut Hersteller bieten die neuen Produkte Rechenzentren folgende Vorteile:

- Verfügbarkeit: Durch den Einsatz bistabiler Relais soll die MPH2 Rack-PDU in Kombination mit dem RPC2-Kommunikationsmodul die grundlegende Stromversorgung für angeschlossene Verbraucher auch dann liefern, wenn die Steuerung der Einheiten ausfallen sollte. Rack-PDUs würden typischerweise an der Rack-Rückseite nahe des Warmgangs verbaut, wodurch sie den höchsten Temperaturen innerhalb des Rechenzentrums ausgesetzt sind. Nicht selten werden hier Temperaturen von 50 Grad Celsius gemessen. Die MPH2 Rack-PDU sei auf Betriebstemperaturen bis zu 60 Grad Celsius ausgelegt, was wiederum die Systemverfügbarkeit erhöhen soll.
- Energie- und Kapazitätsmanagement: Die MPH2 hat laut Hersteller einen geringen Energieverbrauch. Im Vergleich zu anderen Modellen sollen jährlich Einsparungen von bis zu 76 Euro pro Rack machbar sein.
- Integration in Verwaltungs-Tools: Einsparungen lassen sich laut Hersteller ebenfalls durch das Konsolidieren von Benutzer-IP-Verbindungen und Geräteüberwachung erzielen, da bis zu vier MPH2 Rack-PDUs zu einem Rack-PDU-Array zusammengeschlossen werden können. Alle wichtigen Verwaltungs-, Authentifizierungs- und Verschlüsselungsstandards und -protokolle würden unterstützt. Auch lassen sich die Stromversorgungs- und Umgebungsinformationen der Rack-PDUs in die Verwaltungssoftware für Rechenzentren von Emerson oder Drittanbietern einspeisen.

RZ auch im Brandfall 24/7 verfügbar

Rechenzentrum des Niedersächsischen Landtags schützt sich durch aktive Sauerstoffreduzierung vor Bränden

Der Niedersächsische Landtag hat beim Umbau seines Rechenzentrums im Jahr 2011 auch ein modernes Brandschutzkonzept im Regierungssitz an der Leine umgesetzt. Durch das Vermeiden von Bränden soll die Datenverfügbarkeit auch im Brandfall sicher gestellt sein. Ein Blick hinter die (technischen) Kulissen.

Er ist das oberste Verfassungsorgan des Landes Niedersachsen: Der Niedersächsische Landtag. Er verabschiedet Gesetze, wählt den Ministerpräsidenten, den Präsidenten des Landesrechnungshofes und beschließt den jährlichen Haushalt. Zudem wirkt er in der Regierungsbildung – um nur einige Aufgaben des politischen Organs zu nennen. Seinen Sitz hat der Niedersächsische Landtag im Leineschloss in Hannover. Im Jahr 1637 erbaut, diente das Gebäude unter anderem als Kloster, Armenhaus, Hospital, Schule, Münzstätte, Magazin, Kaserne, Volksküche und als Museum.

Heute kommen die Abgeordneten der 87 niedersächsischen Wahlkreise im Leineschloss zusammen, um in Plenar-, Ausschuss- und Fraktionssitzungen die Politik auf Landesebene zu gestalten. Neben dem Plenarsaal, zahlreichen Sitzungssälen, der Bibliothek, dem Lesesaal des Niedersächsischen Landtags befinden sich auch die Büros der Mitarbeiter der einzelnen Fraktionen und der Landtagsverwaltung in dem Gebäude.

Dauerhafte Datenverfügbarkeit – auch im Brandfall

Zum operativen Geschäft des Landtages gehört es, täglich Unmengen an Daten und Informationen zu verarbeiten und weiterzuleiten. Um unter anderem den Forderungen nach steigenden Kapazitäten für die Datenübertragung gerecht zu werden, hat der Landtag 2011 sein Rechenzentrum vollständig erneuert. Damit das Rechenzentrum auch künftig den steigenden Anforderungen an EDV und Kommunikation gewachsen sein wird, war die technische Aufrüstung notwendig geworden. Denn kommt es zu einer internen Unterbrechung in der IT, können Verwaltungs- und Fraktionsgeschäfte nicht nur erheblich gestört, sondern sogar vollständig lahmgelegt werden. Dafür muss noch nicht einmal das gesamte IT-Zentrum betroffen sein. Bereits Ausfälle einzelner Serverschränke oder Komponenten des Rechenzentrums können dazu führen, dass wichtige Daten nicht abgerufen werden können.

Um einen 24-Stunden-Betrieb sieben Tage die Woche zu gewährleisten, sind gewisse Sicherheitsvorkehrungen notwendig. Redundanzen in der Klimatechnik und eine unterbrechungsfreie Stromversorgung sowie regelmäßige Wartungen, ohne den Betrieb zu unterbrechen, haben sich mittlerweile als Standard in hochverfügbaren IT-Strukturen etabliert. Dazu gehört auch das passende Brandschutzkonzept. Letztendlich entschieden sich die Verantwortlichen für eine Kombination aus effektiver Brandvermeidung durch Sauerstoffreduktion, einer Stickstoff-Schnellabsenkung sowie einem aktiven Ansaugrauchmeldesystem.

Quelle: Niedersächsischer Landtag

Im Plenarsaal des Niedersächsischen Landtags finden beispielsweise die Ausschuss- und Fraktionssitzungen statt (Abb. 1).

Klar definierte Anforderungen an den Brandschutz

Bevor das Rechenzentrum mit dem passenden Brandschutzsystem ausgerüstet wurde, definierten die Planer die wesentlichen Kriterien, die erfüllt werden mussten: Der unterbrechungsfreie Betrieb der technischen Anlagen gilt als oberstes Schutzziel. Kommt es zu einem Brand, erfordert die darauffolgende Löschung in der Regel ein Stromlosschalten der IT. Das sollte innerhalb des Rechenzentrums des Landtages vermieden werden. Zusätzlich sollte im Normalbetrieb die Begehbarkeit des Schutzbereiches durch das Personal erhalten bleiben.

Bei der installierten Brandschutzlösung mit Sauerstoffreduzierung bildet eine sogenannte OxyReduct-Anlage das Herzstück. Das aktive Brandvermeidungssystem senkt die Sauerstoffkonzentration von den in normaler Umgebungsluft enthaltenen 20,9 Volumenprozent auf 17 Volumenprozent Sauerstoff ab. Durch diese geringe Sauerstoffverminderung kann das Entwickeln und Ausbreiten eines Brandes bereits verhindert werden. Mittels kontrollierter Stickstoffzufuhr wird die Sauerstoffkonzentration in dem Schutzraum herabgesenkt. Durch die Veränderung des Mischungsverhältnisses von Sauerstoff und Stickstoff in der Umgebungsluft wird dem Brand quasi die Luft zum Atmen ge-

Passen zur Idee Ihres Rechenzentrums – CyberAir 3 Klimasysteme

IT Cooling Solutions

Planen Sie mit der Erfahrung, Effizienz und Flexibilität von CyberAir 3

Seit über 40 Jahren entwickelt und produziert STULZ in Deutschland Präzisionsklimaanlagen für Rechenzentren und Telekommunikationsstandorte. Diese Erfahrung kombiniert mit weltweit tausenden umgesetzten Projekten steckt in unseren Lösungen. CyberAir 3 gibt es mit acht Kältesystemen: luft- oder wassergekühlt, mit zwei Kreisläufen und Redundanz im Gerät, mit EC-Ventilator, EC-Kompressor und – bis zu 90 % sparsamer – mit Indirekter und Direkter Freier Kühlung. Sieben Baugrößen bieten Flexibilität für jeden Raum. Sie wünschen sich eine maximale Verfügbarkeit bei minimalen Kosten und möchten Ihre Server präzise, zuverlässig und effizient klimatisieren? Wir helfen Ihnen gerne.

STULZ GmbH · Holsteiner Chaussee 283 · 22457 Hamburg · Tel.: +49(40)55 85-0 · Fax: +49(40)55 85-352 · products@stulz.de

www.stulz.com

nommen, eine weitere Brandentwicklung ist nicht mehr möglich. Dennoch bleibt der Raum für Personal im Normalbetrieb frei begehbar.

Der für die Sauerstoffreduktion benötigte Stickstoff wird mittels einer Membran direkt aus der Umgebungsluft gewonnen. Wie stark die Sauerstoffkonzentration gesenkt werden muss, wird immer im Hinblick auf die vorherrschenden Materialien und deren unterschiedlicher Entzündungsgrenzen entschieden. Für den IT-Bereich regelt die VdS 3527 die Entzündungsgrenzen der vorhandenen Stoffe und die erforderliche Auslegungskonzentration der Sauerstoffreduzierungsanlage. Auf dieser Basis ist auch die veränderte Sauerstoffkonzentration im Rechenzentrum des Landtages ausgelegt worden.

Schnelle Reaktion im Brandfall

Um das RZ über die Reduktion hinaus noch besser zu schützen, ist zusätzlich ein System zur Brandfrühesterkennung installiert worden. Es soll im Brandfall das frühzeitige und gezielte Ergreifen von Gegenmaßnahmen ermöglichen. Die verwendeten Ansaugrauchmelder können Brände bereits während ihrer Entstehungsphase entdecken. Dafür entnimmt das Ansaugrauchmeldesystem der Luft aktiv Proben und analysiert diese auf Pyrolysepartikel:Im Rechenzentrum befinden sich die Ansaugpunkte, über die das System der Luft aktiv Proben entnimmt, im IT-Zentrum selbst als auch in den Verteilerräumen und in den Kabelschächten.

Bereits zwei Gramm stoffliche Umsetzung innerhalb von 180 Sekunden reichen aus, damit das System anschlägt. Rauch ist während dieser frühen Entwicklung eines Brandes noch nicht einmal sichtbar. In einem Rechenzentrum wäre das beispielsweise ein kleiner Schmorbrand an einer Kunststoffummantelung eines Kabels. Das installierte System ist empfindlicher als ein konventioneller Punktmelder und schafft so einen Zeitvorteil für das Ergreifen von Gegenmaßnahmen.

Schnellabsenkung verhindert Brandausbreitung

Das im Niedersächsischen Landtag eingesetzte Brandschutzkonzept sieht für den Notfall eine Schnellabsenkung vor. Das bedeutet: Detektiert das Ansaugrauchmeldesystem Rauchpartikel innerhalb des Rechenzentrums, wird der durch die Anlage reduzierte Sauerstoffgehalt mithilfe einer Schnellabsenkung binnen kürzester Zeit bis auf eine löschfähige Konzentration von 14,6 Volumenprozent abgesenkt. Die IT-Systeme laufen dennoch weiter. Der für diese Schnellabsenkung benötigte Stickstoff wird dabei aus Flaschen bereitgestellt. In der Folge hält die Anlage das stark abgestufte Sauerstoffniveau so lange aufrecht, bis mögliche Rückzündungen ausgeschlossen werden können (der VdS schreibt eine Haltezeit von zehn Minuten vor). Bei Bedarf kann die Technik die Konzentration beliebig lange halten – auch über Tage hinweg, bis die Stickstoffflaschen für einen möglichen späteren Einsatz wieder neu befüllt wurden.

Quelle: Wagner Group GmbH

Eine Kombination aus aktiver Brandvermeidung sowie einer Schnellabsenkung schützt das RZ des Niedersächsischen Landtags vor Bränden und ihren Folgen (Abb. 2).

Zwar kann die Begehbarkeit der Räume um während der Schnellabsenkung eingeschränkt sein – sie ist für autorisiertes Personal in aller Regel jedoch weiterhin möglich. Das kann nützlich sein, um etwa die Brandquelle zu suchen oder geeignete Gegenmaßnahmen einzuleiten. Grundsätzlich ist eine verminderte Sauerstoffkonzentration für gesunde Menschen ungefährlich. Um jedoch Gefährdungen durch beispielsweise unentdeckte Herz-Kreislauf-Erkrankungen vorzubeugen, sollte sich das entsprechende Personal im Vorfeld einer arbeitsmedizinischen Untersuchung unterziehen – gemäß der Richtlinie BGI/GUV-I 5162 „Arbeiten in sauerstoffreduzierter Atmosphäre“ der Deutschen Gesetzlichen Unfallversicherung.

Brandschutz mit Schallschutz

Strömt das rückstands- und schadstofffrei arbeitende Löschgas (Stickstoff) aus Flaschen unter Druck in den Raum – beispielsweise im Rahmen der Schnellabsenkung oder als Gaslöschanlage –, kann dies die IT-Hardware gefährden. Der hohe Druck, mit dem das Löschgas binnen weniger Minuten in den Schutzbereich eingeleitet wird, erreicht einen Schalldruckpegel mit einer Lautstärke von bis zu 130 dB(A). Dieser kann die Köpfe von Festplatten zum Schwingen bringen. Eine Zerstörung der Platte und der Verlust aller sich darauf befindenden Daten könnte die Folge sein. Daher kommen speziell für diesen Einsatzzweck entwickelte Düsen für die Flaschenbatterien zum Einsatz, die wie ein Schalldämpfer den Schalldruckpegel deutlich senken.

Das Brandvermeidungssystems ist mit der Branddetektionseinheit innerhalb eines Gefahrenmanagementsystems vernetzt, sodass alle Daten in einer Einheit zusammengetragen und stetig überwacht werden können. Damit sind alle Systeme zentral steuerbar. Auch dies kann einen wertvollen Zeitvorteil bedeuten, um geeignete Gegenmaßnahmen einzuleiten – für eine dauerhaft funktionierende IT im Niedersächsischen Landtag.

Katharina Bengsch,
Kommunikation/PR, Wagner Group GmbH

DAS PRINZIP DER BRANDVERMEIDUNG

In IT-Zentren besteht aufgrund der Vielzahl elektrischer Komponenten wie Leiteranschlüsse und -verbindungen und Kabelleitungen ein erhöhtes Risiko für durch technische Mängel ausgelöste Brände – so das VdS-Merkblatt VdS 2837. Ein Schwelbrand, der nicht frühzeitig erkannt wird, findet beispielsweise durch die im Rechenzentrum vorhandenen Kunststoffe wie Kabelummantelungen, Platinen und Servergehäuse ausreichend Nahrung, um sich weiter auszubreiten.

Damit ein Brand überhaupt entstehen kann, müssen grundsätzlich Energie, Sauerstoff und Brennstoff in ausreichend großer Menge vorhanden sein. Wird einer dieser Faktoren verändert, ändert sich damit auch das Brandverhalten. Genau da setzt das Prinzip der Brandvermeidung mittels Sauerstoffreduzierung an, das sich speziell im Einsatz in sensiblen IT-Bereichen bewährt hat.

FNT

// Data Center Infrastructure Management

Erleben Sie das entspannte Gefühl eines erfolgreichen Rechenzentrumsmanagement!

Die FNT Lösung für das Data Center Infrastructure Management (DCIM) ist die zentrale Steuerungs- und Optimierungssoftware für Ihr Rechenzentrum. Von der Gebäudeinfrastruktur (Strom, Kühlung, Fläche etc.) über die IT Infrastruktur (Netzwerk, Server, Speicher etc.) bis hin zu den Services (Software, Anwendungen, Dienste): DCIM von FNT ermöglicht eine umfangreiche und ganzheitliche Sicht auf Ihre wertvollen Ressourcen im Rechenzentrum.

// when transparency matters.

weitere Informationen unter www.fntsoftware.com/DCIM

Auf den äußersten Notfall vorbereitet

Automatisiertes Notfallhandbuch bietet optimale Unterstützung in Ausnahmesituationen

Feuer im RZ oder der Ausfall einer kritischen Kältemaschine – Notfälle sind zwar selten, können jedoch gravierende Folgen haben. Zeichnet sich ein Notfall ab, haben Erhalt beziehungsweise Wiederherstellen der Betriebskontinuität höchste Priorität. Dazu gibt es Notfallhandbücher. Werden diese digitalisiert und das Notfallmanagement automatisiert, können Notfallmanager Probleme schneller beheben.

Im April dieses Jahres machte eine Meldung über ein Feuer in einem südkoreanischen Rechenzentrum von Samsung die Runde. Durch den Unfall kamen über vier Stunden mehrere Dienste auf Smartphones, Tablets und SmartTVs zum Erliegen – und das weltweit. Anscheinend wurde erst durch dieses Unglück die Bedeutung des Rechenzentrums für die global erbrachten Dienste deutlich. Das Unternehmen war offensichtlich nicht auf den Notfall vorbereitet und hatten auch keine Strategien entwickelt, um den Betrieb vor Ort innerhalb kurzer Zeit wieder zum Laufen zu bringen.

Dieser Vorfall zeigt erneut, wie wichtig es für Rechenzentrumsbetreiber heutzutage ist, für den Ausnahmefall gewappnet zu sein. Das gilt sowohl für das Rechenzentrum eines Outsourcing-Providers als auch für jenes eines Unternehmens. Denn die Abhängigkeit von IT-Systemen ist größer denn je und gerade bei kritischen Diensten können selbst geringe Ausfälle zu gravierenden Umsatzeinbußen und Reputationsverlusten führen.

Diese verstärkte Abhängigkeit hat dazu geführt, dass die Anforderungen an die Rechenzentren – formuliert in den Service Level Agreements – immer strikter geworden sind. Infolgedessen sind die Maschinen und Geräte im Dauereinsatz und die Bedienungsmannschaften stehen unter einem immer höheren Leistungsdruck – das erhöht die Fehlerquoten. Laut einer Studie des amerikanischen Marktforschungs- und Beratungsunternehmens Ponemon Institute vom September 2013 fällt ein Datacenter im Schnitt ein Mal im Jahr für 91,3 Minuten komplett aus. Es kann also jeden treffen.

Notfallhandbuch ist ein „Muss“

Auch hierzulande werden Rechenzentrumsbetreiber gelegentlich überrascht, wenn zum Beispiel bei Bauarbeiten ein Bagger die Stromzufuhr kappt, mehrere Kältemaschinen gleichzeitig Probleme melden oder plötzlich ein Nebenfluss Hochwasser führt und die Datenbestände und Prozesse bedroht sind. Wie auch in anderen Branchen ist das Führen eines Notfallhandbuchs für Rechenzentren deshalb unverzichtbar. So haben zum Beispiel in der chemischen Industrie auch kleinere Marktteilnehmer stets ausführliche Notfallhandbücher in der Schublade, damit sie im Ernstfall Schaden an Menschen, Umwelt, Investitionen und ihrer Reputation auf ein Minimum reduzieren können.

Das Notfallhandbuch umfasst alle Informationen und Dokumente, die eine angemessene Reaktion auf existenzbedrohende Ereignisse unterstützen und für die Fortführung der Geschäftsprozesse sorgen. Gute Notfallhandbücher sind außerdem so gestaltet, dass bereits auf erste Anzeichen reagiert wird – beispielsweise durch ein laufendes Überwachen von Pegelständen – damit Gefahren frühzeitig erkannt und entsprechende Maßnahmen eingeleitet werden, bevor es zu einem Notfall kommt.

Diverse Standards und Normen empfehlen den Betreibern von Rechenzentren deshalb schon seit geraumer Zeit das Führen eines Notfallhandbuchs. Dazu zählen zum Beispiel die ISO 27001, die IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI), das Bundesdatenschutzgesetz, die TÜV-Anforderungen für die Rechenzentrumszertifizierung sowie die IT Infrastructure Library (ITIL).

Das schließt folgende Maßnahmen mit ein:

- Den Aufbau einer Organisation, die sich mit dem Bewältigen des Notfalls beschäftigt sowie das Benennen von Notfallmanagern oder IT-Fachleuten in einem Ausweichrechenzentrum
- Das Sicherherstellen des Wiederanlaufs kritischer IT-Services und eines verlässlichen Notbetriebs

Quelle: Fujitsu

Das RZ-Notfallmanagement lässt sich weitgehend automatisieren und mit weiteren Bereichen wie Automatisierung und Bereitstellung von IT-Infrastruktur-Ressourcen koppeln (Abb. 1).

- Hilfe für Kunden und Fachabteilungen, die von dem Ausfall betroffen sind.
- Das Wiederherstellen ausgefallener IT-Services

Notfallhandbuch digitalisieren

Im Ernstfall müssen die Notfallmanager die im Notfallhandbuch vorgeschriebenen Prozesse möglichst schnell nachschlagen und abarbeiten. Dabei gilt es, die unterschiedlichen Eskalationsstufen zu berücksichtigen und parallel dazu alle Vorgänge zu protokollieren. Dies ist wichtig, um Schwachstellen zu identifizieren und zu beheben.

Damit die entsprechenden Notfallkarten schneller gefunden werden können, ist es sinnvoll, das Notfallhandbuch nicht nur in Papierform, sondern zusätzlich als digitale Version vorzuhalten. Eine Datei kann schließlich effizient nach Schlagwörtern durchforstet werden und die gesuchte Notfallkarte noch schneller bereitstellen. Wird für die Digitalisierung des Notfallhandbuchs außerdem eine Software verwendet, bei der die Protokollierungsvorgänge im Hintergrund mitlaufen, können die Notfallmanager weiter entlastet und eine lückenlose Dokumentierung sichergestellt werden. Das ist wichtig, damit das Notfallhandbuch später für künftige Fälle aktualisiert und verbessert werden kann.

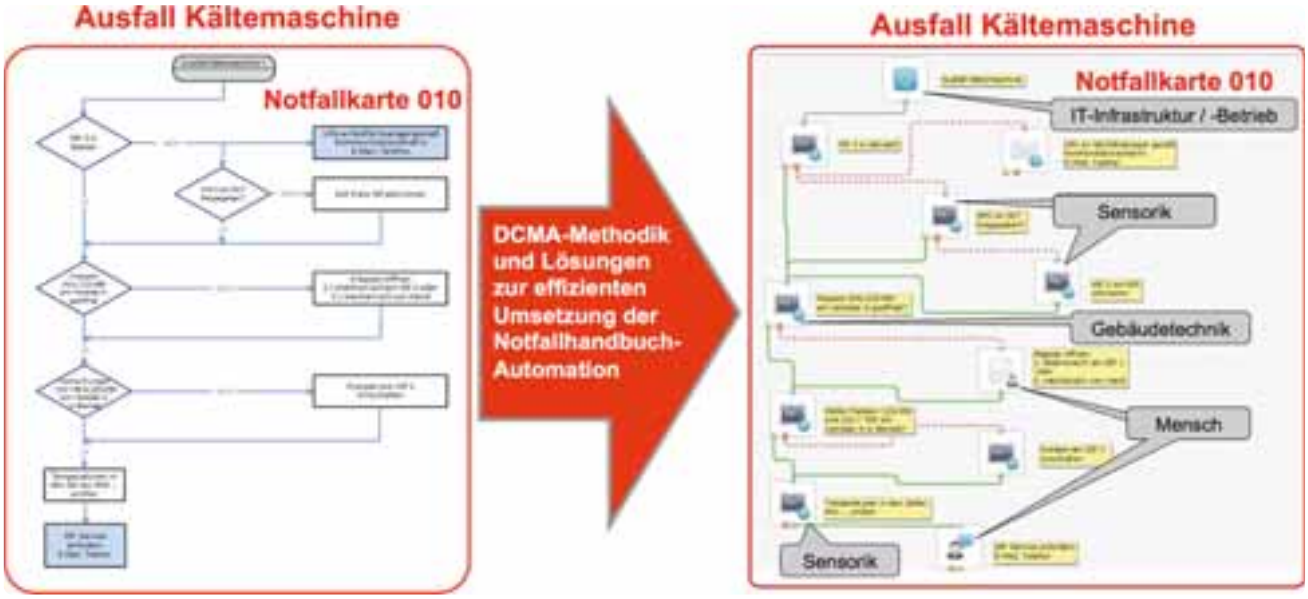
Allerdings sollte auf eine Papierversion keinesfalls komplett verzichtet werden: Im Falle von Stromausfällen und Softwarefehlern muss grundsätzlich ein leicht zugängliches Exemplar des Notfallhandbuchs verfügbar sein. Eine digitale Version, die ein einfaches Ausdrucken und Abheften der aktualisierten Notfallkarten erlaubt ist deshalb empfehlenswert.

Notfallmanagementprozesse automatisieren

Damit die im Notfallhandbuch beschriebenen Maßnahmen schnell und fehlerfrei umgesetzt werden, sollte außerdem ein Automatisieren der Notfallmanagementprozesse in Erwägung gezogen werden – und das nicht nur für die IT-Infrastruktur, sondern auch für die Kühlung und die Gebäudetechnik. Beispielsweise können Ventile, Kugelhähne und Klappen häufig auch ferngesteuert geöffnet oder geschlossen werden. Es ist also nicht zwingend notwendig, dass die Mitarbeiter sämtliche Aufgaben manuell vor Ort erledigen.

Allerdings muss sichergestellt werden, dass sie über ein zuverlässiges Informationssystem verfügen, das sie darüber informiert, ob ein Prozess erfolgreich abgeschlossen werden konnte. Wenn der Notfallmanager über sein digitalisiertes Notfallhandbuch nun erkennen kann, welche Prozesse automatisiert laufen und in welchem Stadium sich ein Prozess befindet, hat er einen besseren Überblick und kann sich auf die wirklich schwierigen Aufgaben zur Behebung des Notfalls konzentrieren.

Ein Beispiel für eine derartige Lösung, ist das automatisierte Notfallhandbuch, das Fujitsu zusammen mit CA Technologies und TDS in Anlehnung an die IT Infrastructure Library (ITIL) entwickelt hat. Es ver-



Quelle: Fujitsu

Notfallkarten zeigen bei einem automatisierten Notfallhandbuch, welche Maßnahmen automatisch ergriffen werden und wo der Notfallmanager selbst Hand anlegen muss (Abb. 2).

bindet ein digitalisiertes Notfallhandbuch mit einer Prozessautomation. Ein solches automatisiertes Notfallhandbuch kann das Erbringen von IT-Dienstleistungen beschleunigen und die Anzahl an manuell verursachten Fehlern minimieren. Sie bietet verschiedene Funktionen zum Definieren, Automatisieren und Verwalten der Prozesse über verschiedene Betriebsabteilungen hinweg sowie Schnittstellen zum Ansteuern bestehender IT-Managementsysteme.

Cockpit für Notfallmanager entwickeln

Interaktionen mit dem Personal sowie logische Funktionen unterstützen die Notfallmanager bei ihren Entscheidungen. Damit ermöglicht ein automatisiertes Notfallhandbuch, alle Beteiligten in einen Prozess einzubinden und über den aktuellen Stand des Prozessablaufs zu informieren – das erleichtert die Arbeit im Team. Wie ein automatisierter Notfallplan funktioniert, zeigt beispielsweise die Notfallkarte in Abbildung 3. Sie definiert die Schritte, die nach dem Ausfall einer Kältemaschine durchzuführen sind. Der IT-Fachmann sieht auf einer Grafik oder einem Flussdiagramm, welche Maßnahmen automatisch ablaufen, etwa dass Klappen an einen Verteiler geöffnet und Pumpen zugeschaltet werden, und wo er selbst aktiv werden muss. Solche Notfallkarten stehen für alle Bereiche zur Verfügung, etwa für solche, die beim Facility-Management angesiedelt sind und Schließsysteme und die Belüftungsanlage betreffen.

Das automatisierte Notfallhandbuch stellt somit die auf ein Rechenzentrum abgestimmten Notfallmanagementprozesse bereit, die im Ernstfall reibungslos über Betriebssystem- und Abteilungsgrenzen hinweg die Wiederherstellung des Betriebs unterstützen. Über ein Dashboard werden die Prozesse und Eskalationsstufen grafisch visualisiert und im Nachgang des Notfalls einfach und bequem angepasst.

Das ist wichtig, denn die Aktualisierung von Notfallplänen ist eine zentrale Anforderung, die in der Praxis bei Papierdokumenten häufig aus Zeitmangel zu kurz kommt. Bei einem automatisierten Notfallhandbuch stehen dem Notfallmanager dagegen ein zentrales Cockpit und eine zentralisierte Datenhaltung zur Verfügung. Über eine Druckansicht lassen sich sämtliche Notfallkarten außerdem schnell und problemlos ausdrucken und damit die Papierversion des Notfallhandbuchs aktualisieren. Weitere Kernpunkte einer automatisierten Lösung sind:

- Vorgefertigte Prozessabläufe, die nur noch kundenspezifisch angepasst werden müssen
- Test-Werkzeuge
- Schnittstellen zur IT-Infrastruktur, zum IT-Betrieb, zu verschiedenen Sensoren sowie zur Gebäude- und Anlagentechnik

Mithilfe der modellierten und automatisierten Prozesse in Verbindung mit einer intelligenten Mensch-Maschine-Interaktion laufen Fehlerbehebungen im Notfall weitestgehend automatisiert ab. Die Notfallmanager haben somit jederzeit den Überblick, welche Maßnahmen sie umgehend ergreifen müssen und welche Kollegen oder Dienstleister zu informieren sind, wenn ein Problem weiter besteht und nicht innerhalb der vorgegebenen Zeit behoben werden kann.

Schlank ist gleich schnell

Um eine maximale Effektivität zu erzielen, sollten die im Notfall ablaufenden Prozesse möglichst schlank gestaltet werden. Beim Modellieren werden die Prozesse deshalb in der Regel ausführlich geprüft. Ziel: Die notwendigen Aufgaben noch schneller erfüllen zu können. Ein ausgeklügeltes Informations- und Warnsystem muss außerdem dafür sorgen, dass die Notfallmanager zu jeder Zeit umfassend über sämtliche Vorgänge im Rechenzentrum informiert sind.

Das automatisierte Notfallhandbuch ist somit ein guter Einstieg in die Prozessautomatisierung. Denn diese ermöglicht es nicht nur, Notfälle schneller zu beheben, sondern kann für alle Prozesse im Rechenzentrum zum Einsatz kommen. Durch diese Technik können sehr effizient auch kleinere Probleme beseitigt werden, bevor die Anwender davon erfahren.

Wilfried Cleres,
Global Portfolio Manager Data Center, Fujitsu
Klaus Pfeiffer,
Manager, Data Center Infrastructure Management,
Fujitsu TDS GmbH

Mehr als nur eine Steckdose

Die passenden Stromverteilungsleisten fürs eigene RZ finden

Statistiken zufolge entfällt etwa die Hälfte der Gesamtkosten auf den Strom. Auch zum Verbessern der PUE-Werte im RZ sind Verbrauchsmessungen notwendig. Eine intelligente Stromverteilung erledigt das mit. Welche Arten an Stromverteilungsleisten gibt es und wie kann jede einzelne sich im RZ nützlich machen?

Stromverteilungsleisten (Power Distribution Units, PDUs) gibt es in den verschiedensten Ausführungen: mit Messfunktion, Monitoring- und Schaltfunktion, Smart PDUs sowie PDUs für die komplette Energieverwaltung. Zwar verwenden nicht alle Hersteller die gleichen Bezeichnungen, die Funktionalität jedoch ist allgemein die gleiche.

PDUs mit Messfunktion sind als Basisversion die simpelste Variante. Nur mit einem Display ausgestattet, zeigen sie den Stromverbrauch in Echtzeit an. Angezeigt werden wie bei Leistungsmessern Leistung und Leistungsfaktor. Allerdings sind die Daten Schrank für Schrank manuell von der Stromverteilungsleiste abzulesen.

PDUs mit Monitoring-Funktion und Smart PDUs bieten zusätzlich die Möglichkeit der Fernüberwachung des Stromverbrauchs auf der Ebene der Stromverteilungsleiste oder auf Steckdosenebene. Zusammen mit einer Software liefern diese Geräte alle wichtigen Informationen per Browser. Sie sind sehr nützlich für personalfreie Rechenzentren mit „Lights Out Management“ (LOM) sowie für große Rechenzentren. Damit ist effektives Verwalten der Energie möglich, ohne dass jemand direkt vor Ort sein muss, um die Werte von der Stromverteilungsleiste abzulesen, wie es bei einer PDU mit Messfunktion der Fall ist. Die Software bietet zudem Trendinformationen

zum langfristigen Verbrauch, die ansonsten bei einer PDU mit Messfunktion manuell zusammengestellt werden müssten.

PDUs mit Schalt- und Managementfunktion bieten zusätzliche Funktionen und besitzen zum Teil Ausgänge, um Temperatur- und Feuchtigkeitssensoren anzuschließen. Manche Stromverteilungsleisten ermöglichen es, Stromausgänge einzeln aus der Ferne ein- und auszuschalten. Je nach Funktionsumfang ist ein Monitoring entweder für die PDU als ganze möglich, oder der Stromverbrauch wird pro Steckdose angegeben. Ein Reporting auf Steckdosenebene bietet eine nützliche Statistik, mit der die Effizienz des jeweiligen Switches oder Servers bestimmt werden kann. Im Allgemeinen kann das Reporting von Remote-Standorten aus erfolgen. Für mehr Funktionalität und Bedienfreundlichkeit werden Smart PDUs in eine Softwareanwendung integriert. Den meisten Nutzen und die größte Flexibilität bieten PDUs, die Statistiken über SNMP (Simple Network Monitoring Protocol) liefern und die Verwendung mit jeder Software ermöglichen, die Messdaten auslesen kann. So lassen sich Produkte von verschiedenen Herstellern als Mix & Match verwenden, ohne an die proprietäre Software eines einzigen Herstellers gebunden zu sein.

Verfügbarkeit absichern

In den Rechenzentren vollzieht sich ein Wandel hin zu einem effizienteren Betrieb und sogar einem „Lights out"-Betrieb ohne Personal. Hier punkten die Stromverteilungsleisten mit handfesten Vorteilen. Zum einen verringert sich das Risiko menschlichen Versagens, zum anderen wird im Betrieb Energie gespart, da ohne Personal das Licht aus bleibt und die Klimatisierungssysteme diese sonst zusätzlich erzeugte Wärme nicht abführen müssen. Der Haken am personalfreien Betrieb ist allerdings, dass bei auftretenden Problemen mit einem Server immer erst jemand zum Standort fahren muss, um das Problem zu beheben.

Auch hier helfen Stromverteilungsleiste. PDUs mit Schaltfunktion ermöglichen es den Administratoren, den Strom zum Server ab- und wieder anzuschalten und damit einen Neustart zu erzwingen. Oder ein Gerät verursacht beispielsweise Netzwerkfehler. Dann kann es remote abgeschaltet werden, bis ein Wartungstechniker da ist.

Energieverbrauch verwalten und optimieren

Neben dem Vorteil der Fernein- und -abschaltung liegt ein weiterer Nutzen der intelligenten Stromverteilung im Optimieren des Energieverbrauchs. Dazu muss dieser zuerst einmal gemessen werden. Hier gilt der Grundsatz, dass nur korrigiert werden kann, was vorher auch gemessen wurde. Für kleinere Rechenzentren mag die Messung des Gesamtenergieverbrauchs der PDU ausreichend sein, komplexere Rechenzentren hingegen bevorzugen wahrscheinlich eine Verbrauchsangabe für jeden einzelnen Ausgangssteckplatz. Bei diesen Modellen lassen sich noch weitergehende Kennwerte ermitteln, wie zum Beispiel das Verhältnis von CPU-Auslastung zu Stromverbrauch, um daraus die Effizienz der einzelnen Server zu berechnen.

Als Unternehmen mit Virtualisierung begannen, diente die CPU-Auslastung als Entscheidungskriterium dafür, welche Server aus dem Betrieb genommen und auf anderen Hardware-Plattformen virtualisiert wurden. Anwendungen mit geringster CPU-Auslastung ließen sich problemlos virtualisieren und sorgten so im Zusammenspiel für eine Spitzenauslastung der Hardware von 80 Prozent und mehr. Allerdings stellten RZ-Betreiber immer wieder fest, dass die zuvor prognostizierten Energieeinsparungen am Ende doch nicht erzielt wurden.

Zu einem großen Teil war das der Tatsache geschuldet, dass die CPU-Auslastung als einziger Kennwert bestimmt wurde. Erst das Verhältnis von CPU-Auslastung zu Stromverbrauch ermöglicht es aber, die Server Usage Effectiveness (SUE) zu ermitteln beziehungsweise den Wirkungsgrad zu berechnen. Auch hier wird eine intelligente PDU, die eine Messwertabnahme auf Steckdosenebene bietet, beide Seiten der notwendigen Gleichung einbeziehen.

Und schließlich ist auch die Kenntnis der genauen Zeiten mit Spitzenauslastung wichtig. Energieversorger, die mit der Smart-Grid-Technik arbeiten, nutzen diese Kenntnis, um über ihre Grids in Zeiten mit höchstem Verbrauch – beispielsweise von 08.00 Uhr bis 17.00 Uhr – auch die höchsten Preise zu berechnen. Die Kenntnis der eigenen vorhandenen Lastspitzen veranlasst Unternehmen, stromintensive Prozesse auf solche Zeiten zu verlegen, in denen die Strompreise günstiger sind. Wenn eine Bank zum Beispiel über die Messungen herausfindet,

dass die größte Datenverarbeitungsleistung immer am späten Nachmittag benötigt wird, lassen sich signifikant Kosten sparen, indem andere Anwendungen auf die Zeit nach 18.00 Uhr verlegt werden.

Trendanalyse und Reporting

Um den Stromverbrauch genau prüfen zu können, sollten Berechnungen und Trendberichte mindestens 30 Tage umfassen, besser noch 90 Tage. Das erst macht es möglich, eine Monats- und Quartalsanalyse der Verbrauchsspitzen durchzuführen. Ein Wert, der zeitlich isoliert als Momentaufnahme abgelesen wird, ist ein unzureichendes Maß für die Effizienz und das ist zugleich ein Hauptkritikpunkt an PUE als direktes Maß der Effizienz. Der Stromverbrauch variiert je nach Phasen hoher beziehungsweise schwacher Auslastung. Auch hier bietet nur die Verlaufserfassung auf Steckdosenebene die notwendigen Informationen, um faktenbasierte Entscheidungen treffen zu können.

Intelligente PDUs zu haben, reicht allerdings allein nicht aus. Die Intelligenz muss auch dokumentiert werden und das erfolgt mittels einer Software. Manchmal werden intelligente PDUs mit einem Softwarepaket geliefert, das nur die Basisanforderungen erfüllt, während andere über eine DCIM (RZ-Infrastruktur-Management) Softwareanwendung überwacht werden können. DCIM Softwareanwendungen unterscheiden sich in Preis und Funktionalität, genauso wie sich die PDUs in ihrem Preis und den Funktionsmerkmalen unterscheiden.

PDUs in der praktischen Anwendung

Unternehmen kaufen mitunter intelligente PDUs und stellen dann fest, dass ihnen das DCIM-Paket zu teuer ist. Andere wiederum haben nur einige PDUs mit Intelligenz. Und wieder andere haben eventuell eine Reihe intelligenter PDUs mit proprietärer Software, die daraufhin untereinander nicht kompatibel oder interoperabel sind. Kurzum, es gibt viele Gründe, warum diese PDUs zwar gekauft, doch nicht in vollem Umfang genutzt werden. Sobald diese jedoch vollumfänglich in die Software integriert sind, ist der Return on Investment durchaus vielversprechend.

Quelle: Siemon

In Verbindung mit Software liefern intelligente Stromverteiler alle wichtigen Daten über eine browserbasierte Schnittstelle.

Fällt die Wahl auf intelligente PDUs, dann sind die Themen Software und Reporting genauso wichtig wie die Auswahl der Hardware. In jedem Fall sollte die Entscheidung auf Grundlage des Funktionsumfangs von Hardware und Software getroffen werden. Offene Systeme mit offenen Protokollen sind äußerst vorteilhaft, wenn ein Unternehmen sich späterhin entschließt, auf komplette DCIM-Systeme aufzurüsten oder – aus welchen Gründen auch immer – den Anbieter zu wechseln.

Carrie Higbie,
Global Director Data Center Solutions und Services, Siemon

Das Rechenzentrum aufs Smartphone gebracht

Cloud-Dienstleister abakus it setzt auf Software zur Remote-Überwachung

Mit rund 800 Servern in ihrem Rechenzentrum Bodensee-Oberschwaben ist die abakus it AG einer der größten Private-Cloud-Dienstleister der Region. Mit einer Software überwacht das Personal des Kontrollzentrums alle Umgebungsparameter im Datacenter von jedem mobilen Endgerät aus.

Im Jahr 2007 nahm die abakus it AG ein Kundenrechenzentrum in Betrieb und bot als erstes Unternehmen in der Bodenseeregion Private-Cloud-Computing-Dienste an. Mit Erfolg: Der Service findet so viel Anklang, dass im Jahr 2013 die Kapazitäten durch ein neues Rechenzentrum erweitert wurden.

Als Private-Cloud-Dienstleister betreibt die abakus it AG in ihrem Rechenzentrum auf etwa 800 Servern rund 90 verschiedene Kundeninfrastrukturen und liefert IT-Dienste für rund 3000 Endbenutzer-Arbeitsplätze. Konsequenterweise sollten nach Wunsch des Vorstands auch die Administratoren des Kontrollzentrums in der Lage sein, möglichst von überall aus den Zustand des Rechenzentrums abzufragen. Um bei Problemen sofort reagieren zu können, suchte Dipl.-Ing. Wolfgang Kölble, Vorstand bei der abakus it AG, nach einer Lösung, die dem Administrator unabhängig von seinem Aufenthaltsort sofort ein klares Bild der Lage verschafft – nicht nur vom Zustand der Server, sondern auch von den Umgebungsbedingungen im Rechenzentrum.

Eine solche Lösung erhöhe nicht nur die Sicherheit des Datacenter-Betriebs, sondern bringe dem Betreiber auch Vorteile in Sachen Wirtschaftlichkeit und Personalmanagement: „Es ist nicht sinnvoll, hochqualifiziertes Personal einzustellen, damit es dann nächtelang auf Monitore starrt. Wenn der Administrator seine Bereitschaftszeiten außerhalb des Büros verbringen kann, erhöht das seine Lebensqualität und senkt zugleich Kosten für das Unternehmen und letztlich auch für unsere Kunden“, so Kölble.

Quelle: dtm Datentechnik Moll GmbH

Immer im Blick: Eine Software stellt die Zustände der verschiedenen Sensoren im RZ im Browser des Smartphones dar (Abb. 1).

Im Zuge des Projekts kamen die Verantwortlichen auch auf das Thema Gefahrenmeldeanlage zu sprechen. In diesem Zusammenhang skizzierte man die Idealvorstellung: Eine Lösung, die weitaus weniger kompliziert ist als umfassende Lösungsansätze wie beispielsweise Microsoft System Center, sondern eher so intuitiv und schnell verständlich wie eine Ampel.

Ein Interface für alle Parameter

Es stellte sich heraus, dass im benachbarten Meckenbeuren bei dtm gerade die Entwicklung der Software EnviMonitor im Gang war. Die Anwendung will alle Sensordaten aus dem Rechenzentrum direkt auf einem beliebigen mobilen Endgerät visualisieren. Neben den einzelnen Messgrößen können damit auch Lage und Zustand aller Sensoren im Überblick gezeigt werden. Der Leistungsumfang kam dem sehr nahe, was sich Wolfgang Kölble wünschte.

Überwacht werden müssen vor allem die klimatischen Bedingungen im Serverraum, um einen ausfallsicheren und energieeffizienten Rechenzentrumsbetrieb zu gewährleisten. Bei der hohen Packungsdichte heutiger Datacenter ist das Abführen der Abwärme eine der wichtigsten Aufgaben der physischen Infrastruktur.

Deshalb ist es wichtig, für alle neuralgischen Punkte innerhalb eines Rechenzentrums die relevanten Parameter zu kennen: Die aufgenommene Leistung, Temperatur, Luftfeuchte und den Taupunkt im Schrank. Außerdem müssen Stärke und Temperatur des Luftstroms an verschiedenen Stellen gemessen werden, um sicherzugehen, dass beispielsweise das Trennen von Kalt- und Warmgängen funktioniert. Auch Sensoren zum Erkennen von eventuellen Leckagen an den wasserbasierten Wärmetauschern gehören dazu. Türkontaktsensoren überprüfen zudem, ob die Racktüren ordnungsgemäß geschlossen sind. Das ist nicht nur wichtig für die Klimatisierung – eine ungeplant geöffnete Tür kann auch ein Indiz für einen unbefugten Zutritt ins Rechenzentrum sein.

Sensoren zum Erfassen des Geräuschpegels können ebenfalls auf Eindringlinge verweisen, warnen aber auch vor Belüftungsproblemen, wenn beispielsweise ein Lüfter plötzlich lauter wird. Alle diese Systeme kann die von der abakus it AG eingesetzte Lösung visualisieren – mit einer Farbcodierung, die ganz im Einklang mit Wolfgang Kölbles Wunsch nach einer „Ampel“ auf einen Blick zeigt, ob alles im grünen Bereich ist. Bilder von Videokameras kann die Software ebenfalls live abrufen.

Für alle Betriebssysteme

Die Software ist eine webbasierte Anwendung für Apache-Tomcat-Server und ist genügsam hinsichtlich der Hardware-Anforderungen: Die Linux-Appliance läuft in einer virtuellen Umgebung mit einem

Hauptspeicherbedarf von 512 MB RAM. Als Serverplattform werden auch alle Netzwerkspeicher von QNAP mit der aktuellen Betriebssystemversion QNAP 4.0 unterstützt. History-Daten werden in einer ebenfalls serverbasierten SQL-Datenbank gespeichert und können grafisch dargestellt werden.

Der Zugriff auf die Software passiert per Browser, sodass neben Windows, iOS und Android auch Citrix und jedes andere denkbare Endgerät, auf dem ein Browser läuft, geeignet ist. Eine lokale Installation von Apps oder Plug-ins ist aufgrund dieser Architektur nicht notwendig. Der passwortgeschützte Zugriff der mobilen Clients aus dem öffentlichen Netz ist per SSL/TLS gesichert.

Logisch strukturiertes Interface

Die Software will dem Anwender mehr Übersicht über das komplexe Vorgehen im Rechenzentrum verschaffen, in dem sie gruppiert: Mehrere Sensoren desselben Typs können zu einer Sensorgruppe zusammengefasst werden. Sensorgruppen können hierarchisch in einer Baumstruktur angeordnet werden. Dem Benutzer ist es dabei freigestellt, ob er sich zum Beispiel in einer Gruppe alle Temperatursensoren anzeigen lassen will oder ob er die Sensoren nach dem Layout seines Rechenzentrums zusammenfasst in Gruppen wie „Serverraum 1“, „Kaltgang 1“ und so weiter. Je nach Sichtweise können Sensoren auch gleichzeitig mehreren Gruppen zugeordnet werden.

Für jede Gruppe können Limits und Aktionen definiert werden, also etwa die Grenzwerte, bei deren Überschreiten ein Alarm oder das Abschalten von Komponenten ausgelöst werden soll. Wenn für eine Sensorgruppe keine Grenzwerte und Regeln für Benachrichtigungen festgelegt wurden, erbt diese Gruppe die Limits und Aktionen von der übergeordneten Gruppe. Der Aufwand für das manuelle Konfigurieren wird damit reduziert.

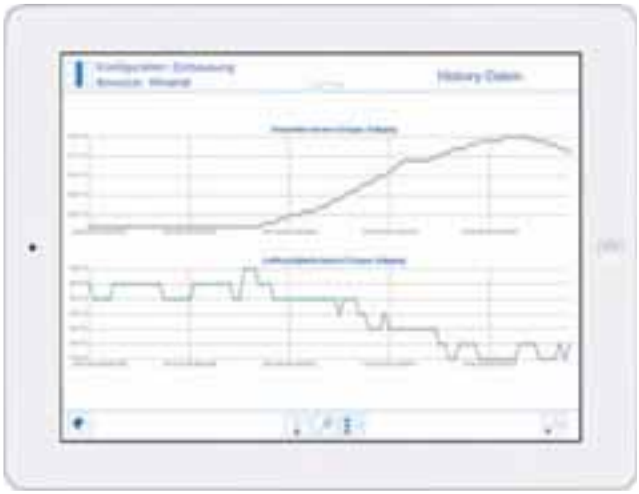
Erfolgt die Vererbung der Konfigurationseinstellungen von einer logischen Ebene des Baumdiagramms zur nächsten nach dem Top-to-Bottom-Prinzip, so verhält es sich im Tagesbetrieb genau umgekehrt. Aktuelle Ereignisse, also Sensorwerte, Alarme und Vorwarnungen, werden Bottom-to-Top immer an die übergeordnete Gruppe weitergegeben. Das Zusammenfassen in Gruppen hält Darstellung auf dem Smartphone kompakt. Es genügt somit, beispielsweise die Gruppen „Serverraum 1“ und „Serverraum 2“ auf dem Display zu haben. Passiert etwas in einem der untergeordneten Racks in diesen Gruppen, wird der Alarm auch in der obersten Gruppe signalisiert. Der Benutzer kann dann im konkreten Bedarfsfall gezielt in die Verzeichnisstruktur einsteigen.

Implementierung bei abakus it

Nach einer In-house-Schulung durch den Hersteller sollen fünf Mitarbeiter der abakus it AG rollierend Zugriffsrechte für die Überwachung der Umgebungsbedingungen erhalten. Für den Zugriff auf physische Infrastruktur-Geräte sieht der Vorstand der abakus it AG diese Personenzahl als Obergrenze. „Bei mehr Personen wäre der Aufwand für das Gewährleisten des Datenschutzes so hoch, dass er die Effizienzgewinne durch die neue Software wieder auffressen würde“, so Kölble. Deshalb erhalten nicht automatisch alle Mitarbeiter, die auf virtuelle Kundensysteme zugreifen dürfen, auch Zugriffsrechte auf die Kontroll-Plattform.

Die abakus it AG betreibt die Software mittels Citrix Receiver auf eigenen virtuellen Servern. „Damit maximieren wir die Ausfallsicherheit und nutzen die Vorteile der neuen Lösung zum Wohle unserer Kunden voll aus“, resümiert der Vorstand. Außerdem wolle man im Rahmen einer Entwicklungspartnerschaft Vorschläge zum Verbessern der Lösung an den Hersteller geben.

Quelle: dtm Datentechnik Moll GmbH



Grafische Darstellung der History-Daten des Rechenzentrums, die von der Kontroll-Software aus einer SQL-Datenbank gezogen werden (Abb. 2).

Jan Moll,
Geschäftsführer, dtm Datentechnik Moll GmbH

Die Punktlandung

Sicherheit von der Spannungsversorgung bis zum Serverrack

In Hannovers Süden ist in den vergangenen Monaten eines der modernsten Rechenzentren Deutschlands entstanden: Die TÜV Nord Group konzentriert hier zukünftig alle EDV-Aktivitäten der nationalen und internationalen Tochtergesellschaften. Neben hoher Verfügbarkeit und Sicherheit stand bei der Planung auch die Energieeffizienz ganz oben auf der Prioritätenliste. Ein Blick hinter die Kulissen.

Über 10.000 Mitarbeiter sind innerhalb der TÜV Nord Group in Deutschland und in über 70 Ländern weltweit tätig. Um die notwendige EDV-Infrastruktur für die Mitarbeiter zur Verfügung zu stellen, betreibt der Anbieter von Beratungs-, Service- und Prüfdienstleitungen vier Rechenzentren in Deutschland und mehr als 70 Kleinstrechenzentren weltweit. Das mittelfristige Wachstum von etwa zehn Prozent pro Jahr konnte mit der aktuellen EDV-Infrastruktur kaum bewältigt werden. Da ein Modernisieren der vorhandenen Rechenzentren finanziell nicht sinnvoll war, entschied sich der Vorstand für den Neubau eines Rechenzentrums am Standort Hannover. Das Ziel: Sämtliche Aktivitäten aller nationalen und internationalen Rechenzentren zu konsolidieren und zu zentralisieren. Insgesamt investierte das Unternehmen rund acht Millionen Euro, wobei die reinen Baukosten etwa ein Drittel der Gesamtsumme ausmachen.

Schutz vor Einbruch, Feuer und Wasser

Das neue Rechenzentrum, das in massiver Bauweise errichtet wurde, hat eine Grundfläche von 1.500 Quadratmeter und ist aufgeteilt in einen zweigeschossigen Mitteltrakt, in dem die Technikzonen untergebracht sind, sowie zwei eingeschossige Hallenflügel mit den Serverräumen. Neben den Technikkomponenten sind im mittleren Gebäudeteil ein Leitstand und Besprechungsraum vorgesehen. Das Rechenzentrum erfüllt höchste Sicherheitsstandards gemäß der TÜViT Zertifizierung „Trusted Site Infrastructure“ Level 3, wobei der TÜViT selbst nach EN 45 011 akkreditiert und zertifiziert ist.

Quelle: Rittal

Ein Dieselmotor hält den Betrieb des neuen RZ bis zu 72 Stunden lang aufrecht (Abb. 1).

Hohe Verfügbarkeit essenziell

Auch den Anforderungen der European Security Systems Association (ESSA) tut die TÜV Nord Group genüge und kann im Rechenzentrum mit dem ECB-S-Standard nach EN 1047-2 punkten: Die Norm besagt, dass die sicherheitstechnischen Einrichtungen wirkungsvoll gegenüber Einbruch, Brand und Wasser geschützt sein müssen. So sind die beiden Serverräume als ECB-S-zertifizierte Sicherheitszellen als Raum-in-Raum-System ausgeführt. Sie können einem Feuer für 180 Minuten standhalten, ohne dass die IT-Infrastruktur im Innern in Mitleidenschaft gezogen wird. Innerhalb der Serverräume sorgt eine automatische Brandlöschanlage von 3M dafür, dass ein entstehendes Feuer schnell und wirkungsvoll gelöscht wird, ohne die Hardware zu beschädigen.

18 Kameras mit 360-Grad-Objektiven überwachen das gesamte Gebäude inklusive des Außenbereichs rund um die Uhr. Fünf gestufte Sicherheitszonen mit Zutrittskontrollanlagen sorgen dafür, dass nur berechtigtes Personal die jeweilige Zone betreten kann. Den Serverbereich selbst kann wiederum nur der betreten, der einen individuellem Zahlencode eingibt. Insgesamt haben bloß zwei oder drei Personen uneingeschränkten Zutritt zu allen Bereichen des neuen Rechenzentrums. Das gesamte Sicherheitsmanagement entspricht den Qualitätsstandards gemäß ISO 27001 und ISO 27002.

Während der Planung haben die Verantwortlichen festgelegt, dass die Verfügbarkeit 99,99 Prozent entsprechen soll – das bedeutet eine maximale Ausfallzeit des Rechenzentrums von 52 Minuten im Jahr. „Weiterhin wurde die externe Energieversorgung so dimensioniert, dass das Rechenzentrum 72 Stunden unabhängig von der externen Netzversorgung betrieben werden kann.“, erklärt Leroy Racette, Bereichsleiter EDV bei der TÜV Nord Group. Um diese hohe Verfügbarkeit zu erreichen, sind alle relevanten Systeme doppelt ausgeführt. Dies fängt bereits bei der Einspeisung aus der Mittelspannungsebene an: Das Rechenzentrum erhält seinen Strom vom Energieversorger über zwei getrennte Linien.

Sicher versorgt und geschützt

Die Niederspannungshauptverteilung (NSHV) ist redundant ausgeführt, sodass zwei komplett getrennte Stränge im gesamten Rechen-

Quelle: Rittal

Intelligente Stromverteilungsleisten, die in den Server-Racks installiert sind, erfassen die Energieaufnahme und leiten die Daten an ein Monitoring-System (Abb. 2).

Quelle: Rittal

Auf Wunsch der TÜV Nord Group wurden die Racks und Türen der Gangeinhausungen im unternehmenstypischen Blau lackiert (Abb. 3).

zentrum vorhanden sind. Die Versorgung der einzelnen technischen Einrichtungen und auch der Serverräume kann alternativ über einen der beiden Stränge erfolgen. Kuppelschalter sorgen dafür, dass sowohl zwischen den beiden Einspeisetransformatoren und der Netzersatzanlage, als auch zwischen den beiden NSHV umgeschaltet werden kann. Die NSHV hat einen Bemessungsstrom von 4.000 Ampere und basiert auf dem Ri4Power-System von Rittal. Durch die formunterteilte Bauweise in 4b ist ein Arbeiten an einzelnen Abgängen möglich – und zwar ohne, dass die gesamte Anlage spannungsfrei geschaltet werden muss. Sollte doch einmal ein Stromausfall auftreten, muss die USV die Versorgung nur einige Minuten aufrechterhalten: Der Dieselmotor der Netzersatzanlage (NEA) leistet 1.500 Kilowatt und kann über einen Generator das komplette Rechenzentrum für 72 Stunden versorgen – bei einem Verbrauch von 250 Litern Diesel pro Stunde. Bis Dieselmotor und Generator synchronisiert sind, dauert es nur wenige Minuten.

Energieeffiziente Kühlung und Stromverteilung

Auch die Kühlung des Rechenzentrums ist redundant aufgebaut. Im Obergeschoss des Mitteltrakts stehen dazu die Kältemaschinen, die die entsprechende Kälteleistung zur Verfügung stellen. Auf dem Gebäudedach sind zwei Hybridkühler installiert, die die Wärmeenergie aus den Serverräumen an die Umgebung abgeben. Diese kühlen das Wasser-Glykol-Gemisch zunächst mit Umgebungsluft, was bis zu einer Außentemperatur von 16 Grad Celsius funktioniert. Bei höheren Temperaturen erfolgt die Kühlung über verdunstendes Wasser. Die damit erzielte Energieeinsparung entspricht einem verminderten CO_2-Ausstoß von etwa 312 Tonnen pro Jahr. Das gekühlte Wasser kühlt in den Serverräumen die Luft/Wasser-Wärmetauscher (LWWT), die dann die Kaltluft für die Server zur Verfügung stellen. Die 120 Serverschränke in Serverraum 1 sind in einem Kalt-/Warmgang-Konzept aufgestellt.

Blau machen erwünscht

Sämtliche Serverschränke im neuen RZ wurden blau lackiert, um dem Corporate Design des Unternehmens zu entsprechen. Die Energieversorgung für die Server erfolgt durch den Doppelboden. Für die Stromversorgung in den IT-Racks ist ein modulares Stromverteilungssystem installiert. Es ist die Grundvoraussetzung für Energieeffizienz, da es die elektrische Leistung messen kann sowie alle weiteren wichtigen elektrischen Betriebsparameter wie Spannung, Strom, Powerfaktor und Energieverbrauch pro Phase.

Überwachung und Optimierung

Das System stellt die Messwerte sowohl über den im Monitoringssystem integrierten Webserver als auch per SNMP zur Verfügung. Durch das Anbinden an ein Energiemanagementsystem lässt sich der Energieverbrauch überwachen und optimieren. Auch andere wichtige Messwerte, wie etwa die Temperaturen im Kalt- und im Warmgang, werden überwacht.

Seit Jahresbeginn läuft die gesamte Rechenleistung nun ausschließlich über das neue Rechenzentrum. Bis zu 1.200 Bladeserver will die TÜV Nord Group zukünftig einbauen. Besonders stolz ist die TÜV NORD GROUP – neben der technischen Leistungsfähigkeit des neuen Rechenzentrums – auf den vollständig eingehaltenen Kostenplan. „Sowohl beim Projektplan als auch bei den Baukosten sind wir im Plan geblieben. Dies ist bei Projekten dieser Größenordnung nicht selbstverständlich“, hebt Leroy Racette heraus. Eine Punktlandung eben.

Michael Schell,
Leiter Produktmanagement Power Distribution, Rittal, Herborn
Bernd Hanstein,
Hauptabteilungsleiter Produktmanagement IT, Rittal, Herborn
Kerstin Ginsberg,
PR-Referentin IT, Rittal, Herborn

Datenverschlüsselung ist kein Hexenwerk

Datenverkehr zwischen Unternehmensstandorten wirksam absichern

Unzureichend geschützte Datentransportleitungen bergen die Gefahr massiver wirtschaftlicher Schäden für Unternehmen. Auf Sicherheitslösungen zum Verschlüsseln der Verbindungen setzt bislang allerdings nur knapp ein Drittel aller Unternehmen. Dabei ist das Absichern der Übertragungen durchaus machbar.

Die Faustregel klingt einfach: Alle zwischen Unternehmensstandorten ausgetauschten Daten sind zu schützen. Der Haken: Anbieter globaler Datenverbindungen bieten standardmäßig keine Nutzdatenverschlüsselung an. Daher ist ein gleichermaßen hoher datenschutzrechtlicher Standard in sämtlichen Ländern oft nicht gewährleistet – Unternehmen müssen für ihren Schutz selbst sorgen.

Das Netzwerk wird allgemein als eine Schichtenarchitektur begriffen, die sich aus sieben aufeinanderfolgenden Schichten – den sogenannten OSI-Layern – zusammensetzt. Eine Verschlüsselung ist prinzipiell in jedem Layer möglich. Für Unternehmen und staatliche Einrichtungen, die ihre Daten ausreichend absichern wollen, ergibt sich bislang die Wahl zwischen einer IPsec-basierten Verschlüsselung auf OSI Layer 3 oder der Ethernet-basierten Layer 2-Verschlüsselung. Beide Varianten haben ihre Daseinsberechtigung; daher ist es sinnvoll, den Verschlüsselungs-Layer je nach Einsatzszenario auszuwählen.

Behörden und die geheimschutzbetreute Industrie unterliegen im Datenschutz den höchsten Sicherheitsauflagen, wofür eine Verschlüsselung auf Layer 3 nicht ausreicht: Sie kann nur den IP-Verkehr codieren, der Rest – beispielsweise die darunterliegenden Layer 2-Protokolle – bleibt unverschlüsselt. Zudem bleibt der Header teilweise zugänglich: Informationen, etwa wer mit wem kommuniziert, könnten beispielsweise über eine Verkehrsfluss- oder eine Infrastrukturanalyse ausgelesen und für Angriffe genutzt werden.

Hinzu kommt, dass die IPsec-basierte Verschlüsselung mit einer enormen Overhead-Belastung einhergeht. Der kryptografische Protokoll-Overhead, der für die Verschlüsselung den übertragenen Paketen hinzugefügt wird, variiert abhängig von der Paketgröße, verbraucht aber bis zu 60 Prozent der Bandbreite. Die Folge sind mögliche und im Vorhinein unkalkulierbare Bandbreiteneinbußen, je nach den aktuell laufenden Anwendungen. Auch darf nicht vergessen werden, dass das Auswerten und Verarbeiten der Paket-Header gemäß IPsec-Protokoll Zeit kostet. Dadurch kommt es zu einer erhöhten Latenz und einer eingeschränkten Performance gegenüber unverschlüsselter Übertragung. Es gibt aber auch Vorteile: IPsec-basierte Verschlüsselung funktioniert in allen gerouteten Netzwerken und ist daher ein weit verbreitetes Standard-Verfahren.

Die Alternative ist eine Layer 2-Verschlüsselung, die auf Ethernet-Frames angewendet wird. Ihr wesentlicher Vorteil gegenüber IPsec-basierten Verschlüsselern ist der Bandbreitenzugewinn durch das optimierte Overhead-Verhalten. Die Verschlüsselungsprotokolle für Layer 2 sind jedoch auf die Kommunikation zwischen den Verschlüsselern begrenzt und dadurch um bis zu 40 Prozentpunkte geringer als auf Layer 3. So wird der Datenfluss weniger stark ausgebremst. Mögliche Payload-Durchsatzraten von 10 bis 40 Gigabit pro Sekunde stehen hier den in der Praxis auf etwa 3 Gigabit pro Sekunde beschränkten Layer 3-Lösungen gegenüber. Zudem werden auf Layer 2 neben der Payload auch die IP-Adressen verschlüsselt und damit für Unbefugte unlesbar.

Quelle: Rohde & Schwarz SIT

Moderne Highspeed-Verschlüsseler sorgen für abhörsichere Datenübertragung mit bis zu 40 Gbit/s.

Sicherheit ist mehr als Technik

Der Erfolg einer Datenverschlüsselung hängt nicht ausschließlich an den technischen Aspekten. Zur Sicherheit gehören ebenfalls Zuverlässigkeit und Ausfallsicherheit einer Lösung, daher ist auch die richtige Wahl des Anbieters wichtig. Dessen finanzielle Stabilität sowie seine Herkunft und Service-Lokationen stellen erste Orientierungspunkte dar – nicht erst seit den Snowden-Enthüllungen gibt es viele offene Fragen, wenn US-basierte Anbieter zum Zug kommen. Um sich auf die hohen deutschen Datenschutzstandards verlassen zu können, empfiehlt sich ein europäischer Anbieter für IT-Sicherheitslösungen, im Idealfall mit eigenen Entwicklungs- und Produktionsstätten im Inland.

Einen optimalen Schutz vor unberechtigtem Datenzugriff bieten Verschlüsselungslösungen von Anbietern, die vom BSI zertifiziert sind. Ein weiterer Anhaltspunkt: Die Verschlüsselung sollte in einem separaten Gerät erfolgen – nur dann bleibt sie beim Angriff auf die Netzwerktechnik unangetastet.

Peter Rost,
Leiter Produktmanagement, Rohde & Schwarz SIT

Alle Partner in einer Wolke

Clouds für definierte Gruppen, sogenannte Community Clouds, schützen gespeicherte Inhalte durch definierte Eintrittsbarrieren

Datenschutz ist beim Cloud Computing nach wie vor ein kritischer Punkt – und wird es auch bleiben. RZ-Verantwortliche, die größere Datenmengen auslagern oder Möglichkeiten zum Austausch mit anderen Unternehmen schaffen wollen, sollten daher auf größtmögliche Sicherheit achten. Eine Lösung können Community Clouds sein.

In die bekannten Anwendermodelle von Public, Private und Hybrid Cloud eingeordnet, rangiert die Community Cloud zwischen dem privaten und dem öffentlichen Wolken-Modell. Hier schließen sich Unternehmen, Institutionen oder Behörden mit ähnlichen Interessen zu einer Community zusammen. Entweder betreibt eine der Partner-Institutionen die Cloud-Infrastruktur oder ein Dritter, beispielsweise ein Cloud Service Provider (CSP). Die gemeinsamen physischen Ressourcen stehen als Shared Infrastructure ausschließlich diesem eingeschränkten Nutzerkreis zur Verfügung. Besonders in Hinblick auf gemeinsame Teilprozesse oder Projekte unterschiedlicher Unternehmen bietet die Community Cloud enorme Vorteile für die Zusammenarbeit.

Dabei sind verschiedene Einsatzszenarien denkbar: Unternehmen mit Partnerstrukturen, die den Zugriff auf gemeinsame Ressourcen realisieren wollen, bietet sich die Community Cloud an. In der Automotive-Industrie hat sich dieses Modell beispielsweise etabliert: OEMs, Zulieferer und Partner nutzen eine gemeinsame Infrastruktur für den sicheren Austausch kritischer Entwicklungs-, Einkaufs-, und Produktionssteuerungsdaten. Ein unabhängiger Verein betreibt die technische Infrastruktur dieses Netzwerks.

Quelle: Zimory

Eine Community Cloud sollte verschiedene Anforderungen erfüllen, damit sie ihren Zweck erfüllt und möglichst sicher betrieben werden kann (Abb. 1).

Vertrauen durch Kontrolle und einheitliche Standards

Die Community Cloud bringt einige zentrale Vorteile: Sie stellt einen Schutzraum dar, in dem mehrere Teilnehmer untereinander sensible Daten – beispielsweise vertrauliche Entwicklungs-, Logistik- oder Steuerdaten – austauschen. Im Vergleich zur klassischen Public Cloud bietet die Community Cloud ein deutliches Mehr an Sicherheit: Das ist durch den beschränkten Nutzerkreis begründet, vor allem wenn dieser über klar definierte Eintrittsbarrieren wie Audits oder Zertifizierungen verfügt. Diese Barrieren sollten gleichzeitig das Einhalten von Mindeststandards sicherstellen, auf die sich die Teilnehmer der Community Cloud im Vorfeld geeinigt haben.

Das kann beispielsweise die ISO 27001 für Informationssicherheit sein, die Sicherheitsempfehlungen für Cloud-Computing-Anbieter des BSI (Bundesamt für Sicherheit in der Informationstechnik) oder der Einsatz von FIPS 140-2 (Federal Information Processing Standard) zertifizierten kryptografischen Modulen, die beispielsweise für die Zusammenarbeit mit US-amerikanischen und kanadischen Behörden Pflicht sind.

Die verschiedenen Parameter wie Security Policies, Data Segregation, Business Continuity, Intrusion Prevention oder Compliance-Anforderungen definiert die Nutzer-Gemeinschaft spezifisch nach ihren eigenen Ansprüchen und den erforderlichen rechtlichen Rahmenbedingungen. Je einheitlicher und höher die Standards sind, desto größer ist auch das Vertrauen in die Sicherheit der Community Cloud – besonders wenn die Standards durch unabhängige Dritte beispielsweise durch Zertifizierungen bestätigt sind.

Das Netz – der Weg in die Community

Der Zugang zur Public Cloud erfolgt in der Regel über das Internet. Bei der Community Cloud ist es hingegen möglich, darauf vollständig zu verzichten und über eigene Netzanbindungen der Teilnehmer den Zugang zu regeln. Das funktioniert meist per IPSec verschlüsselte Virtuelle Private Netzwerke (VPN) oder Multi-Protocol Label Switching (MPLS). Das Internet nicht einzubeziehen, bedeutet eine potenzielle Gefahrenquelle auszuklammern, die als Einfallstor für Malware und Attacken dient. Die direkte VPN-Anbindung weist geringere Latenzzeiten und garantierte Verfügbarkeiten auf – und damit eine bessere Performance, was über SLAs sicherzustellen ist. Außerdem ist über ein

MPLS-VPN Quality of Service (QoS) realisierbar, sodass das gesamte Community-Netz Ende-zu-Ende kontrollierbar bleibt.

Die CA – Türsteher mit VIP-Liste

Zur Kontrolle der Cloud-Nutzer empfiehlt sich eine eigene Certificate Authority (CA). Die CA erstellt, verwaltet und prüft die von ihr an die einzelnen User oder Geräte ausgegebene Zertifikate. Darüber hinaus legt die CA Certificate Revocation Lists (CRL) an, also Sperrlisten für zurückgezogene Zertifikate. Allerdings kann eine CA nur so gut sein wie die Organisationsprozesse um sie herum. Auch hier gilt: je unabhängiger desto verlässlicher. Aus diesem Grund sollten Dienstanbieter und CA-Betreiber immer eine Gewaltenteilung anstreben. Die Zugriffskontrolle liegt dann nicht mehr beim Dienstanbieter sondern beim CA-Betreiber als unabhängige Stelle. Dieser sollte auch für das Überprüfen der von der Community festgelegten Sicherheitsstandards verantwortlich sein und Zugänge für neue Teilnehmer nur bei positiv ausfallenden Resultaten gewähren. Genau dies ist innerhalb einer einzigen Institution oder eines einzigen Unternehmens nicht zu gewährleisten.

Verschlüsselung ist ein Muss

Nur Verschlüsselung gewährleistet letztendlich, dass diejenigen Zugriff auf Daten haben, die dazu auch berechtigt sind. Verschlüsselung setzt an drei Stellen an: Beim Transport der Daten in den Datenträgern und Datenbanken sowie bei der Verarbeitung. Je länger die Schlüssel und je sicherer die Algorithmen sind, desto stärker und sicherer ist auch die Verschlüsselung. Der Haken daran: Je härter die Verschlüsselung ist, desto langsamer werden in der Regel auch die Systeme. Das stellt vor allem an den Echtzeit-Gebrauch hohe Ressourcenanforderungen.

Die Transportverschlüsselung erfolgt heute in der Regel per IPSec oder TLS mit 2048 Bit Schlüssellänge. Die entsprechenden SSL/TLS-Zertifikate sind beispielsweise wieder über die CA auszugeben und zu kontrollieren.

Die Verschlüsselung der Datenbank auf Block-Ebene ist beispielsweise über systemweit gültige Schlüssel zu realisieren. Diese Schlüssel werden in speziellen Schlüsselspeichern aufbewahrt. Empfehlenswerter ist das Erzeugen nutzerindividueller Schlüssel, die nach dem Abmelden wieder zerstört werden. Ein starkes Blockchiffre wie AES256 (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit gewährleistet in dieser Variante eine hohe Sicherheit.

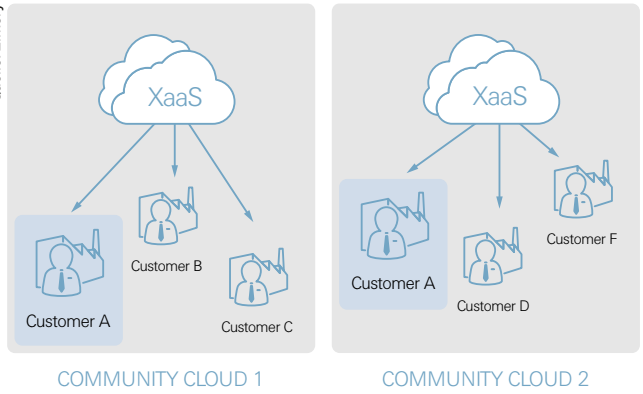
Selbstverständlich sollte der Cloud-Betreiber keinen Zugriff auf die Schlüssel der Clients beziehungsweise der Cloud-Nutzer haben. Nur so ist eine Vertraulichkeit der Daten gewährleistet. In der Regel sind es nicht gebrochene Algorithmen, die Sicherheitsprobleme verursachen, sondern Korruptionen der Umgebung oder der jeweiligen Implementierung.

Damit die Daten auch physisch sicher sind, werden sie in der Praxis häufig gesplittet, also auf unterschiedliche Rechner und Lokationen verteilt. Auf diese Weise ist sichergestellt, dass auch bei Diebstahl der Hardware die Cloud-Daten nicht vollständig in unbefugte Hände gelangen.

Alles im Gleichklang dank Standards

Die jeweiligen Nutzer einer Community Cloud bringen in der Regel unterschiedliche Voraussetzungen ihrer eigenen IT-Infrastruktur mit und verwenden unter Umständen zusätzlich eigene Private Clouds. Werkzeuge zur Cloud Orchestration, wie sie unter anderem Citrix, IBM oder Zimory anbieten, helfen beim Harmonisieren heterogener IT-Landschaften. Gleichzeitig unterscheiden sie zwischen den Private- und Community-Cloud-Ressourcen und bieten den einzelnen Usern einen getrennten Überblick über die genutzten Kapazitäten.

Quelle: Zimory



Anwender können prinzipiell auf mehrere Community Clouds zugreifen (Abb. 2).

Hier sind Standards wichtig, denn ohne diese sind Kompatibilität und Übertragbarkeit virtueller Maschinen und Datenformate in keiner Weise gegeben. Gleiches gilt für das Management der Cloud-Ressourcen genauso wie für Datensicherheit und Datenschutz oder für einheitliche SLAs. In diesem Kontext spielen vor allem zwei Standards eine wesentliche Rolle, Openstack und CIMI. Hersteller, die auf offene Strukturen und offene APIs setzen, bauen ihre Lösungen auf beiden Standards auf.

Zu den weltweiten Organisationen und Institutionen, die sich um die Cloud-Standardisierung bemühen, gehört auch die Distributed Management Taskforce (DMTF), der inzwischen 200 Unternehmen angehören. Sie hat die international erste standardisierte Management-Schnittstelle für virtuelle Maschinen verabschiedet, das Cloud Infrastructure Management Interface (CIMI). Diese Spezifikation beschreibt Modell und Protokoll, die Management und Interaktion zwischen den Clouds sowie zwischen dem Provider und dem Nutzer regeln. CIMI bezieht sich in erster Linie auf IaaS, ist aber auch für PaaS oder SaaS nutzbar. OpenStack beschreibt ein Cloud-Software-Projekt, das eine freie Architektur für Cloud Computing unter der Apache Lizenz bereitstellt. Diverse Firmen unterstützen das Projekt wesentlich, beispielsweise Citrix, Dell, HP, Redhat und IBM.

Open-Source-Lösungen mit CIMI und OpenStack haben nicht nur hinsichtlich der Standardisierung wesentliche Vorteile. Aus Security-Sicht ermöglichen sie im Gegensatz zu vielen proprietären Modellen eine umfangreiche Überprüfung der jeweiligen Sicherheitslösung. Open-Source-Standards gewährleisten darüber hinaus die Abstraktion unterschiedlicher APIs, sodass für ein Unternehmen notwendige Spezial-Funktionalitäten darüber abzubilden sind.

Gerade bei der Zusammenarbeit verschiedener Partner bietet sich ein Orchestration Tool an, da es eine einheitliche Plattform erzeugt. Es ermöglicht das Etablieren von Prozessstandards innerhalb der Community Cloud und erleichtert damit die Zusammenarbeit untereinander. Insgesamt gesehen bergen Community Clouds das Potenzial innerhalb einer Partnergruppe verschiedene Prozess- und Sicherheitsstandards zu etablieren und langfristig – auch über nationale Grenzen hinweg – durchzusetzen.

Josef Glöckl-Frohnholzer,
Managing Director, Zimory

DDoS: Geballte Angriffskraft

Gegen moderne verteilte Attacken helfen lokale Lösungen kaum noch

Denial-of-Service-Attacken sind seit über einem Jahrzehnt bekannt. Seit kurzem wachsen sie sich aber zum Problem aus, da bei DDoS-Angriffen aus zehntausenden oder mehr Rohren gleichzeitig gefeuert wird – und so selbst leistungsstarke Rechenzentren de facto nicht mehr erreichbar sind. Herkömmliche Sicherheitsinfrastruktur hat solchen verteilten Attacken nichts entgegen zu setzen. Hilfe winkt – einmal mehr – aus der Cloud.

Datenmüll, der sich mit über 400 Gigabit pro Sekunde auf ein Rechenzentrum oder gar ein einzelnes Webangebot ergießt, sieht man nicht alle Tage im Internet. Der Dienstleister Cloudflare wehrte Anfang 2014 eine Attacke dieser Größenordnung auf einen bislang nicht näher bezeichneten Kunden ab. Quelle der riesigen Bandbreite der Angreifer: Eine Distributed Denial of Service (DDoS)-Attacke, ausgeführt über eine der neuere Varianten dieser Gattung.

Laut Akamai stünden vor allem Unternehmensnetzwerke im Fokus der DDoS-Angreifer. An zweiter Stelle der Liste finden sich Handelsunternehmen, gefolgt von Firmen aus dem Sektor Unterhaltung/Medien. Auch Behörden geraten regelmäßig ins Visier der Kriminellen. Die Motivation der Angreifer variiert: Mal versuchen sie ihre Opfer zu erpressen, mal sollen missliebige Wettbewerber mit kriminellen Methoden geschädigt oder geschwächt werden.

Der von Cloudflare gemessene Durchsatz, mit der die Attacke erfolgte, mutet gigantisch groß an im Vergleich zu früheren Angriffen: Der kräftigste im Jahr 2002 verzeichnete DDoS-Angriff brachte es auf 400 Megabit pro Sekunde. 2009 wurden Werte um 50 Gigabit gemessen. Auf diesem Bandbreiten-Niveau dürften auch die DDoS-Attacken der Hacktivisten von Anonymous gegen die Webserver von Mastercard, Paypal und anderen Unternehmen gelegen haben. Dabei kam in aller Regel eine modifizierte Version des frei zugänglichen DDoS-Tools Low Orbit Ion Cannon (LOIC) zum Einsatz. Die Modifikation sorgt für eine IRC-Anbindung, so dass sich die LOIC-Installationen zu einem zentral gesteuerten Botnet umfunktionieren lassen.

Angriffe wie der von Cloudflare beschriebene sind aber nur die Spitze des Eisbergs. Dienstleister Prolexic gibt an, dass er alleine pro Jahr zehntausende DDoS-Attacken abwehrt, die auf die Netze oder Webangebote seiner Kunden zielen. Konkurrent Arbor Networks spricht von mehreren tausend DDoS-Angriffen, die täglich im Internet auftauchen. Diese sind längst nicht so mächtig wie der 400-Gigabit-Brocken – aber für finanziellen Schaden und Imageverlust können auch schwächere Attacken sorgen, wenn die Opfer keine Abwehrmaßnahmen am Start haben.

Screenshot: Uli Ries

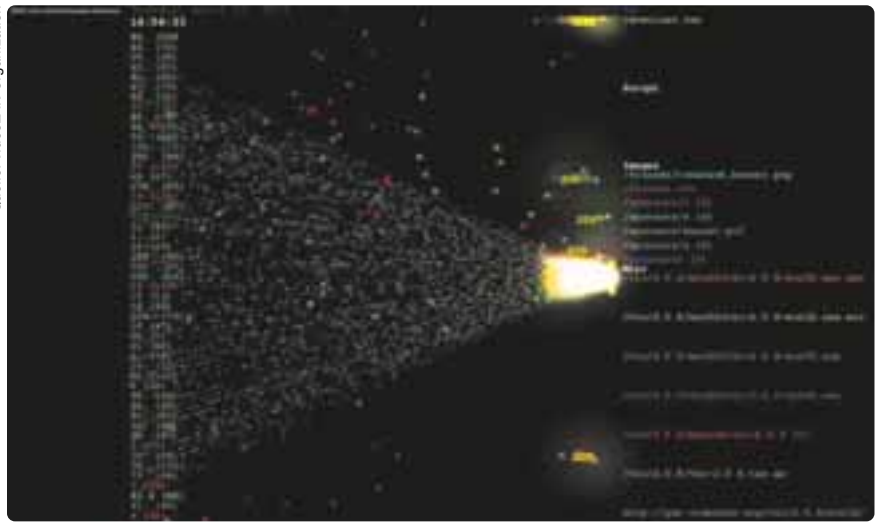
Mit dem Low Orbit Ion Cannon genannten Tool haben Hacktivists wie Anonymous legitime Zugriffe auf Webseiten wie die von Mastercard erfolgreich verhindert (Abb. 1).

Angefangen hat alles mit der lange Zeit gängigste Form der DDoS-Attacke, dem TCP-Flood. Diese Angriffsart macht sich eine Eigenheit des Netzwerkprotokolls TCP zu eigen: Zum Aufbau einer TCP-Session zwischen Client und Server ist zu erst ein Handshake notwendig. Hierzu schickt der Client ein SYN-Paket an den Server, der darauf antwortet. Bei einem SYN-Flood verschicken zehntausende von PCs oder DSL-Router in Haushalten, die zumeist als Zombies unter der Kontrolle eines Botnet-Betreibers stehen, eine riesige Anzahl solcher SYN-Anfragen – die der Server nicht mehr beantworten kann, weil die Clients sonst keine weiteren Daten mehr schicken und so die Ports blockieren. Letztendlich kann das auch zu überlasteten Prozessoren im Server oder zusammenbrechenden Netzwerk-Switches führen.

Neue Angriffstechnik per Reflektor

Neben den SYN-Überflutungen hat sich in jüngerer Vergangenheit eine neue, erheblich perfidere und durchschlagkräftigere Art der DDoS-Attacken manifestiert: Bei den sogenannten Reflective-Angriffen missbrauchen die Kriminellen legitime, frei über das Internet zugängliche DNS (Domain Name System)- oder NTP (Network Time Protocol)-Server. Laut dem Sicherheitsanbieter Link 11 machen diese Attacken inzwischen rund 20 Prozent aller DDoS-Angriffe aus, gut 55 Prozent basieren auf TCP- oder UDP-Floods. Der eingangs beschriebene 400-Gigabit-Angriff wurde mittels der jüngeren NTP-Reflektion geritten; DNS-Reflektor-Attacken gibt es hingegen schon seit 2006.

Bei der Reflektor-Attacke schicken Angreifer bösartig manipulierte Datenpakete an die DNS- oder NTP-Server und setzen dabei die betreffenden IP-Adresse des Opfers als Absender ein. Die DNS-/NTP-Server antworten automatisch auf die Anfragen und senden Daten an die vermeintliche Absender-IP-Adresse zurück. Bei den beobachteten DNS-Amplification-Angriffen wiesen die kriminellen Hacker die DNS-Server an, das gut 3000 Byte große DNS-Zonen-File an die IP-Adresse des Opfers zu senden. Im Fall der NTP-Methode schicken die Server gleichzeitig auf Geheiß der Kriminellen eine Liste ihrer letzten Kommunikationspartner (monlist) an das Opfer – das diese Liste niemals angefragt hat.



Quelle: VideoLAN Organization

Die Macher von VLC visualisieren in einem Video, dass während einer DDoS-Attacke hunderte von Zugriffen pro Sekunde auf die URL zum Download des Videoplayers erfolgen und den Server damit lahmlegen (Abb. 2).

Aus Sicht der Angreifer hat das gleich mehrere Vorteile: Zum einen ist die Quelle der Angriffe nicht auszumachen. DNS-Server reagieren auf UPD-Pakete, die sich manipulieren und mit gefälschten Absender-Adressen versehen lassen. Zudem ist keine Zwei-Wege-Kommunikation notwendig: Der Angreifer schickt das gefälschte Paket ab, der Server antwortet ohne weitere Nachfrage mit der Antwort an das Opfer.

Zum anderen lässt sich auf diese Weise die Wucht der DDoS-Attacke verstärken, da etliche NTP- und DNS-Server gleichzeitig missbraucht werden können und eine vergleichsweise kleine Anfrage zu einer ungleich größeren Antwort (monlist) führt. Verstärkungen um den Faktor 200 sind in der Praxis realistisch. Bei DNS-Attacken führt beispielsweise eine 64 Byte große Anfrage zu einer 3222 Byte großen Antwort. Cloudflare gibt an, dass für eine DDoS-Attacke mit 75 Gigabit pro Sekunde dank DNS-Reflection nur 750 Mbyte an Ausgangsdatenverkehr notwendig sind. Die ließen sich leicht mit einem kleinen Botnet oder einigen gemieteten Instanzen der Amazon Web Services erzeugen, die dann mittels gut 30.000 offen zugänglicher DNS-Server verstärkt wurden.

Diese Art Angriff liefe ins Leere, wenn die Betreiber der missbräuchlich verwendeten DNS- und NTP-Server ihre Maschinen gegen beliebige Anfragen schützen würden. Im Fall von NTP bedeutet dies beispielsweise, dass die Maschinen die monlist nicht verschicken. Die hierzu notwendigen Schritte sind in der Dokumentation des NTP-Servers zu finden.

Auch Mailserver unter den Opfern

Per DDoS-Attacken lassen sich prinzipiell auch E-Mail-Server zum Stillstand zwingen. Angesichts der hohen Relevanz, die E-Mail nach vor im Unternehmensalltag hat – nicht alle Mitarbeiter mögen Instant Messenger wie Skype oder Lync beziehungsweise Kommunikation über Soziale Netzwerke wie Facebeook und Twitter –, ist ein Ausfall der E-Mail-Infrastruktur gleichbedeutend mit einer Kommunikationssperre nach und von außen.

Anfällig sind E-Mail-Server durch die zumeist betagte Prozess-Struktur ihrer Mail Transfer Agents (MTA). MTAs sind die Komponenten, die zum Annehmen und Verschicken der Nachrichten notwendig sind. Experten halten insbesondere die weit verbreiteten Server exim, postfix, qmail und sendmail für anfällig. Ausknipsen lassen sich die E-Mail-Postämter wiederum durch Botnets: Die Zombies bauen massenhaft Verbindungen zu Port 25 beziehungsweise 587 auf und schicken dann sehr langsam Daten. Alternativ halten sie die Verbindung einfach nur offen und blockieren den E-Mail-Dienst so für legitime Nutzer. Denn pro Verbindung starten die Server unter Unix/Linux zumeist einen separaten Prozess überlasten die Maschine damit.

Die Anwendung im Visier

Den genannten DDoS-Varianten ist eines gemeinsam: Sie finden sämtlich in den Schichten 3 und 4 des OSI-Schichtmodells statt. Aber auch auf Anwendungsebene (Schicht 7) sind DDoS-Angriffe zu beobachten. Solche Attacken sind aufwändiger und als die vergleichsweise simplen – wen auch mächtigen – und einheitlichen Layer-3-Attacken. Die Kriminellen missbrauchen bei Layer-7-Angriffen Schwächen in der jeweiligen Web-Applikation. Vor der Tat muss also erst ein wenig Nachforschung betrieben werden, welche Anwendung es genau ist und wie sie sich zum Schweigen bringen lässt.

So lassen sich WordPress-Installationen beispielsweise in die Knie zwingen, wenn per Botnet massenhaft Anfragen an die Suchfunktion von WordPress geschickt werden. Aber auch einige tausend GET-Requests, die pro Sekunde an Phantasie-URLs auf dem Server geschickt werden oder Downloads des Webseiten-Logos anstoßen, verkraftet kaum ein auf WordPress basierendes Web-Angebot.

Solche Angriffe auf die Applikationsebene lassen sich üblicherweise durch eine Web Application Firewall (WAF) in den Griff bekommen – vorausgesetzt, die Firewall-Administratoren schaffen es, im Fall eines Angriffs anhand der vorliegenden Logfiles Muster in der Attacke zu erkennen und anhand dieser Signaturen entsprechende Filterregeln zu erstellen. Ohne eine solche Regel schreitet die WAF nicht ein.

Rettung aus der Wolke?

Die klassische Lösung gegen DDoS-Angriffe auf Ebene 3 und 4 sind eigens konzipierte Hardwarelösungen. Sie werden zwischen die Unternehmens-Firewall und das Internet geklemmt und blockieren alles, was nach Angriff aussieht. Nur legitimer Datenverkehr soll zu den dahinter liegenden Servern, Clients und Netzwerken durchdringen.

Soweit die Theorie. In der Praxis kommt es aber oft vor, dass die Wucht des Angriffs die eigentliche Internetanbindung lahmlegt – und damit das ganze RZ und eventuell auch die über die selbe Leitung mit dem Netz verbundenen Clients im Unternehmen offline sind. Selbst wenn die Anbindung mit 10 Gigabit pro Sekunde betrieben wird, geht in dem Moment nichts mehr, in dem der Angriff 11 Gigabit an Daten-

müll in Richtung Opfer spült. Die Schutzhardware ist dann gar nicht mehr gefragt, die Leitungsüberlastung sorgt für den Zusammenbruch sämtlicher Kommunikation. Nutzt das Unternehmen zur Telefonie ausschließlich VoIP-Dienste, bleibt nur noch der Griff zum Mobiltelefon. Andere Formen der Kommunikation sind nicht mehr möglich bis zum Nachlassen der Attacke.

Mehr Schutz versprechen Cloud-Lösungen, wie sie von diversen Dienstleistern wie Cloudflare, Prolexic, Arbor oder Link11 weltweit angeboten werden. Das Grundprinzip dieser Dienste ist immer das gleiche: Sämtlicher Datenverkehr zum und vom Netzwerk des Kunden fließt durch das Netzwerk des Dienstleisters und nur saubere Datenpakete landen bei den Firewalls und Routern des Kunden. Dies setzt natürlich großes Vertrauen des Kunden in die Integrität des Serviceproviders voraus. In der Post-Snowden-Ära dürften es europäische Anbieter wie Link11 oder myracloud etwas leichter haben, sich gegen die US-Dickschiffe wie Cloudflare oder Prolexic zu behaupten. Platzhirsch Prolexic beispielsweise wirbt mit einer Gesamtbandbreit von 1,8 Terabit pro Sekunde und sieht sich damit auch kräftigsten Angriffen gegenüber gerüstet. Von solchen Anbindungen dürften hiesige Anbieter ein Stück entfernt sein.

Wird keine Attacke festgestellt, passiert der Datenverkehr ungestört das Provider-Netz und die dort zur DDos-Erkennung und –Abwehr betriebenen BPG- und Netflow-Cluster. Schlägt jedoch ein Sensor in der Infrastruktur des Kunden oder beim Serviceprovider an, leitet der Dienstleister binnen kürzester Zeit – Interroute beispielsweise spricht von maximal 60 Minuten, Prolexic will nach spätestens fünf Minuten auf dem Posten sein – sämtlichen Datenverkehr durch seine Schutzmechanismen. Als bösartig erkannte Datenpakete werden verworfen und nur legitime Anfragen erreichen das Netzwerk und die Server des Kunden. Neben der drohenden Überlastung werden so gleichzeitig explodierende Abrechnungen aufgrund massiver Bandbreitenanstiege verhindert.

Um die Erkennungsrate der unerwünschten Datenpakete im Bedarfsfall möglichst hoch zu halten, analysieren Dienstleister wie Interroute in Zeiten ungestörten Datenflusses die übertragenen Inhalte. Die Schutzlösung ermittelt so den Normalzustand soll Abweichungen so leichter erkennen können. Zudem setzen Dienstleister auf Whitelists, mit denen sie die IP-Bereiche von der Überwachung durch das DDoS-Abwehrsystem ausklammern. Hierzu gehören beispielsweise die IP-Adressen externer Backup-Systeme.

Cloudflare wehrt DDoS-Attacken auf eine etwas andere Art ab: Jedes der 23 von Cloudflare weltweit betriebenen Rechenzentren reagiert auf Anfragen, die eine IP-Adresse eines Cloudflare-Kunden betreffen. Es gibt also nicht nur einen, vergleichsweise leicht zu überflutenden Knotenpunkt, sondern 23 mit hinreichend Bandbreite versehene Passagepunkte auf dem Weg zum Zielserver. So sollen sich Angriffe leichter verwässern lassen, ohne dass die geschützten Webserver in Mitleidenschaft gezogen werden. Angesichts des im Netz üblichen Katz-und-Maus-Spiels zwischen Angreifern und Verteidigern dürfte es jedoch nur eine Frage der Zeit sein, bis die Kriminellen auch diese Art von Schutz aushebeln.

Uli Ries,
freier Journalist, München

Impressum
Themenbeilage Rechenzentren und Infrastruktur

Redaktion just 4 business GmbH
Telefon: 080 61/348 111 00, Fax: 080 61/348 111 09,
E-Mail: tj@just4business.de

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

Autoren dieser Ausgabe:
Katharina Bengsch, Wilfried Cleres, Kerstin Ginsberg, Josef Glöckl-Frohnholzer, Bernd Hanstein, Carrie Higbie, Jan Moll, Klaus Pfeiffer, Uli Ries, Peter Rost, Michael Schell

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

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

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 Bels -205, E-Mail: stefanie.bels@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

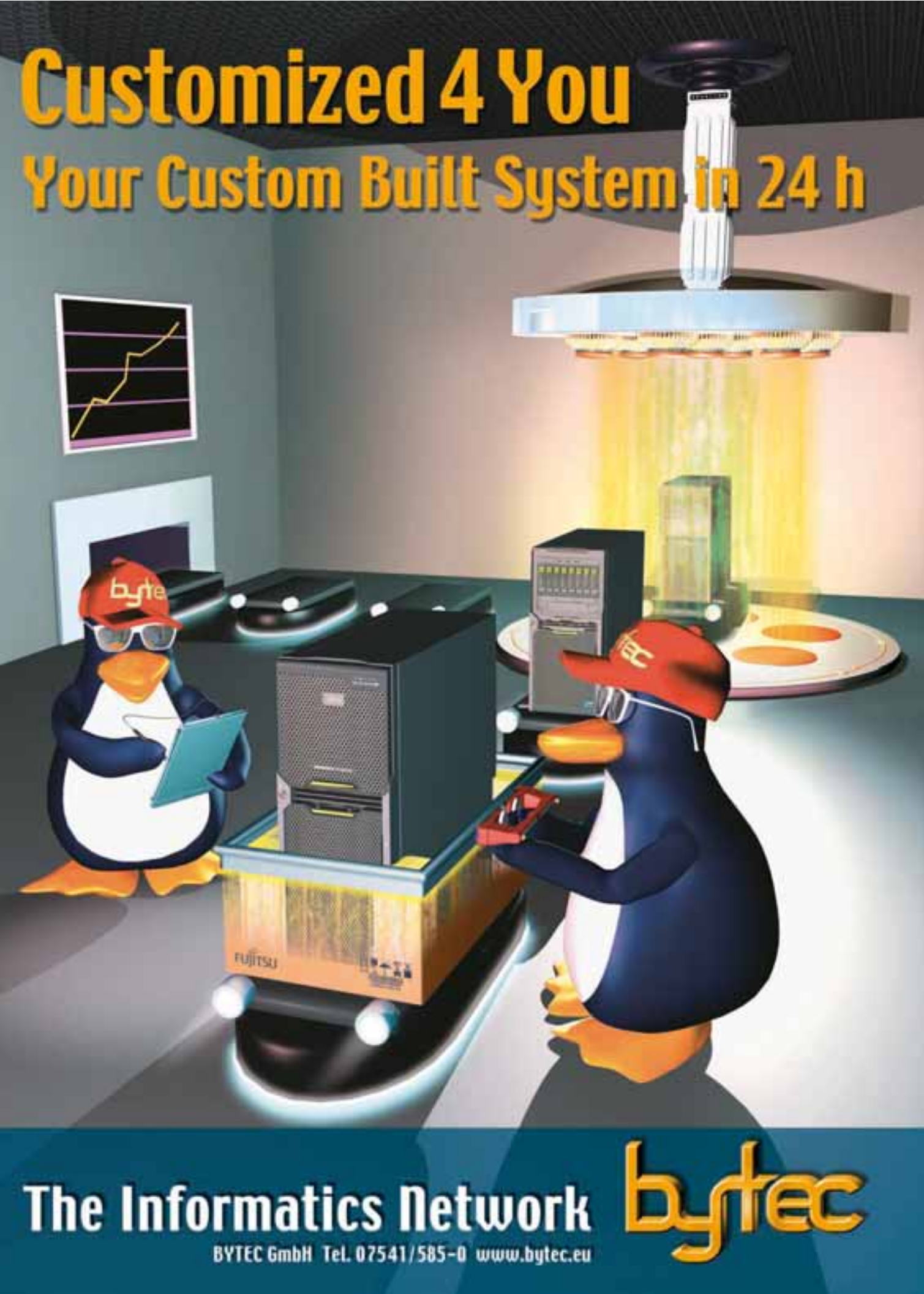
Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.

Wenn Sie von München nach Frankfurt wollen, fliegen Sie ja auch nicht über Fort Meade, Maryland.

Warum sollte man nicht auch beim Datenaustausch den direkten Weg nehmen? In unserer in Deutschland gehosteten **clouD** kommunizieren virtuelle Server direkt untereinander oder mit Ihnen. Direkte Wege gehen heißt: Daten geschützt zur Verfügung stellen. Die Sicherheit von Daten in unserer **clouD** ist für uns selbstverständlich, weil es um Ihre Daten geht. Wir stehen für Ihre Sicherheit. **Das nennen wir Hosting – safe in Germany.** filoo.de/sicher

filoo®

member of Thomas-Krenn.Group


Customized 4 You
Your Custom Built System in 24 h
byte
FUJITSU
The Informatics Network
BYTEC GmbH Tel. 07541/585-0 www.bytec.eu
bytec