Sichere Infrastruktur für Informations- und Kommunikationssysteme

04.06.2007, 19:00 | Handel, Wirtschaft, Finanzen, Banken & Versicherungen

Pressemitteilung von: *gk-marketing*
Presseagentur: *gk-marketing*

"Anwender der Informations- und Kommunikationstechnik machen sich wenige oder gar keine Gedanken über Wärmeentwicklung und steigende Anforderungen hinsichtlich der Betriebssicherheit", sagt Frank Jensen, Fujitsu Siemens Computers IT Product Services.

Server, Storage- und andere Informations- und Kommunikationskomponenten (IuK) werden immer leistungsfähiger und dabei in ihren Bauweisen immer kompakter und benötigen deswegen weniger Raum. Die Anforderungen an die Infrastruktur eines Rechenzentrums werden sich dramatisch verändern, insbesondere, um den Wärmelasten technisch-physikalisch beizukommen und diese klimatechnisch zu bewältigen.

Dem Wärmekollaps im Rechenzentrum ist vorzubeugen - denn allein in den letzten zehn Jahren hat sich die Server-Leistungsdichte im Rack verzehnfacht. Effizient Kühlen wird zur Überlebensfrage.
Wer glaubt, dass sich darüber nur Rechenzentren internationaler Großunternehmen Gedanken machen müssen, irrt. Das Verhältnis von Stromversorgung und Kühlung sowie die damit verbundenen Kosten sind für Firmen jeder Größenordnung von Bedeutung. Leider fehlt mancherorts das Bewusstsein, dass es eigentlich um den Lebensnerv des Betriebes geht. Wer böses Erwachen ausschließen will, hat zwei Möglichkeiten: Die Racks entweder nur zur Hälfte zu füllen oder in zusätzliche „Kühlkapazität“ zu investieren. Dabei kann man entweder Geld in die vorhandene Klimaanlage stecken – viel Geld allerdings – oder man bekämpft die „Hot Spots“ mit einer individuellen und gezielt wirksamen Rack-Kühlung lokal. Beide Lösungen dienen gleichermaßen dem Ziel, die Systemverfügbarkeit zu sichern.

Aktuell ist eine Server-Leistungsdichte von bis zu 30 kW pro Rack keine Seltenheit. Diese Leistung muss einerseits elektrisch zur Verfügung gestellt werden, die erzeugte Wärme ist andererseits sicher abzuführen. Damit sind vor allem schon bestehende Rechnerräume überfordert, die auf der Basis von konventioneller Luftkühlung eingerichtet wurden. „Auf diese Situation treffe ich bei vielen meiner Kunden: Entweder werden bestehende Rechnersysteme aufgrund der gestiegenen IT-Kapazität stärker gefordert, oder es sollen neue Systeme eingebaut werden; nur hat man sich entweder wenige oder gar keine Gedanken über Wärmeentwicklung und steigende Anforderungen hinsichtlich der Betriebssicherheit gemacht“, merkt Frank Jensen von Fujitsu Siemens Computers IT Product Services an.

Eines aber steht fest: IT-Systeme werden kontinuierlich leistungsfähiger, und entsprechend rasant wird ihr Energiehunger weiter steigen. "Die Systeme (Blade Server, FR) stellen deutlich höhere Ansprüche an Energieversorgung und Kühlung als die vorherige Hardwaregeneration", warnt ein Gartner-Analyst. Überall dort, wo hohe Serverdichten gewünscht werden, also komplett gefüllte Racks mit aktuellen Blade Servern und Server Cluster in einem Rack betrieben werden sollen, wo aber nicht ausreichend Raum-Kühlleistung zur Verfügung steht, sind Innovationen gefragt, die mit dieser Entwicklung Schritt halten können und auf die vor allem unter dem Aspekt der Ausfallsicherheit zu 100 Prozent Verlass ist.
Eine hohe Sicherheit und Performance wird nicht nur durch laufende Aktualisierung der Rechner- und Speichertechnologien erreicht, notwendige Randbedingungen liegen vielmehr auch in den „Niederungen“ der Haustechnik, der Sicherstellung geeigneter Betriebsbedingungen.

Die Belastungsgrenzwerte für Datenträger und IuK-Sytemen betragen nach EN 1047:

Maximal zulässige Belastungsgrenzwerte nach EN 1047

Datenträger: Temperatur 50 °C Relative Luftfeuchtigkeit 85 %

Informations- und
Kommunikationssysteme: Temperatur 70 °C Relative Luftfeuchtigkeit 85 %

Eine zwingende Notwendigkeit zur Sicherstellung der Funktionsfähigkeit und permanenten Verfügbarkeit ist also eine ausreichende Klimatisierung des Rechnerraums. Erste thermisch bedingte Funktionseinschränkungen können bei frei belüfteten Racks (z.B. über die Schrankfronten) bereits bei Raumtemperaturen von ca. 24 °C auftreten. Ab Raumtemperaturen von ca. 32 °C sind Überhitzungsschäden nicht nur nicht mehr auszuschließen, sondern sehr wahrscheinlich. Bei diesen Umgebungsbedingungen entstehen interne Temperaturen auf den Computer-Chips von deutlich über 35 °C. Dies kann zu Einbußen bei der Performance bis hin zu einer Überhitzung führen. Für einen Rechnerraum, in dem sich IuK-Systeme für einen 24x7x365-Betrieb (Rund-um-die-Uhr-Betrieb) befinden, sind redundante Klimasysteme demnach zwingend notwendig. Nur so kann beim Ausfall einer Klimakomponente eine Schadensentwicklung vermieden werden.

Die ideale Betriebstemperatur luftgekühlter Rechnersysteme ist in den jeweiligen Handbüchern der Hersteller benannt. Folgende Grenzwertbereiche für Rechnerräume sind üblich:

Raumtemperatur von 21 ° C bis 28 °C
Raumluftfeuchte von 30 % relative Luftfeuchte bis 68 % relative Luftfeuchte

Temperatur und relative Luftfeuchte sollen an verschiedenen Orten des Rechnerraumes von einem von der Klimatechnik unabhängigen System überwacht werden.

Schwerpunkt der Infrastruktur ist die Realisierung energieeffizienter und qualitativ hochwertiger Klimatisierung unter Berücksichtigung steigender Rechnerleistungsdichte durch technologisch bedingte erhöhte Wärmelasten sowie Lösungen zur redundanten und unterbrechungsfreien Stromversorgung kritischer Informations- und Kommunikationssysteme.

Für den Bau von Rechenzentren / Data Centern existieren keine standardisierten Stromversorgungslösungen aus der Schublade. Erfahrungswerte für die individuell anzupassende Stromversorgung sind allerdings vorhanden. Für den Planer besteht die Herausforderung darin, diese Fakten speziell auf den Kunden unter Berücksichtigung seiner spezifischen Wünsche und Bedürfnisse und nicht zuletzt auch seinem Budget anzupassen und dabei die gewünscht IT-Sicherheit zu gewährleisten. Dabei sind die Verfügbarkeitsanforderungen stets im Auge zu behalten.

Die elektrische Stromversorgung von Rechenzentren ist ein besonders sensibler Bereich. Störungen oder gar Ausfälle haben einen direkten Einfluss auf die Funktionsfähigkeit und Verfügbarkeit der Systeme.

Bei der Auslegung der Energieversorgung sind die relevanten Verfügbarkeitsansprüche der Informations- und Kommunikationsdienste zu beachten. Sicherheitsgründe sprechen eindeutig für eine redundante Energieversorgung.

Mögliche Ursachen für eine Unterbrechung der Stromversorgung können sein:
- technische Fehler in den Geräten (zum Beispiel bei Servern)
- technische Fehler in der Stromverteilung (zum Beispiel der Leitungen, Unterverteilungen)
- Fehler in den Stromersatzlösungen (zum Beispiel bei Generatoren oder Netzersatzanlagen und batteriegepufferten unterbrechungsfreien Stromversorgungsanlagen - USV-Anlagen)
- Prozessbedingte Fehler (zum Beispiel Fehler in der Konzeption und Installation der Stromversorgung oder logistische Fehler)

Teilausfall der Stromversorgung im Rechenzentrum DESY Hamburg, den die Presse wie folgt meldete:
"Am Dienstag, dem 4. April 2006, kam es um 11:50 Uhr zu einem teilweisen Ausfall der Stromversorgung im Rechenzentrum, als dessen Ursache ein Kurzschluss im Maschinenraum vermutet wurde. Dadurch waren einige zentrale und dezentrale Dienste nur eingeschränkt oder gar nicht nutzbar. Nach Wiederherstellen der Stromversorgung konnten ab 14:30 Uhr die betroffenen Systeme wieder angefahren werden. Zentrale Dienste waren ab 16:30 Uhr praktisch vollständig verfügbar. Datenverluste traten durch Software-Funktionsfehler beim E-Mail-Empfang und -Versand auf. Ca. 50 dezentrale Server wiesen am nächsten Morgen noch Funktionsstörungen auf, die von der Frühschicht beseitigt

wurden."

Eine entscheidende Bedeutung beim Betreiben von Serverschränken oder ganzen Rechenzentren kommt der Stromversorgung zu.
Da ein Abreißen der Informationsversorgung durch
- Netzstörung,
- Spannungsabfall,
- Spannungsspitzen,
- Über- und Unterspannung,
- Schaltspitzen,
- Leitungsrauschen,
- Frequenzspannungen und
- harmonische Oberwellen sowie den
- totalen Stromausfall

unter Umständen riesige Schäden anrichten kann, ist die unterbrechungsfreie Stromversorgung der EDV- und Telekommunikations-Systeme quasi überlebenswichtig und zwingend Bestandteil eines Grundschutzkonzeptes.
Eine sichere Stromversorgung ist der energietechnische Lebensnerv einer jeden Unternehmung.

Um bei einer unerwarteten Unterbrechung der Stromversorgung aus dem öffentlichen Netz den abrupten Ausfall der IuK-Systeme zu verhindern, ist ein modernes unterbrechungsfreies Stromversorgungssystem (USV) notwendig. Ein USV erlaubt beispielsweise das geregelte Herunterfahren der Systeme. Bei längeren Ausfällen der Energiezufuhr übernimmt eine hausinterne Netzersatzanlage die Stromver-sorgung der Rechner und Kommunikationseinrichtungen. Vom Netz des Energieversorgers (Mittelspannung / Niederspannung) bis hin zur Steckdose, in der die Server eingesteckt sind ist somit ein durchgängiges und schlüssiges Sicherheitsversorgungssystem zu realisieren. Neben den IuK-Systemen müssen Netzersatzanlagen auch die Funktionalität der Sicherheitsbeleuchtung, der Überwachungseinrichtungen und die Funktion der Klimaanlage sicher stellen.

Ein Informations- und Kommunikationsnetz ist nur so sicher wie die am wenigsten geschützte Komponente. Deshalb gilt: Je komplexer ein Informations- und Kommunikationsnetz ist, desto anfälliger ist es für Gefahren. Dabei vernachlässigen Firmen oft physikalische Gefahren für Informations- und Kommunikationssysteme, die etwa durch Feuer, Wasser, Einbruch oder Vandalismus entstehen. Diese Risiken, die in 80% aller Fälle durch äußere Einflüsse hervorgerufen werden, führen zu Störungen oder gar zum kompletten Stillstand des RZ- oder Netzbetriebes.

Zumindest die gesetzlichen Mindestanforderungen an den physikalischen Schutz gegen Feuer, Wasser, Staub, magnetische Störfelder, unbefugten Zugriff, Vandalismus, Sabotage oder Spionage sollten vor allem zentrale IT-Bereiche erfüllen. Oft sind diese Anforderungen den Verantwortlichen nicht einmal bekannt. Im Bereich der physikalischen IT-Sicherheit ist der Schutz vor Bränden eine der Hauptaufgaben. Brände können sowohl von der IT ausgehen als auch im Umfeld entstehen. Der Schutz der IT vor Bränden sollte die Besonderheiten der Systeme berücksichtigen und gleichzeitig Bestandteil der Organisation des Brandschutzes des Unternehmens sein.

Nicht nur der Brand des Flughafens Düsseldorf hat gezeigt, dass der Brandschutz oft vernachlässigt wird. Brandschutz kostet Geld - jedoch ist es mit finanziellen Mitteln allein nicht getan. Der IuK-Verantwortliche muss die Tücken der Richtlinien und Vorschriften kennen. Hier hilft ein externer Brandschutzberater weiter. Der Brandschutz muss neben allen anderen Maßnahmen in das Gesamtsicherheitskonzept einbezogen werden. Verantwortlich für den störungsfreien Betrieb eines Rechenzentrums ist laut BGB § 611 und aktueller Rechtssprechung die oberste Managementebene, die verpflichtet ist, alle erforderlichen Sicherheitsmaßnahmen zu veranlassen, zu überwachen und zu verantworten.

Die Leistungsfähigkeit der Informations- und Kommunikationstechnik zeigt sich in der Leistungsfähigkeit des Rechenzentrums und dessen reibungslosem Betrieb. Die zuverlässige Verfügbarkeit des Rechenzentrums bildet die Grundlage für die effiziente Unterstützung aller Geschäftsprozesse und den Erfolg des Unternehmens.

Fazit
Gefordert ist ein Sicherheits-Gesamtkonzept, welches von der Risikoanalyse über die Planung bis hin zur Realisierung von wirtschaftlichen Sicherheitslösungen dem individuellen Sicherheitsbedarf gerecht wird. Zur langfristigen

Absicherung eines erreichten Sicherheitsniveaus für Informations- und Kommunikationssysteme bieten regelmäßige Überwachungsaudits zusätzliche Bestätigung. Sowohl die in Deutschland geltenden Vorschriften als auch die zusätzlichen Vorschriften für internationale und amerikanische Konzerne, welche aufgrund der Vorgaben durch Versicherer Berücksichtigung finden müssen, sollten für Anbieter von Sicherheits-Leistungen Standard sein.

Portrait

Fujitsu Siemens Computers:
Fujitsu Siemens Computers ist der führende europäische IT-Hersteller und zugleich Marktführer in Deutschland. Mit seinem strategischen Fokus auf innovative Mobility und Dynamic Data Center Produkte, Services und Lösungen bietet das Unternehmen eine einzigartige Bandbreite an Produkten und Services - vom Handheld über Desktops bis hin zu IT-Infrastrukturlösungen und Services. Fujitsu Siemens Computers ist in allen Schlüsselmärkten Europas, Afrikas und des Nahen Ostens präsent, der Bereich Services ist in 170 Ländern weltweit tätig. Das Unternehmen profitiert von der globalen Kooperation und der Innovationskraft seiner beiden Shareholder Fujitsu Ltd. und Siemens AG. Im Fokus stehen die spezifischen Anforderungen seiner Kunden: Großunternehmen, kleine und mittelständische Firmen sowie Privatkunden. Das Unternehmen ist Mitglied der Global Compact Initiative der Vereinten Nationen.

News-ID: 138856 • Views: 94 (Stand: 03.06.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/138856/Sichere-Infrastruktur-fuer-Informations-und-Kommunikationssysteme.html