IT-BUSINESS

Channel Fokus: Stromversorgung & Klimatisierung

Ganzheitlicher Schutz für Klima und IT

15.01.2021
Autor: Dr. Andreas Bergler

Ob an den Cloud-Servern von Providern, im Rechenzentrum von Unternehmen oder an den Endgeräten im Homeoffice, überall muss eines sicher sein: die Stromversorgung. In komplexen Umgebungen ist ein integriertes Konzept mit Klimatisierungslösungen sinnvoll.

Wer die Stromversorgung für die IT-Systeme, Rechenzentren und Gebäude schützt, schützt auch das Klima.
(Bild: LuckyStep - stock.adobe.com)

Während alle Welt über die Corona-Pandemie, die wirtschaftlichen Folgen und die Verteilung der Impfstoffe spricht, sind die Berichte über den Kampf gegen den Klimawandel in den Hintergrund gerückt. So entfiel auf die Entscheidung des Europäischen Rats über das neue Klimaziel im Dezember 2020 leider wenig öffentliche Aufmerksamkeit. Doch der Rat hatte sich richtig ins Zeug gelegt: Nach langen Verhandlungen wurden die Treibhausgasminderungs-Ziele von den bisher verankerten 40 Prozent jetzt auf 55 Prozent angehoben. Speziell im Stromsektor müssen daher die sogenannten „Erneuerbaren Energien“ zügig ausgebaut werden, fordert der gleichnamige Bundesverband.

Stromversorgung und teure Ausfälle

Die ehrgeizigen Ziele von Politik und Verbänden verschärfen allerdings eine prekäre Situation: Der ökologisch notwendige Umbau des Stromnetzes kann zu großflächigen Stromausfällen führen. Diese können mitunter, wie im Sommer 2019 geschehen, nur noch mit schneller Hilfe in Form von Stromlieferungen aus dem Ausland verhindert werden. „Die Situation war kritisch. Da durfte nicht mehr viel passieren", hieß es damals von Seiten der Netzbetreiber.

Ein Ausfall in der Stromversorgung kann sich für die IT-Systeme allerdings schnell zur Katastrophe auswachsen. Nicht jeder Datenverlust ist auf physische Ursachen wie Stromausfälle zurückzuführen, aber sie sind eine Größe, mit der man rechnen muss und die man einfach vermeiden kann. In dem aktuellen Bericht „Managing The Impact Of Increasing Interconnectivity – Trends In Cyber Risk" von der Allianz Global Corporate & Specialty (AGCS) kommen die Autoren zum Ergebnis, dass Fehler von Mitarbeitern und technische Probleme zahlenmäßig die häufigste Ursache für Schadenfälle in der Cyberversicherung sind.

„Obwohl Cyberkriminalität die Schlagzeilen beherrscht, sind es vielfach alltägliche Systemausfälle und menschliche Fehler, die Unternehmen große Probleme bereiten, selbst wenn ihre finanziellen Auswirkungen meistens nicht so gravierend sind", bemerkt dazu Catharina Richter, globale Leiterin des Allianz Cyber Kompetenzzentrums. Hauptkostentreiber für Cyberschäden, so die Allianz-Studie, sind Betriebsunterbrechungen. Sie machen etwa 60 Prozent der Schadensummen aus. An zweiter Stelle stehen die Kosten für die Bewältigung von Datenpannen. Speziell für das Jahr 2020 kommen noch wachsende Gefahren hinzu, die durch die Pandemie bedingt sind. „Die potenziellen Auswirkungen von Mitarbeiterfehlern oder technischem Versagen durch die Arbeit im Homeoffice könnten verstärkt werden", so die Studienautoren. Im Umfeld von Cyberversicherungsfällen ließe sich hier zwar noch kein eindeutiger Trend bestätigen, aber die Zahl der im Jahr 2020 gemeldeten Versicherungsschäden sei in etwa zehnmal so hoch wie noch vor vier Jahren.

Gleichzeitig gehen die geschätzten, durchschnittlichen Folgekosten für Störereignisse quasi durch die Decke. So betrugen laut dem „Global Data Protection Index 2020 Snapshot" von Dell die geschätzten jährlichen Kosten für Ausfallzeiten im Jahr 2019 im Durchschnitt rund 719.000 Euro. Im Vorjahr lagen sie noch bei rund 467.000 Euro.

ERGÄNZENDES ZUM THEMA

Schlaglichter auf die Datensicherheit

Vor allem ungeplante Downtime und allgemeine Datenverluste haben in den letzten Jahren deutlich zugenommen.
(Bild: Dell)

Der „Global Data Protection Index 2020 Snapshot“ von Dell zeichnet ein eher schlechtes Bild in puncto Unternehmenssicherheit. So ist die Zahl der Unternehmen, die im untersuchten Zeitraum von zwölf Monaten einen Schadensfall wie Ausfallzeiten oder Datenabfluss erlitten haben, deutlich gestiegen. Ebenso ist die Zeit, die durchschnittlich zur Wiederherstellung der Daten benötigt wurde, von sieben auf acht Stunden angewachsen. Dass Unternehmen die Probleme immer weniger in den Griff bekommen, könnte am gewaltigen Datenwachstum liegen, das die Studie ebenfalls offenbart. So hatten Unternehmen 2019 durchschnittlich 13,5 Petabyte an Daten zu verwalten – fast 40 Prozent mehr als im Vorjahr (9,7 PB).

Weil ganz einfach die Menge der Daten rasant wächst, mit denen Unternehmen zu tun haben, wachsen auch die Schäden an diesen Daten, selbst wenn das Sicherheitsniveau erhöht wird. „Unternehmen haben heute schon Schwierigkeiten damit, die enormen Datenmengen in ihren IT-Systemen angemessen zu schützen. Da wir auf dem Weg in ein neues Datenzeitalter sind, wird diese Herausforderung immer größer“, sagt Robert Laurim, Vice President & General Manager Channel bei Dell Deutschland. Es sei deshalb wichtiger denn je, den Unternehmen ein Extralevel an Unterstützung zu bieten. „Dem Channel kommt dabei eine Schlüsselrolle zu“, so Laurim.

Dimensionierung der USV

Die Bereitstellung von Systemen zur Unterbrechungsfreien Stromversorgung (USV) ist so eine wichtige Möglichkeit, für ein gewisses Schutzlevel zu sorgen. Die Geräte schützen vor Stromausfällen, wie einfachen Unterbrechungen, Unter- und Überspannung, Verzerrungen der Wellenform bei der Stromkurve bis hin zu Frequenzvariationen. Doch schon die korrekte Dimensionierung der USV zu finden, ist nicht immer einfach, denn im Dauerbetrieb können täglich schon einige Megawatt an Strom durch die Geräte fließen. Bei ineffizienter Planung kommen schnell hohe Stromkosten auf die Verbraucher zu. Eine einfache Faustregel sagt hier, dass etwa zwei Drittel der Nennlast als tatsächlicher

Verbrauch geplant werden sollten, da die Strom verbrauchenden Systeme selten oder nie ihre Nennlast tatsächlich abrufen würden. Doch auch von Seiten der Hersteller besteht offensichtlich Nachholbedarf. So fordert etwa Markus Dietz, Business Development bei Grass-Merkur, das besagte „Extralevel an Unterstützung“ auch von den Anbietern, die durch genauere Angaben bei den Wirkungsgraden von USV-Anlagen, diese näher an den Praxisbetrieb rücken sollten.

ERGÄNZENDES ZUM THEMA

Partner-Kommentar: Markus Dietz, Grass-Merkur

Markus Dietz, Business Development, Grass-Merkur
(Bild: Grass-Merkur)

Wir wünschen uns präzise Angaben zur Effizienz und Leistungsfähigkeit von Klima- und USV-Systemen in realen Umgebungssituationen. Das ist wesentlich für die Auswahl eines geeigneten Produktes (USV, Klimatisierung). Als Betreiber eines eigenen ISO 27001-zertifizierten Sicherheits-Rechenzentrums (für Housing, Cloud-Services, Managed-Services) ist der effiziente und zuverlässige Betrieb von RZ-Infrastrukturen (Klima, Energieversorgung) eine grundlegende Voraussetzung. „Prospekt-Angaben“, zum Beispiel zu Wirkungsgraden von USV-Anlagen, sind oft unter „Laborbedingungen“ ermittelt und entsprechen nicht den Rahmenbedingungen, die im realen Betrieb in einem Rechenzentrum vorzufinden sind.

Cool und effizient

Noch effizienter – und nebenbei auch noch sicher – wird der IT-Betrieb von Servern und Rechenzentren durch den richtigen Einsatz von Kühlsystemen. Mit der dort verbrauchten Energie, so gehen Schätzungen aus, könnten etwa zweieinhalb Millionen durchschnittliche Privathaushalte versorgt werden. Etwa ein Drittel bis die Hälfte der Energie, die ein Rechenzentrum insgesamt benötigt, entfällt auf die Kühlung. „Optimierungsmaßnahmen können die Energieeffizienz der Kühlung signifikant verbessern“, folgert Ingo Gdanitz, Business Development Manager bei Technotrans SE, einem Anbieter für Kühlung, Temperierung, Filtration und Dosiertechnik.

Maßgeblich bei der Auswahl des Kühlsystems sind die individuellen Kundenanforderungen. Handelt es sich etwa um die Hardware eines Telco-Providers oder um ein Rechenzentrum für High-Performance Computing? Dann stehen

Skalierbarkeit und Leistungsanforderungen auf der Prioritätenliste. Geht es um die Absicherung von Public-Cloud-Applikationen, um die Versorgung von Systemen im Banking-Umfeld oder gar um HPC-Datacenter, dann gilt es, am Verfügbarkeitslevel zu arbeiten. Liegen die Anforderungen an die Verfügbarkeit nicht auf dem höchsten Level, kann eine Durchschnittstemperatur von 25 Grad toleriert werden. Das spart erheblich Strom. Denn, so eine weitere Faustregel, mit jedem Grad, das nicht gekühlt werden muss, lassen sich zwei bis fünf Prozent an Kühlenergie einsparen.

Das Monitoring der Hardware ist speziell für Rechenzentren von Colocation-Anbietern sehr wichtig. Die Betreiber sind hier oft verpflichtet, die Rahmenbedingungen im Serverraum, wie Lufttemperatur oder Feuchtigkeit, zu dokumentieren. Ist ein Rechenzentrum in mehreren Ausbaustufen geplant, wird auch die Erweiterbarkeit essenziell, um die Kühlleistung nachträglich anpassen zu können. Laut Gdanitz müssen vier Aspekte beachtet werden: Die Wärmelast, die von der Rechenleistung abhängt, die klimatischen Bedingungen wie die Außentemperatur, die oft über die Art der Kühltechnik entscheidet, das Investitionsbudget der Kunden und deren Anforderungen an Verfügbarkeit und Erweiterbarkeit.

Die Klimatisierung sollte modular und redundant aufgebaut sein, damit beim Ausfall einer Einheit die anderen Systeme übernehmen können. Technotrans empfiehlt, aktive Kühlung möglichst mit freier Kühlung, also an der Außenluft, zu kombinieren. So lassen sich bis zu 50 Prozent des Energiebedarfs reduzieren.

(ID:47031392)

ÜBER DEN AUTOR

Dr. Andreas Bergler

CvD IT-BUSINESS, Vogel IT-Medien

WEITERE ARTIKEL DES AUTORS

Preview: IT-BUSINESS vom 8. Februar 2021

Früher informiert sein: die IT-BUSINESS 2 / 2021

Neuer VP und größeres Channel-Team

Trend Micro baut Deutschland-Präsenz aus

Neuer Channel Manager DACH

Michael Berg kommt zu F5