

Hochverfügbarkeit der IT-Infrastruktur sichert die Kontinuität der Geschäftsprozesse

Irgendwann einmal erwischt es jeden

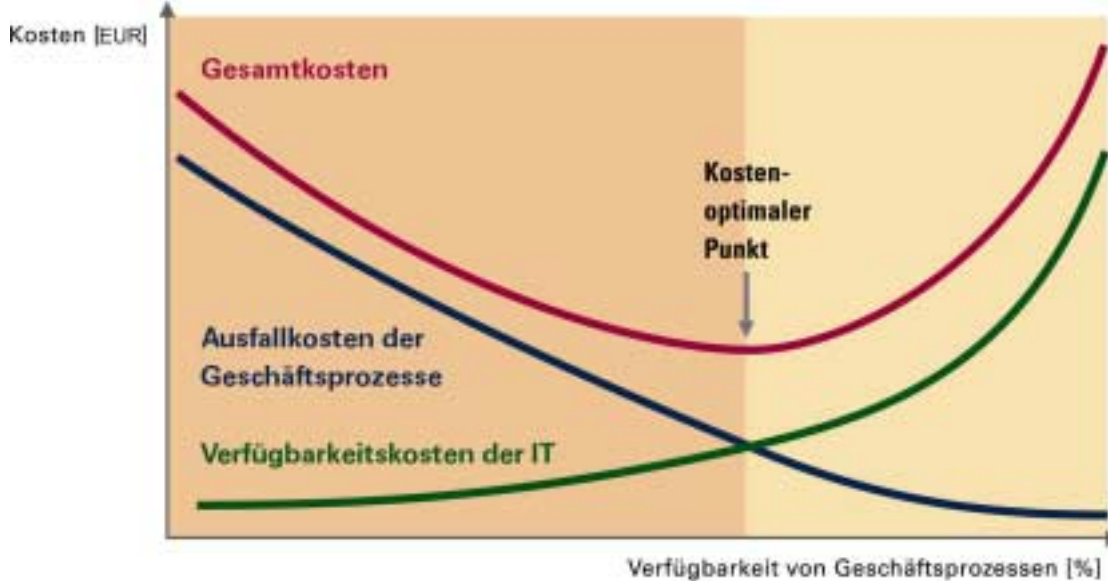
Von Manfred Ruttmar, Principal Consultant bei Siemens Business Services

Je komplexer die IT-Infrastruktur im Unternehmen, desto größer ist das Risiko eines Ausfalls. Störungen verursachen schnell enorme Kosten und führen zur Unzufriedenheit der Kunden. Dabei lässt sich die Hochverfügbarkeit der IT-Systeme und damit der unterbrechungsfreie Geschäftsablauf durch intelligente Lösungen durchaus sichern.

Gegen Ausfälle seiner IT-Infrastruktur ist grundsätzlich kein Unternehmen gefeit. Der berüchtigte Sand im Getriebe kann jedes Unternehmen unabhängig von der Größe oder der Branche treffen. Nach einer Security-Studie der Unternehmensberatung Price Waterhouse Coopers und der Fachzeitschrift InformationWeek aus dem Jahr 2001 hatten nur 26 Prozent der rund 4.900 befragten Unternehmen keinen Ausfall zu verzeichnen. Im Jahr 1998 waren noch über fünfzig Prozent nicht betroffen gewesen. Die Ursachen für diese zunehmende Gefahr sind unterschiedlich. So wurden im vergangenen Jahr weltweit über 12.000 neue Computerviren und -würmer identifiziert, die sich über die vernetzten E-Mail-Systeme zum Teil innerhalb von Stunden rund um den Erdball verbreiteten und die Rechner lahm legten.

Seit den Anschlägen in New York und in Washington am 11. September letzten Jahres sind vielen Unternehmen die Gefahren jedoch schlagartig vor Augen geführt worden. Dabei spielt vor allem die zunehmende Vernetzung der Märkte im Zuge der Globalisierung eine große Rolle. So basieren viele Unternehmen der „New Economy“ fast vollständig auf rund um die Uhr funktionsfähigen Informations- und Kommunikationssystemen zur reibungslosen Abwicklung ihrer geschäftlichen Transaktionen. Mit der zunehmenden Verwendung komplexer IT-Strukturen steigt gleichzeitig jedoch auch die Anfälligkeit für Fehler, die dann zu einem mehr oder weniger vollständigen Ausfall führen können. Die Komplexität von heterogenen IT-Systemen mit verteilten Daten und Applikationen erschwert es, eine ständig hohe Verfügbarkeit zu erreichen.

Wenn Web-Seiten nicht erreichbar sind, hat das für Unternehmen, die ihre Produkte über das Internet vertreiben, jedoch fatale Folgen: Da der Kunde davon ausgeht, rund um die Uhr auf ein attraktives Angebot zugreifen zu können, ärgert er sich, wenn das nicht der Fall ist und klickt einfach weiter zum nächsten Anbieter. Solch ein direkter Verlust von Kunden infolge eines streikenden Servers oder einer streikenden Netzwerkkomponente kostet viel Geld. Das Interesse an der Hochverfügbarkeit ist jedoch nicht nur aus diesem Grund gestiegen. Vielen Unternehmen ist es anders als früher inzwischen bewusst, dass die IT-Struktur verletzlich ist. So erweist es sich als ebenso kritisch, wenn eine Störung die Kommunikation mit Lieferanten einschränkt oder den Zugriff auf wichtige Daten unmöglich macht. Kommt beispielsweise der E-Mail-Verkehr oder der Druckdienst zum Erliegen, geht in so mancher Firma gar nichts mehr. Immense Kosten bringt es auch mit sich, wenn sich Lieferungen oder Zahlungen verzögern und Kunden oder Lieferanten Schadensersatzansprüche stellen.



Verärgerte Kunden und Mitarbeiter

So machte beispielsweise der Online-Dienst AOL bei einer plötzlich aufgetretenen Störung von mehreren Stunden Verluste von drei Millionen US-Dollar, der Telekommunikationsriese AT&T verlor sogar 40 Millionen US-Dollar und der Börsenwert des Auktionshauses eBay sank nach einer technisch bedingten Pannenserie um 26 Prozent. Eine Studie des Marktforschungsunternehmens Dataquest errechnete bereits im Jahr 1998, dass nur eine einzige Stunde Ausfall der zentralen IT-Infrastruktur enorme Kosten mit sich bringen kann. Sie liegen zwischen durchschnittlich 6,5 Millionen Dollar bei Wertpapierhandelsfirmen und 14.500 Dollar bei der Flugreservierung einer Airline.

Werden Geschäftsprozesse unterbrochen, zieht das jedoch nicht nur direkt messbare materielle Einbußen in Form von entgangenen Umsätzen oder Schadensersatzforderungen von Kunden und Lieferanten nach sich. Als langfristig ebenso schädlich für Unternehmen – so Experten – erweisen sich missmutige Kunden, ein allgemeiner Image- und Vertrauensverlust, verärgerte und dadurch demotivierte Mitarbeiter oder gestörte Geschäftsprozesse zwischen der jeweiligen Firma, ihren Kunden und Lieferanten. Ungeplante Ausfälle verursachen immer einen Imageverlust der betroffenen Firmen.

Was ist Hochverfügbarkeit?

Das Ziel der Hochverfügbarkeit – auch „High Availability“ genannt – besteht darin, ein weitestgehend reibungsloses Funktionieren der IT-Infrastruktur zu gewährleisten, um die eigentlichen Geschäftsabläufe sicherzustellen. Herrscht im Rahmen einer Definition von High Availability (HA) über diese Zielrichtung noch Einigkeit, so sind andere Elemente nicht so eindeutig zu benennen. Das hängt mit der oftmals verwirrenden Verwendung der Begriffe rund um die Hochverfügbarkeit zusammen. So werden Begriffe wie „Ausfallsicherheit“ und „Fehlertoleranz“ beispielsweise oftmals für ein und dieselbe Sache verwendet. Dabei bezeichnen sie etwas Unterschiedliches und sollten deshalb eigentlich getrennt werden. Denn Hochverfügbarkeit lässt zum Beispiel zwar geringe Ausfallzeiten zu, zeigt aber keine Toleranz gegenüber Fehlern.

Verwirrung herrscht auch bei einer weiteren zentralen Komponente der Hochverfügbarkeitssysteme: Den so genannten Clustern. Siemens Business Services versteht darunter eine Gruppe von Rechnern, die durch Zusammenarbeit eine einzige Datenverarbeitungsquelle bilden. Das bedeutet, dass in einem Cluster eine verteilte Form von paralleler Datenverarbeitung ausgeführt wird. Clustering-Lösungen der vierten Generation, die Hochverfügbarkeit, Wartbarkeit und Skalierbarkeit – das heißt, die Fähigkeit zu einer dynamischen Reaktion auf das Ansteigen der Systemlast – bieten, können unabhängig von Betriebssystem und Hardware-Plattform betrieben werden. Sie basieren unter anderem auf einer modularen Software-Architektur. Diese besteht aus einer Basisgruppe von Modulen, die auf allen Rechnern – den so genannten Knoten – in einem Cluster bereitgestellt wird, und weiteren optionalen Modulen, die bestimmte Arten von Anwendungen unterstützen.

HA-Cluster verwenden in der Regel redundante Komponenten, um Systemausfälle zu kompensieren, und verfügen über eine Umgebung mit gemeinsam genutztem Speicher. Ein wesentliches Element ist dabei ihre Skalierbarkeit. Dies ist insbesondere bei Internet-Anwendungen unentbehrlich, denn die bisher

ständig zunehmenden Nutzerzahlen bringen auch ein Hochverfügbarkeitssystem sonst schnell an seine Kapazitätsgrenzen. Im Hinblick auf die Implementierung unterscheidet der Münchener IT-Dienstleister zwei grundlegende Anwendungstypen. Zum einen Applikationen, die eng mit der Cluster-Software zusammenarbeiten und speziell für eine verteilte Umgebung entwickelt wurden, und zum anderen Anwendungen, denen die Existenz des Clusters gar nicht bekannt ist und die ursprünglich für ein Einzelsystem programmiert wurden. Ein Beispiel für eine skalierbare Anwendung, die mit der Cluster-Software kommuniziert, ist der Oracle Parallel Server (OPS). Diese Datenbankapplikation kann gleichzeitig auf einigen oder allen Knoten des Clusters laufen und so ihre Performance entsprechend der aktuellen Anforderung steigern.

Wenn allerdings der Massenspeicher einem Crash zum Opfer fällt, helfen auch skalierbare Cluster nicht mehr weiter. Hier haben sich inzwischen so genannte RAID-Lösungen (Redundant Arrays of Independent Disks) für die Plattenspiegelung etabliert, bei denen die Daten gleichzeitig auf verschiedenen Festplatten gespeichert werden. Dieses Verfahren hat sich bisher als sehr wirksam und relativ einfach einzurichten bewährt.

Faktor Mensch ebenfalls entscheidend

Neben einer zunehmend komplexeren Struktur erhöht jedoch auch der Faktor Mensch in beträchtlichem Maße die Gefahren für einen ungeplanten Stillstand der Systeme. Denn nach einer aktuellen Studie des Beratungsunternehmens Gartner Group lassen sich die meisten Ausfallzeiten von Computernetzwerken auf menschliches Versagen zurückführen. So basierten nur 20 Prozent der Ausfälle auf fehlerhafter Hardware, Störungen in Betriebssystemen und Umwelteinflüssen. Den weitaus größeren Teil – nämlich 40 Prozent – verursachen fehlerhafte Anwendungen. Weitere 40 Prozent sind auf Bedienungsfehler oder menschliches Versagen zurückzuführen.

An dieser Verteilung wird sich nach Expertenmeinungen auch in den kommenden Jahren nicht viel ändern. Allerdings sollen die Probleme durch fehlerhafte Hardware und Betriebssysteme sowie durch physikalische Unzulänglichkeiten nach Meinung der Analysten im Jahr 2003 nur noch bei 15 Prozent liegen. Gleichzeitig werden aber die anwendungsbedingten Fehler auf 45 Prozent anwachsen. Deshalb wird es auch als nicht ausreichend bewertet, wenn Unternehmen lediglich auf die Redundanz von Systemen setzen, um ihre IT-Infrastruktur hochverfügbar zu halten. Das kann und sollte nicht das einzige Mittel zum Schutz darstellen. Mindestens genauso wichtig ist es, die Fehlerquellen durch menschliches Versagen und unreife Prozesse wirksam zu minimieren. Hier empfehlen sich Investitionen in Automatisierungstools. Darüber hinaus sollten Unternehmen besonders darauf achten, welche Inhalte und Garantieleistungen die Service Level Agreements der Anbieter von Hochverfügbarkeitslösungen vorsehen.

Haftungsrisiken für IT-Verantwortliche

Hochverfügbarkeit ist jedoch nicht nur notwendig, um Kunden und Lieferanten zufrieden zu stellen oder Geschäftsprozesse reibungslos zu gestalten. Ebenso notwendig machen die Haftungsrisiken, denen IT-Verantwortliche vom Vorstand über den Geschäftsführer oder Behördenleiter bis hin zum IT-Manager unterliegen, funktionierende High Availability-Systeme. Denn dieses Haftungsrisiko reicht weiter, als das für gewöhnlich angenommen wird. Jedes Unternehmen ist vor die Aufgabe gestellt, sich im Bereich der Sicherheit seiner Informationstechnologie nicht nur Gedanken zu machen, sondern aktiv möglichen Risiken eines Datenverlustes entgegenzuwirken. Zumeist sind sich die leitenden Mitarbeiter in einem Unternehmen jedoch nicht darüber bewusst, dass entsprechende Maßnahmen nicht allein im Interesse ihres Unternehmens stehen. Sie sollten schon im Hinblick auf eine mögliche Eigenhaftung geeignete Maßnahmen ergreifen, die einer Gefährdung der unternehmenseigenen Informationssysteme sowie der dazugehörigen Daten vorbeugen. Ein Beispiel zeigt plakativ, welche Folgen solch ein Ausfall haben kann: Die Tochter einer ausländischen Großbank verfügt zur Abwicklung ihrer Geschäfte in Deutschland über eine eigene Rechneranlage, die durch ein Feuer innerhalb des Gebäudes zerstört wird. Das Unternehmen verfügt weder über eine eigene Ausweichanlage, noch besteht ein entsprechender Vertrag mit einem Dienstleister, so dass die Datenverarbeitung erst nach mehreren Wochen wieder aufgenommen werden kann. In einem solchen Falle hätte der zuständige EDV-Leiter bereits aufgrund seiner Fachkompetenz wissen müssen, dass eine derartige Katastrophe zu immensen Schäden des Unternehmens führen muss,

wenn eine schnelle Wiederaufnahme der Datenverarbeitung nicht möglich ist. Aus diesem Grund hätte er jedenfalls entsprechende Vorsorgemaßnahmen ergreifen müssen. Hat der Geschäftsführer dieser Gefahr nicht vorgebeugt, so ist dieses Verhalten auch in Anbetracht der zu erwartenden hohen Schäden, die bis zum Konkurs des Unternehmens führen können, als zumindest grob fahrlässig zu bewerten.

Überdies gerät er mit gesetzlichen Bestimmungen in Konflikt. Denn bei Banken ist ein Minimum an Betriebsbereitschaft gesetzlich gefordert und in den Mindestanforderungen für das Betreiben von Handelsgesellschaften (MaH) festgelegt. Die MaH verlangen unter anderem eine Notfallplanung und kurzfristig einsetzbare Ersatzlösungen, falls die für das Handelsgeschäft erforderlichen Systeme ausfallen sollten. Hinzu kommen weitere gesetzliche Rahmenbedingungen, wie in Deutschland beispielsweise das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG). Es verlangt von der Geschäftsleitung eines Unternehmens, ein angemessenes Risiko-Management-Konzept einzuführen.

Ganzheitliche Lösungen sind gefragt

Nach einer Untersuchung des Marktforschungsunternehmens IDC dauert ein durchschnittlicher Ausfall vier Stunden und kostet etwa 250.000 Euro. Grundsätzlich variieren die Ausfallkosten je nach Branche jedoch sehr stark. Deshalb kommt es immer auf die individuellen Bedingungen des jeweiligen Unternehmens an. Unternehmen, die eine Hochverfügbarkeitslösung für ihr E-Business optimal unter Kosten-/Nutzen-Gesichtspunkten einsetzen wollen, sollten sich gründlich beraten lassen und nicht nur auf den Einkauf technologischer Komponenten beschränken. Denn IT-Verfügbarkeit ist ein Prozess und keine technische Disziplin. Mit Siemens Business Services können Kunden auf einen Dienstleister zurückgreifen, der von der Analyse über das Design und die Umsetzung bis hin zum Betreiben einer Lösung mit einer langfristigen Hochverfügbarkeitsbetreuung alles aus einer Hand bietet. Ziel ist es, die ideale Balance zwischen Über- und Unterversorgung zu finden und somit einen kostenoptimalen Schutz zu ermitteln. Der Systemintegrator kann auf ein breites Know-how und viele Spezialdienstleistungen im Siemens-Konzern zurückgreifen. Dazu gehören etwa der Bereich Security, der sich in einem umfassenden Paket mit der Rund-Um-Absicherung der IT-Infrastruktur widmet. Der richtige Grad an Availability muss sorgfältig geplant werden. Je höher sie ist, desto geringer sind die Ausfallkosten. Zunehmende Verfügbarkeit erfordert aber zugleich Investitionen in die IT. Der kostenoptimale Schutz hierfür wird im Rahmen des Consulting ermittelt.

Jedes Hochverfügbarkeitskonzept individuell entwickelt

Um herauszufinden, welches Verfügbarkeitskonzept sich für das jeweilige Unternehmen empfiehlt, kommt im Rahmen einer sorgfältig durchgeführten Analyse der Geschäftsprozesse das gesamte IT-Umfeld bis hin zum Rechenzentrum und zur Notfallplanung auf den Prüfstand: Hard- und Software, Netzwerke und die gesamte „Außenlandschaft“ wie zum Beispiel Stromversorgung, Klimaanlage etc. Im einzelnen umfasst die Analyse folgende Stufen:

- Definition der unternehmens- und geschäftskritischen Prozesse
- Transparentmachen der Ausfallrisiken von Geschäftsprozessen und Entwicklung von Schadensszenarien
- Betrachtung der Abhängigkeit zwischen Geschäftsprozessen und der Informationstechnologie
- Analyse der IT-Infrastruktur
- Identifizierung der Schwachstellen und Ausfallwahrscheinlichkeit der einzelnen IT-Komponenten

Die Erkenntnisse aus diesen Detailuntersuchungen münden schließlich in einem unternehmensspezifischen Verfügbarkeitskonzept. Ein intensiver Dialog zwischen Siemens Business Services und dem Kunden stellt sicher, dass alle weiteren Schritte sorgfältig und kompetent geplant und praxisgerecht entwickelt werden. Damit soll ein optimales Konzept entwickelt und sowohl eine Unter- als auch eine zu teure Überversorgung vermieden werden.

Prävention, reaktive Services und zuverlässige Technologie – die richtige Kombination entscheidet

Die ganzheitliche Dienstleistung von Siemens Business Services setzt sich anhand des erarbeiteten Verfügbarkeitskonzeptes unter anderem aus proaktiven und reaktiven Services zusammen. Dabei ist das Konzept plattformübergreifend, das heißt es umfasst die Angebote aller führenden Software- und Hardwarehersteller auf dem Markt.

Das Paket enthält umfangreiche proaktive Bausteine, die der Vorbeugung gegen Ausfälle dienen. Dazu gehört zum Beispiel die kontinuierliche Kontrolle der IT-Systeme ebenso wie die Analyse und gegebenenfalls die Behebung von Störungen. Hinzu kommt mit dem „System Health Check“ eine Fernüberprüfung von Hardware, Firmware und Systemsoftware nach zuvor definierten Checklisten, das Durchführen von Updates und Performance-Analysen. Außerdem gehört eine ausführliche Berichterstattung dazu, die den Kunden rechtzeitig auf Schwachstellen aufmerksam macht. Beim Element „Eskalationsmanagement“ erstellt Siemens Business Services einen Eskalationsplan, der bei komplexen Systemausfällen in Kraft tritt.

Die Premiumangebote beinhalten auch so genannte reaktive Services, wie etwa den Teleservice, der im Falle einer Störung genutzt wird, um sich sofort auf die Kundensysteme aufzuschalten und die Fehlerquelle aus der Ferne zu lokalisieren und das Problem gegebenenfalls gleich zu lösen. Dazu verfügt Siemens Business Services beispielsweise über einen Premiumservice für Hard- und Software. Der ServiceContract Premium für Hardware zeichnet sich dadurch aus, im Störfall schnell zu reagieren, um bei einem Ausfall die Hardware wiederherzustellen. Je nach Anforderungen stehen hier dem Kunden Wiederherstellungszeiten von sechs beziehungsweise vier Stunden zur Verfügung. Partner für Backup Recovery Services runden hier das Angebot von Siemens Business Services ab. Sie stellen Lösungen und Equipment für die unterschiedlichen Wiederanlaufverfahren von Rechenzentren zur Verfügung - warm- und cold-Backup.

Der Weg ist das Ziel

In enger Kooperation und im intensiven Dialog mit dem Kunden einerseits und mit Business Partnern andererseits entsteht so ein ganzheitliches Konzept, das jederzeit die Verfügbarkeit der IT-gestützten Geschäftsprozesse gewährleistet.

Außerdem gewährleistet die sorgfältige Analyse, die Beratung und Technologiekompetenz des Dienstleisters, dass die für die Sicherheit notwendige IT nach inhaltlichen und finanziellen Kriterien optimal ausgewählt und genutzt werden kann. Ziel ist die Gewährleistung sicherer Geschäftsprozesse. Denn nur mit einem umfassenden Konzept ist der Kunde für den Ernstfall gut gerüstet. Und dass dieser eines Tages trotz aller Vorsorge tatsächlich einmal eintritt, kann niemand ausschließen. Denn: Irgendwann erwischt es jeden, es kommt nur darauf an, wie lange es dauert, was es kostet und ob vorher wirksame Gegenmaßnahmen getroffen worden sind.

Weitere Informationen zum Thema unter:

[http:// www.sbs.de/verfuegbarkeit.de](http://www.sbs.de/verfuegbarkeit.de)