Sicherheit ist planbar

Wie wichtig die Verfügbarkeit der Ressource Netzwerk ist, wird manchem Anwender erst dann bewußt, wenn ein längerer Ausfall das Unternehmen lahmlegt und somit technische und organisatorische Mängel deutlich macht. Welche Folgen ein ganztägiger Ausfall haben kann, sollte sich jeder Verantwortliche möglichst vor Eintritt dieses Falles vor Augen führen und auch gegenüber den Budgets vergebenden Instanzen kostenmäßig verdeutlichen. Viele Unternehmen, die im Bereich klassischer Versicherungen eine durchgängige Vorsorge betreiben, haben Ihr Netzwerk aus Kostengründen oder auch manchmal aus mangelndem Problembewußtsein nur mangelhaft abgesichert.

Ein optimaler Grad an Ausfallsicherheit ist das Ergebnis einer ganzheitlichen Planung, die dann in eine Summe aufeinander abgestimmter Einzelmaßnahmen mündet.

Im folgenden werden einige planerische, technische und organisatorische Aspekte zur Verbesserung der Verfügbarkeit von Netzwerken dargestellt. Manches mag vielen Anwendern selbstverständlich erscheinen, anderes wird vielleicht zu einer Überprüfung der aktuellen Situation führen.

Die Ausführungen sind sicherlich nicht vollständig, sollen aber häufige Schwachpunkte in Netzwerkprojekten aufzeigen und sind somit allgemeiner Natur. Bei einer konkreten Projektierung ist es in jedem Fall unerläßlich, frühzeitig einen erfahrenen Netzwerkintegrator in die Planungen einzubeziehen.

Der Netzwerkschrank

Ein entscheidender Punkt, der in vielen Planungen oft nur unzureichend berücksichtigt wird, ist die Ausstattung des Netzwerkschrankes. Der Schrank beeinflußt die Umgebungsbedingungen und damit die Betriebsbedingungen der aktiven Elemente wesentlich. Zu hohe Temperaturen können zu sporadischen, nicht nachvollziehbaren Fehlfunktionen oder zu Totalausfällen der Netzwerkelektronik führen. Belastungen durch Staub und Schmutz belasten die Ventilatoren der Netzteile und führen ebenfalls zu Ausfällen.

Der wichtigste Faktor ist die ausreichende thermische Regulierung des Schrankes durch eine durchdachte Belüftung, die die gesamte Wärmeleistung der Geräte im Schrank berücksichtigt. Üblicherweise werden hierfür thermostatgesteuerte Ventilatoren eingesetzt Hier bietet der Hersteller Schroff 2 Varianten an: Sauglüfter als Standardlösung und Drucklüfter mit dem Vorteil des erhöhten Staubschutzes. In jedem Fall sollten beim Einsatz von Schranklüftungsystemen entsprechende Filtersysteme eingesetzt werden, um Staubeintritt zu vermindern. Je nach Umgebungsbelastung gibt es verschiedene Klassen von Schutzarten durch Gehäuse, nach denen man die Art und Ausstattung eines Netzwerkschranks definieren kann:

IP - Schutzklassen IP= (International Protektion)

	Berührung	**Fremdkörper**		**Wasserschutz**		
0	Kein Schutz	Kein Schutz		**0**	Kein Schutz	
1	Großflächige Körperteile (Handrücken)	Große Fremdkörper > 50mm		**1**	senkrecht fallendes Tropfwasser	
2	Finger	mittelgroße Fremdkörper >12 mm		**2**	schräg fallendes Tropfwasser bis	

					15 Grad gegen die Senkrechte	
3	Werkzeuge und Drähte > 2,5 mm	Kleine Fremdkörper > 2,5 mm		**3**	Sprühwasser bis 60 Grad gegen die Senkrechte	
4	Werkzeuge und Drähte > 1 mm	kornförmige Fremdkörper > 1 mm		**4**	Spritzwasser allseitig	
5	vollständiger Schutz	Staub-ablagerung		**5**	Strahlwasser	
6	vollständiger Schutz	Staubeintritt		**6**	starkes Strahlwasser	
--	---	---		**7**	zeitweiliges Untertauchen	
--	---	---		**8**	Untertauchen	

Schroff bietet eine breite Palette von Schranksystemen von Standardschränken bis hin zu Systemen mit IP Schutzklasse 55.

Der Einsatz von Druck oder Sauglüftern setzt die IP - Schutzklasse deutlich herab, daher muß bei erhöhten Anforderungen an den Schutz vor Umgebungseinflüssen auf eine externe Belüftung verzichtet werden und eine Kühlung erfolgt dann z.B. über Luftzirkulation durch Umlüfter im geschlossenen Schranksystem.

Für höchste Anforderungen an Sicherheit gibt es von Schroff ein Schrankkontrollsystem, das entscheidende Parameter wie z.B. Temperatur, Feuchtigkeit, Betätigung von Türkontakten etc. erfaßt und über SNMP eine Warnmeldung an den Administrator weitergibt.

Serversysteme

Disk-Array Systeme oder gespiegelte Plattensysteme in Mission - Critical - Servern sind sicherlich in vielen Fällen als Standard zu bezeichnen. Führende Hersteller wie HP bieten für ihre Serversysteme zusätzliche Optionen wie fehlerkorrigierender ECC - RAM, redundante Netzteile, doppelte Lüfter und auf gute thermoregulierung optimierte Gehäuse an. Der HP Netserver Assistent überwacht z.B. selbsttätig den Zustand von Novell Netware und fährt den Server nach einem erkannten Absturz selbsttätig wieder hoch. Proaktive Überwachung erfolgt bei HP durch einen speziellen Managementbus, der Temperatur, Plattenzustand und Multiprozessor überwacht und Statusmeldungen an HP Open View oder an eine remote Management Karte weitergibt.

Unterbrechungsfreie Stromversorgungen (USV)

Server über USV - Anlagen abzusichern, ist heute ebenfalls Stand der Dinge. Wer jedoch ausschließlich seine Server gegen Stromausfall absichert, hat ggf. im Fall der Fälle zuwenig getan. Bei komplexen Transaktionen in Client - Server Systemen, in der Produktionssteuerung oder vergleichbaren Anwendungen sollten in jedem Fall die wichtigsten Clients und natürlich auch die aktiven Komponenten im Pfad zwischen den kritischen Clients und den Servern durch USVs solange abgesichert sein, daß die Transaktion konsistent beendet werden kann. Sicherlich ist es für die Mehrzahl der Anwender fraglich, ob eine Komplettabsicherung aller Clients und aktiven Geräte wirtschaftlich vertretbar ist, jedoch sollte jeder Netzwerkverantwortliche seine

Applikationen daraufhin überprüfen, welche Folgen ein plötzlicher Verbindungsabbruch z.B. während eines Buchungslaufs oder während laufender Produktion hat. In jedem Fall sollten hier echte Online USV, die eine kontinierliche Spannung für die angeschlossenen Verbraucher generieren und Optionen auf Verlängerung der Autonomiezeit durch zusätzliche Batterieeinheiten bieten zum Einsatz kommen. Bei den USV des Herstellers Fiskars ist dies der Fall.

USV schützen zwar gegen Stromausfall und Stromschwankungen, können jedoch den Ausfall eines Netzteils eines aktiven Gerätes nicht kompensieren. Da das Netzteil aufgrund der integrierten Lüftung das einzige mechanische belastetet Teil eines Hubs, Switches oder Routers darstellt, ist hier im Vergleich zur reinen Elektronik das Risiko des Ausfalls am größten. Hier gibt es für viele Hubs und Switches redundante Netzteile, die im Load - Sharing Verfahren arbeiten und so den Ausfall eines Netzteils auffangen können. In Verbindung mit einer guten USV ist so eine optimale Absicherung möglich. Insbesondere 3COM ist hier an dieser Stelle hervorzuheben, da alle wichtigen Mitglieder der Superstack II Produktfamilie über redundante Netzteile versorgt werden können, wobei sogar eine Einbindung der Stomversorgung in das Netzwerkmanagementsystem Transcend von 3COM möglich ist. Für die Corebuilder Produktlinien von 3COM sind Optionen auf doppelte Netzteile ebenfalls selbstverständlich.

Netzwerktopologien mit Redundanz

Zur Schaffung von Redundanz im Bereich der Verkabelung basieren viele Netze bzw. Backbonestrukturen auf FDDI. FDDI Dual Attached konfiguriert basiert auf einer physikalischen Ringstruktur, die durch doppelte Ausführung gegen den Ausfall des Mediums geschützt ist. Wird die Kabelstrecke unterbrochen, so wird die Verbindung über den zweiten Ring weitergeführt. Wenn jetzt allerdings ein weiterer Fehler auftritt, z.B. der Ausfall einer Station, so zerfällt der Ring dann in zwei voneinander unabhängige Ringe. Um diesem Szenario vorzubeugen, kann die kritische Stelle mit einem optischen Bypass-Switch überbrückt werden. Des weiteren bietet FDDI die Option, Stationen Dual Homed zu konfigurieren, wobei der betreffende Server oder Station mit einem primären und sekundären Konzentrator angeschlossen wird. Beide Konzentratoren befinden sich gleichen Ring, der dual attached konfiguriert ist, womit ein erhöhter Schutz gegen Ausfall eines Konzentrators gegeben ist. FDDI bietet somit eine Reihe interessanter Features für höchste Ansprüche an Ausfallsicherheit, wobei jedoch in jedem Einzelfall abgewogen werden muß, ob eine Infrastruktur in FDDI die richtige Entscheidung ist, da diese Topologie für die führenden Hersteller keine strategische Rolle mehr einnimmt und wesentliche Weiterentwicklungen bis auf die Integration in neue Systemplattformen nicht mehr zu erwarten sind.

Auch unter Ethernet können redundante Strukturen unter Verwendung von Systemen geschaffen werden, die Spanning Tree 802.1d unterstützen. Dadurch können ebenfalls redundante Wege im Netz geschaffen werden. Eine weitere interessante Alternative zu Spanning Tree stellt 3COMs Resilient Link Technologie dar, mit der ebenfalls intelligente redundante Strukturen realisiert werden können.

Auch ATM bietet entsprechende Sicherheit, in dem z.B. mehrere physikalische Verbindungen zu einer logischen Verbindung zusammengefaßt werden. Der Ausfall einer physikalischen Verbindung führt dann lediglich zu einer Reduzierung der Bandbreite, nicht aber zu einem Wegfall der Verbindung.

Unabhängig von Redundanz durch entsprechende Protokolle oder aktive Komponenten ist sinnvoll, kritische Kabelwege parallel über verschiedene Strecken zu führen, um bei Unterbrechung eines Kabelweges durch Umpatchen auf den zweiten Kabelweg den Netzbetrieb wieder aufnehmen zu können. Bei der Planung solcher Optionen sollte man jedoch sehr große Sorgfalt walten lassen, da z.B. eine LWL - Backupstrecke, die für Ethernet noch verwendet werden kann, für Fast Ethernet aufgrund der Längenrestriktionen schon zu lang sein kann. Bei Verwendung redundanter LWL Wege ist insbesondere zu beachten, daß der Backupweg oft länger ist als der ursprüngliche Weg, und zudem zusätzliche Übergabepunkte enthält, was auf der Gesamtstrecke zu einer erhöhten Signaldämpfung führt.

Netzwerkmanagement

Netzwerkmanagement wird noch oft aus dem Blickwinkel der Diagnose und Fehlerbehebung betrachtet. Ist der Fehler jedoch schon aufgetreten, ist die Situation, die es zu vermeiden gilt, schon eingetreten. Modernes Netzwerkmanagement ist als proaktives Handeln zu verstehen, bei dem durch die Überwachung des Netzes kritische Parameter kontinuierlich überwacht werden. Durch Fortschreibung dieser Werte in die Zukunft können Entscheidungen wie z.B. die Einführung von Fast Ethernet und / oder Switching auf der Basis klarer Auswertungen erfolgen, wie z.B. der Identifizierung von " Top Talkern ", die besonders viel Netzlast generieren. Wer die Entscheidungen über die Struktur seines Netzes aufgrund solcher empirisch gewonnener Daten trifft, wird sicherlich manchen Zusammenbruch des Netzes durch Überlast im Vorfeld vermeiden. Darüber hinaus können moderne SNMP Systeme auf RMON Basis bei Überschreitung definierter Werte einen Alarm auszulösen, der es dem Administrator ebenfalls ermöglicht, vor einem Crash im Netz aktiv zu werden und die Probleme im Vorfeld zu beheben.

Sicherheit im WAN

Immer mehr Mission - Critical Applikationen sind von WAN - Verbindungen abhängig. Hier bieten insbesondere die Router des Marktführers CISCO vielfältige Möglichkeiten redundanter Wegewahl bei Ausfall einer Verbindung. Bei nicht allzu hohen Anforderungen an die Verfügbarkeit der Verbindung kann z.B. ein einzelner Router so konfiguriert werden, daß bei Ausfall einer Festverbindung automatisch eine Wählverbindung aufgebaut wird. Hierbei wird dem Ausfall der Verbindung selber vorgebeugt, mit dem Ausfall des Routers selber jedoch fällt auch die Verbindung endgültig aus. Für höchste Sicherheitsanforderungen kann daher z.B. folgende Lösung realisiert werden: Es werden ein primärer und ein Backup Router definiert. Primäre Verbindung ist eine Festverbindung, Backupverbindung ist eine Wählverbindung. Fällt die Festverbindung aus, übernimmt das Dial-Backup Interface die Verbindung. Fällt der primäre Router oder dessen LAN - Verbindung aus, so übernimmt der sekundäre Router dessen Funktionen und Einstellungen. Da der sekundäre Router physikalisch nur über eine Wählverbindung verfügt, stellt er bei Aktivierung das Fehlen dieser Verbindung fest und aktiviert die Dial-Backup-Verbindung. Für noch höhere Sicherheit kann man die Wählverbindung über eine andere Ortsvermittlungstelle als die Festverbindung führen, um auch dem sehr unwahrscheinlichen Szenario des Totalausfalls der Vermittlungstelle vorbeugen zu können.

In einem Umfeld mit mehreren Routern können natürlich auf Basis definierter Backupverbindungen sowohl lokal als auch im WAN Bereich vermaschte, sehr sichere Strukturen eingerichtet werden.

Organisatorische Voraussetzungen:

Um im Fall der Fälle schnell Abhilfe schaffen zu könne, sind einige Voraussetzungen unerläßlich:

Für die kritischen Komponenten sollten Serviceverträge mit definierten Austauschzeiten abgeschlossen werden, um die Wiederherstellung in einem vertretbaren Zeitraum zu ermöglichen.

Es jedoch keinesfalls damit getan, die ersetzte Komponente in den Netzwerkschrank zu montieren und einzuschalten. Jeder Router und nahezu jeder professionelle Switch müssen individuell konfiguriert werden. Daraus ergibt sich die Notwendigkeit, alle Konfigurationsfiles so zu archivieren, daß sie auch während eines Ausfalls im Zugriff sind. Ein detaillierter Ablaufplan stellt sicher, daß die Inbetriebnahme so schnell wie möglich durchgeführt werden kann. Da in vielen Unternehmen die EDV Abteilungen personell oft recht knapp besetzt sind, ermöglicht ein gut dokumentierter Ablaufplan auch eine Inbetriebnahme durch EDV -Personal, das nicht primär aus dem Netzwerkbereich kommt, wenn die Personen der eigentlichen Netzwerkadministration nicht anwesend sind.

Externe Partner einbinden

Sicherlich läßt nicht jedes Budget eine Maximallösung zu. Da eine solche Lösung auch nicht für jeden Anwender nötig und wirtschaftlich vertretbar ist, sollte jeder Verantwortliche sowohl bei Neuprojekten als auch bei einer kritischen Überprüfung der vorhandenen Installation mit einem

erfahrenen Netzwerkintegrator in Dialog treten, um gemeinsam mit dem Integrator die unter technischen und wirtschaftlichen Aspekten optimale individuelle Lösung zu erarbeiten. Ein solcher Partner sollte sowohl im Bereich der Planung als auch in der Ausführung aktiver und passiver Strukturen im Netz über weitreichende Erfahrungen verfügen, um sicherstellen zu können, daß die Zielsetzungen des Anwenders im Projekt auch erreicht werden.

Oliver Wichmann

Der Autor ist Produktmanager bei der Bell Computer - Netzwerke GmbH in Bonn. Sie können Ihn bei Fragen unter der 0228-42104-20 erreichen.