Sicherheitsdesign für die Netzinfrastruktur

Rolf Henze

Universität Kassel

Zusammenfassung Datenkommunikationstechnik hat in den vergangenen zehn Jahren zunächst die Informationsmedien im Wissenschaftsbereich revolutioniert und beginnt zunehmend auch die Geschäftsprozesse in Wirtschaft, Verwaltung und im privaten Umfeld zu bestimmen. Mitentscheidend für den Erfolg des Internet war das liberale und unreglementierte Umfeld der Universitäten, aus dem ein großer Teil der tragenden Innovationen hervorgegangen ist. Mit wachsender Abhängigkeit von der Kommunikationstechnik steigen die Anforderungen an Sicherheit und Zuverlässigkeit. Hier wirken sich die innovationsfördernden Ursprünge der Technik negativ aus. Die Infrastruktur ist in der Regel unübersichtlich, oft zufällig gewachsen. Technik und Leistungsfähigkeit der Netze sind heterogen. Die Integration von Telefon- und Datennetz bringt zwei Welten mit sehr unterschiedlichen Sicherheits- und Verfügbarkeitsstandards zusammen, was mit technischen und organisatorischen Problemen verbunden ist. Sicherheitsanforderungen an die Infrastruktur sind selten klar definiert. Der Bericht beschreibt den Aufbau einer modernen Kommunikationsinfrastruktur an einer Universität unter den Aspekten Sicherheit und Zuverlässigkeit. Verkabelungstechniken, Lichtwellenleiter und Kupferkabel, werden verglichen. Eine Strategie zur Schaffung einer einheitlichen, leistungsfähigen, sicheren und nachhaltigen Infrastruktur wird vorgestellt.

1 Einleitung

Drei grundlegende Faktoren haben die Entwicklung von Kommunikationsnetzen in den letzten zehn Jahren beeinflußt. Erstens die rasche Innovation in der Computertechnik. Damit war auch ein entsprechend rascher Anstieg der Leistungsfähigkeit und der Dienstevielfalt der Datennetze im Inhouse-Bereich verbunden. Durch die breite Akzeptanz einiger Schüsselanwendungen wie Email und WWW, stieg zweitens der Bedarf nach Netzanschlüssen um Größenordnungen. Drittens hat die Deregulierung der Weitverkehrnetze unter anderem einen Innovationsschub bewirkt, wodurch neue Dienste entstanden und die Preise sanken. (Sie hat aber auch durch komplexere Strukturen und Verantwortlichkeiten in anderen Bereichen den Fortschritt gehemmt und Versorgungslücken erzeugt.)

Während der zweite Faktor, die rasch wachsende Nutzung der Netze, bei immer weiter sich differenzierender Dienstepalette, einen hohen Bedarf an die Sicherheit der Netze stellt, erzeugen die anderen beiden Faktoren im wesentlichen Probleme, was die Sicherheit betrifft. Oft werden auch technische Lösungen von Sicherheitsproblemen durch die Entwicklung rasch überholt.

Grundlage für die Lösung eines Sicherheitsproblems ist eine saubere Analyse der Risiken. Dies ist allerdings konsequent nur in isolierten Teilbereichen, wie z.B. bei einigen Endgeräten und Anwendungen möglich. Eine Netzinfrastruktur hat immer eine Vielfalt

unterschiedlicher Anwendungen zu unterstützen, die auch sehr unterschiedliche Sicherheitsanforderungen haben. Dabei ist oft zwischen Sicherheit auf der einen Seite und einfachem Betrieb und einfacher Zugänglichkeit der Anwendungen auf der anderen Seite abzuwägen. Zudem muß die Netzinfrastruktur offen bleiben für innovative Entwicklungen. Sie darf nicht durch zu restriktive technische oder organisatorische Einschränkungen die Anwendungen behindern.

Im folgenden wird über Erfahrungen und konzeptionelle Überlegungen beim Aufbau eines großen, regional verzweigten Inhouse-Netzes, wie es für Universitäten typisch ist, berichtet. Der Aspekt Sicherheit steht dabei im Vordergrund. Wegen oben genannter Schwierigkeit folgt die Vorgehensweise dabei nicht der Reihenfolge Sicherheitsanalye, -konzept und Realisierung, sondern es wird ein pragmatischer "Bottom-UpÄnsatz gewählt, der von der realen Entwicklung der Netze ausgeht, die in erster Linie von Leistungsbedarf und technischen Neuerungen getrieben wird. Sicherheitsaspekte werden beim Aufbau der Infrastruktur berücksichtigt, durch Maßnahmen, die möglichst anwendungsneutral und nachhaltig sind.

2 Anforderungen an Kommunikationsnetze

Leistungsfähigkeit, das bedeutet in erster Linie Übertragungsrate und Quality of Service (QoS), ist wichtigste Anforderung an Kommunikationsnetze. Unterschiedliche Anwendungen benötigen sehr verschiedene Übertragungsraten. Während der Bedarf bei File-Server-Diensten ständig steigt, ist er bei Multimedia-Anwendungen durch die Darstellungskomplexität im wesentlichen festgelegt. Mit Übertragungsraten bis in den Gigabit-Bereich hinein decken moderne Netztechniken diesen Bedarf in lokalen Netzen ab (vgl. Abb. 1). Bezüglich QoS ist ihre Leistungsfähigkeit allerdings sehr unterschiedlich.

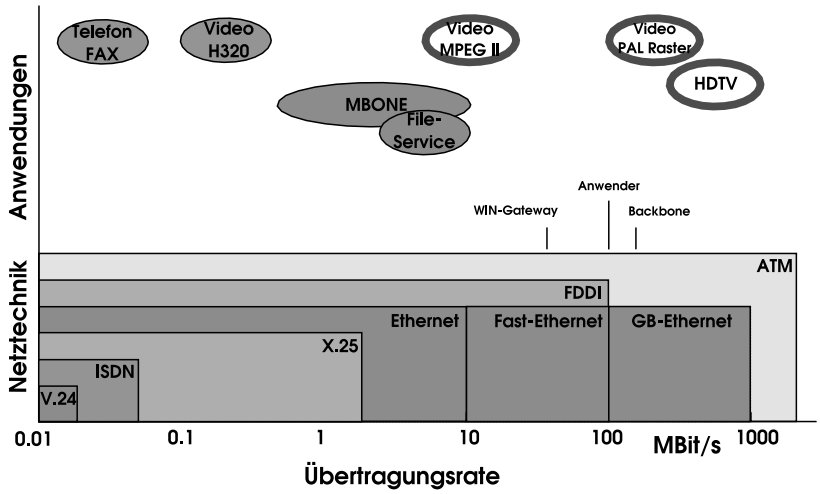

Abbildung 1: Anwendungen, Bandbreite, Netztechnik

Neben den Anforderungen der Nutzer sind auch die betrieblichen Aspekte des Netzes zu berücksichtigen. Sie bestimmen nicht nur die Kosten, sondern haben indirekt auch Einfuß auf die Sicherheit. Unter drei Punkten lassen sich die Anforderungen einordnen:

Leistung

- Unterstützung isochroner Dienste (Multimedia)
- hohe Bandbreite (Multimedia)
- Verfügbarkeit (Netzanschluß, Protokolle, Netzdienste)
- Mobilität

Sicherheit

- Verfügbarkeit (Betriebssicherheit)
- Vertraulichkeit
- Integrität
- Verbindlichkeit
- Umweltneutralität

Betriebsaufwand

- einheitliche Endgeräteschnittstelle
- einfache Infrastruktur (geringer Betriebsaufwand)
- nachhaltige Verkabelung

Während bisher, bedingt durch die rasche Entwicklung der Technik, der Leistungsaspekt im Vordergrund stand, hat der Netzbetreiber zunehmend Sicherheitsaspekte zu berücksichtigen und die Infrastruktur in Hinblick auf einen reduzierten Betriebsaufwand zu sanieren. Dabei spielt die Integration von Sprach- und Datennetz eine wichtige Rolle.

Der Aufbau eines leistungsfähigen und zukunftssicheren integrierten Netzes in einer großen Organisation ist aus Kostengründen kaum in einem Schritt möglich. Computer- und Netzwerktechnik sind weiterhin in vitaler Entwicklung begriffen. Das Netzwerkdesign muß daher flexibel sein gegenüber Änderungen, die neue Anwendungen und Protokolle fordern. Ein Netz ist ein verteiltes System, mit einer immer aufwendiger werdenden Technik und Organisation. Es läßt sich nicht so einfach erneuern, wie in der Vergangenheit ein Mainframe-Computer.

3 Die Entwicklung klassischer Datenverarbeitungsnetze

Bei Telekommunikationsnetzen entwickelte sich die Technik relativ langsam, verglichen mit der Zeit, die für die Organisation der Infrastruktur zur Verfügung stand. Die von Anfang an hohe Reichweite dieser Netze und die damit verbundene Monopolisierung des Betriebs erleichterte ebenfalls den geordneten Aufbau der Infrastruktur.

Datenkommunikatonsnetze dagegen entwickelten sich lokal, angepaßt an den Bedarf der sich rasch ändernden Computertechnik. So wurden zunächst Telefonleitungen zur Verbindung von Mainframe-Computern genutzt. Mit dem Aufkommen der Abteilungs- und

Laborrechner entstand Ethernet, das die Übertragungskapazität von Telefonleitungen um eine Größenordnung übertraf und dabei minimale Voraussetzungen an die Infrastruktur stellte (nur ein Koaxialkabel wurde benötigt). Zuverlässigkeit und Datenschutz waren dagegen beim ersten Ethernet wenig ausgeprägt. Die Technik war eben den Anforderungen eines Netzes angemessen, das sich maximal über ein Gebäude erstreckte und eine relativ kleine Organisationseinheit versorgte.

Mit wachsenden Anforderungen an die Übertragungsrate entstanden Token-Ring, FDDI, Fast-Ethernet und ATM. Die Verkabelung mußte entsprechend angepaßt werden. Zunehmend wurde Lichtwellenleiter (LWL) eingesetzt. Strukturierte Verkabelung löste die Bus-Struktur ab (vgl. Abb. 2). Über einen Zeitraum von 20 Jahren, 1980 bis 2000, mußte entsprechend die Verkabelung etwa alle 5 Jahre erneuert werden. Dies geschah selten flächendeckend und koordiniert, so daß als Ergebnis heterogene, unstrukturierte Datennetze entstanden.

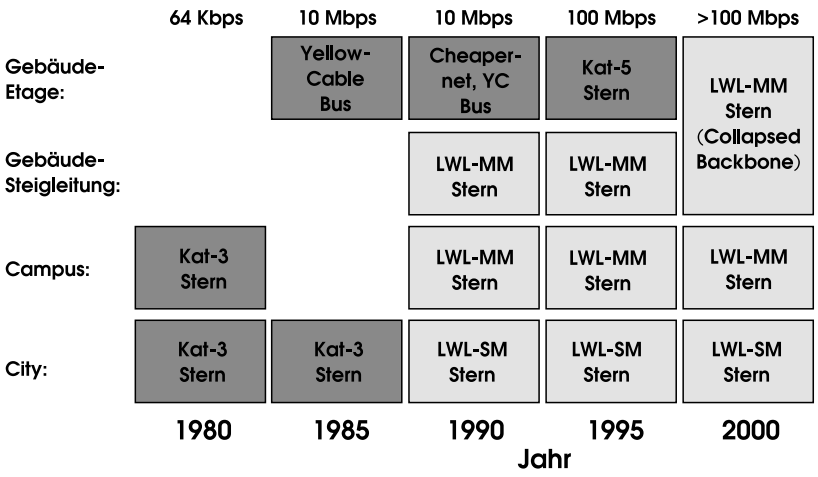

Abbildung 2: Verkabelung von Datennetzen

Die verschiedenen Verkabelungstechniken unterscheiden sich deutlich bezüglich Betriebssicherheit und Datenschutz. Ein einheitlicher Sicherheitsstandard in einem klassischen heterogenen Datennetz ist daher schwer zu erfüllen. Verteilte Zuständigkeiten für den Betrieb der Teilnetze, die zudem von Organisation zu Organisation unterschiedlich geregelt sind, verschärfen die Situation.

Die Leistungsfähigkeit des Netzes, d.h. die verfügbare Bandbreite pro Anschluß und die Anzahl der Anschlüsse, änderte sich in den vergangenen zehn Jahren über Größenordnungen. Damit wuchs auch die Funktionalität der Netzknoten. Während die Yellow-Cable-Ethernet Technik zunächst ganz ohne aktive Netzknoten auskam, wurden bald Bridges, Hubs, Router und Switches eingesetzt und die Funktionalität reichte über die OSI-Ebene 2 hinaus (vgl. Tab. 1). Ihre wachsende Funktionalität, Differenzierung und Anzahl macht die

aktiven Komponenten im Netz komplexer und anfälliger. Zudem nimmt dabei der Betriebsaufwand zu.

		1985	1990	1995	2000
Ethernet		Shared YC	Shared TP	Switched TP	Switched SUTP
Datenrate (Mbps)	Endgerät brutto	10	10	10	100
	Endgerät netto	0,5	0,5	10	100
	Backbone	10	100	100	1000
QoS		-	-	ja	ja
Anz. Endgeräte		20	1000	10.000	10.000
Aktive LAN Komponenten	Backbone	-	HUB	Switch	Switch L3-Switch MPLS
		Bridge	Router	Router	Router

Tabelle 1: Funktionalität wandert ins Netz

Ein Sicherheitskonzept für das Kommunikationsnetz muß daher bereits an der Infrastruktur ansetzen. Die Grundforderungen sind:

- Einheitliche und nachhaltige Verkabelung
- klare Strukturierung des Netzes
- klare Definition der Netzfunktionen.

4 Verkabelung

Die wichtigsten Eigenschaften bei der Beurteilung eines Kabels sind Bandbreite und Reichweite. Da die Parameter etwa reziprok voneinander abhängen, wird das ausgedrückt im Bandbreite-Längen-Produkt. Tabelle 2 vergleicht die Reichweite der im Inhouse-Bereich überwiegend eingesetzten Kabelarten, Kategorie-3 und -5 Kupferkabel sowie Multimode-Lichtwellenleiter (MM-LWL). Dabei wird von Werten ausgegangen, wie sie im realen Betrieb mit verschiedenen Ethernet-Varianten erreichbar sind. Bei 10 Mbps (Mega Bit pro Sekunde) wird die geforderte Reichweite für Etagenverkabelung, 100 m, mit allen Kabelarten erreicht. Bei 100 Mbps (Fast Ethernet) erreichen Kat-5 Kupferkabel und LWL diesen Wert. Bei 1 Gbps ist Kat-5 Kabel nur noch mit Einschränkungen (ausreichende Adernzahl) brauchbar. Höhere Reichweiten und Übertragungsraten sind nur noch mit LWL zu realisieren.

Für Nachhaltigkeit und Betriebsicherheit der Verkabelung sind Bandbreitenreserve und einfache Struktur von entscheidender Bedeutung. Hier hat LWL-Multimode klare Vorteile. Die derzeit maximale Übertragungsrate liegt bei 10 Gbps (bei 300 m Reichweite). Bei der

	10 Mbit-Ethernet	Fast-Ethernet	Gigabit-Ethernet	10 GBit Ethernet
Kat-3	100	-	-	-
Kat-5	100	100	(100)	-
LWL-MM	2000	2000	500	300 (10GBase-LX4, WWDM)

Tabelle 2: Maximale Reichweite im LAN (m)

für den Einzelarbeitsplatz voraussichtlich maximal erforderlichen Übertragungsrate von 1 Gbps lassen sich 500 m Reichweite realisieren. LWL-Multimode sollte daher für den Inhouse-Bereich genügen. Besondere Fälle mit höherem Bedarf, z.B. Anbindung eines Servers mit 10 Gbps über Entfernungen von mehr als 300 m, sollten so selten auftreten, daß für diese Fälle eine bedarfsorientierte Nachverkabelung mit Single-Mode (SM) -LWL ausreicht.

Eine Reichweite von 500 m ermöglicht es, die Anzahl der Netzknoten deutlich zu reduzieren. Das verringert den Betriebsaufwand und erhöht die Sicherheit. Die beiden typischen Verkabelungsstrukturen für Kupferkabel und LWL zeigt Abb. 3:

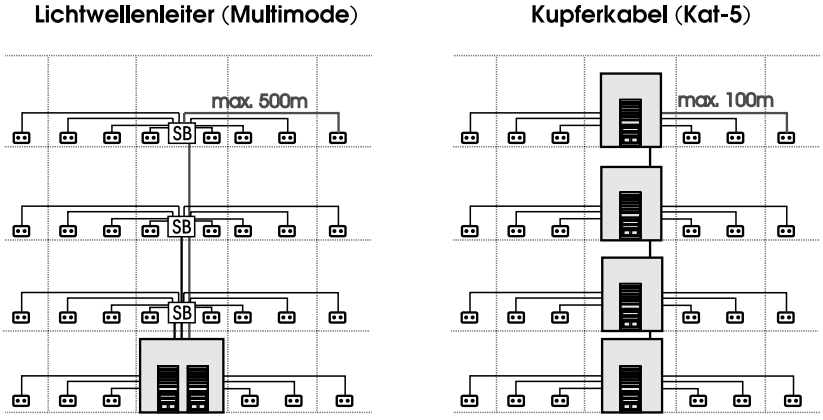

Abbildung 3: Verkabelungsstrukturen

In beiden Fällen ist das 3-Ebenen Konzept der strukturierten Verkabelung eingehalten (Ebene1: Gebäudeverbindung, Ebene 2: Steigleitungen zur Anbindung der Etagen, Ebene

3: Verkabelung innerhalb der Etagen). Bei der Kupfervariante werden von einem zentralen Gebäudeverteiler ausgehend die Steigleitungen in weitere Etagenverteilerräume geführt. Hier stehen Switches (oder Hubs), die die Endgerätesteckdosen versorgen. Bei der LWL-Variante kann, wegen der höheren Reichweite, auf die Etagenverteilerräume verzichtet werden. Der Etagenverteiler besteht hier nur aus einer Spleißbox (Maße ca. 30x40x10 cm), die unauffällig in normalen Räumen oder im Flurbereich untergebracht werden kann. Der Radius einer Etagenverkabelungszelle, d.h. der Anschlußdosen, die von einen Etagennoten aus erreicht werden können, beträgt bei Kupfer ca. 60 m, was durch die Kabelreichweite von 100 m bestimmt wird. Bei der LWL-Variante ist, wegen der Reichweite von 500 m, dieser Radius größer als die Ausdehnung des Gebäudes. Die Ausdehnung der Etagenverkabelungszelle hängt hier nur von der Anzahl der Fasern im Steigkabel ab. Bei 144-fasrigem Steigkabel z.B. können 36 Doppelanschußdosen pro Spleißbox erreicht werden.

Einen Vergleich der wichtigsten Parameter der beiden Verkabelungsvarianten zeigt Tab. 3. Die Anzahl der Netzknotenräume ist für die LWL-Lösung etwa um den Faktor 16 geringer. Man kommt auch in größeren Gebäuden oder Gebäudekomplexen mit einen Knotenraum aus. Bei kleineren, verteilten Gebäuden läßt sich die Verkabelung oft in einem zentralen Gebäude zusammenführen, so daß in den anderen auf den Knotenraum verzichtet werden kann. Eine geringere Anzahl der Knotenräume bringt deutliche Kostenvorteile bei der Versorgung mit Energie, Klimatisierung und Gefahrenmeldeanlage sowie bei der Raumabsicherung. Zudem sind alle aktiven Netzkomponenten in wenigen Räumen konzentriert. Stattet man diese Räume bezüglich Verfügbarkeit und Datenschutz nach Regeln aus, wie sie für den Betrieb von Telefonanlagen üblich sind, so ist für den sicheren Betrieb von Sprachübertragung (Voice over IP (VoIP)) schon ein entscheidender Schritt getan. Weitere Vorteile sind geringerer Verwaltungs- und Wartungsaufwand sowie erhöhte Sicherheit. Weniger potentielle Fehlerquellen erhöhen die Betriebssicherheit. Die einfachere Struktur erleichtert die Bildung von Redundanzen. Redundanzmaßnahmen sind allerdings, wegen der höheren Konzentration von Anschlüssen in den Knotenräumen, auch eher notwendig.

	Lichtwellenleiter	Kupfer, Kat-5/6
max. Übertragungsrate	10 Gbps (160 Gbps, 1 Tbps)	600 Mbps
max. Länge	500 – 2000 m	100 m
Anzahl IT-Räume	1	16
Kabelquerschnitt Pro 10 Endgeräte	ca. 50 mm^2 (1)	ca. 800 mm^2 (16)
Störungssicherheit	+	-
Elektromagnetische Abstrahlung	+	-
Telefonanschlüsse	-	+
Kosten	Kupferverkabelung etwa 15% teurer als LWL	

Tabelle 3: Etagenverkabelung mit Lichtwellenleiter oder Kupferkabel

Die erforderlichen Kabellängen sind bei der LWL-Variante höher. Dieser Nachteil wird allerdings ausgeglichen durch den geringeren Kabelquerschnitt (Faktor 16, bei Verwendung von 4-adrigen LWL-Voliton-Kabel in der Etage, verglichen mit Kat.5 Kupferkabel). Dies erleichtert nicht nur die Installation. Auch die Handhabung der Patchfelder in den Verteilerräumen ist mit LWL deutlich einfacher und übersichtlicher.

LWL-Kabel bieten wegen ihrer Unempfindlichkeit gegenüber elektromagnetischen Störungen außerdem deutliche Vorteile für die Betriebssicherheit. So entfällt das Übersprechen zwischen Übertragungskanälen und die Beeinflussung durch fremde Signalquellen. Insbesondere entfällt das bei größeren Kupferinstallationen lästige Problem der Potentialtrennung.

Ein weiterer sicherheitsrelevanter Vorteil der LWL-Verkabelung ist die nicht vorhandene elektromagnetische Abstrahlung. Damit wird nicht nur die Störung anderer Systeme vermieden. Auch negativer Einfluß auf den Arbeitsplatz, durch einen Beitrag zum Elektrosmog, wird vermieden.

Die wichtigsten Merkmale einer LWL-Verkabelung sind für ein reales Beispiel in Tab. 4 aufgelistet. Es handelt sich um einen Gebäudekomplex mit 3 Teilgebäuden, einer Nutzfläche für Büro- und Laborräume von insgesamt 19425 m^2 und einer Gesamtzahl von 1770 Doppeldosen, was 3540 Anschlußports entspricht. Im Mittel kommt auf 11 m^2 eine Doppeldose. Die Anzahl der Fasern in den Steigkabeln ist etwas überdimensioniert, so daß bei Bedarf zusätzliche Anschlüsse von den Spleißboxen zu Arbeitsplätzen geführt werden können. Bei Ausnutzung dieser Reserve beträgt die Gesamtzahl der Anschlußports 4250.

Verkabelung	Datenverteilerraum
• 1770 Doppeldosen (3540 Ports) (max. 4250 Ports)	• Grundfläche 55 m^2
• Portdichte: 1 D-Dose/ 15 m^2	• 18 Verteilerschränke
• Steigkabel: 144 Fasern	• Klimatisierung max. 24 kW
• Etagenkabel: 4 Fasern	• Brandmeldeanlage
• 36 D-Dosen / Spleißbox	• Zugangssicherung

Tabelle 4: Gebäudevernetzung LWL-Collapsed-Backbone (Beispiel)

Der Gebäudekomplex kommt mit einem Verteilerraum aus. Bei Aktivierung aller Anschlußports wird eine Klimatisierung für die Abfuhr einer Wärmeleistung von 24 kW benötigt. Es wird allerdings im Mittel mit einer Aktivierung von nur ca. 30% der Ports gerechnet. Die Klimaanlage ist deshalb modular ausgelegt. Aus Kostengründen und auch aus Gründen der Betriebssicherheit sollten Abwärme und Klimatisierung möglichst gering gehalten werden. Es ist zu hoffen, daß der Energieverbrauch der aktiven Netzkomponenten in Zukunft weiter sinken wird. Im vorliegenden Beispiel reduzierte sich der betreffende

Leistungswert schon in der Zeit zwischen der Planungsphase und der Realisierung (ca. 18 Monate) um den Faktor 2.

5 Sicherheitsgrundlage durch geeignete Verkabelung und Netzstruktur

Eine Netzwerkinstallation in Glasfasertechnik bis zu den Arbeitsplätzen ist die Basis für eine sichere und langlebige Infrastruktur. Die wichtigsten Sicherheitsmerkmale sind:

1. Unempfindlichkeit gegenüber elektromagnetischen Störungen
2. Vereinfachung von Redundanzmaßnahmen
3. erhöhte Sicherheit gegen Abhören
4. Erhöhte Sicherheit durch zentralen Netzknotenraum
5. keine elektromagnetische Belastung

Damit ist den Sicherheitsanforderungen bezüglich Verfügbarkeit (Punkte 1,2 und 4), Vertraulichkeit (Punkt 4) und Umweltneutralität (Punkt 5) entsprochen.

Im nächsten Schritt wird durch Redundanzmaßnahmen die Betriebssicherheit weiter erhöht. Die wichtigsten Ansatzpunkte für Redundanz sind:

- Netzanschluß am Arbeitsplatz
- Netzwerkknoten
- Gebäude
- Campus.

Der Anschluß am Arbeitsplatz sollte immer doppelt vorhanden sein (Doppelanschlußdosen). Die Struktur der Gebäudeverkabelung kann diese Redundanz mehr oder weniger unterstützen (was weiter unten erläutert wird). In den Netzwerkknoten ist die Betriebssicherheit der aktiven Komponenten (Switches, Router) zu gewährleisten. Dies geschieht durch redundante Netzteile, modularen Aufbau und unterbrechungsfreie Stromversorgung. Im Campusbereich wird Redundanz durch entsprechende Leitungsführung zwischen den Gebäuden erreicht.

Redundanz ist in verschiedenen Stufen möglich, angepaßt an geringere oder höhere Sicherheitsanforderungen. Für den Gebäudebereich soll im folgenden etwas näher darauf eingegangen werden. Die beiden Anschlußports einer Doppeldose am Arbeitsplatz bieten dann eine echte Redundanz, wenn sie auf unterschiedliche Switches aufgelegt sind. Dazu sind keine Änderungen in der Verkabelungsstruktur notwendig. Es ist allein durch entsprechendes Patchen in den Netzknoten getan (vgl. Abb. 4, Teil a). Will man die Sicherheit weiter erhöhen und Maßnahmen gegen den Ausfall ganzer Netzknotenräume, etwa durch Brand oder Katastrophen, treffen, so ist das wegen der hohen Reichweite der LWL-Verkabelung leicht möglich. Die Spleißverteiler in den Etagen müssen in diesem Fall so verschaltet werden, daß die beiden Anschlußports einer Doppeldose über zwei verschiedene Steigkabel in verschiedene Netzknotenräume geführt werden, die sich in unterschiedlichen Gebäuden befinden (vgl. Abb. 4, Teil b).

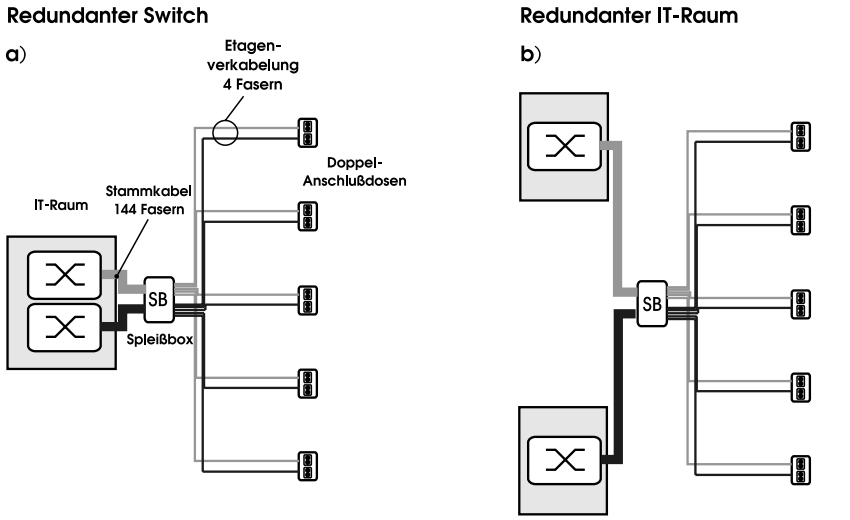

Abbildung 4: Redundanz bei Collaped-Backbone-Verkabelung

6 Sicherheit für Netzdienste und Anwendungen

Sicherheitsmaßnahmen sind normalerweise eine äußerst spezifische Angelegenheit. Sie hängen stark von den Eigenschaften des zu sichernden Systems sowie vom erforderlichen Sicherheitsgrad ab. Der Sicherheitsgrad bestimmt auch die Kosten, die über Größenordnungen variieren können. Eine unter Beachtung von Sicherheitsaspekten aufgebaute Netzinfrastruktur kann keine spezifischen Belange berücksichtigen und bietet daher im allgemeinen auch keinen hohen Sicherheitsgrad für spezielle Anforderungen, sondern eine Sicherheitsgrundausstattung. Sie kann Anwendungen mit geringen Sicherheitsanforderungen eine verläßliche Basis bieten, die keine weitere Maßnahmen erforderlich macht oder aber Grundlage für weitere Maßnahmen sein. Zum Beispiel kann die Gewährleistung der Vertraulichkeit einer Datenübertragung durch geeignete Verschlüsselung auf der Anwendungsebene geschehen. Dazu ist nicht unbedingt ein abhörsicheres Netz notwendig. Aber es ist hilfreich, wenn der Anwender in diesem Fall schon ein betriebssicheres Netz und ggf. auch eine Zertifizierungsinstanz für die kryptographischen Schlüssel vorfindet.

Ein sicheres Kommunikationsnetz kann man sich als gestuftes System vorstellen, bei dem die Infrastruktur die Basis bildet. Sie wird zentral betrieben oder mindestens zentral reguliert. Darauf setzen Maßnahmen auf, die mehr oder weniger anwendungsspezifisch sind. Sie können ebenfalls zum Netz gehören, wenn es z.B. um die Gewährleistung der Vertraulichkeit von Netzdiensten wie WLAN (Wireless-LAN) oder VoIP geht. Sie können aber auch auf Anwendungsebene vom Nutzer realisiert sein. Letzteres ist oft der Fall, wenn es sich um sehr spezifischen Bedarf mit hohen Anforderungen und Kosten handelt.

Bevor auf weitere technische Sicherheitsmaßnahmen eingegangen wird, die teilweise anwendungsspezifisch und dezentral sein können, sollen organisatorische Maßnahmen erwähnt werden, die unbedingt zur Basisausstattung und zum zentralen Betrieb des Netzes

gehören. Ein wichtiger Punkt ist die Verwaltung der Netzadressen (IP-, evtl. MAC-Adresse, Internet-Domain). Die zentrale Verwaltung dieser Adressen durch den Netzbetreiber dient der Funktionssicherung (der Betrieb kann z.B. bei doppelter Verwendung von IP-Adressen empfindlich gestört werden) und der Verbindlichkeit der Kommunikation. Ein weiterer Punkt ist die Regulierung der Netzzugänge. Durch einfache technische Maßnahmen (Modems, ISDN-Router) können an jedem Arbeitsplatz externe Zugänge in das Netz geschaffen werden. Die Einrichtung solcher Zugänge und die damit verbundenen Sicherheitsmaßnahmen müssen vom Netzbetreiber reguliert werden.

Nach Verkabelung und Redundanzmaßnahmen sind virtuelle LANs (VLANs) die dritte Stufe der zur Infrastruktur gehörenden technischen Maßnahmen. VLANs bieten virtuelle Inseln zur internen Kommunikation von Arbeitsgruppen, mit einer minimalen Absicherung nach außen. Sie entsprechen den Segmenten (Broadcast-Units) des alten, segmentierten Ethernet-Netzes. Virtuelle LANs sind wesentlich flexibler als Ethernet-Segmente, da sie sich über Etagen und sogar Gebäude hinaus erstrecken können. Sie können auf Basis von Switch-Ports, MAC- oder IP-Adressen gebildet werden. Dabei variieren Flexibilität und Verwaltungsaufwand. Die Nutzung von Switch-Ports z.B. erfordert den geringsten Verwaltungsaufwand für den Netzbetreiber, bietet aber wenig Flexibilität für den Anwender.

Eine weitere technische Maßnahme, die die Sicherheitsanforderungen Vertraulichkeit, Verbindlichkeit und Integrität unterstützt, ist IPv6. Schon allein aus diesem Grund ist die Einführung von IPv6 anzustreben.

Spezifische Sicherheitsmaßnahmen sind Firewalls und Virtual Private Networks (VPNs). Sie sind nicht generell erforderlich. Ihr Einsatz hängt von den Erfordernissen des jeweiligen Teilbereichs des Netzes ab. Entsprechendes gilt auch für Chipkarten, biometrische Indentifizierung, Zertifizierung. Diese Techniken können zum Einen zur unerläßlichen Ausstattung der Netzinfrastruktur gehören, wenn etwa VoIP oder WLANs betrieben werden (VPNs) oder eine Schlüsselzertifizierung erforderlich ist. Dagegen müssen z.B. Firewalls sehr anwendungsbezogene Sicherheitspezifikationen erfüllen und bedürfen einer Betreuung, die eng mit dem Anwender kooperiert. Ein zentraler Netzbetreiber kann solche dezentralen Firewalls mangels Personal nicht effektiv betreiben. (Andererseits ist auch dezentral selten die erforderliche Personalkapazität vorhanden. Dies ist ein Problem, das generell mit der Dezentralisierung und Differenzierung der Informationstechnik verbunden ist).

Die Netzwerkinfrastuktur sollte eine Sicherheitsbasis bieten, auf der Anwendungen, anwendungsspezifische Sicherheitsmaßnahmen und zentral betriebene Netzdienste mit höheren Sicherheitsanforderungen aufsetzen können. Abb. 5 skizziert dieses Stufenmodell und gibt an, welche Sicherheitsanforderungen durch die jeweiligen Maßnahmen erfüllt werden. Zudem wird versucht sie bezüglich der Merkmalspaare Infrastruktur/Anwendung und zentral/dezentral zu ordnen.

Die Zuordnung zentral/dezentral ist nicht statisch. Was heute noch eine exotische Anwendung ist, kann morgen zur Grundausstattung des Netzes gehören.

Je höher eine Maßnahme im Stufenmodell steht, um so größer sind Sicherheitsanforderung und/oder Anwendungsnähe. Damit steigt auch der Verwaltungsaufwand, entweder beim Netzbetreiber oder beim Anwender.

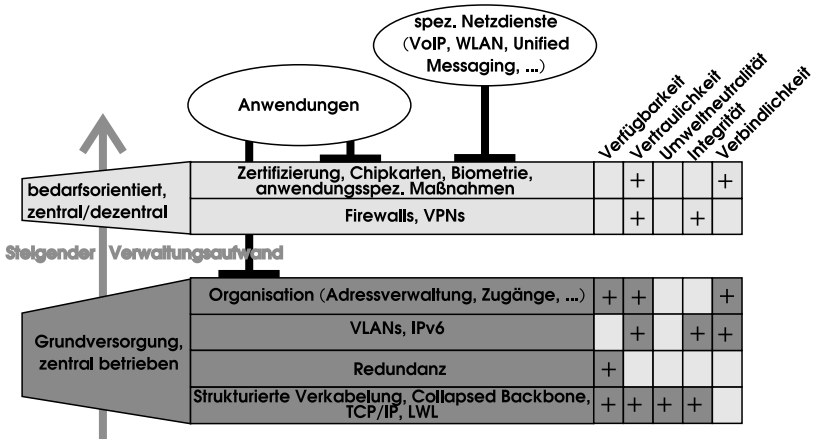

Abbildung 5: Stufenmodell Sicherheitsmaßnahmen

7 Ausblick

Die oben vorgestellten Sicherheitsmaßnahmen für die Netzinfrastruktur bieten etwa einen Sicherheitsgrad, wie man ihn von klassischen Telefonnetzen kennt. Das sollte eine ausreichende Basis sein für Multimedia-Anwendungen und für die Integration von Sprach- und Datennetzen. Es ist zu erwarten, daß wegen fortschreitender Digitalisierung und Ausbreitung der Übertragungsprotokolle Ethernet und TCP/IP auch die Netze der Gefahrenmeldeanlagen und der Gebäudeleittechnik in ein einheitliches Netz integriert werden. Entsprechende Ansätze sind schon vorhanden. So nutzen z.B. Gefahrenmeldeanlagen teilweise das Telefonnetz zur Alarmmeldung. Und die Signalübertragung der Leittechnik wird auf Ethernet und IP umgestellt. Bei der Integration dieser Netze sind noch höhere Sicherheitsmaßstäbe anzulegen. Voraussichtlich wird das aber durch weitere Redundanzmaßnahmen zu erfüllen sein, so daß das beschriebene Sicherheitskonzept für die Infrastruktur nur ergänzt und nicht verworfen werden muß.

Es wurde dargestellt, daß zur einer sicheren und ökonomischen Netzinfrastruktur auch organisatorische Maßnahmen gehören, wie zentrale Netzplanung, zentraler Betrieb und Regulierungsmaßnahmen, soweit sie für die Sicherheit erforderlich sind und die Dezentralisierung der Anwendungen nicht behindern. Voraussetzung dafür ist, daß in der Institutionsleitung oder in den zuständigen Entscheidungsgremien das Bewußtsein für die Notwendigkeit einer leistungsfähigen und sicheren Netzinfrastruktur und der damit verbundenen organisatorischen Maßnahmen vorhanden ist. Das ist in einer Zeit, wo die Deregulierung der Telekommunikation ein Paradigma ist, nicht selbstverständlich.

An vielen Universitäten wird derzeit Facilitymanagement für Verwaltung und Betrieb von Gebäuden eingeführt. Die Kommunikationsinfrastruktur, als Bestandteil der Gebäudeinfrastruktur, sollte dabei von vornherein mit berücksichtigt werden. Und es ist zu wünschen, daß die einheitliche und umfassende Sicht auf die Infrastruktur, wie sie in einem Facilitymanagement-System angelegt ist, sich nicht nur auf den kaufmännischen Blickwinkel beschränkt, sondern auch den technischen berücksichtigt.

Die Sicherheit der Kommunikationsinfrastruktur könnte mit einem Zertifikat nach ISO 9000 oder ISO 17799-1 bestätigt werden.

Danksagung: Am Aufbau der Glasfaserinfrastruktur der Universität Kassel sind beteiligt Fa. LAN Consult Hamburg und Dipl.-Ing. Horst Faupel und Dipl.-Ing. Ugur Koc von der Universität Kassel, die mit wichtigen Informationen zu diesem Bericht beigetragen haben.