ComConsult Research

Der Netzwerk Insider

Juli 2013

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Zonenarchitekturen: Notwendige Ordnungspolitik in Rechenzentrums- und Campus-Netzen

von Dr. Simon Hoff

Zonenarchitekturen dienen der sicherheitsorientierten Segmentierung von Netzen in Rechenzentrum (RZ) und Campus. Dabei kommen Techniken der logischen Netztrennung, der Kontrolle der Verkehrsflüsse an Netzübergängen sowie ggf. auch der Netzzugangskontrolle (Network Access Control, NAC) an Netzzugangspunkten zum Einsatz.

Solche Zonenarchitekturen verkomplizieren automatisch die Struktur der Netze und erhöhen den Betriebsaufwand erheblich. Ist ein solches Strukturierungsinstrument angesichts Virtualisierung und Cloud Computing überhaupt noch zeitgemäß? Interessanterweise ist die Antwort: Gerade dann! Sichere Virtualisierung erfordert beispielsweise eine sichere Trennung von produktivem und administrativem Netzverkehr, und Cloud Computing ist ohne mandantenfähige virtuelle Infrastrukturen nicht denkbar.

In diesem Artikel werden zunächst die grundlegenden Sicherheitsanforderungen diskutiert, die in der Praxis wesentlichen Architekturvarianten vorgestellt und typische Aspekte wie den Umgang mit Kurzschlüssen zwischen Sicherheitszonen betrachtet. Die Administration und Überwachung von Sicherheitszonen stellt dabei besondere Herausforderungen dar. Einführung und nachhaltige Umsetzung von einer Zonenarchitektur erfordern außerdem zwingend eine Anpassung und Erweiterung der IT-Prozesse.

weiter auf Seite 7

Zweitthema

Verkabelung am Arbeitsplatz: Alles wie gehabt?

von Dipl.-Ing. Hartmut Kell

Mit jeder in den letzten Jahren aufgetretenen technischen Innovation, insbesondere im Bereich der Arbeitsplatzverkabelung, erfolgte durch unterschiedlichste Interessengruppen eine Neudefinition der Nutzeranforderungen und sich daraus ableitender zwingender Orientierung hin zu besseren Kabel- und Steckerkomponenten. Selten entstand der Bedarf nach besseren Materialien beim Nutzer selbst, beispielsweise durch spürbare Einschränkungen der Nutzbarkeit von schlechten Verkabelungen. Prognostizierte man beispielsweise Anfang der 90er-Jahre einen kurzfristigen Bedarf nach „sehr hohen“ Datenraten am Arbeitsplatz (das waren „damals“ 100 Mbit/s), so entstand ein wirklicher Bedarf erst Mitte der 2000er, also 10-15 Jahre nach dem vorausgesagten Zeitraum der meisten Herstellerprognosen. Selbst heute, 20 Jahre später, kann festgestellt werden, dass in vielen Netzen erstaunlich viele Endgeräte noch mit 10 Mbit/s auskommen.

Die Tatsache, dass die meisten, auch älteren Tertiärverkabelungen eine Qualität besitzen, die eine Nutzbarkeit für die nächsten weiteren 5 bis 10 Jahre sicherstellen könnte liegt darin begründet, dass der Mehrpreis für eine Tertiärverkabelung mit einem höheren technischen Mehrwert in der Vergangenheit nur sehr gering war und somit die Entscheidung für bessere Verkabelungssysteme leicht zu treffen war.

weiter Seite 22

Geleit

SDN: Bedarf und offene Fragen

von Dr. Jürgen Suppan

ab Seite 2

Standpunkt

Jumbo Frames als „Nachbrenner“?

ab Seite 20

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2013

ab Seite 4

Neues Seminar

Seminar*plus* - IPv6 Grundlagen

ab Seite 21

Zum Geleit

SDN: Bedarf und offene Fragen

Das ComConsult-SDN-Forum gab einen guten Überblick über die aktuelle Situation, vor allem aber stellte es den gegebenen Bedarf den offenen Fragen gegenüber. Im folgenden soll ein kurzer Ausschnitt der vielen Diskussionspunkte gegeben werden, dies kann die Teilnahme an der Veranstaltung nicht ersetzen, aber wir werden das Thema zum RZ-Forum im November wieder aufgreifen.

Auch wenn SDN noch in den Kinderschuhen steckt, so gibt es durchaus einen greifbaren Bedarf. Darunter fallen u.a. folgende Anforderungen:

- Vereinfachter und preiswerterer Betrieb
- Selektive Umleitungen insbesondere in Sicherheits- und Analyse-Architekturen
- Dynamische Anpassungen an die vorhandene Bandbreite über starre QoS-Regeln hinaus
- Abstrahierung zur Trennung zwischen RZ-Architekturen und Netzwerken
- Steuerung von Netzwerk-Eigenschaften durch Anwendungen
- Zentrale Steuerung von Sicherheits- und Zonen-Architekturen

In den Diskussionen und auch Ankündigungen der Hersteller fallen dabei immer wieder die Bereiche Abstraktion und Sicherheits-Architekturen ins Auge.

Abstraktion ist eine wesentliche Voraussetzung für die weitere Automatisierung im Rechenzentrum insbesondere bei der Schaffung von automatischen Provisionierungen von Anwendungen und Diensten. Dabei geht es nicht nur um die Umsetzung neuer Service-Kataloge für die Anwender, sondern auch um mögliche Vereinfachungen und Optimierungen im 24/7-Operating. Automatisierung erfordert die Umsetzung einer ortsneutralen Kommunikation zwischen den verschiedenen Bestandteilen einer Applikation sowohl zum Zeitpunkt des Starts als auch während des Betriebs. Dies kann mit heutigen Netzwerk-Lösungen nicht geleistet werden. Die bisher zur Lösung dieses Problems geschaffenen Overlay oder Edge-Computing-Lösungen sind sicher geeignet das Problem zu lösen, schaffen aber in ihrer technischen Umsetzung neue Probleme gerade auch auf der Netzwerkseite.

Im Sicherheitsbereich geht es um eine verbesserte zentrale Kontrolle vieler verschiedener Sicherheits-Punkte zum Beispiel als Teil einer Zonenarchitektur, aber auch um die dynamische Reaktion auf kri-

tische Ereignisse. So fehlt in heutigen Lösungen die Möglichkeit eines dynamischen Re-Routings auf der Basis reiner Sicherheits-Erwägungen.

Ohne bei den genannten Bereichen in die Tiefe gehen zu wollen kann man klar feststellen, dass es einen messbaren und begründbaren Bedarf für SDN als Technologie gibt. Dies bedeutet allerdings nicht, dass alles bestehende durch SDN abgelöst werden wird. Aus heutiger Sicht schafft SDN ein weiteres, aber in seiner Ausprägung sehr wichtiges und effizientes Werkzeug, um den Netzwerk-Betrieb an immer komplexere Anforderungen anpassen zu können.

Betrachtet man die Produkt- und Technologie-Situation, dann muss SDN auch als mehrjährige Entwicklung gesehen werden, die in verschiedenen Phasen erfolgen wird. ComConsult Research hat auf dem SDN-Forum seine Prognose zur Marktentwicklung vorgestellt. (siehe Abbildung 1)

Die technische Bewertung des Bedarfs und der Fähigkeiten von SDN fällt überraschend positiv aus. Allerdings stehen dem durchaus kritische Fragen gegenüber, die in Summe das Potenzial haben, die gesamte Entwicklung auch zu blockieren. Beispiele für solche kritischen Fragen sind:

- Wie Hersteller-neutral und offen wird SDN?
- Wo kommen die Switches der Zukunft her, sind sie austauschbar?
- Sollen Applikationen wirklich Netzwerke steuern?
- Werden wir je SDN in Reinform erleben oder bleibt es bei hybriden Lösungen?
- Geht es auch ohne SDN?

Lassen Sie mich zu diesen Fragen einzeln Stellung beziehen:

Die zentrale Frage zur Zukunft der Netzwerke ist sicher die Hersteller-Neutralität. Die Fähigkeit, das jeweils beste Produkt zum Einsatz zu bringen und auch Produkte verschiedener Hersteller mischen zu können, ist für viele Umgebungen unverzichtbar und essentiell. In gewissen Grenzen ist das heute erfolgreich möglich. So wie die SDN-Entwicklung im Moment aber verläuft, muss durchaus die Frage gestellt werden, ob wir durch SDN nicht eine stärkere Hersteller-Bindung bekommen als bisher. Der Know-How-Bedarf und der Umfang der notwendigen Entwicklung

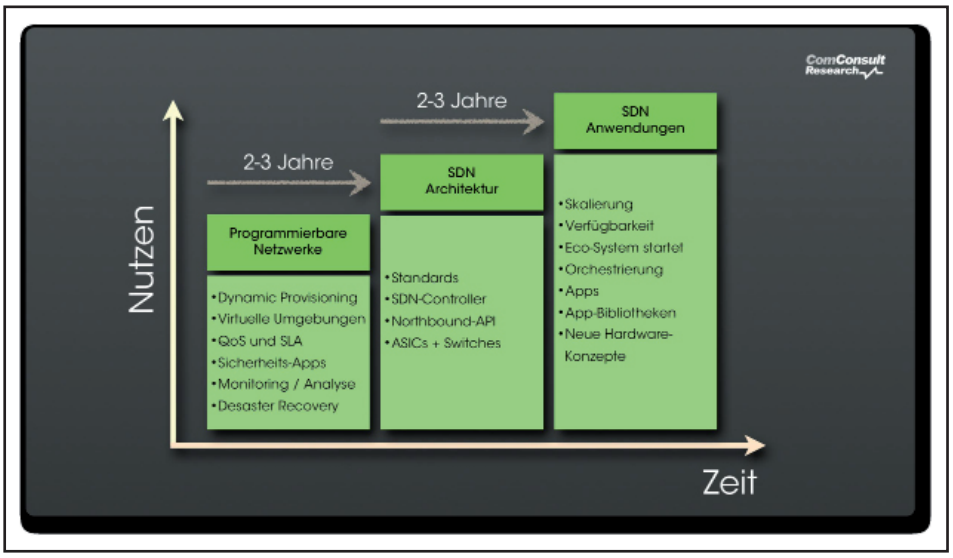

Abbildung 1: Prognose ComConsult Research

Schwerpunktthema

Zonenarchitekturen: Notwendige Ordnungspolitik in Rechenzentrums- und Campus-Netzen

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Fortsetzung von Seite 1

1. Zonenarchitekturen als natürlicher Bestandteil der Enterprise Architecture

Manchmal muss es vielleicht erst zu Sicherheitsvorfällen kommen!

Erinnern wir uns kurz an typische, immer wieder auftretende Sicherheitsvorfälle:

- Kundendaten im internen Netz eines Providers waren bis zur Beseitigung einer Sicherheitslücke in einer Web-Applikation ungeschützt vom Internet aus abgreifbar.
- Durch den Anschluss eines Fremd-PCs eines Besuchers schaffte es ein Virus doch in das interne Netz und befiel PCs, die nicht mit einem (aktuellen) Virenschutz versehen werden konnten, da die PCs integriertes Element eines Geräts (z.B. in der Gebäudetechnik) waren, auf das die IT keinen direkten administrativen Zugriff hatte. Als Konsequenz fiel beispielsweise die Zutrittskontrolle zum und im Gebäude aus und Türen blieben verschlossen.
- Ein Angreifer konnte durch einen Trojaner auf einem Mitarbeiter-PC (oder einfach als Innentäter) einen Zugriff auf kritische Daten einer Institution erlangen und diese Daten über den Internet-Zugang der Institution nach draußen schmuggeln.

Diese Liste lässt sich wahrscheinlich beliebig fortsetzen. Solchen Vorfällen ist jedoch oft gemeinsam, dass von einem System oder einem Netz eingeschränkter Vertrauenswürdigkeit auf ein schützenswertes System bzw. Netz zugriffen wird. In vielen Fällen ist dann der Grund des Sicherheitsvorfalls in der unzureichenden Trennung von Systemen eingeschränkter Vertrauenswürdigkeit von den anderen IT-Systemen zu finden. Nicht selten ist dann eine Feststellung z.B. bei einem Sicherheits-Audit, dass das Netz aus dem Blickwinkel der Informationssicherheit nicht geeignet strukturiert ist.

Übertragung von Konzepten der Perimeter-Sicherheit auf das Intranet

Wir haben uns natürlich daran gewöhnt, dass wir unsere IT-Infrastruktur gegenüber externen, nicht oder eingeschränkt vertrauenswürdigen Netzen abschotten müssen. Wir haben dabei akzeptiert, dass eine Perimeter-Sicherheit komplexe Sicherheitskonstrukte erfordert, die aus ggf. mehrstufigen Firewall-Systemen und Demilitarized Zones (DMZs) an und zwischen den Firewall-Stufen zur Aufnahme von Gateways, Proxies, etc. besteht.

Die Vielfalt der unterschiedlichen Nutzergruppen und der Dienste und Anwendungen im Intranet und der damit verbundenen höchst heterogenen Sicherheitsanforderungen im Intranet erfordert nun, dass wir verstärkt Konzepte der Perimeter-Sicherheit auch zur Strukturierung des Intranet heranziehen müssen.

Notwendigkeit virtueller Tresore

Die Absicherung kritischer Daten vor unberechtigtem Zugriff (und damit verbunden vor Abfluss und Verlust) ist stets eines der wesentlichen Ziele der Informationssicherheit.

Für virtuelle Wertsachen, d.h. Daten mit hohem Schutzbedarf insbesondere hinsichtlich Vertraulichkeit und Integrität gilt das gleiche wie für physische Wertsachen: Sie kommen in einen Tresor, d.h. in

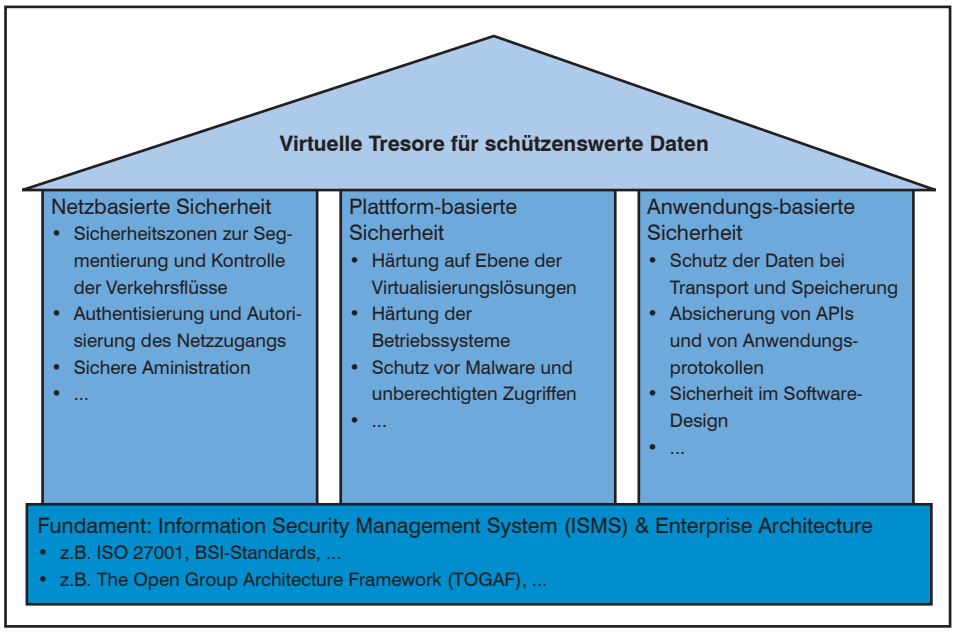

Abbildung 1: Fundament und tragende Säulen für den Aufbau von virtuellen Tresoren für schützenswerte Daten

einen Sicherheitsbereich. Ein solcher virtueller Tresor wird primär auf einer Kombination von drei Säulen der Informationssicherheit aufgebaut (siehe Abbildung 1):

- Netzbasierte Sicherheit
- Plattformbasierte Sicherheit
- Anwendungsbasierte Sicherheit

Dieser Artikel konzentriert sich auf die erste Säule der netzbasierten Sicherheit. Kernelemente sind dabei:

- Segmentierung eines Netzes in unterschiedliche Sicherheitszonen
- Kontrolle der Verkehrsflüsse zwischen Sicherheitszonen.
- Authentisierung und Autorisierung für einen entsprechenden Zugang zu einer Sicherheitszone
- Sichere Administration

Verankerung von Zonenarchitekturen in Standards zur Informationssicherheit

Die Forderung einer Zonierung ist auch in diversen Maßnahmenkatalogen zur Informationssicherheit entsprechend verankert. Schlägt man z.B. ISO 27001 (siehe [1]) im normativen Anhang A.11.4 „Zugangskontrolle für Netze“ auf, wird man über die Maßnahme A.11.4.5 „Trennung in Netzwerken“ stolpern: „Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzen getrennt gehalten werden.“

Diese kurze Formulierung hat es in sich, denn es wird klar und deutlich gemacht, dass auf Ebene des Netzes etwas geschehen muss. Diese Anforderung wird im Standard ISO 27002 (der als Best Practice für die Umsetzung von ISO 27001 zu verstehen ist) dann auch entsprechend konkretisiert. Die Umsetzung kann entweder mit den Mitteln einer Netztrennung und dem Einsatz einer Firewall am Netzübergang (jedoch grundsätzlich auch mit Access Control Lists, ACLs) oder durch kryptographische Techniken (z.B. VPN) erfolgen.

Maßnahme A.11.6.2 „Isolation sensibler Systeme“ von ISO 27001 fordert sogar verschärfend „Sensible Systeme müssen sich in einer dedizierten (isolierten) Umgebung befinden.“

Insgesamt kann also festgestellt werden, dass Zonenarchitekturen keinesfalls eine exotische Anforderung darstellen, sondern ein Standardelement moderner Unternehmensarchitekturen der IT sind.

2. Notwendige Bausteine einer Zonenarchitektur

Eine Zonenarchitektur muss zwingend einen modularen Bausteincharakter haben, denn es muss möglich sein, bei Bedarf flexibel im RZ neue Sicherheitszonen hinzufügen oder Server zu bestehenden Sicherheitszonen zuzuordnen. Aus dem Blickwinkel IT-Service muss es sogar möglich sein, für eine neue Sicherheitszone einen Bestellvorgang einzuleiten, der dann eine entsprechende Prozesskette in Bewegung setzt.

Terminologie: Ohne gemeinsame Sprache geht es nicht

Wie jede Architektur ist eine klare und konsequente Begriffsbildung für eine Zonenarchitektur entscheidend. Wie definiert sich der Begriff Sicherheitszone? Gibt es eine hierarchische Struktur oder eine logische Gruppierung von Sicherheitszonen an einem Standort einer Institution? Welche generellen Festlegungen zur Kommunikation zwischen Sicherheitszonen oder auf höheren Ebenen gibt es?

Folgende Festlegungen zu den grundlegenden Bausteinen einer Zonenarchitektur haben sich in der Praxis bewährt (was natürlich eine entsprechende andere, institutionsspezifische Anpassung keinesfalls ausschließt):

- Eine **netzbasierte Sicherheitszone** (im Folgenden kurz Sicherheitszone) ist ein IP-Netzwerk, das aus Sicherheitsgründen von anderen Netzen getrennt wird.

- Die Kommunikation in eine Sicherheitszone hinein oder aus einer Sicherheitszone heraus, wird durch Sicherheitsmaßnahmen kontrolliert. Hierzu werden die Sicherheitszonen durch **Sicherheitselemente** vernetzt.

- Sicherheitselemente werden je nach Anforderung ausgewählt. Beispiele sind Firewall oder Intrusion Prevention System (IPS).

- Innerhalb einer Sicherheitszone wird auf Ebene des Netzes die Kommunikation nicht eingeschränkt.

- Ein Sicherheitselement kann an mehrere Sicherheitszonen angebunden werden und eine Sicherheitszone kann ebenso mit mehreren Sicherheitselementen verbunden werden.

Auf diese Weise stellt sich das Intranet letztendlich als Netzwerk von Sicherheitszonen dar.

Festlegungen zur logischen und physischen Trennung

Wenn Sicherheitszonen durch IP-Netze gebildet werden, muss geregelt werden, unter welchen Rahmenbedingungen eine physische Trennung notwendig ist und wann eine logische Trennung auf Ebene von Netz, Servern und Clients erlaubt ist.

In Rechenzentren ist es beispielsweise heute inzwischen sogar üblich – sofern im Einzelfall keine spezifischen Sicherheitsanforderungen dem widersprechen – lediglich DMZ-Bereiche physisch zu trennen und ansonsten eine logische Trennung auf Ebene der Server und Netze zu gestatten. Dies erfordert natürlich eine entsprechende Absicherung von Netz und Virtualisierungsplattform. Ähnlich geht man auch in Campus-Bereichen vor.

Für eine logische Trennung in Netzen kommen beispielsweise auf Layer 2 Virtual LAN (VLAN) in Frage und oberhalb von Layer 2 sind Multiprotocol Label Switching (MPLS) sowie Virtual Routing and Forwarding (VRF) zu nennen. Auf Ebene der Endgeräte sind Server-Virtualisierung und Virtual Desktop Infrastructure (VDI) relevante Techniken.

Netztechnischer Aufbau einer Sicherheitszone

Im einfachsten Fall besteht eine Sicherheitszone aus einem einzelnen VLAN. Eine Firewall, die als Sicherheitselement an die Sicherheitszone angeschlossen ist, würde dann als Default Gateway für die Endgeräte in der Sicherheitszone dienen. Wenn eine Sicherheitszone aus mehreren VLANs, d.h. IP-Subnetzen, besteht, kann mit VRF gearbeitet werden (siehe Abbildung 2).

Bei standortübergreifenden Sicherheitszonen können die Sicherheitszonen im WAN mit MPLS-VPNs oder bei Carrier Ethernet letztendlich wieder per VLANs getrennt werden.

Die Anschaltung von Sicherheitselementen zur Kontrolle der Kommunikation zwischen den Sicherheitszonen erfolgt dann redundant an zentraler Stelle z.B. an Core Switches im Data Center.

Bei Firewalls ist dabei festzulegen, ob mit statischem Routing oder einem dynamischen Routing-Protokoll wie OSPF gearbeitet wird. In letzterem Fall würde OSPF dann auch das Redundanzverfahren bilden. Während OSPF bei Firewalls am Perimeter eher unüblich ist, kann OSPF für eine interne Firewall in jedem Fall in Betracht gezogen werden, sofern im LAN mit OSPF gearbeitet wird, um eine Einheitlichkeit, eine einfachere Konfiguration und eine Active-Active-Konfiguration der Firewalls zu erreichen. Andernfalls kann – wie im Perimeter-Bereich üblich – mit den Mitteln einer First-Hop-Redundanz per VRRP (oder einem vergleichbaren Verfahren) eine Active-Passive-Firewall-Redundanz geschaffen werden.

Zweitthema

Verkabelung am Arbeitsplatz: Alles wie gehabt?

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Anforderungsanalyse

Bei jeder Einführung von neuen, gegebenenfalls besseren und insbesondere teureren Techniken sollte sich die Bewertung von sinnvollen und nicht sinnvollen Materialien immer am Nutzen innerhalb des erwarteten Nutzungszeitraumes orientieren. Die erwartete Nutzung muss die technische Anforderungen an die Übertragungsqualiät und den weiteren Materialqualitäten definieren, nicht die reine technische Machbarkeit oder das Marktangebot. Unter diesem Gesichtspunkt erfolgt zunächst eine kurze Anforderungsanalyse, betrachtet werden allgemeine und spezielle Anforderungen an eine Tertiärverkabelung.

Universalität

Das Ziel einer Tertiärverkabelung muss sein, dass sich Kommunikationsendgeräte am Arbeitsplatz beliebig an vorhandene passive Kommunikationsanschlüsse anschließen lassen, ohne dass ein komplexer „handwerklicher“ Montagevorgang notwendig wäre. Es muss selbstverständlich ein Telefon gegen einen Drucker ausgetauscht werden können, ohne einen Elektriker oder IT-Techniker dazu heranziehen zu müssen. Daraus entsteht die Konsequenz, dass alle passiven Kommunikationsanschlüsse (die DIN/EN bezeichnet diese als Teilnehmeranschlüsse TA) eine identische Anschlusstechnik besitzen und jede am Arbeitsplatz denkbare Übertragungstechnik nutzbar macht.

Aus dieser einfachen und trivialen Forderung entsteht bereits eine erste Technologieentscheidung, nämlich eine seit vielen Jahren praktizierte Abkehr von verschiedenen Medien im Tertiärbereich. Wie sinnvoll bzw. betriebsfreundlich wäre es, sowohl Glasfaser- als auch Kupferports am Arbeitsplatz bereitzustellen und diese verschiedenen Techniken bei Änderungen der Endgerättypen bzw. deren Anschlüsse einzusetzen.

Die hohe Durchdringung der Ethernet-Techniken für (fast) jedwede IT-Kommunikation am Arbeitsplatz macht die Planung deutlich einfacher. Denn mit einer weiterhin erwarteten Dominanz des Ethernets gibt es nur noch zwei wichtige technische Aspekte, die im Rahmen der Nutzeranforderungen betrachtet werden müssen,

- die Datenrate
- die Nutzung von Power over Ethernet.

Nutzungszeitraum

Wie bereits angesprochen sollten die geforderten technischen Anforderungen bzw. Qualitäten sich unbedingt am Nutzungszeitraum einer Verkabelung orientieren. Sowohl die DIN/EN 50173 als auch ein allgemeines „Planer-Ethos“ sehen die Nutzbarkeit einer Tertiärverkabelung von 10 bis 15 Jahren, besser sogar 20 Jahren vor, in der es zu möglichst wenig Nachverkabelungen und Installationsänderungen kommen darf. In der Vergangenheit zeigte sich, dass der Bedarf an Nachverkabelung eher durch eine nicht ausreichende Anzahl von geplanten Tertiäranschlüssen als durch mangelhafte Qualität der Verkabelung entstanden ist.

Dies gilt selbst bei einer Betrachtung von sehr alten Verkabelungssystemen wie z.B. die IBM-Typ-1-Verkabelung, ein Produkt der 80er-Jahre, welches heute noch in Einzelumgebungen im Einsatz ist. Eine weitere Nutzbarkeit wäre bedingt durch die hohe Qualität weiterhin denkbar gewesen, wenn diese durch systembedingte 4-Adrigkeit nur 100 Mbit/s übertragen könnte.

Andererseits muss man aber auch ein Gegenbeispiel aufzeigen, bei dem für bestimmte Übertragungsqualitäten und damit prognostizierter Nutzbarkeitszeitraum sich dieser nicht erfüllte: Die Ende der 90er bzw. Anfang 2000er eingeführte Übertragungsqualität der Klasse E (Achtung: nicht Klasse E_A) brachte überhaupt keinen nutzbaren Vorteil im Vergleich zur Klasse D. Bei Installationen mit dieser 250MHz-Tertiärverkabelung, insbesondere im Rechenzentrumsumfeld, muss möglicherweise im Nutzbarkeitszeitraum mit Einschränkungen gerechnet werden.

Installations- und Betriebsfreundlichkeit

Selbst wenn in einem langen Nutzbarkeitszeitraum alle benötigten Übertragungstechniken im Tertiärbereich verwendet werden, können die verschiedenen Verkabelungen unterschiedliche Vor- und Nachteile bei der Installation und auch beim späteren Betrieb haben. Die Installationsfreundlichkeit spielt aus der Sichtweise des Nutzers zunächst eine untergeordnete Rolle (dazu später mehr), sie ist relevant für den Planer der Erstinstallation, dort verursacht sie höhere Investitionskosten.

In Zusammenhang mit der Betriebsfreundlichkeit einer Kommunikationsverkabelung sind Anforderungen zu nennen, die zum einen in Zusammenhang mit der Fehleranfälligkeit und der Fehlerbehebbarkeit zu sehen sind. Beispielsweise ist eine Anschlussschnur (bestehend aus Anschlusskabel und Stecker) zwar nicht Gegenstand der festen Verkabelung, hat aber erfahrungsgemäß einen großen Einfluss auf die Übertragungsqualität der zu nutzenden Strecke und damit deren Verfügbarkeit. Auf der anderen Seite kommt neben der Betrachtung dieser Fehleranfälligkeit auch eine Bewertung der Änderungsflexibilität bei Umzügen oder Nutzungsänderungen hinzu. Wie einfach lassen sich z.B. in Gebäuden mit vermieteten Büroflächen Mieterwechsel durchführen, ohne dass mehr-

Verkabelung am Arbeitsplatz: Alles wie gehabt?

fach eine vollständige Neuverkabelung notwendig wird, weil der Nachfolgemieter andere Anforderungen an die Tertiärverkabelung, z.B. durch veränderte Möblierung, stellt.

Kostenminimierung

Bei allen technischen Anforderungen bleibt natürlich am Ende auch die Bewertung der Kosten, die zur Einrichtung der Infrastruktur aufzuwenden sind. Die Notwendigkeit ein bestimmtes Maximalbudget einzuhalten wird in vielen Fällen die entscheidende Anforderung sein und eine Analyse der zu erwartenden Kosten bzw. der damit verbundenen Optimierungspotenziale muss viele Aspekte berücksichtigen. Installationskosten lassen sich relativ einfach und genau mit Hilfe von Kostenschätzungen ermitteln, dagegen ist die Schätzung von Betriebskosten mit sehr vielen spekulativen Annahmen verbunden.

Nutzbare Datenrate

Den meisten Lesern wird bekannt sein, dass für die Ethernet-Technologien derzeit IEEE-Standards bis zu einer maximalen Datenrate von 100 Gbit/s bestehen. Die Übertragungstechniken für 40 Gbit/s und 100 Gbit/s lassen sich (noch) nicht mit Twisted Pair realisieren. Da davon auszugehen ist, dass die deutlich größere Menge an Tertiärinstallationen mit dem Medium Twisted Pair realisiert worden ist, kann die Nutzbarkeit dieser beiden Datenraten für den Tertiärbereich ausgeschlossen werden. Aktuell läuft eine sehr intensive Diskussion, ob 40 Gbit/s möglicherweise doch über Twisted Pair möglich sein könnte, die Nutznießer einer derartigen Innovation dürften wohl eher im Rechenzentrumsbereich gesehen werden. Damit stehen für den Tertiärbereich Datenraten bis zu 10 Gbit/s mit einer brauchbaren Reichweite von ca. 100 m zur Verfügung. (siehe Abbildung 1)

Umfragen des Autors im Rahmen seiner Seminartätigkeit und auch im Rahmen seiner Projektierungen ergeben, dass nur in ca. 50% der Netzwerkumgebungen eine Datenrate von mindestens 100 Mbit/s flächendeckend, also an jedem Arbeitsplatz, wirklich benötigt wird (es steht natürlich fast überall 100 Mbit/s zur Verfügung). Damit lässt sich die Aussage treffen, dass eine Datenrate von 1 Gbit/s für die nächsten 10 bis 15 Jahre als „mehr als ausreichend“ zu sehen ist. Was ist dazu notwendig?

Die im Zusammenhang mit 1 Gbit/s zu berücksichtigende IEEE-Spezifikation 802.3ab stellt keine wirklich „Herausforderung“ an die Verkabelungskomponenten dar, es reicht eine Verkabelung in der Güte Klasse D mit Kategorie-5-Komponenten nach aktueller EN 50173; Klasse E oder mehr ist nicht notwendig. Erfahrungsgemäß ist davon auszugehen, dass nahezu alle 8-adrigen Twisted-Pair-Verkabelungen in Deutschland Gigabit-tauglich sind.

IEEE-Standard	Bezeichnung	Jahr	Datenrate	Kabel
802.3j	10Base-T	1990	10 MBit/s	TP-Kabel (RJ-45)
802.3j	10Base-FL	1992	10 MBit/s	Glasfaserkabel
802.3u	100Base-TX	1995	100 MBit/s	TP-Kabel (RJ-45)
802.3u	100Base-FX	1995	100 MBit/s	Glasfaserkabel
802.3z	1000Base-SX 1000Base-LX	1998	1 GBit/s	Glasfaserkabel
802.3ab	1000Base-T	1999	1 GBit/s	TP-Kabel (RJ-45)
802.3an	10GBase-T	2006	10 GBit/s	TP-Kabel (RJ-45)

Abbildung 1: Übersicht der im Tertiärbereich relevanten Ethernet-Techniken

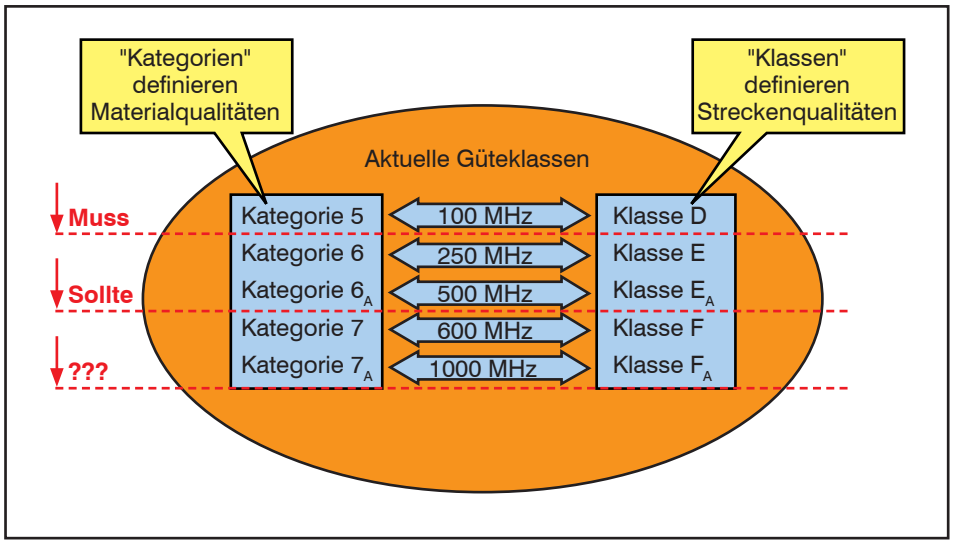

Abbildung 2: Güteklassen bei Kupfer

Gerade im Umfeld von Planungen im deutschen Umfeld reicht den meisten Planern aber eine ausschließliche Einforderung der Klasse D nicht aus, hier herrscht (im Unterschied zum Ausland) ein sehr ausgeprägtes „Reservebewusstsein“ mit dem Ziel, kein Risiko bezüglich des Nutzbarkeitszeitraumes einzugehen und damit jede denkbare Datenrate im Tertiärbereich sicherstellen zu müssen. Wie oben bereits ausgeführt würde das zu einer Verkabelung mit einer nutzbaren Datenrate von 10 Gbit/s am Arbeitsplatz führen. Daraus leitet sich eine Forderung nach Nutzbarkeit der 10GBase-T-Technik gemäß IEEE 802.3an ab und dies wiederum führt zu einer Forderung nach Klasse E_A (oder besser) im Tertiärbereich, Klasse E bringt hier gar nichts. Es ist einem Umstand zu verdanken, dass in allen aktuellen Planungen von Gebäudeverkabelungen diese Klasse E_A vorgesehen wird: Der Kostenunterschied zwischen einer Klasse D/E-Verkabelung und einer Klasse E_A-Verkabelung ist so gering, dass sich ein Verzicht auf die niedrigere Qualität nicht lohnt. Teilweise ist es schwieriger auf dem Markt Kategorie 5-Systeme oder Kabel zu bekommen als Kategorie 6_A-Komponenten. (siehe Abbildung 2)

Bleibt die Frage, ob eine weitere Verbesserung der Streckenqualität durch Schaffung von noch größeren Systemreserven zu einer besseren Funktionalität der Strecke und damit zu einem längeren Nutzbarkeitszeitraum führt. Eine höhere Datenrate als 10 Gbit/s ist zum aktuellen Zeitpunkt nicht möglich, falls dies überhaupt jemals am Arbeitsplatz von Nutzen sein würde, aber wie sieht es mit völlig anderen Techniken aus?

Lange Zeit wurde als Vorteil der nächst höheren Leistungsklasse F und F_A das Cable-Sharing angepriesen, denn mit Anschlusstechniken der Kategorie 7 bzw. 7_A lässt sich dies besonders „verlustarm“ nutzen. Da angesichts der 8-adri-