Dr. Suppan International Institute

Der Netzwerk Insider

Juni 2003

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Auf dem Weg zum virtuellen Arbeitsplatz

von Dr. Behrooz Moayeri

Je intensiver man über den teilweise vollzogenen und teilweise noch bevorstehenden strukturellen Wandel in den hochentwickelten Länder nachdenkt, umso deutlicher wird es, dass wir als Ergebnis dieses Wandels eine Gesellschaft vorfinden werden, indem die Mehrheit der Erwerbstätigen sich bei der Arbeit hauptsächlich damit befasst, Informationen zu gewinnen und daraus neue Informationen zu produzieren.

Die Warenproduktion wird zunehmend den Maschinen überlassen, die jedoch die von den Menschen produzierten Informationen benötigen, um zu funktionieren.

Matrix - Loaded?

Diese Art Erwerbsarbeit ist nicht mehr an einen Ort gebunden. Jede Information kann von jeder beliebigen Lokation aus abgerufen werden. Auch die Steuerung der Verarbeitung der Information und der Produktion der neuen Information erfordert nicht die physikalische Präsenz des Schaffenden an einer bestimmten Stelle.

In diesem Artikel wollen wir uns schwerpunktmäßig mit der technischen Problematik befassen und der Suche nach einer Antwort auf die Frage nachgehen, ob und inwieweit auf dem Weg zum virtuellen Arbeitsplatz zumindest die technischen Voraussetzungen geschaffen sind.

weiter Seite 12

Zweitthema

Wireless Overlay Networking: der neueste Trend

von Dr. Jürgen Suppan

Ein neuer Netzwerk-Typ ist im Entstehen. Er besteht aus der Ergänzung eines Kabel-basierten LANs durch eine separate Wireless-Infrastruktur.

Die damit verbundenen Vorteile sind erheblich. Wichtige Schwachstellen traditioneller Lokaler Netzwerke können beseitigt werden.

Und: Betriebs- und Investitionskosten können gesenkt werden ohne dass es zu Leistungseinbußen kommt.

Wir bezeichnen diesen neuen Netzwerk-Typ als Wireless-Overlay-Netzwerk.

Wireless-Overlay-Netzwerke werden im Detail mit allen technischen und wirtschaftlichen Vorteilen auf der Sommerschule der ComConsult Akademie im Juli zusammen mit dem neuen Antennen-Guide vorgestellt.

An dieser Stelle soll ein Überblick über die grundsätzlichen Merkmale von Wireless-Overlay-Netzwerken gegeben werden.

Unter Wireless Overlay Networking wird die bewusste Kombination eines kabelbasierten Netzwerks mit einem Funknetz verstanden. Damit ist nicht eine partielle Ergänzung gemeint wie sie heute mit WLANs vielfach üblich ist (zur Zeit ist es üblich, Access Points an Etagen Switches anzuschließen) sondern der bewusste Aufbau einer neuen und vor allem separaten Infrastruktur mit klaren Architektur- und Design-Merkmalen.

weiter Seite 4

Seminar des Monats

Anwender berichten: Erfahrungen mit dem Cisco Call Manager

auf Seite 9

Zum Geleit

VOIP-Kooperation Siemens/ Microsoft: was ist das Ziel?

auf Seite 2

Studie des Monats

Design-Varianten lokaler Netzwerke im Vergleich

auf Seite 10

Zum Geleit

VoIP-Kooperation Siemens/Microsoft: was ist das Ziel?

Die bereits auf der Winterschule der ComConsult Akademie angekündigte Zusammenarbeit zwischen Microsoft und Siemens im Bereich IP-Telephonie und IP-Messaging wird nun konkret. Das Produkt soll unter dem Namen OpenScape im 3. Quartal auf den Markt kommen. OpenScape geht neue Wege in der Kommunikation und schafft neue Funktionalitäten und neue Ansätze der Kommunikation.

Wir arbeiten zur Zeit an einer Analyse und Bewertung dieser Entwicklung und werden die Ergebnisse im Rahmen der Sommerschule im Juli präsentieren. Die folgenden Überlegungen stammen aus den Analyse-Arbeiten.

OpenScape generiert viele Fragen: wenn die Grundannahmen der OpenScape-Entwicklung richtig sind, welchen Stellenwert hat dann noch eine HiPath 5000? Und wie lässt sich der im OpenScape enthaltene Trend der Anwesenheits-basierten Telephonie mit der traditionellen Telephonie-Sicht verbinden? War schon vorher nicht wirklich klar, auf welche Produktlinie der HiPath-Familie den strategischen Schwerpunkt legt, so wird dies nun noch diffuser.

Die OpenScape-Entwicklung trifft aber auch alle anderen Hersteller, vor allem Alcatel und CISCO. Microsoft hat in der Vergangenheit bewiesen, dass das Unternehmen über das Potenzial verfügt, Märkte völlig umzukrempeln. Mit OpenScape kommen nun zwei Faktoren zusammen: die Macht von Microsoft und ein neuer funktionaler Ansatz für Telephonie. Dies beinhaltet für Hersteller wie Alcatel, CISCO und Nortel eine große Gefahr. Wenn der funktionale Ansatz trifft und im Markt akzeptiert wird, dann wird dies gerade in der Kombination mit der Macht von Microsoft den Markt verändern. Interessanterweise sieht CISCO schon seit längerer Zeit in Microsoft einen der größten Konkurrenten im Bereich IP-Telephonie. Aber auch Siemens ist davon betroffen. Open Scape und HiPath haben keine gemeinsame Ausrichtung. Eigentlich ist nicht zu verstehen, warum Siemens nicht, wenn man wirklich an OpenScape glaubt, einen integrierten Ansatz schafft. Die Strategie scheint im Moment zu lauten: mal ausprobieren und wenn es Erfolg hat, dann denken wir über unsere Strategie nach.

Was steckt hinter dem Begriff OpenScape? Technisch basiert das Produkt OpenScape

auf dem Microsoft Real Time Communication Server 2003 (auch Greenwich-Server genannt). Dieser seit Mitte 2002 immer wieder von Microsoft in der Freigabe verschobene Server realisiert ein Instant Messaging Konzept auf Basis SIP und liefert damit das Fundament für viele andere Anwendungen, die auf einem SIP-Server dieser Art aufsetzen können. OpenScape ist eines dieser Produkte. Es ist nicht exklusiv, d.h. der Microsoft Real Time Communication Server RTC 2003 kann auch von anderen Herstellern genutzt werden. Entsprechende Produkte dürften im Jahr 2004 vermehrt auf den Markt kommen.

Siemens nutzt die funktionale Basis des RTC Servers zur Realisierung von OpenScape. Das Produkt hat mehrere funktionale Elemente:

- OpenScape realisiert Kommunikation auf Basis SIP, Teilnehmer können vom PC aus kommunizieren, aber auch von einem SIP-Telefon
- es zeigt, ob ausgewählte Kommunikations-Partner anwesend und erreichbar sind
- es gibt einer Person die Möglichkeit, Regeln für seine Erreichbarkeit zu definieren (managed availability) und dabei auch einen Medienmix zu verwenden (SIP-Phone, Handy, Mail, SMS). Im Rahmen der Erreichbarkeitsanzeige sieht der Kommunikationspartner, mit welchem Medium er zur Zeit arbeiten kann bzw. warum der Partner nicht erreichtbar ist (zum Beispiel: im Meeting). Die Regeln können Personen-bezogen sein, man kann also die Erreichbarkeit individuell gestalten
- Konferenzen werden in einer besonderen Form unterstützt. So beinhaltet OpenScape eine automatische Planungs-Funktion für eine Terminplanung, allgemein ist eine Gruppenfunktion vorhanden (My Collaboration Groups)
- OpenScape integriert ein Dokumenten-Sharing, so dass alle Teilnehmer während einer Kommunikation auf ein Dokument zugreifen und damit arbeiten können
- Die Integration mit der „normalen“ Telephonie erfolgt mit einem SIP-Gateway (noch nicht klar, voraussichtlich eine HiPath 3000)

Vorerst ist OpenScape auf 500 Teilnehmer begrenzt. Allerdings ist dies eine künstliche Grenze. Der betriebene Architektur-Aufwand in Kombination mit der sehr hohen Skalierbarkeit von Windows Server 2003 lässt im Moment keine wirkliche Grenze erkennen. Allerdings ist Exchange Voraussetzung für die Nutzung, IBM/Notes-Anwender werden damit ausgegrenzt.

Eine abschließende Bewertung ist erst möglich, wenn stabile Beta-Versionen auf dem Markt sind und auch eine verbindliche Roadmap vorliegt (es sind mehrere Versionen geplant, V1 wird nicht alle Funktionen beinhalten). Aber schon jetzt bleiben primär auf der Siemens-Seite viele Fragen offen: welche Strategie steckt dahinter, welche Plattform sieht Siemens für 3 bis 5 Jahre als strategisch an? Was ist mit Funktionen wie HiPath ProCenter (ACD) oder HiPath Xpression (Unified Messaging)? Wie sieht eine integrierte Architektur aus?

Auch eine spannende Frage: was bedeutet der zunehmende Schwenk des gesamtes Marktes auf SIP für die traditionellen TK-Produkte? Bei Siemens wird SIP zur Zeit in allen Plattformen umgesetzt (HiPath 4000 nach Freigabe Version 2 in 2004). Langfristig ist eine Ablösung der bisherigen Signalisierung durchaus denkbar. Gleichzeitig arbeitet man einer Ausweitung der Betriebssystem-Basis der 4000 in Richtung Linux. Wie laufen diese Trends zusammen? Was bedeutet das für Alcatel, Avaya, Cisco, Nortel u.a. ?

Mehr dazu auf unserer Sommerschule im Juli.

Ihr Dr. Jürgen Suppan

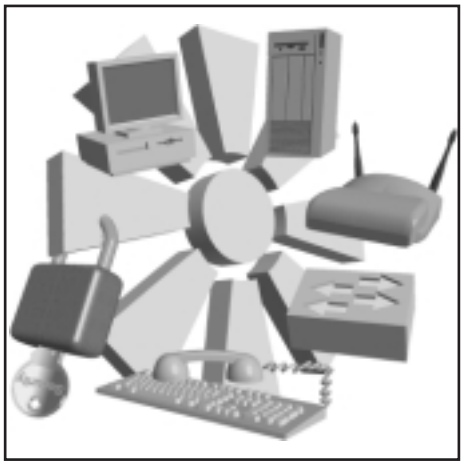
Sommerschule der ComConsult Akademie

Sommerschule 2003: Redesign und technisch/ wirtschaftliche Optimierung von Netzwerken

Vom 14. bis 18. Juli befasst sich die diesjährige Sommerschule der ComConsult Akademie intensiv mit dem Thema „Redesign und technisch/wirtschaftliche Optimierung von Netzwerken“. Diese Top-Veranstaltung bietet die umfassende Analyse und Diskussion der aktuellsten und wichtigsten Technologie- und Marktentwicklungen.

Zu den schon veröffentlichten Schwerpunkten der Sommerschule sind in den letzten Tagen noch folgende hinzugekommen:

- Client/Server/Speicher-Konsolidierung und die Konsequenzen für Netzwerke, wo besteht Änderungsbedarf
- Analyse IP-Telephonie: wo steht Siemens mit der HiPath-Entwicklung? Wie sind die Widersprüche in der Siemens-Strategie zu bewerten, welche der angebotenen Produktlinien ist strategisch? Wie ist das Microsoft/Siemens Kooperationsprodukt OpenScape zu bewerten? Stellt Siemens damit Teile der bisherigen Produktlinien mittelfristig in Frage?
- Was bedeutet die Weiterentwicklung der Wireless-Technologie in Richtung 320 Mbit/s?
- Wireless Overlay Networking: was ist das, was steckt dahinter, wie groß sind die Kosten- und Betriebsvorteile?



Zur Erinnerung noch einmal die sonstigen Highlights der Sommerschule

- Client/Server/Speicher-Konsolidierung, Analyse der technischen Entwicklung und die Konsequenzen für Netzwerk-Design
- Analyse und Evaluierung IP-Telephonie
- Wireless LANs in der kritischen Analyse – Teilnehmer erhalten den brandaktuellen Antennen-Guide, der speziell für die Sommerschule erarbeitet wird und einen messtechnischen Vergleich wichtiger Antennen für WLAN beinhaltet
- Designvarianten lokaler Netzwerke im Vergleich: wirtschaftliche und technische Optimierung Lokaler Netzwerke
- Ablösung Spanning Tree, Umstieg auf Rapid Reconfiguration Spanning Tree und Multiple Spanning Trees, Integration in OSPF
- Wichtige Änderungen von Sicherheitstechnologien: VPN und NAT-Traversal, Sicherheitslücke im Microsoft VPN-Clienten umgehen, WLAN-Security mit WPA

Natürlich findet am ersten Abend unsere traditionelle Happy-Hour statt: Die Teilnehmer starten in gemütlicher und gepflegter Atmosphäre in eine anstrengende, aber erfolgreiche Woche.

Die Sommerschule 2003 ist die ideale Gelegenheit, sich intensiv und kompakt mit den neusten Entwicklungen auseinander zu setzen. Die Mischung aus herstellerneutralen Top-Referenten, den neuesten Technologie-Entwicklungen, hochaktuellen Projekterfahrungen und direkt umsetzbaren Empfehlungen aus der Praxis hat die Sommerschule in der Vergangenheit zu einem beliebten Treffpunkt gemacht.

Da die Teilnahmeplätze begrenzt sind wird eine rechtzeitige Anmeldung empfohlen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sommerschule 2003

☐ Ich melde mich an zur
Sommerschule
der ComConsult Akademie 2003
vom 14.07. - 18.07.03 in Aachen
(Preis € 2.290,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Zweitthema Juni 2003

Wireless Overlay Networking: der neueste Trend

Fortsetzung von Seite 1

Der Autor:

Dr. Jürgen Suppan gilt als einer der führenden deutschen Berater für Kommunikationstechnik. Unter seiner Leitung wurden diverse Netzwerkprojekte aller Größenordnungen erfolgreich umgesetzt.

drsuppan@comconsult-research.com

Ein Wireless-Overlay-Netzwerk hat vier Primärziele:

- Senkung der Überversorgung innerhalb des kabelbasierten Netzwerks
- Senkung der Change- und Betriebskosten
- Integration mobiler Endgeräte inklusive einer ausreichenden Sicherheit
- Flexible Integration von Peripherie

Diese Ziele beziehen sich nicht nur auf die gezielte Ergänzung eines bereits vorhandenen Kabel-Netzwerks mit einem Wireless-Netzwerk sondern auch auf Neuinstallations- bzw. Migrations-Situationen (speziell bei der Migration Token Ring nach Ethernet, dort können je nach Situation die Migrationskosten massiv gesenkt werden).

Im Einzelnen sind die vier Primärziele wie folgt zu verstehen:

Ziel 1: Senkung der Überversorgung

Bei der Schaffung einer Verkabelungs-Infrastruktur werden grundsätzlich mehr Dosen geplant und realisiert als wirklich benötigt werden. Hintergrund sind die räumlichen Schwankungen in der Belegungsdichte über die Zeit und das unklare Mengengerüst der Zukunft. So lassen sich punktuell hohe Belegungsdichten mit vielen Endgeräten und Druckern pro Raum kaum seriös prognostizieren, zusätzlich ändert sich diese Situation permanent durch die vielen Umzüge pro Jahr. Auch das anzunehmende Mengengerüst ist im Rahmen eines Planungszeitraums von 10 Jahren nicht wirklich präzise vorhersagbar. Da aber eine punktuelle Nachverkabelung bei einem Fehlen von Netzwerkdosen sehr hohe Kosten verursacht, hat es sich in der Planung Lokaler Netze bisher als wirtschaftlich erwiesen, eine Überversorgung zu realisieren. In Anlehnung an die ISO11801/EN50173 kann man dabei grob von einer Anschlussdichte von 2 Dosen pro Arbeitsplatz als Minimum ausgehen. Durch die gezielte Ergänzung des Kabel-LAN durch ein Wireless-Netzwerk kann diese Übervorsorgung weitestgehend abgebaut werden. Für Neuinstallationen entsteht somit ein massiver Kostenvorteil.

Ziel 2: Senkung der Betriebskosten

Seit fast 20 Jahren befassen wir uns mit der Frage, wie die Betriebskosten eines Lokalen Netzwerks gesenkt werden können. Dabei wird ein wesentlicher Teil der Kosten durch Umzüge und ähnliche Veränderungen erzeugt. Das weitestgehende Konzept der Vergangenheit war Fiber-to-the-Desk, da es die Versorgung eines kompletten Gebäudes aus einem zentralen Verteilerraum vorsah. Die damit entstehenden Kostenvorteile im Change-Betrieb wurden den nicht unerheblichen Mehrkosten dieses Netzwerk-Typs gegenüber gestellt, in Konsequenz damit die Wirtschaftlichkeit begründet. Weniger extrem war in der Vergangenheit der Kompromiss, die Betriebskosten durch eine gezielte Senkung der Zahl der Verteilerräume zu senken. Dabei konnte die übliche Verkabelungs-Systematik beibehalten werden und im Gegensatz zu Fiber-to-the-Desk war diese Lösung auch im Invest kostengünstiger als die übliche Etagen-Verteiler-Lösung.

Wireless Netzwerke bieten nun eine völlig neue Perspektive. Eine flächendeckende Infrastruktur vorausgesetzt erfordern Umzüge keinerlei Änderungsarbeiten. Dabei sind allerdings zwei Infrastruktur-Merkmale erforderlich: die Wireless-Infrastruktur muss Roaming-fähig sein und sie sollte getrennt vom Kabelnetzwerk mit einem zentralen Übergangspunkt realisiert werden.

Speziell für Filialen oder kleinere Betriebsbüros ist die Senkung der Betriebskosten durch Vermeidung von Change-Arbeiten eine herausragende Perspektive. Wer einmal den Betriebsaufwand für ein räumlich verteiltes Filial-Szenario für eine Versicherung, eines Immobilienverwaltung oder Automobilniederlassungen in der Praxis gesehen hat, dem werden die immensen Potenziale von Funknetzen deutlich. Häufig entstehen in diesen Umgebungen mehr als die Hälfte der Betriebskosten durch Fahrtzeiten, da sich lokales Betriebspersonal nicht rechnet. Und häufig endet eine lange Anreise mit einer 5-minütigen Service-Maßnahme. Das Einsparpotenzial ist hier erheblich. Funknetze haben für derartige Filialsituationen einen weiteren Vorteil: sie können so installiert werden, dass das lokale Personal keinerlei Zugang zur Infrastruktur hat. Es kann kein Endgeräte- oder Drucker-Anschlusskabel ausgestöpselt oder vertauscht werden, es kann keine Rangierung in einem Verteilerraum falsch durchgeführt werden.Hinzu kommt ein Zugewinn an Mobilität, der in Filialen zur flexiblen Kundenbetreuung gewünscht werden kann.

Ziel 3: Integration mobiler Endgeräte

Die Zahl der Notebooks in den Unternehmen wächst permanent. Längst werden diese Geräte nicht nur bei reisenden Mitarbeitern/innen eingesetzt. Nutzungsvorteile auf der einen und Life-Style-Orientierung auf der anderen Seite erhöhen den Notebook-Bestand permanent. Und dies trotz der signifikant höheren Gerätekosten. Insbesondere im Bereich der höheren Führungskräfte ist der Trend zum Notebook ungebrochen.

Wireless Overlay Networking: der neueste Trend

Notebooks und andere mobile Endgeräte führen fast immer zu mindestens folgenden Problemen:

- Handhabung der Sicherheitsrisiken, wenn das Notebook auch außerhalb des Unternehmens in unvorhersehbaren und unklaren Sicherheits-Zusammenhängen benutzt wird
- Physikalischer Netzwerk-Anschluss, wenn das Notebook nicht direkt an einem darauf ausgelegten Arbeitsplatz angeschlossen werden soll.
- Umsetzung des Konfigurations-Management, da die Notebooks bei Release-Wechseln, Neuinstallation von Software etc. nicht immer anwesend sind und sich somit dem regulären Rollout entziehen

Alle diese Probleme lassen sich fast perfekt lösen, wenn Notebooks nicht mehr an das normale Kabel-LAN angeschlossen werden dürfen sondern bewusst ein Overlay-Netzwerk für Notebooks und andere mobile Endgeräte geschaffen wird:

- das Wireless-Overlay-Netzwerk wird als separate Infrastruktur ausgeführt, die nur an einem zentralen Punkt Zugang zum Kabel-LAN erhält. Diese wird mit einer Firewall kombiniert, ggf. wird hier auch ein VPN-Server integriert
- ein direkter physikalischer Netzwerk-Anschluss ist nicht mehr erforderlich, das mobile Endgerät kann tatsächlich auch mobil genutzt werden. Im Konferenz- oder Besprechungsraum, in der Kantine, im Büro des Kollegen/der Kollegin usw.
- mit dem separaten Wireless-Overlay-Netzwerk wird ein eigenes Konfigurations-Management verbunden. Geräte in diesem Netzwerk können gescannt, inventarisiert, geprüft werden. Dies macht auch dann Sinn, wenn ein Konfigurations-Management für den Rest des Unternehmens nicht im Betrieb ist. Speziell bei Notebooks ist die Zahl der illegal installierten Anwendungen und individuellen Konfigurations-Änderungen sehr hoch. Die Integration des Konfigurations-Managements ins Wireless-Overlay-Netzwerk senkt die Kosten dieser Lösung und erlaubt es, sich speziell auf die mobilen Endgeräte zu konzentrieren.

Ziel 4:
Flexible Integration von Peripherie

Drucker haben eine gemeinsame Eigenschaft: sie stehen immer da, wo kein Netzwerk-Anschluss vorhanden ist. Speziell aber die Fähigkeit, Arbeitsgruppen flexibel mit Druckern zu versorgen und auf betriebstechnisch sehr teure Desktop-Drucker verzichten zu können, kann Druckkosten deutlich senken. Die Integration ins Wireless-Overlay-Netzwerk schafft die perfekte Flexibilität.

Speziell mit der Unvorhersehbarkeit der notwendigen Zahl von Peripherie-Anschlüssen wird auch die Überversorgung mit Netzwerk-Dosen begründet. Wird dieser Gerätetyp generell aus dem normalen Kabel-Netzwerk entfernt, können also Überversorgungen reduziert und die Standort-Flexibilität gesteigert werden. Hinzu kommt, dass gerade diese Geräte keine hohen Datenraten erfordern, also sehr gut zur Leistungs-Charakteristik heutiger Wireless-Netzwerke passen.

Zentrale Merkmale
eines Wireless Overlay Netzwerks

Fasst man die beschriebenen Ziele zusammen, dann werden die zentralen Eigenschaften eines Wireless Overlay Netzwerks deutlich:

- es ist eine separate Infrastruktur, die an einem zentralen Punkt mit dem bestehenden Kabel-LAN verschaltet wird
- es ist eine weitestgehend flächendeckende Infrastruktur
- es beinhaltet eine Sicherheits-Infrastruktur, typischerweise eine Kombination aus WPA, Firewall und VPN
- es beinhaltet ein Konfigurations-Management für mobile Endgeräte

Betrachtet man diese Merkmale, dann sind noch einmal folgende Aspekte zu betonen:

- es wird eine flächendeckende Infrastruktur erforderlich
- es kommt ein eigenes Distribution-System zum Einsatz, das vorhandene Kabel-LAN wird nicht als Distribution-System genutzt
- Kabel- und Funk-LAN werden an einem zentralen Punkt verbunden. An diesem Punkt kommen Firewall und/oder VPN-Server zum Einsatz

Wireless Overlay Networking: der neueste Trend

Beim Aufbau einer flächendeckenden Wireless-Infrastruktur sind eine Reihe von Rahmenbedingungen zu beachten. Der zentrale Punkt ist, dass die übliche Try and Error Methode, mit der Wireless-Netze geplant werden hier nicht zum Einsatz kommen darf. Zwei Grundprobleme sind zu lösen:

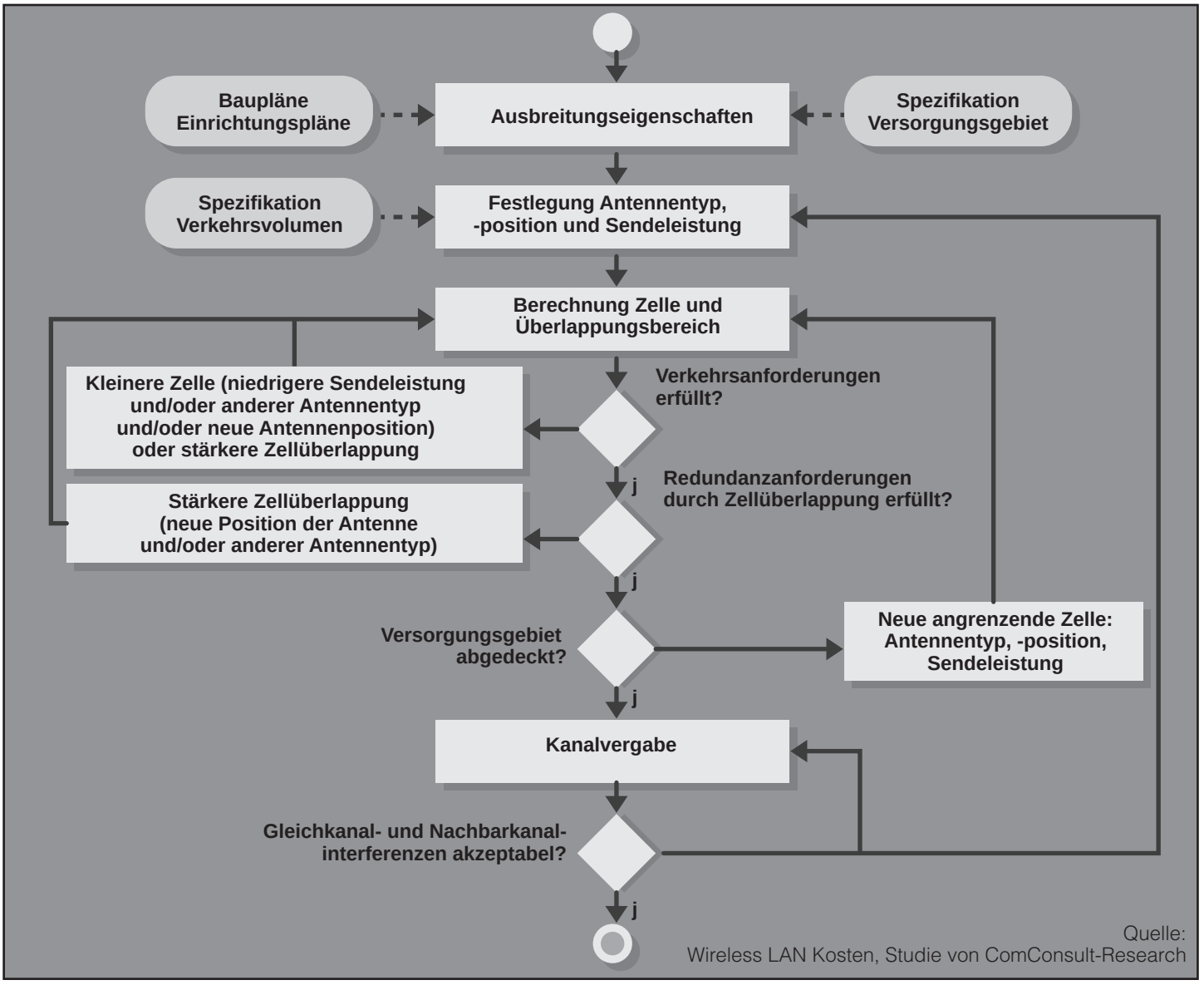
- Wireless-Netzwerke sind nicht stabil in ihrem Leistungsverhalten, speziell Reflexionen durch Multi-Path-Fading führen zu einem Schwanken der Signalstärke. Aus diesem Grund muss eine bewusste Zellplanung (siehe Bild 1) erfolgen. Nach Inbetriebnahme der Zelle sollte an allen Punkten innerhalb der Zelle das Signal-Rausch-Verhältnis über 20dB (siehe Tabelle) liegen

SNR-Wertebereich	Bedeutung
SNR ≥ 30 dB	Sehr guter Empfang
25 dB ≤ SNR < 30 dB	Guter Empfang
20 dB ≤ SNR < 25 dB	Zufriedenstellender Empfang
15 dB ≤ SNR < 20 dB	Ausreichender Empfang, jedoch schon deutliche Paketverluste auf physikalischer Schicht möglich
10 dB ≤ SNR < 15 dB	Mangelhafter Empfang, der jederzeit zusammenbrechen kann
SNR < 10 dB	Kein Empfang, jedoch Störung anderer Stationen oft noch möglich

Quelle: Wireless LAN Kosten, Studie von ComConsult-Research

Tabelle: Signal-Rausch-Verhältnis und seine Bedeutung

Bild 1: Ablauf einer Zell-Planung für ein Wireless-Overlay-Netzwerk



- Es darf keine Abdeckungs-Planung (coverage plan) erfolgen, bei der das Ziel die komplette funktechnische Abdeckung einer Fläche ist. Der Planungsansatz muss eine Kapazitätsplanung sein, bei der das Planungsziel aus einem erreichbaren Zelldurchsatz von x Mbit/s liegt. Dies sind zwei völlig verschiedene Planungsansätze.

Kapazitätsplanung führt fast immer zu Minizellen (siehe Bild 2) und ist mit eigenen Planungsaufgaben und Problemen verbunden. Zum Beispiel dominiert bei 802.11b und 802.11g bei einer Kapazitätsplanung das Problem der Überschneidungsfreiheit der Kanäle (Vermeidung von Intel-Kanal-Interferenzen). Ebenso müssen Access Points bei einer Kapazitätsplanung zwingend über die Fähigkeit der Senkung der Sendeleistung verfügen, auch der Einsatz von Richtantennen kann zwingend erforderlich werden.

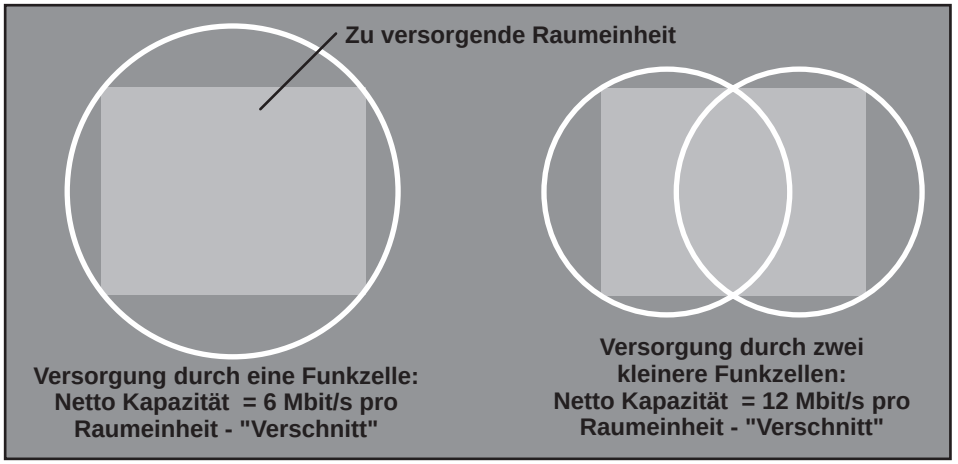


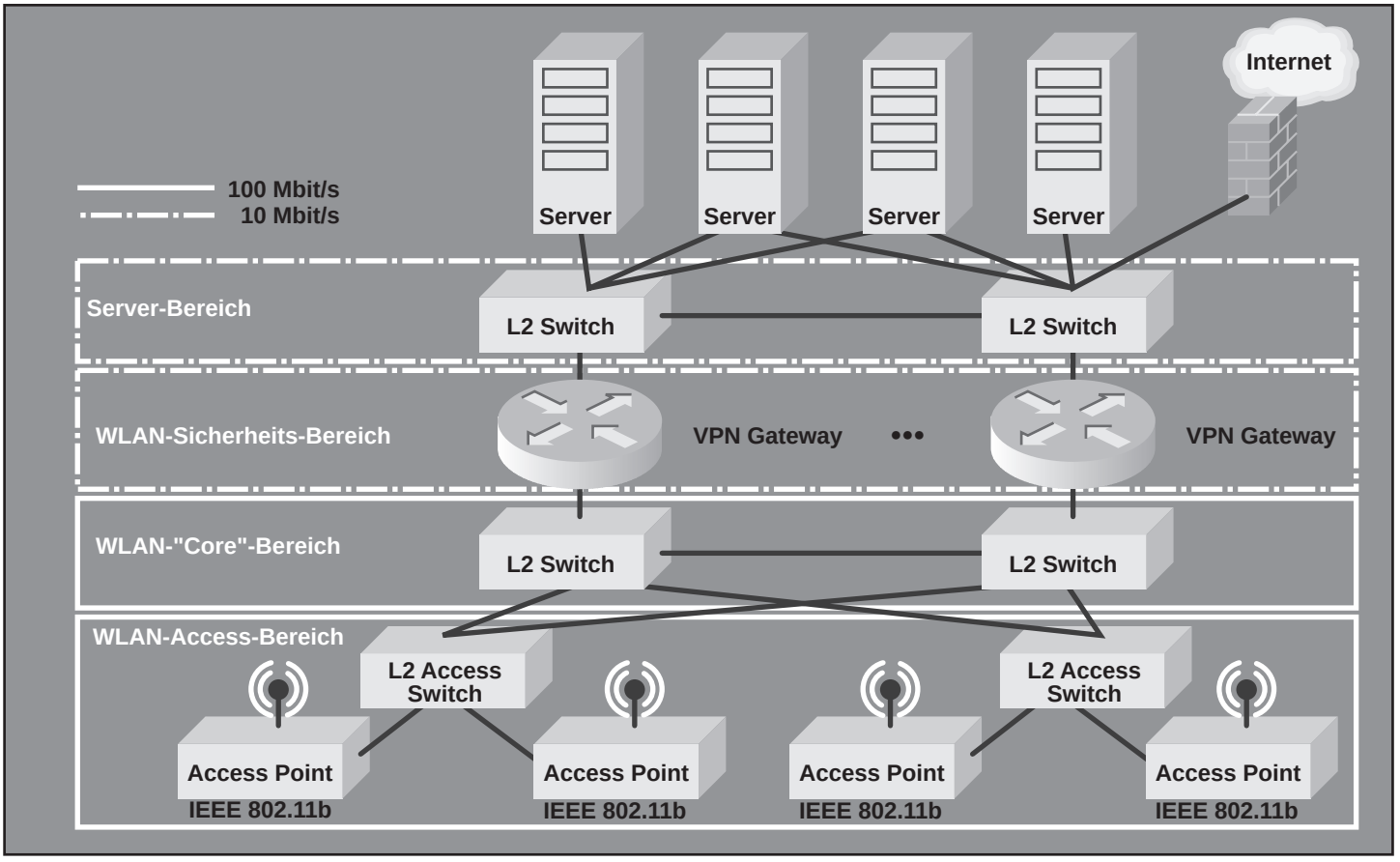
Bild 2: Typisch für Wireless-Overlay-Netzwerke sind kleine Funkzellen

Beispiele

Nachfolgend werden zwei typische Beispiele eines Wireless-Overlay Netzwerks beschrieben. Ziel dieser Beispiele ist es, die Grundsätze der Overlay-Technik deutlich zu machen. Im Detail kann die Umsetzung in der Praxis deutlich von diesen Beispielen abweichen.

Fall A beschreibt die Ergänzung eines Kabel-LAN durch ein WLAN als separate Infrastruktur mit definiertem Übergangspunkt zwischen WLAN und Kabel-LAN. Fall A stellt die typische Praxis-Situation nur vereinfacht dar. So ist auf jeden Fall eine Diskussion der IP-Adressproblematik notwendig. Fall A realisiert Roaming in einem Layer-2-Verbund. In größeren Umgebungen wird dies nicht ausreichen. Ein Layer-3-Core wird erforderlich sein und eine damit korrespondierende Roaming-Lösung (nicht trivial). Der dargestellte VPN-Server ist auch gleichzeitig Firewall. Dazu gibt es eine Reihe von sehr interessanten Produkten.

Bild 3 (Fall A): Wireless-Overlay-Netzwerk mit eigenem Distribution-System



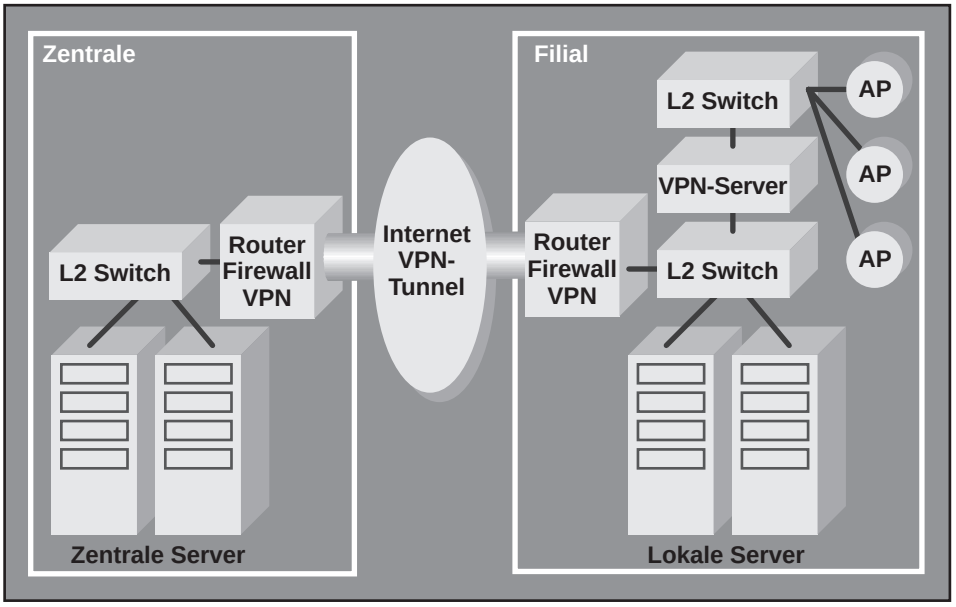


Bild 4 (Fall B): Filial-Lösung

Fall B beschreibt eine Filial-Situation. Ziel ist es hier, eine komplette Filiale (Automobil-Niederlassung, Versicherungs-Agentur, …) nur mit Wireless abzudecken. Für die Mitarbeiter/innen entsteht zusätzlich der Vorteil der Mobilität innerhalb der Niederlassung bzw. der integrierte Notebook-Einsatz. Innerhalb einer Filialsituation muss generell, aber speziell in Umgebungen mit Besucher-Verkehr ein erhöhter Sicherheitsbedarf angenommen werden. Der Zugang über ein VPN wird deshalb die Regel sein.

Nachteile bzw. offene Fragen

Bei großen Wireless-Overlay-Netzwerken kommen sehr viele Access Points zum Einsatz. Diese müssen konfiguriert und überwacht werden. Die Überwachung und Auswertung der jeweils gegebenen Funk-Qualitäts-Situation (zum Beispiel Analyse der Wiederholungs-Übertragungen, Aufteilung der Sendungen auf Datenraten) kann sehr gut mit einem Reporting-Tool realisiert werden (wenn die AP´s über geeignete MIB´s verfügen, dazu sollte die Verfügbarkeit der notwendigen MIB-Variablen ein Teil der Produktauswahl sein). Ein Problem bleibt der sehr hohe Konfigurations-Aufwand. Hier findet im Moment eine Diskussion über Lösungsansätze statt (Stichwort: fat kontra thin kontra fit Access Point). Auf jeden Fall erfordert ein größeres Wireless-Netzwerk eine von einem Kabel-LAN abweichende Betriebssystematik. Durch das immer gegebene Überlastungsrisiko von Funkzellen und die noch fehlende Quality of Service ist eine weitergehende Auswertung der Betriebssituation erforderlich. Generell wird auch immer das Problem der Überlagerung mit illegalen/unbekannten APs bestehen, dass eine gezielte Überwachung auf derartige Geräte erfordert (Störrisiko, Sicherheitsrisiko). Durch diese vom Kabel-LAN abweichenden Aufgaben entstehen Mehrkosten, die in der Planung zu berücksichtigen sind.

Ein weiteres gravierendes Problem ist die unklare Abnahme einer Wireless-Installation. Die Natur eines Funknetzes erschwert die Abnahme deutlich. Die unvermeidbaren Qualitäts-Schwankungen über die Zeit in der Fläche machen es schwer, die Qualität einer realisierten Zellplanung zu prüfen. Im Endeffekt muss die Abnahme eine Würdigung der gesamten Planungs- und Installationssystematik beinhalten. Ein klar geregelte Messtechnik wie im Kabelbereich ist jedenfalls nicht gegeben.

Fazit

Wireless-Overlay-Netzwerke sind ein deutlicher Schritt vorwärts. Sie beseitigen einige Altlasten der Vergangenheit (speziell Notebook-Integration, Drucker-Einbindung), reduzieren die Notwendigkeit der Überversorgung im Kabel und senken die Betriebskosten.

Trotzdem sind Wireless-Overlay-Netzwerke keine triviale Infrastruktur. Planung und Umsetzung sind durch die Integration aus Funk-, Sicherheits- und Konfigurations-Technologien anspruchsvoll. Speziell für den Funkbereich sollte ein Funkerfah-render Planer hinzu gezogen werden.

In der Gegenüberstellung aller Vor- und Nachteile überwiegen die Vorteile deutlich. Für viele Umgebungen stellt dieser neue Netzwerk-Typ eine interessante Perspektive dar. Auch die zur Zeit moderne Sichtweise der Senkung der Betriebskosten findet ihre Berücksichtigung.

Aktuelle Sonderveranstaltung

Anwender berichten: Erfahrungen mit dem Cisco Call Manager

Am 7. Juli 2003 berichten erfahrene Administratoren im Hilton Bonn über die Einsatzerfahrungen mit dem Cisco Call Manager.

Wir freuen uns, dass wir speziell eine Installation wie sie im Rechenzentrums der Finanzverwaltung NRW (RZF) betrieben wird mit Ihnen diskutieren und analysieren können, weil dort der Call Manager sehr intensiv genutzt wird und eine Reihe zusätzlicher Leistungsmerkmale realisiert worden sind. Auch ist die Installation sehr umfangreich, da neben dem Call Manager auch Unified Messaging und CTI betrieben werden.

Die Installation und Konfiguration der Systeme wird auf der Veranstaltung live präsentiert. So kann auf alle Fragen der Bedienkomplexität und der Ergonomie der Oberfläche, der Veränderbarkeit von Eigenschaften direkt und live eingegangen werden.

Es wird auf folgende Fragen eingegangen:

- Vorstellung der Gesamtlösung mit den eingesetzten Komponenten und Anwendungen
  - Besondere Highlights der Lösung
  - Welche Funktionen werden von den Anwendern besonders geschätzt
  - Welche Funktionen machen Probleme
  - warum IP-Telephonie und keine klassische TK-Lösung
  - warum der Cisco-Call-Manager
  - was bringt ein CTI-Paket an Zugewinn
  - wie sind die bisherigen Betriebserfahrungen

  - ist der Betrieb stabil und sicher
  - wie komfortabel ist IP-Telephonie aus der Sicht der Anwender
  - werden die Telephonie und die Art der Bedienung akzeptiert
  - wie ist die Sprachqualität
  - wie gut sollte das zu Grunde liegende Netzwerk sein

- Die Architektur des Call Managers

- Wie wird der Call Manager konfiguriert
  - Beispiele: Benutzer, Telefon, Device Profile, Hotline; Gateways etc.
  - mit welchem Aufwand lässt sich der Call Manager erweitern
  - welches Know-how sollte der Betreiber haben
  - wie können Anwender-Profile unter mobiler Nutzung realisiert werden
  - wie wird eine große Anzahl User / Telefone konfiguriert oder administriert

- Sicherungsmechanismen

- Softwareupdates

- Wie wird der Unity-Server installiert und konfiguriert

- Wie werden die CTI Anwendungen installiert und konfiguriert

- Praxisteil

Die präsentierenden Administratoren haben den Call Manager intensiv analysiert und verfügen über umfangreiches Wissen. Auch innerhalb von Cisco gilt diese Installation als eine der professionellsten in Europa.

Lernen Sie, was mit dem Cisco Call Manager möglich ist und wo seine Grenzen liegen.

Intensiver Erfahrungsaustausch und Diskussion ist ein Kern dieser Veranstaltung. Die Teilnehmer sollen maximal von der Erfahrung der Referenten profitieren. Aus diesem Grund ist die Zahl der Teilnehmerplätze begrenzt.

Zögern Sie deshalb nicht, sich schnell einen Platz auf dieser herausragenden und einmaligen Sonderveranstaltung zu sichern.

Referenten: Karl-Heinz Hommen-Menz, Achim Puetz und Axel Schemberg vom Rechenzentrum der Finanzverwaltung NRW

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Cisco Call Manager

☐ Ich buche die Sonderveranstaltung
Erfahrungen mit dem Cisco Call Manager
am 07.07.03 in Bonn
(Preis € 698,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Aktueller Report

Studie des Monats: Designvarianten lokaler Netzwerke im Vergleich

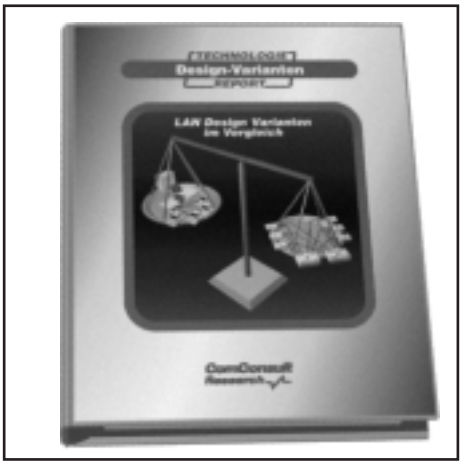
Moderne Switching- und Routing-Verfahren gestatten eine erhebliche Spannbreite an Design-Alternativen lokaler Netzwerke. Zusätzlich kommen kontinuierlich neue Verfahren auf den Markt, die den Gestaltungsumfang lokaler Netzwerke weiter erhöhen. Rapid Reconfiguration und Multiple Spanning-Trees sind Beispiele für den erheblichen Zugewinn an Funktionalität. Viele bestehende lokale Netzwerke können durch eine perfekte Kombination der verfügbaren Verfahren signifikant optimiert werden.

Man kann feststellen:

- Moderne Switching-Verfahren in Kombination mit modernen Switching-Architekturen ermöglichen eine wirtschaftliche Optimierung und eine deutliche Senkung der Betriebskosten. Zusätzlich können bestehende Investitionen optimal ausgenutzt und in vielen Fällen umfangreiche Neuinvestitionen vermieden werden.

- Historisch gewachsene LANs können technisch mit geringem Aufwand deutlich optimiert werden, wenn der ideale Mix an Verfahren zum Einsatz kommt. Die Stabilität kann verbessert werden, der Leistungsumfang kann ausgebaut werden, die Skalierbarkeit steigt und damit die schnelle und preisgünstige Reaktion auf veränderte Anforderungen.

- Die zunehmende Verbreitung von Gigabit-Ethernet im Endgerätebereich und die



Erweiterung der Backbone-Kapazitäten erfordern eine Neukalkulation der Buchungsfaktoren und ein entsprechendes Redesign.

- Service-Level-Zusagen für Netzwerke können unter Einsatz neuester Technologien seriös gegeben und auch in der Praxis umgesetzt werden

Wie kann dieses Design-Potenzial sinnvoll genutzt werden? Nach welchen Kriterien und Zielsetzungen kann ein modernes LAN-Design aufgebaut werden?

Hier setzt die Studie des Monats Juni an. Sie zeigt auf:

- wo die Schwachstellen und Gefahrenpunkte in einem Netzwerk liegen,
- wie die etablierten und wie die neuen Redundanzverfahren funktionieren,
- ob und wie Sie die neuen Verfahren nutzen können,
- wo die technischen und betrieblichen Vor- und Nachteile der verschiedenen Verfahren liegen,
- wie die Weiterentwicklung der unterschiedlichen Verfahren im Markt zu bewerten ist,
- wie Sie Netze einstufen und klassifizieren können, um zu einem angemessenen Design zu gelangen,
- wie anhand der Anforderungen ein angemessenes Design für die Weiterentwicklung eines vorhandenen Netzwerks gefunden wird und
- wie Sie gezielt Kosten sparen können

An Hand einer Reihe von Beispielen zeigt die Studie, wie sich Design Lokaler Netzwerke optimieren lässt. Dabei kommen viele Beispiele direkt aus der Praxis und zeigen aktuelle Umsetzungen modernsten Netzwerk-Designs in aktuellen Projekten.

In dem Umfang der analysierten Verfahren, der Umsetzung in vielen praxisnahen Beispiel-Konfigurationen und der Berücksichtigung sowohl technischer als auch wirtschaftlicher Gesichtspunkte ist diese Studie einmalig.

Der Research Report "Designvarianten" ist für jeden Betreiber oder Planer eines Lokalen Netzwerks eine wichtige und einmalige Arbeitsgrundlage und somit ein absolutes Muss.

Fax-Antwort an ComConsult 02408/955-399

Bestellung Designvarianten

☐ Ich bestelle den Research Report
Designvarianten
lokaler Netzwerke im Vergleich
April 2003, 543 Seiten
(Preis € 398,-- zzgl. MwSt.)

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ, Ort _____

eMail _____ Unterschrift _____

Bestellen Sie über unsere Web-Seite
www.comconsult-akademie.de

Aktuelle Sonderveranstaltung II

Migration von Windows NT nach Windows Server 2003

Vom 24. - 25. Juni 2003 veranstaltet die ComConsult Akademie im Hilton Bonn die einmalige Sonderveranstaltung "Migration von Windows NT nach Windows Server 2003".

Nachdem Microsoft den Support für Windows NT zumindest immer mehr minimiert (die Extended Support Phase für Windows NT Workstation endet am 30.06.2003) und diverse Patches nur noch für Windows 2000/XP/Server 2003 zur Verfügung stehen, sollte der Umstieg jetzt erfolgen bzw. vorbereitet werden.

Dieses hochaktuelle Seminar analysiert die in Frage kommenden Alternativen, beschreibt die zum Umstieg notwendigen Arbeiten, bewertet die neuen technischen Möglichkeiten von Windows Server 2003 und zeigt alternative Migrationswege auf.

Betrachtet man die Eigenschaften der als Zielversion in Frage kommenden Windows Server Versionen, so hat die Windows Server 2003 Version eine Reihe von Vorteilen gegenüber Windows 2000 und steht deshalb im Mittelpunkt des Seminars (Leistung, Stabilität, Skalierbarkeit). Die Analysen und Empfehlungen des Seminars können aber auch an vielen Stellen auf Windows 2000 übertragen werden.

In der Regel wird man bei einem Umstieg mit mindestens 3 Themenbereichen und den zugehörigen Fragen konfrontiert:

Nutzung von Active Directory

Kernelement jeder Migrations-Lösung wird der Einsatz von Active Directory sein. Hier liegt ein wesentlicher Mehrwert der neueren Windows Server Versionen. Windows Server 2003 hat hier noch weitere Möglichkeiten geschaffen. Allerdings muss eine derartige Nutzung von vornherein projektiert werden. Eine spätere Erweiterung kann komplex und teuer werden. Dieses Seminar zeigt, wie Sie Active Directory erfolgreich nutzen und wo die Potenziale liegen. Profitieren Sie von der Projekt-Erfahrung der Referenten und vermeiden Sie typische Fehler.

Server-Konsolidierung

Mit Windows Server 2003 ist die Leistung der Windows-Server-Version massiv gewachsen (bis zu 900% im TCP/IP-Betrieb). Verbindet man parallel den Umstieg mit einem Wechsel der Hardware, so ergeben sich gewaltige Konsolidierungs-Möglichkeiten. Dies gilt sowohl für den File-Server-Einsatz als auch für Datenbank-Server. In diesem Seminar werden die Potenziale aufgezeigt, die Ihnen hier geboten werden.

Nutzung der neuen Zusatzfunktionen

Im 3. Themenbereich, der bei jeder Migration zu beachten ist, stehen die neuen Funktionen von Windows Server 2003 im Vordergrund. Diese sind vielfältig und bieten eine Reihe von Zusatzpotenzialen. Von der Vereinfachung der Administration über Remote Management bis hin zum massiven Ausbau der Speicher-Funktionalität müssen entsprechende Entscheidungen getroffen werden. Hier wird stets die Frage entstehen: Windows-Bordmittel einsetzen oder Spezial-Produkte benutzen. Dieses Seminar analysiert und bewertet die neuen Möglichkeiten.

Dieses Seminar bildet für alle, die sich mit der Migration von NT auf Windows Server 2000/2003 befassen, eine ideale Analyse und Bewertung der dabei entstehenden Fragen. Zusammen mit den Empfehlungen der Projekt-erfahrenen Referenten bietet dieses Seminar eine echte Hilfe für diese Projekte.

---

* Zu diesem Themenbereich bieten wir auch die (technisch detailliertere) Seminarreihe ".NET Server 2003 plan, build & run", Information unter **www.comconsult-akademie.de**

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Windows Server 2003

☐ Ich buche die Sonderveranstaltung
Migration von Windows NT nach Windows Server 2003
am 24.06. - 25.06.03 in Bonn
(Preis € 1.390,-- zzgl. MwSt.)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ, Ort
eMail	Unterschrift

Schwerpunktthema Juni 2003

Auf dem Weg zum virtuellen Arbeitsplatz

Fortsetzung von Seite 1

Autor:

Dr. Behrooz Moayeri, Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH, Aachen

moayeri@comconsult.com

Die Bezeichnung „Arbeitsplatz" für eine berufliche Beschäftigung impliziert, dass diese Tätigkeit an eine Lokation gebunden ist. Ob im produzierenden Gewerbe oder in der Dienstleistungsbranche, im privaten Sektor oder in Behörden - das Urverständnis über eine Erwerbstätigkeit geht bisher immer von einer an einen „Platz" gebundenen Arbeit aus. Menschen müssen sich zu diesem Platz begeben, um der Arbeit nachgehen zu können. An anderen Orten können sie im Sinne ihrer beruflichen Aufgaben nicht produktiv wirken. Sie brauchen in ihrer unmittelbaren räumlichen Nähe Maschinen, Werkzeuge und Informationsträger, um die ihnen anvertrauten Arbeitsschritte durchzuführen. Ohne diese Hilfsmittel können sie das Produkt nicht erzeugen, das ihre Arbeit hervorbringen soll - sei es eine Ware oder eine Dienstleistung.

Diese Beschreibung eines „Arbeitsplatzes" trifft noch auf die meisten Erwerbstätigen zu. Automobile werden in Werkshallen gebaut, und Werkshallen bewegen sich nicht. Aber bei einer zunehmenden Zahl von Tätigkeiten kann mittlerweile die Bindung der Arbeit an eine Lokation infrage gestellt werden. Warum muss heute ein Büroarbeitsplatz ein solcher im wörtlichen Sinn des Wortes sein? Welche Werkzeuge und Informationen sind nur an bestimmten Plätzen verfügbar? Eine langfristig beständige Antwort auf eine solche Frage fällt einem immer schwerer, wenn es sich um Arbeiten handelt, deren Rohmaterial und Erzeugnis Informationen sind.

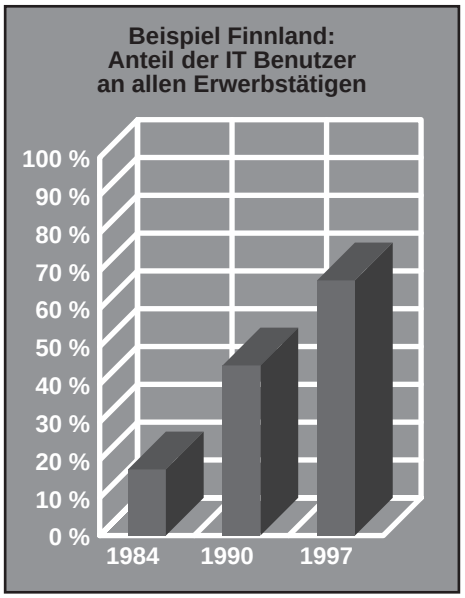
Solche Tätigkeiten werden von mehr Menschen ausgeübt als auf den ersten Blick ersichtlich.

Ein Bankkaufmann, der für einen Kunden einen maßgeschneiderten Darlehensvertrag ausarbeitet, erzeugt aus den vom Kunden zur Verfügung gestellten Informationen über dessen finanzielle Situation, Zukunftsplanung etc. weitere Informationen, die in den Vertrag einfließen.

Ein Arzt diagnostiziert auf der Basis der Informationen über die Symptome die Krankheit. Eine Diagnose ist eine vom Arzt produzierte Information. Diese Information verarbeitet er weiter zu den für die Behandlung erforderlichen Informationen, z. B. darüber, welche Medikamente und in welcher Dosis einzunehmen sind und wann er einen nächsten Informationsaustausch mit dem Patienten als notwendig erachtet.

Ein Manager erhält Informationen über die neuesten Geschäftszahlen und erteilt davon abhängig Anweisungen, auch eine Art Information.

Bild 1: Finnland ist führend, aber der Trend zur IT-Nutzung ist EU-weit festzustellen



Vision und Wirklichkeit

Doch gibt es diverse Gründe, weshalb diese Beschreibung der Zukunft der Arbeit vielen Betrachtern als reine Vision und weit entfernt von der heutigen Realität vorkommen mag:

- Der Prozess der Automatisierung der Warenproduktion und sonstiger Tätigkeiten, die eine körperliche Betätigung von Menschen erfordern, ist noch nicht abgeschlossen. Noch immer werden zahlreiche Arbeiten, die theoretisch von Maschinen übernommen werden könnten, durch Menschen ausgeführt, weil eine Automatisierung nach dem heutigen Stand unmöglich oder unwirtschaftlich wäre. Man denke z. B. an das Transportwesen. Aber selbst diese Bereiche kommen mit immer weniger Menschen aus. Es geht nicht darum, dass die Menschen aus den Produktionsstätten oder anderen Orten der körperlichen Erwerbsarbeit vollständig verschwinden. Die Aussage ist: Der Anteil solcher Erwerbstätigen geht in den hochentwickelten Ländern bereits seit Jahrzehnten zurück, und dieser Prozess wird fortgesetzt. Die Arbeitskräfte, die somit freigesetzt werden, widmen sich zunehmend Aktivitäten, die überwiegend aus der Gewinnung, der Verarbeitung und der Produktion von Informationen bestehen. Die körperliche Erwerbsarbeit wird nie aus der Gesellschaft verschwinden, jedoch weiterhin eine abnehmende Zahl Menschen beschäftigen. Dieser Prozess ist noch nicht am Ende angelangt. Die Kosten der Automatisierung werden im Zuge der Fortschritte der Elektronik und der Informationstechnik (IT) im Verhältnis zu den steigenden, mit dem Faktor Arbeit verbundenen Kosten weiter sinken, sodass die Wirtschaftlichkeitsberechnung für Bereiche, in denen die Automatisierung noch keinen Einzug gefunden hat, immer wieder neu anzustellen ist.

Auf dem Weg zum virtuellen Arbeitsplatz

- Noch herrscht in der Gesellschaft ein von den vorangegangenen Jahrhunderten übernommenes, im Prinzip nicht verändertes Bild der Arbeit vor. In diesem Bild wird die Erwerbsarbeit in einem sozialen Umfeld vollbracht, das ohne Kommunikation der Arbeitenden von Angesicht zu Angesicht nicht auskommt. In unserer Gesellschaft wird die Erwerbsarbeit auch als Flucht aus der Vereinsamung verstanden. Die Folgen der Versäumnisse der Gesellschaft, das menschliche Bedürfnis nach Zusammenleben und persönlicher Kommunikation mit anderen Menschen zu befriedigen, werden auf die Erwerbsarbeit abgewälzt. Die Erwerbstätigkeit bekommt so plötzlich auch die Funktion, das Fehlen der menschlichen Kommunikation in anderen Lebensbereichen zu kompensieren. Dabei hat die Erwerbstätigkeit eigentlich eine andere Funktion, nämlich die Produktion von materiell messbaren Werten (auch geistige Produktion erzeugt materiell Messbares). Dadurch, dass man die Erwerbsarbeit mit einer zusätzlichen, vom Urzweck dieser Tätigkeit entfernten Funktion belastet, wird diese Arbeit ineffizienter. Nichtsdestotrotz wird die Erwerbstätigkeit von der heutigen Gesellschaft immer noch im Zusammenhang mit dieser Zusatzfunktion gesehen. Die Erfüllung dieser Funktion erfordert nach dem bisherigen Modell, dass sich Menschen zu festen Zeiten zu vorgegebenen Orten begeben und sich an diesen Orten neben der Erfüllung ihrer produktiven Aufgabe auch begegnen. Diese menschliche Kommunikation von Angesicht zu Angesicht wird auch dann als notwenig erachtet, wenn die für die produktive Arbeit erforderliche Kommunikation schon längst auch standortübergreifend und durch den Einsatz technischer Werkzeuge realisierbar ist.

- Nicht zuletzt sind die technischen Gründe zu benennen, die bisher der Virtualisierung von Arbeitsplätzen entgegengewirkt haben. Ein Telefongespräch ist nicht geeignet, jegliche Kommunikation von Angesicht zu Angesicht zu ersetzen. Die Netze sind nicht in der Lage, beliebig große Datenmengen wie z. B. sehr hoch auflösende, medizinisch genutzte, stehende oder bewegte, möglicherweise dreidimensionale Bildinformationen innerhalb einer akzeptablen Zeit zu jedem anderen beliebigen Ort zu transportieren. Theoretisch wären zwar solche Netze realisierbar, jedoch nicht unter wirtschaftlich vertretbaren Randbedingungen. Die Werkzeuge zur Gewinnung, Verarbeitung und Generierung von Informationen sind immer noch nicht so benutzerfreundlich, dass jeder Mensch damit umgehen könnte. Der Betrieb und die Administration der technischen Werkzeuge wird noch von einer im Vergleich zur ganzen Gesellschaft zu kleinen Zahl von Experten beherrscht. Die Werkzeuge basieren auf zum Teil sehr neuer Technik und naturgemäß nicht ganz stabil und zuverlässig. Zu allen diesen Problemen muss man den Aspekt der Sicherheit hinzufügen. Die Menschen müssen erst einmal den neuen Techniken in dem Sinne vertrauen können, dass sie von bestimmten sicherheitsrelevanten Eigenschaften der IT-Lösung ausgehen können. Erstens müssen vertrauliche Informationen vertraulich übertragen und gespeichert werden können. Zweitens muss die Authentizität der gewonnen Information für denjenigen Menschen, der sie empfängt, sichergestellt sein. Drittens muss diese Authentizität im Sinne einer Verbindlichkeit und Unbestreitbarkeit auch Dritten gegenüber nachgewiesen werden können. Viertens ist die Integrität der gespeicherten und übertragen Informationen zu schützen. Fünftens müssen die technischen Hilfsmittel auch bei mutwilligen Angriffen verfügbar bleiben. Die vielen negativen Erfahrungen mit der IT haben dazu beigetragen, dass der Prozess der Vertrauensbildung in die IT-Sicherheit langsamer voranschreitet als nach dem Stand der Technik möglich.

Elektronische Erfassbarkeit von Informationen

Entscheidend für die Virtualisierung von Arbeitsplätzen ist die elektronische Erfassbarkeit von Informationen. Fast jede für die Erwerbsarbeit erforderliche Information ist mittlerweile elektronisch zu erfassen, zu übertragen, zu verarbeiten und zu speichern. Dies gilt vor allem für Informationen, die der Mensch akustisch und visuell wahrnehmen bzw. in Worten und Zahlen fassen kann. Ob und wann die IT-Netze auch andere Informationen wie z. B. über Gerüche übertragen können (bisher steht ein „Chemical Transport Protocol" noch aus), ist für die meisten produktiven Tätigkeiten nicht relevant. Relevant sind vor allem:

- Daten in verschiedenen digitalen Formaten (binär, zeichenorientiert)
- akustische Informationen wie Sprachsignale
- stehende zwei- oder dreidimensionale Bilder mit verschiedenen Auflösungen und Farbtiefen
- Sequenzen aus den genannten stehenden Bildern mit verschiedenen Bildhäufigkeiten pro Zeiteinheit

Auf dem Weg zum virtuellen Arbeitsplatz

Zwar könnte die möglichst originalgetreue Abbildung der Realität in eine virtuelle Realität einschließlich der Art, wie sich ein Gegenstand anfühlt, für einige Tätigkeiten wie z. B. im medizinischen Bereich interessant sein, aber die vier genannten Typen von Information decken den „Rohstoff" bzw. das „Erzeugnis" der meisten produktiven Tätigkeiten ab. Die meisten Menschen, die an ihrem Arbeitsplatz Informationen gewinnen, verarbeiten und generieren müssen, können diese Informationen in einer oder mehreren der vier genannten Formen aufnehmen und erstellen:

- Was Daten betrifft, ist die IT überhaupt und ursprünglich dafür entstanden, diesen Informationstyp zu erfassen, zu speichern, zu verarbeiten und zu übertragen.

- Akustische Informationen wurden zunächst in der Telekommunikation und im Hörfunk und Fernsehen als analoge Signale übertragen. Obwohl die analoge Technik noch weit verbreitet ist, gewinnt in der Telekommunikation bereits seit vier Jahrzehnten und beim Hörfunk und Fernsehen seit dem letzten Jahrzehnt die digitale Informationsübertragung immer mehr an Bedeutung. Die Telekommunikation, die für die Erwerbsarbeit zumeist von größerem Interesse ist, durchläuft nach mehreren Umstellungen im Zusammenhang mit der digitalen Vermittlung und Übertragung zurzeit mit der Einführung von Voice over IP (VoIP) eine Veränderung, an deren Ende nach Ansicht der meisten Fachleute die Konvergenz von Daten und Sprache steht.

- Der Faxdienst, vor 20 Jahren als revolutionäre Erfindung gefeiert, war nur der Anfang auf dem Weg zur heutigen digitalen Fotografie, die zusammen mit den standardisierten Kompressions- und Übertragungsverfahren die Anforderungen der meisten Anwendungen, die mit stehenden Bildern arbeiten, abdecken kann. Mithilfe immer leistungsfähigerer terrestrischer und drahtloser Netze zeichnen sich die übertragbaren Bilder durch ständig höhere Auflösungen und Farbtiefen aus.

- Gleiches gilt für die bewegten Bilder. Die Kosten für die Integration der Erfassung, Verarbeitung, Speicherung und Übertragung von bewegten Bildern sinken, und die Qualität der Bilder steigt. So können immer mehr Anwendungen von der digitalen Videotechnik profitieren, von virtuellen Meetings bis zu Lernprogrammen.

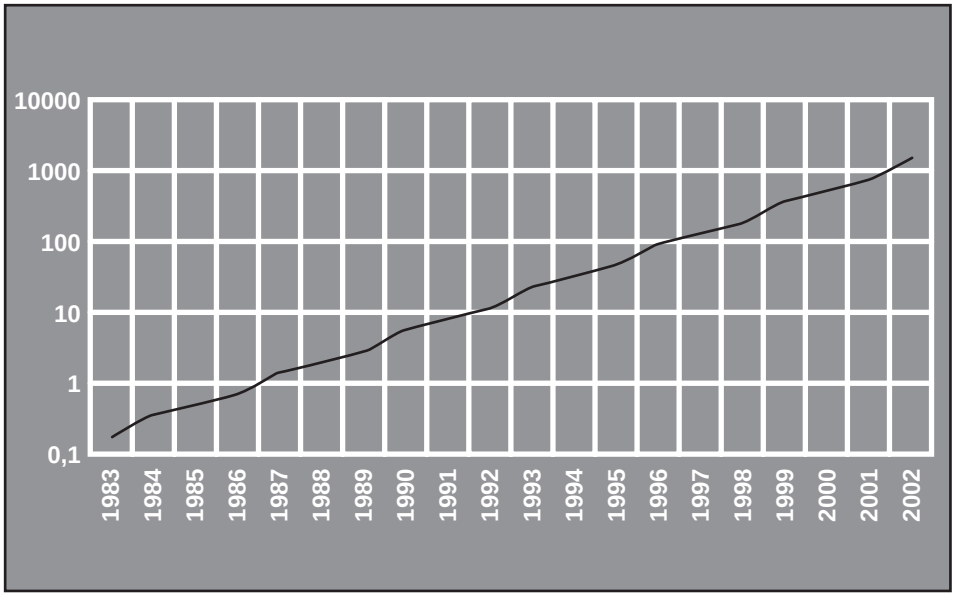


Bild 2: Entwicklung der Prozessorengeschwindigkeit in MHz

Endgeräte

Die Endgeräte, mit dessen Hilfe sich die verschiedensten Informationstypen (Daten, Sprache, stehende und bewegte Bilder) erfassen, verarbeiten, speichern und übertragen lassen, unterliegen einem stetigen Prozess der Verbesserung des Preis-Leistungs-Verhältnisses. Die Prozessorgeschwindigkeit hat sich in den letzten 20 Jahren durchschnittlich alle 18 Monate verdoppelt. Gleiches gilt für die durchschnittliche Größe des Arbeitsspeichers eines PC, während das Verdopplungsintervall bei der Festplattenkapazität 16 Monate betrug. So ist der PC von heute fast zehntausendmal leistungsfähiger als der erste, vor ca. zwei Jahrzehnten verkaufte PC. Heutige Notebooks sind um den Faktor 10 leichter als die PC von damals. Und sie sind nicht einmal teurer als die PC von 1981, wenn man die Inflationsrate berücksichtigt.

Dabei spiegeln die reinen Zahlen nicht die das ganze Ausmaß der PC-Revolution wieder. Ein PC kann heute fast so flach und leicht sein wie ein Notizblock, und er kann genau so wie ein Notizblock Informationen aufnehmen, nämlich über einen Stift. Der PC kann Sprachsignale und Bilder aufnehmen und wiedergeben. Er ist von Hause aus kommunikationsfähig. Man kann ihn über eine komfortable Oberfläche bedienen. Er ist mit mächtiger Software für Text- und Bildverarbeitung, für Berechnungen, für Präsentationen und für den Nachrichtenaustausch ausgestattet. Er ist ein kleines portables Rechenzentrum, Archiv, Videokonferenzraum etc. Er kommt stundenlang ohne Stromanschluss aus.

Hinzu kommen noch kleinere, noch portablere Endgeräte, die zwar nicht so mächtig sind wie der PC, dafür aber geeigneter für den mobilen Einsatz. Von den Mobiltelefonen mit zusätzlicher Textverarbeitungs-, Terminkalender-, E-Mail- und Datenbankfunktionalität bis hin zu Persönlichen Digitalen Assistenten (PDA) der Größe und Dicke einer Hand erstreckt sich das Spektrum an kleinen Hilfsmitteln, die bei der Gewinnung der Informationen aus dem Internet und anderen Netzen sowie der Speicherung, Verarbeitung und Übertragung diverser Informationstypen eingesetzt werden können.

Durchdringungsgrad der IT-Netze

Bevor die persönlichen Endgeräte vernetzt wurden, dienten sie nur der Verarbeitung der auf ihnen gespeicherten Information zu neuer Information. Mit zunehmender Vernetzung wurden diese Endgeräte auch zum Mittel des Informationsaustauschs, nämlich der Gewinnung von bestehender und der Übermittlung von selbst produzierter Information. Für die Realisierung des virtuellen Arbeitsplatzes ist es wichtig, diese Fähigkeit der Geräte für den zeitnahen Informationsaustausch zu nutzen. Der Wert einer Information sinkt mit ihrem Alter. Je kürzer der Abstand zwischen der Generierung der Information und des Empfangs dieser durch den Adressaten, umso effizienter ist die geleistete Arbeit.

Auf dem Weg zum virtuellen Arbeitsplatz

Einige Beispiele sollen diese Aussage untermauern:

- Während ein Manager auf einem Flughafen oder Bahnhof auf seinen nächsten Anschluss wartet, erreicht ihn die Nachricht, dass ein wichtiger Kunde innerhalb kürzester Zeit ein qualifiziertes Angebot wünscht und mit sofortiger Beauftragung „droht". Der Manager hat alle technischen Möglichkeiten zur Verfügung, um sich mit allen involvierten Kollegen und Mitarbeitern abzustimmen, auf die internen Datenbestände seiner Firma zuzugreifen und binnen zwei Stunden das Angebot auf den Weg zu bringen. Zumindest den Wettlauf mit der Zeit hat der Manager so gewonnen. Diese Art Flexibilität wird von Kunden belohnt.

- Während sich der Entwickler einer hochkomplizierten Anwendung irgendwo auf der Welt befindet, erfahrt sein Arbeitgeber, dass ein Problem mit dem Produkt zum Stillstand einer ganzen Produktionslinie in München geführt hat. Der Entwickler kann als die Fachkraft mit dem umfassendsten Wissen zu dem Produkt durch einen Blick auf die Ereignisprotokolle und Fehlermeldungen binnen Minuten etwas vollbringen, wofür andere Mitarbeiter durch mühsames Eindenken Stunden oder Tage brauchen würden: den Fehler zu erkennen und einen Workaround zu realisieren. Der Entwickler hat von seinem Standort aus Zugriff auf die IT-Ressourcen und kann das Problem lösen. Es ist nicht notwendig, ihn einfliegen zu lassen und so kostbare Zeit zu verlieren.

- In einer Besprechung hängt eine Entscheidung von einer Information ab. Die Besprechung könnte unterbrochen oder vertagt werden, um die Information zu besorgen. Besser wäre es, online auf die Information zugreifen und den Entscheidungsprozess verkürzen zu können.

Die Voraussetzung für dieses Maß an Flexibilität und Reaktionsgeschwindigkeit ist die Durchdringung aller infrage kommenden Orte, an denen sich der arbeitende Mensch befinden kann, mit einem Netz.

Das allgegenwärtige Netz muss überall dort verfügbar sein, wo sich der Mensch aufhalten mag: in Wohnungen, auf der Straße, in Autos, Flugzeugen, Zügen, Bahnhöfen, Flughäfen, Hotels. An einigen dieser Orte wie in Wohnungen und Hotels kann das Netz drahtgebunden sein. An einigen anderen Orten kommt nur eine drahtlose Verbindung infrage.

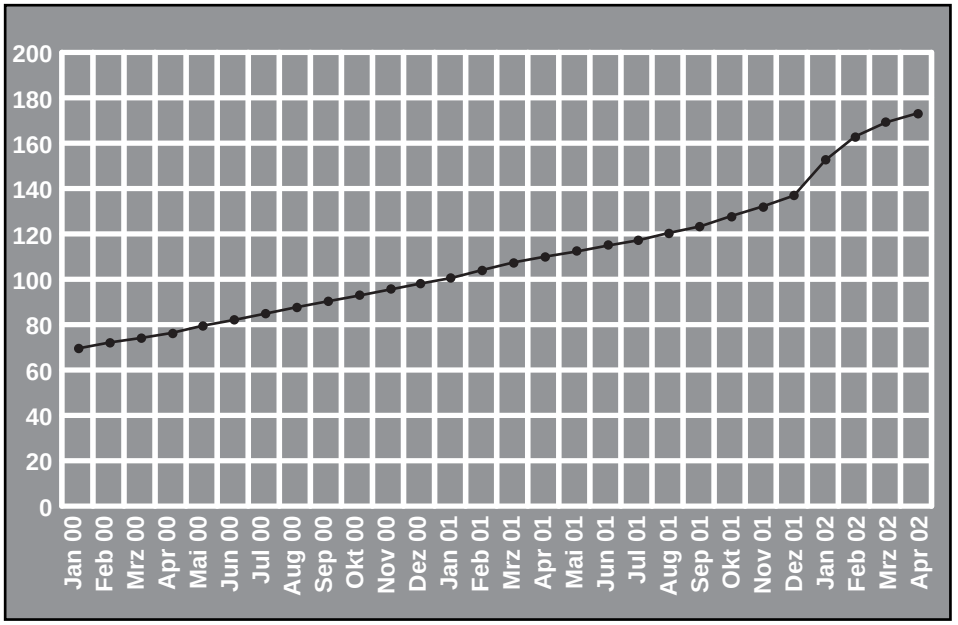


Bild 3: Anzahl der Internet Hosts in Millionen

Die heutige Telekommunikation basiert auf einem solchen allgegenwärtigen Netz. Der Mobilfunk hat den Durchdringungsgrad der Telekommunikation wesentlich erhöht. Zumindest hier in Westeuropa ist man fast überall in der Lage, mithilfe eines streichholzschachtelgroßen Endgerätes wen auch immer auf der Welt anzurufen und von wem auch immer auf der Welt angerufen zu werden. Der Transport der Informationen, die über Sprache übertragen werden können, scheitert nicht mehr am fehlenden Werkzeug hierzu.

Viele Arbeitsplätze kommen allein damit aus. Bei den meisten virtuellen Arbeitsplätzen reicht jedoch die Fähigkeit der mobilen Sprachkommunikation allein nicht aus. Die damit verbundenen Tätigkeiten benötigen Daten und Bilder und erzeugen auch solche. Es wird ein Netz benötigt, welches auch solche Informationen übertragen kann.

Dieses Netz ist schon längst vorhanden. Es ist das Internet. Das Internet ist auf dem Weg, zum allgegenwärtigen Netz zu werden. Dem Internet und allen mit dem Internet verbundenen Technologien wurde mit der Erfindung des World-wide Web zum endgültigen Durchbruch verholfen. Mit dem Web wurde das Internet zum Netz für Jedermann. In der zweiten Hälfte der 90er Jahre nahm die Zahl der an das Internet angeschlossenen Knoten (Internet Hosts) jährlich um ca. 50 % zu. Ca. 200 Millionen Knoten sind inzwischen an das Internet angeschlossen. Die Zahl der Internet-Benutzer wird mit ca. 500 Millionen geschätzt.

Zunächst beschränkte sich die Durchdringung durch das Internet auf Orte, die über terrestrische Leitungen versorgt werden können. Das weltweite Telekommunikationsnetz kann mittlerweile an jedem Ort von jedem PC aus, der mit einem Modem ausgestattet ist, als Trägernetz für das Internet dienen. Allerdings ist die Nutzung des Internet nur dann wirtschaftlich vertretbar, wenn sich nicht weit von dem PC aus ein Point of Presence (PoP) des Internet befindet. Diese Bedingung ist mittlerweile fast in jedem Land der Welt erfüllt, zumindest in den meisten Ländern, die mit einem Telekommunikationsnetz ausgestattet sind. Ein Blick in die Länderliste, die von Internet-Dialern zur Verfügung gestellt wird, zeigt, dass selbst in Ländern wie Tuvalu und Samoa der lokale Internet-Zugang möglich ist. Somit kann sich der Mensch fast überall auf der Welt aufhalten und trotzdem sämtliche durch das Internet ermöglichte Dienste nutzen, wenn die Bandbreitenanforderungen dieser Dienste vor Ort erfüllt sind.

Die Bindung an das Telefonkabel bedeutet jedoch eine wesentliche Einschränkung, einerseits für die nutzbare Bandbreite und andererseits für die Mobilität. Die qualitativ besten Telefonleitungen ermöglichen eine Übertragung mit 56 kbit/s, für viele Anwendungen zu wenig. Aber selbst diese Bitrate wird an den meisten Lokationen nicht annähernd erreicht. Für die Mehrheit der Telefonleitungen weltweit dürften die maximal erreichbaren Werte bei 9600 oder 19200 kbit/s liegen. Außerdem kommt ein drahtgebundener Anschluss auf der Straße, in Autos, Flugzeugen, Zügen, Bahnhöfen und Flughäfen meistens nicht infrage.

Was die Übertragungsrate betrifft, werden bereits seit Jahren breitbandige Internet-Anschlüsse angeboten. Die Flächendeckung solcher Anschlüsse ist noch nicht mit dem Telefonnetz vergleichbar, nähert sich in vielen Regionen der Welt jedoch dem Zustand der lückenlosen Versorgung. Wir in Deutschland profitieren diesbezüglich einerseits von der Bevölkerungsdichte und andererseits von der allgemein als fortgeschritten einzustufenden informationstechnischen Entwicklung hierzulande. So ist es zumindest in allen Ballungszentren des Landes möglich, einen Internet-Anschluss zu nutzen, der hinsichtlich Bitrate um eine Größenordnung leistungsfähiger als die ISDN-Basisrate von 64 kbit/s ist. Dabei handelt es sich meistens um eine Leitung des Typs Digital Subscriber Line (DSL) mit der Download-Rate, die ungefähr beim Zehnfachen der ISDN-Basisrate liegt. Eine weitere Variante ist die Nutzung von Fernsehkabeln für einen Internet-Anschluss, in der Regel mit einer Übertragungsrate, die noch eine Größenordnung höher liegt als die Geschwindigkeit der meisten DSL-Anschlüsse.

Der wichtigste Nachteil dieser Varianten im Vergleich zur Nutzung von Modems und Telefonleitungen liegt darin, dass die Aktivierung eines DSL- und Kabelmodem-Anschlusses nicht ad hoc möglich ist. Die Netzbetreiber brauchen eine sogenannte Provisioning-Zeit, um die genannten breitbandigen Dienste zu aktivieren, während die Anwahl eines Dial-in-PoPs mittels eines Modems von überall und ohne Vorbereitung möglich ist.

Dafür eignen sich DSL und Kabelmodems für viele Anwendungen, die über eine 56- oder 64-kbit-Leitung nicht genutzt werden können. Deshalb sind DSL und Kabelmodem insbesondere für Heimarbeitsplätze (Home Offices) prädestiniert. Dass ein Netzbetreiber in der Regel Wochen für die Aktivierung solcher Dienste benötigt, wird angesichts der immensen Vorteile eines Breitband-Anschlusses akzeptiert. Einige Hotels nutzen ebenfalls solche Anschlussvarianten, um ihren Gästen einen schnelleren Internet-Zugang anbieten zu können als über das Telefonnetz möglich.
Das Problem der fehlenden Mobilität ist allen drahtgebundenen Anschlussvarianten gemeinsam. Dabei sind die Anforderungen an die Mobilität von Datenendgeräten zurzeit noch nicht so hoch wie die Mobilitätsanforderungen von Telefonendgeräten. Ein Mobilfunkbenutzer möchte auch mittels einer Freisprecheinrichtung telefonieren können, wenn er mit 200 km/h auf der Autobahn unterwegs ist. Der Benutzer eines mobilen Internet-Anschlusses hat in der Regel keine solche Anforderung. Er möchte an verschiedenen Orten – auch dort, wo es keine Kabel gibt – vernetzt werden können.

Um diese Anforderung zu erfüllen, sind in den letzten Jahren verschiedene Zweige der Informations- und Telekommunikationsindustrie verschiedene Wege gegangen. Es gibt einerseits die Mobilfunkindustrie, die zurzeit in Form der Generation „2 1/2" und bald in Form der dritten Mobilfunkgeneration die Möglichkeit bietet, über Kanäle, deren Bitrate ungefähr mit der von Modems oder der ISDN-Basisrate vergleichbar sind, Daten auszutauschen. Stichworte sind HSCSD, GPRS und UMTS.

Andererseits erfreuen sich Wireless LAN gemäß dem Standard IEEE 802.11 zunehmender Akzeptanz. Ursprünglich als drahtlose Erweiterung von Local Area Networks (LAN) konzipiert, gelten Wireless LAN mittlerweile als die aussichtsreichste Technologie für die Bildung sogenannter Hot Spots. Ein Hot Spot dient dem Anschluss drahtloser Endgeräte an das Internet und wird an öffentlichen Stellen wie Flughäfen eingerichtet. Das Endgerät ist mit einer Wireless-LAN-Adapterkarte (in der Regel ein PC Card in einem Notebook) ausgestattet. Über diese Karte kommuniziert das Endgerät mit dem von einem Netzbetreiber aufgestellten Wireless LAN Access Point, der den Zugangspunkt zum Netz des Betreibers und darüber zum Internet darstellt.
Verglichen mit den Technologien wie HSCSD, GPRS und UMTS, die von der Mobilfunkindustrie entwickelt worden sind, bieten Wireless LAN eine wesentlich höhere Bitrate, sind jedoch in ihrer räumlichen Reichweite sehr eingeschränkt. Die zurzeit gängige Version von Wireless LAN gemäß der Spezifikation IEEE 802.11b arbeitet mit einer Bitrate von 11 Mbit/s, die allerdings von allen Teilnehmern einer Zelle (des Abdeckungsbereiches eines Access Points) geteilt wird. Ein Standard für eine leistungsfähigere Anschlussvariante ist als die Spezifikation IEEE 802.11a bereits verabschiedet. Diese Variante, die mit der wiederum in der Zelle von allen Teilnehmern geteilten Bitrate von 54 Mbit/s arbeitet, ist in Nordamerika bereits im Einsatz. Die betreffenden Komponenten werden zurzeit zur Lösung des Problems der Überschneidung mit geschützten Frequenzbereichen an die europäischen Vorschriften angepasst. Spätestens mit der Verfügbarkeit dieser Variante stellt die drahtlose Verbindung zwischen dem Endgerät und dem Access Point für die meisten Anwendungen keinen Engpass mehr dar.

Bild 4: Lufthansa wirbt mit Wireless LAN Hot Spots in den eigenen Lounges

Wirtschaftlichkeit

Die Gegenüberstellung von Nutzen und Kosten jeder technischen Lösung muss den Aufwand für die einmalige Beschaffung und den laufenden Betrieb berücksichtigen.

Zur Anbindung eines Arbeitsplatzrechners unabhängig von dessen Standort sind die folgenden Komponenten erforderlich:

- Das Endgerät muss mit den physikalischen Schnittstellen ausgestattet sein, die für den Netzanschluss erforderlich sind. Diese sind je nach infrage kommenden Anschlusstypen ein Ethernet-Port, ein Modem und/oder eine Wireless-LAN-Karte. Bisher mussten diese Schnittstellen in der Regel zusätzlich beschafft und installiert werden. Es gibt jedoch den Trend, dass zumindest Notebooks bereits mit allen diesen Schnittstellen geliefert werden. Langfristig ist davon auszugehen, dass zur Realisierung der technischen Möglichkeit von virtuellen Arbeitsplätzen die Erweiterung der Hardware von Notebooks nicht erforderlich ist. Selbst die für Sprachkommunikation erforderlichen Komponenten wie Mikrofon und Lautsprecher sind in viele Notebooks bereits integriert. Diese Situation stellt sich jedoch bei den kleineren PDA anders da. Um Platz zu sparen und die Kosten für diese Geräte zu minimieren, rüsten die Hersteller dieser Produkte ihre Geräte nicht mit allen der genannten Schnittstellen aus. Dies schränkt die Flexibilität der PDA beim Anschluss an diverse Netztypen ein.

- Was die Software auf den Endgeräten betrifft, gibt es ebenfalls eine ähnliche Situation wie bei der Hardware. Während in die Notebooks in der Regel alle erforderlichen Software-Komponenten für die Realisierung eines virtuellen Arbeitsplatzes integriert sind, ist dies bei PDA nicht der Fall. Neben den für die Herstellung der Netzverbindung erforderlichen Programme wie Dialer ist nämlich eine Client-Software auf dem Endgerät erforderlich, über die sich das Endgerät an ein Virtual Private Network (VPN) anschließen kann. Ein VPN nutzt Verschlüsselungsmechanismen, um eine von anderen Netzen abgeschottete Kommunikationsinfrastruktur auf ein unsicheres Netz wie das Internet abzubilden. Ohne ein VPN erfüllt das Internet keinesfalls die Anforderungen an eine sichere Kommunikation, da das Internet allen Teilnehmern zugänglich ist. Die erforderliche Client-Software für den Anschluss des Endgerätes an ein VPN ist in den aktuellen Betriebssystemen von Microsoft, die für den Einsatz auf Unternehmensrechnern angeboten werden, enthalten und verursacht keine zusätzlichen Lizenzkosten. Dies ist bei den meisten PDA noch nicht der Fall.

- Wenn sich die vom virtuellen Arbeitsplatz aus zu nutzenden Applikationen auf Web-Applikationen beschränken, kommt man auch ohne VPN aus. Jeder Web-Browser bietet heute die Möglichkeit der verschlüsselten Kommunikation mit einem Web-Server mithilfe des Verfahrens Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS). Bei Ausstattung von Browsern und Servern mit starker Verschlüsselung (mittlerweile bei den in Europa gängigen Versionen gegeben) erfolgt die Kommunikation zwischen diesen beiden Endpunkten vertraulich. Ergänzt man diese Funktionalität mit starker Authentifizierung (s. nächsten Abschnitt), sind die Sicherheitsanforderungen der gängigsten Anwendungen erfüllt, ohne dass eine zusätzliche Software-Komponente auf dem Endgerät erforderlich ist.

- Um höhere Sicherheitsanforderungen abzudecken, muss ein VPN- oder Web-Server-Betreiber dafür Sorge tragen, dass bei der Gewährung des Zugriffs von Teilnehmern auf das VPN stärkere Authentifizierungsverfahren als nur die Überprüfung eines Kennworts eingesetzt werden. Das Wissen eines Kennworts ist nämlich duplizierbar und übertragbar, sogar ohne dass der rechtmäßige Benutzer dies mitbekommt. Wenn zusätzlich zu diesem Wissen der Besitz eines Gegenstands zur Authentifizierung erforderlich ist, oder wenn sogenannte biometrische Daten wie Netzhaut-Scans oder Fingerabdrücke zur Feststellung der Identität des Benutzers eingesetzt werden, spricht man von starker Authentifizierung. Die Kombination der Überprüfung der beiden Parameter Wissen und Besitz kann z. B. derart sein, dass eine sogenannte Token-Karte nach Eingabe einer geheimen persönlichen Identifikationsnummer (PIN) eine nur einmalig nutzbare Zahl generiert, die als Zugangs-Code dient. Solche Token-Karten kosten in der Regel ca. 100 Euro. Noch mehr Sicherheit für ungefähr die zwei- bis dreifache Summe bieten die sogenannten Smart Cards, auf denen u. a. die für die Verschlüsselung erforderlichen Parameter (geheime Schlüssel) gespeichert sind und den Vorteil bieten, dass sämtliche kryptografische Operationen statt im PC auf der Smart Card durchgeführt werden. Somit entfällt das Risiko, das durch die Speicherung der geheimen Schlüssel auf den PC entsteht.

- Geht man davon aus, dass die Internet-Infrastruktur einschließlich solcher Komponenten wie Access Points an den Hot Spots von kommerziellen Netzbetreibern zur Verfügung gestellt und mit den Verbindungsgebühren verrechnet werden, braucht der Betreiber eines privaten Netzes, der in dieses Netz auch virtuelle Arbeitsplätze unabhängig von ihrem Standort anbinden will, lediglich an einem oder (z. B. aus Gründen der Ausfallsicherheit) zwei Standorten das erforderliche Equipment für einen Internet-Anschluss zu installieren. Eine solche Installation umfasst bei Web-basierenden Applikationen eine Web-Server-Farm und bei sonstigen Anwendungen eine VPN-Gateway-Farm. Die Kosten für eine solche Serverfarm sind stark von der Applikation und der Zahl der damit zu bedienenden Anwender abhängig. Im Falle eines VPN-Gateways kann man von einem ungefähren Richtwert für eine mittlere Lösung für 100 Benutzer ausgehen, der bei 20.000,00 Euro liegt.

Die Betrachtung der einmaligen Kosten zeigt, dass diese Kosten in den meisten Fällen nur unwesentlich die Kosten für den Betrieb eines Notebooks erhöhen, wenn sie auf die gesamte Nutzungsdauer des Gerätes umgelegt werden. Was die laufenden Kosten für die Internet-Nutzung betrifft, sind diese einerseits sehr stark vom Standort und der Bitrate abhängig und andererseits dem Produktivitätsgewinn gegenüberzustellen, die mit der Lösung erreicht wird. In vielen Fällen rechtfertigt die Effizienzsteigerung die Mehrkosten dafür, dass ein Arbeitsplatz auch dann online bleibt, wenn er weit außerhalb des Unternehmensstandortes ist.

Doch ist das Bild über die Wirtschaftlichkeit von virtuellen Arbeitsplätzen keinesfalls vollständig, wenn man nur den einmaligen Einrichtungsaufwand und die Kosten für die Internet-Nutzung betrachtet. Wie fast jeder Bereich der IT macht auch hier der laufende Support-Aufwand den größten Anteil der Total Cost of Ownership (TCO) aus. Jede technische Lösung für die Virtualisierung von Arbeitsplätzen ist nur dann wirtschaftlich, wenn sie beherrschbar und managebar bleibt. Angesichts der Komplexität von solchen Lösung ist diese Anforderung als keinesfalls einfach einzustufen, zumal die drei Aspekte Flexibilität, Sicherheit und Wirtschaftlichkeit immer in einem Zielkonflikt stehen.

Sicherheit

Bei der Gestaltung von virtuellen Arbeitsplätzen haben sich die beiden Verfahren IPsec-bsierende VPN und die reine Browser-basierende SSL-Nutzung als Methoden zur Realisierung der Sicherheitsziele etabliert. Diese beiden Verfahren sind die beiden zukunftsträchtigen Technologien, mit deren Hilfe eine sichere Kommunikation über unsichere Netze möglich ist. Sie unterscheiden sich dadurch, dass der IPsec-Mechanismus auf der Ebene der Schicht 3 und SSL auf der Ebene der Schicht 4 arbeitet. Während IPsec lediglich eine IP-Connectivity ohne Manipulation der Adressen (also auch ohne Network Address Translation, NAT) voraussetzt, funktioniert SSL nur bei Anwendungen, die auf TCP-Basis arbeiten. Außerdem muss das Session-Layer-Protokoll derart angepasst werden, dass es mit SSL arbeitet. Im Falle von HyterText Transport Protocol (http) ist dies bereits seit Jahren geschehen. Alle HTTP-basierenden Anwendungen können auch HTTPS-, d. h. SSL-basierend arbeiten, wenn einige Anpassungen bei der Web-Seiten-Gestaltung vorgenommen werden. Zwar eignet sich SSL für jede TCP-basierende Anwendung und arbeitet auch bei Anwendung von NAT, aber bisher gibt es kaum SSL-Anwendungen außer im Web-Bereich.

Genau dieser Umstand ist die Daseinsberechtigung von IPsec. Weil nicht alle Anwendungen im Unternehmen kurzfristig auf Web-basierende Verfahren umgestellt werden können, braucht man noch ein Verfahren, bei dessen Anwendung man an der Applikation nichts zu verändern braucht. Ein solches Verfahren muss für die Applikation transparent bleiben, d. h. auf der Netzebene arbeiten. Bis auf die Restriktion, dass eine Ende-zu-Ende-Connectivity ohne NAT existieren muss, erfüllt IPsec diese letztere Anforderung. So hat sich IPsec in vielen Unternehmen zu dem universellen Verfahren entwickelt, mit dessen Hilfe sichere Kommunikation über unsichere Medien realisiert wird. Die unsicheren Medien können das Internet oder Wireless LAN sein. Unabhängig davon, welche Netzverbindung der Client nutzt, sorgt der VPN-Tunnel mit starker Verschlüsselung dafür, dass ein sehr wirksamer Schutz für die übertragenen Daten und die angeschlossenen Systeme sichergestellt wird. Der VPN-Client ist Standard-Bestandteil der Betriebssysteme Windows 2000 und Windows XP. Lediglich auf der Seite des Unternehmensnetzes muss ein dedizierter VPN-Tunnel-Gateway aufgestellt werden. Hinzu kommen sicherlich die Aufwände für die Administration von Benutzern und Zertifikaten sowie sicherheitsrelevante Aufgaben wie Log-Auswertung. Aber diese Aufwände fallen zum Teil sowohl bei IPsec- als auch bei SSL-basierenden Verfahren an.

VPN als Universallösung

Ein Virtual Private Network ist, wie aus der Bezeichnung hervorgeht, virtuell in dem Sinne, dass sich in Wirklichkeit mehrere virtuelle Netze ein physikalisches Netz teilen, und privat, da die verschiedenen privaten Netze gegeneinander abgeschottet sind. Somit stellt sich ein VPN für jeden Nutzer als eine exklusive Infrastruktur dar, quasi wie ein Netz, das aus eigenen physikalischen Leitungen (Fest- und Wählverbindungen) besteht.

Die Motivation für die Virtualisierung des Netzes als Ersatz für eigene Leitungen besteht vor allem in der Vermeidung der hohen Leitungskosten, die mit einem eigenen Netz verbunden wären. Aber auch die Vermeidung der Abhängigkeit von einem einzigen Provider kann bei der Nutzung einer VPN-Lösung eine Rolle spielen. Wenn die VPN-Technik von dem darunter liegenden Leitungsnetz unabhängig ist, kann man unter Beibehaltung der VPN-Architektur die physikalische Netzstruktur beliebig austauschen. Der administrative Aufwand für den Betrieb des physikalischen Netzes wird dadurch reduziert, dass ein Provider diesen Aufwand gleich für viele Kunden betreibt. So entstehen Synergieeffekte. Zugleich ist jeder der Kunden insoweit flexibel, dass er die Netz-Services auf dem freien Markt beschaffen kann.

Folgende drei Kategorien von Verfahren für die Bildung von VPN sind zu unterscheiden:

- VPN über Layer-2-Netze wie ATM und Frame Relay
- VPN auf der Basis eines IP-Netzes unter Anwendung von Multiprotocol Label Switching (MPLS)
- VPN über IPsec

Der wichtigste Vorteil von Layer-2-VPN liegt darin, dass es sich dabei um eine konventionelle, stabile Technik handelt. Zahlreiche Layer-2-VPN sind weltweit im Betrieb. Diese VPN-Variante ist jedoch in der Regel mit hohen Kosten verbunden, die durch den administrativen Aufwand für die Administration des Layer-2-Netzes, die Konfiguration der virtuellen Verbindungen und das Management des IP-Netzes, verursacht werden. Es handelt sich dabei um verschiedene, entkoppelte Technologien, die in der Regel von den Providern separat administriert werden.

Einmalige Sonderveranstaltung

Umstellung von Token Ring auf Ethernet – Projekterfahrungen

Am 30. Juni 2003 veranstaltet die ComConsult Akademie im Hilton Bonn die einmalige Sonderveranstaltung „Umstellung von Token Ring auf Ethernet: Projekterfahrungen“ für alle IT-Verantwortlichen in Unternehmen und Organisationen, die noch Token Ring einsetzen.

Die lokalen IT-Netze vieler Institutionen wie Sparkassen, Banken und Verwaltungen basieren immer noch auf Token Ring. Für diese Anwender wird es höchste Zeit, die Umstellung von Token Ring auf Ethernet vorzunehmen. Die jahrelang geltende Feststellung, dass man sich in guter Gesellschaft befinde und eine Netztechnik einsetze, die in vielen Branchen dominiere, gilt nicht mehr. Die überwiegende Mehrheit der Token-Ring-Anwender hat dieser Technik bei sich selbst bereits einen endgültigen Schlusspunkt gesetzt. Der jahrzehntelang führende IT-Hersteller IBM hat Anfang des neuen Jahrtausends sang- und klanglos als Netzhersteller abgedankt und die Token-Ring-Anwender mit den Problemen allein gelassen. Mit Madge ist nur ein einziger Token-Ring-Hersteller übrig geblieben. Es ist nur noch eine Frage der Zeit, wann sich das Engagement in diesem schrumpfenden Markt auch für diesen einzigen Hersteller wirtschaftlich nicht mehr rentieren wird. Die Token-Ring-Anwender kämpfen zunehmend mit dem Problem, dass seitens der Hersteller die Unterstützung für Token-Ring-orientierte Produkte (Hardware wie Software) aufgekündigt wird. Zusätzlich ist das Problem entstanden, dass die Entwicklung von Token Ring bei 100 Mbit/s stehen geblieben ist. Der Aufbau von leistungsfähigen Serverfarmen ist bei dieser Leistungsobergrenze nicht mehr möglich.

Die Umstellung von Token Ring auf Ethernet ist keineswegs nur ein Austausch von Netzkarten und Netzkomponenten, da sich die beiden Techniken Token Ring und Ethernet grundlegend unterscheiden und der Wechsel zwangsläufig auch mit Änderungen der Netzarchitektur verbunden ist.

Der Referent Dr. Behrooz Moayeri von der ComConsult Beratung und Planung lässt die Teilnehmer profitieren von den Erfahrungen, die das in Deutschland führende herstellerunabhängige Consulting-Unternehmen im Bereich IT-Infrastruktur in den letzten fünf Jahren bei den zahlreichen Migrationsprojekten Token-Ring/Ethernet gewonnen hat.

Die Inhalte

- Neues Netzdesign – Konsequenzen aus dem Untergang von Token Ring: Zukunftssicherheit durch Verfahren, die weitestgehend standardisiert sind und von möglichst vielen konkurrierenden Herstellern unterstützt werden
- Ausschließlicher Einsatz des Internet Protocol (IP): Was geschieht mit SNA?
- Hochverfügbare Netzinfrastruktur für Serverfarmen, u. a. für den IBM Mainframe
- Schwierigkeiten in der Übergangsphase: Probleme beim Translational Bridging von Token Ring zu Ethernet etc.
- Ist die Typ-1-Verkabelung Ethernet-tauglich?

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Sonderveranstaltung

☐ Ich buche die Sonderveranstaltung
Umstellung von Token Ring auf Ethernet – Projekterfahrungen
am 30.06.03 in Bonn
(Preis € 398,-- zzgl. MwSt.)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ, Ort
eMail	Unterschrift

Auf dem Weg zum virtuellen Arbeitsplatz

Hohe Anforderungen an die Quality of Service (QoS) können von Layer-2-VPN in der Regel gut erfüllt werden, allerdings durch erhöhten administrativen Aufwand unter Nutzung der ggf. vorhandenen Layer-2-Mechanismen. Layer-2-VPN implementieren keinen Schutz der Vertraulichkeit der übertragenen Daten durch Verschlüsselung. Die Abschottung der privaten Netze gegeneinander ist von der Sicherheit des schwächsten Gliedes im physikalischen Netz abhängig (das z. B. eine nicht ausreichend geschützte Komponente sein kann). Da es sich bei den Nutzern der VPN Services um namentlich bekannte, geschlossene Benutzergruppen handelt, ist dieses Sicherheitsniveau für die meisten Nutzer ausreichend.

IPsec-VPN basieren auf der Nutzung des Internet, das allgegenwärtig und relativ preiswert zu nutzen ist. Oft trifft man auf eine Kombination des VPN mit dem Internetzugang, der ohnehin in meisten Unternehmen an allen Standorten benötigt wird. Als der größte Nachteil von IPsec-VPN wird häufig angeführt, dass keine QoS realisierbar ist und die Restrisiken der Internetnutzung trotz des Einsatzes starker Verschlüsselung hingenommen werden müssen, vor allem der Umstand, dass die Verfügbarkeit des VPN von keiner Instanz gewährleistet werden kann.

Trotz dieser Nachteile sind bereits die Einsatzszenarien von IPsec-VPN vielfältig, von Teleworking und Mobile Computing bis hin zum Ersatz für teure Leitungen von Providern. Allein die Reduzierung der Abhängigkeit von einzelnen Providern stellt oft eine Motivation dar, IPsec- und Internetbasierende VPN aufzubauen. Man denke an die Risiken der Worldcom-Insolvenz für die Kunden.

Diese vielfältigen Einsatzszenarien haben bereits dazu geführt, dass sich IPsec-VPN sehr schnell ausbreiten, manchmal schneller, als manchem IT Manager recht wäre. Denn die schnelle Implementierung einer IT-Lösung ist bisher immer mit Lösungen einher gegangen, die sich langfristig als unbeherrschbar und zu kostspielig im Betrieb erwiesen haben. Provisorien, die zu permanenten Lösungen werden, treiben in der Regel das IT-Budget dadurch in die Höhe, dass sie entweder mit einem permanent hohen Betriebsaufwand oder mit einem unvertretbaren Sicherheitsrisiko verbunden sind.

Da jedoch der Druck seitens der Anwender wächst, die in den Genuss der genannten Vorteile der Virtualisierung der Arbeitsplätze kommen wollen, können die IT Manager diesen Trend nicht aufhalten. Wenn sie nichts tun, droht die IT-Sicherheit angesichts der verlockenden Flexibilität von IP-VPN ins Hintertreffen zu geraten.

Die wichtigsten Herausforderungen im Zusammenhang mit der Implementierung und dem Betrieb von IPsec-VPN sind:

- Benutzerverwaltung
- Schlüsselverwaltung
- Zertifikatsverwaltung
- Client Management
- Management von Personal Firewalls

Dies alles muss bei gleichzeitiger Einbindung in die unternehmensweite Verzeichnisstruktur bewerkstelligt werden.

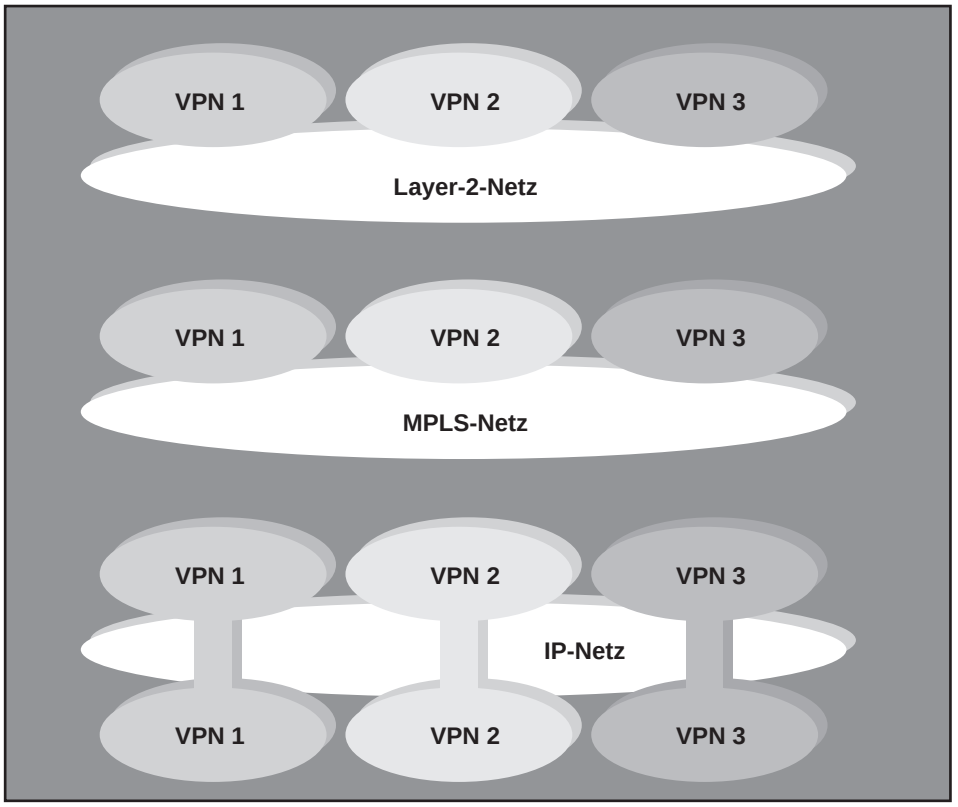
Nun bietet Microsoft seit der Einführung von Windows 2000 und Active Directory eine VPN-Lösung, welche den oben genannten Herausforderungen in einer homogenen Lösung gerecht wird. Heißt die Schlussfolgerung daraus, dass man für das IPsec-VPN eine Microsoft-Lösung einsetze, und alle Probleme werden damit gelöst?

Die Realität sieht komplexer aus, als dass eine solche einfache Antwort alle Probleme lösen würde. In vielen Unternehmen gibt es außer Microsoft-Produkten auch andere IT-Bereiche, die auch von der VPN-Lösung profitieren müssen. Außerdem ist die Frage angebracht, ob die Performance und Sicherheit reiner Software-VPN-Lösungen wie der Microsoft-Lösung für alle Einsatzszenarien ausreiche. Die Einbindung vieler Appliances, Smart Cards und sonstiger Nicht-Microsoft-Produkte in das Management ist ebenfalls nicht trivial.

Darüber hinaus gibt es viele offene Fragen und Alternativen, die selbst mit einer reinrassigen Microsoftlösung verbunden sind, z. B.:

- Sind bei den Clients Personal Firewalls erforderlich, um den Internet-Zugang des Clients, der für den VPN-Tunnel genutzt werden muss, gegenüber Angriffen abzusichern? Wenn ja, was sind die Kriterien für die Auswahl einer Personal-Firewall-Lösung? Wie werden die Personal Firewalls auf den Clients zentral administriert und überwacht?
- Wo wird der VPN-Tunnel-Gateway platziert: im Internet, im internen Netz oder in der Demilitarisierten Zone (DMZ)?

Bild 5: Verschiedene VPN-Modelle



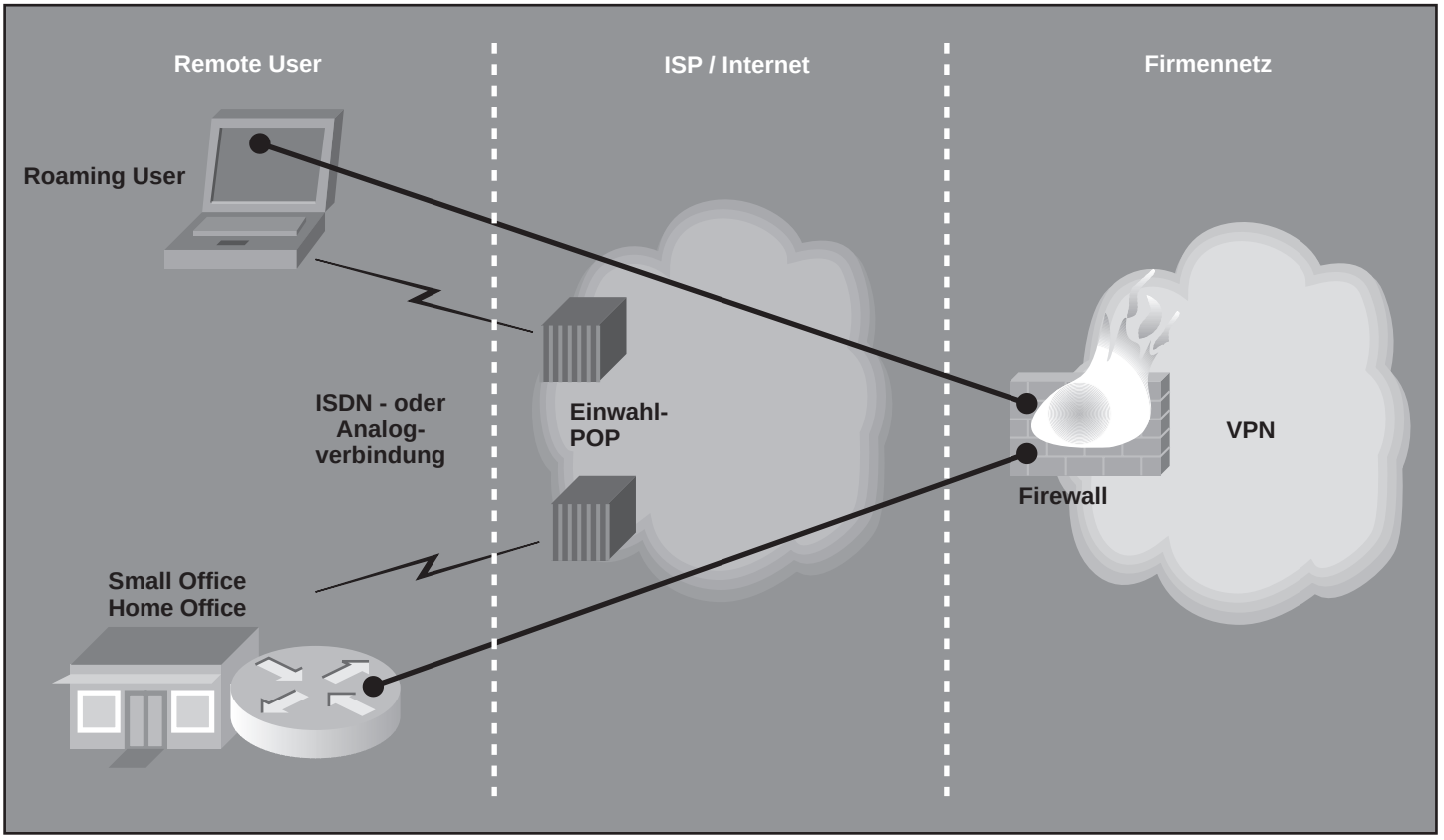


Bild 6: Einsatz von IPsec VPN

- Vertragen sich Network Address Translation (NAT) und die VPN-Lösung? Braucht man unbedingt eine VPN-Lösung, die auch bei modizierten IP-Adressen im Trägernetz funktioniert, wenn z. B. über NAT-Grenzen hinweg VPN-Tunnels aufzubauen sind?

- Können alternativ zur Microsoft-Lösung nicht vorhandene Firewall-Strukturen genutzt werden, um VPN aufzubauen? Was sind die Vor- und Nachteile der verschiedenen Lösungen?

- Wie führt man diverse Benutzerverwaltungen in verschiedenen Betriebssystem-, Firewall- und VPN-Lösungen zusammen?

Eine für alle Unternehmen gültige Antwort auf diese Fragen kann nicht gegeben werden. Je nach dem, welche Kriterien für das Unternehmen wichtig sind, sieht die Lösung anders aus.

Zum Beispiel kann eine harte Anforderung nach Unterstützung von NAT dazu führen, dass die reine Microsoft-Lösung ohne Modifikation nicht zum Tragen kommen kann.

Auf dem Weg zum virtuellen Arbeitsplatz

Die Herausforderungen beim Betrieb sind mindestens genauso ernst zu nehmen wie die Implementierung. Bereits in der Phase der Implementierung muss man an die Betriebsanforderungen denken. Wichtig für die Positionierung des Tunnel-Gateways sind z. B. auch Monitoring-Aspekte. Wenn man den VPN-Tunnel-Gateway am zentralen Standort im internen Netz positioniert, hat dies den Vorteil, dass keine umfangreiche Anpassung der Firewall-Regeln erforderlich ist, da der Tunnel bis zum internen Netz durchgereicht und lediglich die für die VPN-Nutzung erforderlichen Ports auf der Firewall geöffnet werden müssen. Der Nachteil dieser Lösung besteht darin, dass im verschlüsselten Tunnel keine Monitoring-Möglichkeit gegeben ist. Dieser Tunnel endet im internen Netz, d. h. auf der Firewall kann keinerlei Überwachung und Logging des VPN-Verkehrs vorgenommen werden. Angesichts der Tatsache, dass es sich immerhin um Kommunikationsbeziehungen aus dem offenen Internet handelt, ist die fehlende Möglichkeit der Überwachung ein Sicherheitsnachteil.

Die Positionierung des VPN-Tunnel-Gateways im externen Netz wäre mit dem Nachteil verbunden, dass viele Sicherheitslücken durch die zu öffnenden Kanäle auf der Firewall entstehen würden.

Aus diesen Gründen stellt sich eine Positionierung in der DMZ als die beste Lösung dar. Ein Satz von Firewall-Regeln muss dafür sorgen, dass die Kommunikation aus dem Internet unter Nutzung der VPN-spezifischen Ports nur mit dem Gateway möglich ist, und der zweite Regelsatz dient dazu, den ungetunnelten Verkehr des Gateways mit dem internen Netz zu steuern. Die Kommunikationsbeziehungen, die diesem Regelsatz unterliegen, können überwacht werden. Sonstige Firewall-Regeln wie das Blocken bestimmter Protokolle können auf den letzteren Kanal angewandt werden.

Eine besondere Herausforderung stellt die Analyse der Kommunikationsbeziehungen im VPN-Tunnel dar, die z. B. für Fehlersuche erforderlich werden kann. Eine solche Analyse ist mit dem Einsatz herkömmlicher Werkzeuge wie Protokollanalysatoren nicht ohne Weiteres möglich, da es sich um eine verschlüsselte Kommunikation handelt. Daher muss eine Überwachungskonsole auf dem VPN-Tunnel-Gateway mindestens alle aktiven VPN-Verbindungen anzeigen und möglichst auch die Analyse der darüber ausgetauschten Pakete erlauben. Dies ist eine wichtige Anforderung an den VPN-Tunnel-Gateway.

Darüber hinaus muss der VPN-Tunnel-Gateway in ein Ereignis-Management integriert sein. Gerade das Ereignis-Management ist nicht eine besondere Stärke der reinen Microsoft-Lösung. Der in Windows eingebaute Ereignis-Manager generiert zu viele Meldungen, darunter auch Meldungen mit geringer Aussagekraft wie z. B. „Fehler Nr. ... ist eingetreten".

Die Überwachung und Log-Auswertung kann ein entscheidendes Auswahlkriterium für die VPN-Lösung sein.

Sicherheitsrelevante Ereignisse im Zusammenhang mit der VPN-Lösung sind wie alle anderen Ereignisse an eine zentrale Konsole zu übermitteln. Von dort aus können nach einer Filterung die Ereignisse dem Sicherheits-Monitoring weitergeleitet werden.

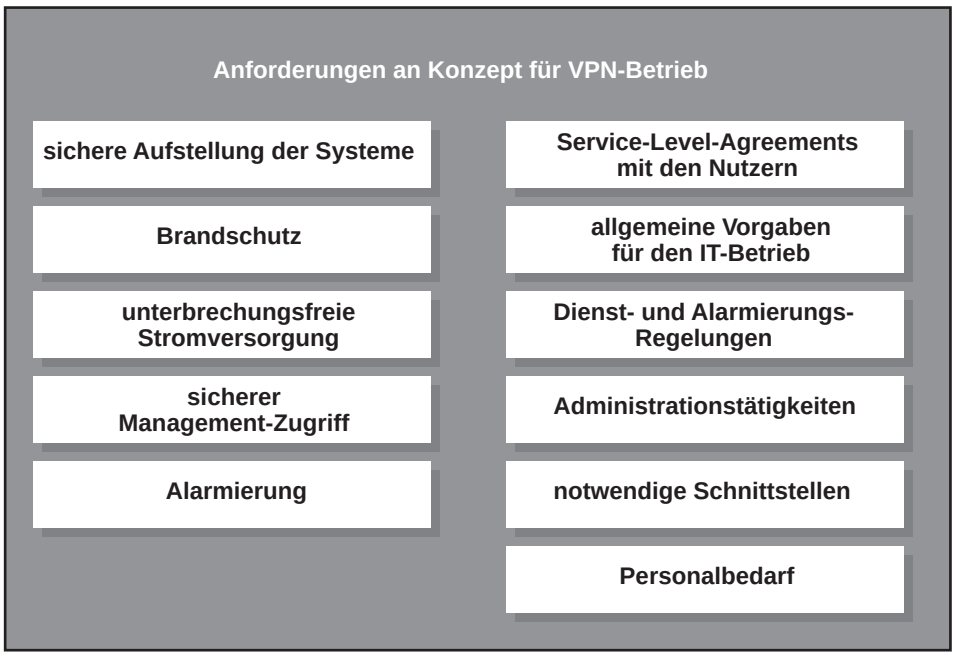
Allein diese Fragen, die nur einen Teil der relevanten Problemstellungen ausmachen, zeigen, dass für den erfolgreichen und effizienten Betrieb einer VPN-Lösung die Erarbeitung eines Betriebskonzeptes unerlässlich ist. Die Grundlagen des Betriebskonzepts sind die unternehmensweite Sicherheitspolitik und das Sicherheitskonzept, die alle schützenswerten Ressourcen und Daten festlegen, die potenziellen Bedrohungen aufzeigen und berücksichtigen, welche Dienste zur Verfügung zu stellen sind. Um den Schutz der Daten und Ressourcen sicherzustellen, muss man eine Entscheidung darüber treffen, welche Sicherheitsmechanismen einzusetzen sind. Somit sind die Realisierung und der Betrieb eines VPN ein weiterer Baustein in der Umsetzung des IT-Sicherheitskonzepts. Die Auswahl der VPN-Architektur muss entsprechend den Anforderungen der Sicherheitspolitik erfolgen, und auch der Kriterien-Katalog und die Auswahl eines passenden Produkts muss auf der Basis der Anforderungen der Sicherheitspolitik vorgenommen werden.

Neben der Festlegung der Sicherheitsmechanismen trägt die sichere Installation und die Konfiguration der geforderten Dienste entscheidend zur Sicherheit der VPN-Lösung bei.

Das Konzept für den VPN-Betrieb muss die externen Anforderungen wie z. B. die der die Lösung nutzenden Fachabteilungen neben den internen Anforderungen für einen sicheren Betrieb berücksichtigen. Dazu zählt die Festlegung der Dienst- und Alarmierungs-Regelungen (Tagesdienst, Bereitschaft), der Administrationstätigkeiten, der notwendigen Schnittstellen und des Personalbedarfs mit Angabe des Skill-Levels.

Externe Anforderungen umfassen z. B. Service-Level-Agreements (SLA) mit den Nutzern und allgemeine Vorgaben für den IT-Betrieb.

Interne Anforderungen decken solche Fragen wie die sichere Aufstellung der Systeme, z. B. in Serverräumen mit Zugangskontrolle, den Brandschutz, die unterbrechungsfreie Stromversorgung, den sicheren Management-Zugriff und die Alarmierung ab.



Verwaltung von Schlüsseln, Signaturen und Zertifikaten

Das am weitesten verbreitete Verfahren für die zentrale Verwaltung von Schlüsseln, die für den Betrieb einer VPN-Lösung unerlässlich ist, basiert auf Zertifikaten. In einem Zertifikat ist der öffentliche Schlüssel der Instanz, zu der das Zertifikat gehört (z. B. eines Clients oder eines Benutzers), enthalten, signiert von einer Zertifizierungsstelle, zu der alle potenziellen Kommunikationspartner direkt oder indirekt eine Vertrauensstellung haben. Nicht nur die Ausstellung von Zertifikaten, sondern auch deren Annullierung muss möglich sein. Letzteres ist zum Beispiel dann dringend notwendig, wenn man von der Kompromittierung des zum Zertifikat gehörenden privaten Schlüssels ausgeht.

Dies sind die Aufgaben einer PKI („Public Key Infrastructure"), die sämtliche Bereiche des Schlüsselmanagements wie Schlüsselerstellung, Schlüsselverteilung und Schlüsselsperrung abdecken und die kryptografischen Dienste zur Abbildung des Schlüsselmanagements auf eine Client-/Server-Struktur anbieten soll. Der ITU-Standard X.509 v3 ist der aktuelle Standard für Zertifikate.

Der Aufbau einer PKI soll es erlauben, solche und andere anfallende Probleme bei der Verwaltung der Zertifikate und Schlüssel zu lösen. Beim Aufbau einer PKI ist es unbedingt notwendig, alle zukünftigen Einsatzgebiete von Verschlüsselungsverfahren mit zu berücksichtigen. Die Entstehung von mehreren Insel-PKI-Lösungen ist zu vermeiden.

Man kann davon ausgehen, dass in Zukunft die Zertifikatverwaltung nicht mehr von der Benutzerverwaltung zu trennen sein wird. Die Zeiten, in denen Schlüssel nur für eine kleine Untermenge der Benutzer zu verwalten waren, sind endgültig vorbei. Heute werden Public-Key-Verfahren nicht nur für VPN, sondern auch für eine Reihe anderer Mechanismen wie die Verschlüsselung der Daten auf Notebooks eingesetzt, die als unverzichtbarer Bestandteil für die Sicherheit von virtuellen Arbeitsplätzen gilt.

Somit müssen die organisatorischen Prozesse für das Anlegen neuer Benutzer, das Löschen der nicht mehr gebrauchten Konten etc. neu definiert werden. Bei jedem neuen Benutzer muss an die Generierung des Zertifikats gedacht werden. Die Verwaltung von Zertifikaten ist die einzige Chance, die Schlüsselverwaltung sicher und trotzdem handhabbar zu gestalten.

Die praktischen Erfahrungen aus dem bisherigen Umgang mit IPsec-VPN und deren Implementierung können helfen, die Phasen der Realisierung und des Betriebs effizienter zu gestalten. Im Folgenden wird auf einige dieser Erfahrungen eingegangen:

- Wenn die VPN-Lösung nicht nur Site-to-Site-, sondern auch Client-to-Site-Kommunikation abdecken soll, muss sie einen zugehörigen VPN-Client umfassen. Entweder kann man die Festlegung treffen, dass der von Microsoft mit den Betriebssystemen Windows 2000 bzw. Windows XP zur Verfügung gestellte Client verwendet wird was mit einigen Einschränkungen wie z. B. der fehlenden NAT-Unterstützung einhergehen würde, oder man kann sich für einen VPN-Client eines anderen Herstellers entscheiden. Dabei ist zu berücksichtigen, dass manche VPN-Clients tief in das System eingreifen und daher in vielen Fällen Änderungen der Hardware-Konfiguration und/oder eine Neuinstallation des VPN-Clients erforderlich machen. Generell kann man davon ausgehen, dass die Entscheidung für einen Non-Microsoft-Client zwar einige Einschränkungen des Microsoft-Clients umgeht, jedoch immer mit dem Problem verbunden ist, dass die kombinierte Gesamtlösung auf dem Client von zwei Herstellern stammt. Das Risiko, dass z. B. Updates des Betriebssystems aufgrund der fehlenden Unterstützung durch den VPN-Client-Hersteller blockiert werden, darf nicht unterschätzt werden. Außerdem ist der Zusatz-Client immer mit Zusatzkosten verbunden, sei es in der Beschaffung oder auch beim Support, der sich für alle Beteiligten als sehr kostspielig darstellen kann. Es ist immer eine gute Idee, die Domäne der so nah um das Betriebssystem angesiedelten Software-Komponenten möglichst dem Betriebssystemhersteller zu überlassen.

- Die Wiederherstellung der VPN-Verbindung muss für den Endbenutzer auf einfache Weise möglich sein, am besten durch Doppelklick auf einem Desktop-Objekt. Darauf ist bei der Auswahl und der Konfiguration des VPN-Clients zu achten.

- Die Funktion Netz-Browsing, die häufig in Microsoft-Windows-Umgebungen an einem Standort verwendet wird sollte aufgrund des damit verbundenen Overheads nicht freigeschaltet werden. Alternative Verfahren sind einzurichten, z. B. eine feste Zuordnung von Laufwerk-Mappings bei Aktivierung der VPN-Verbindung durch eine Batch-Datei.

- Für die Abbildung von Namen auf IP-Adressen ist die DNS-Auflösung statt WINS zu verwenden. Mit dieser Maßnahme und der Nichtnutzung von Browsing vermeidet man die Freischaltung von gefährlichen UDP-basierenden NetBIOS-Ports auf Firewalls.

- Wenn der Provider NAT verwendet, ist eine VPN-Lösung, die auf dem bisherigen IPsec-Standard basiert, nicht einsetzbar. Proprietäre Abhilfen einiger kleiner Hersteller (z. B. ashleylaurent.com) oder proprietäre Clients von VPN-Herstellern wie Cisco sind als Ausweg geeignet.

- Da einige IP-Netze IP-Fragmentierung durchführen, ist bei Nutzung solcher Netze zu klären, ob die ausgewählte VPN-Lösung eine Fragmentierung unterstützt.

- Zur Sicherstellung der Verfügbarkeit auch bei Ausfall eines VPN-Tunnel-Gateways können VPN-Gateway-Cluster wie z. B. der IP Cluster von Nokia eingesetzt werden. Außerdem sind relevante Fragen im Zusammenhang mit der Ausfallsicherheit wie z. B. Wartungsvertrag und Reservebevorratung am zentralen Standort frühzeitig zu klären. Den zentralen VPN Gateways kommt eine große Bedeutung zu, da alle VPN-Nutzer über diese Komponenten kommunizieren.

- Wenn die Administration des ganzen VPN von einem zentralen Standort aus erfolgen soll, müssen die entsprechenden Verfahren einschließlich der starken Authentifizierung beim Zugriff auf die VPN-Komponenten vorgesehen werden.

- Die zentralen VPN Gateways stellen kritische Infrastrukturkomponenten dar, die physikalisch zu schützen sind. Die Aufstellung im geschützten Rechenzentrum oder Technikraum sowie speziellem Schrank, die Zugangsbeschränkung aufBetriebspersonal, eine Zugriffsbeschränkung über möglichst sichere Identifikationsmethode (Token Card, Smart Card) und eine starke Kennwortrichtlinie sind vonnöten. Ferner kann vorgesehen werden, dass die Aktivierung der remote-Zugriffsmöglichkeit nur bei Bedarf erfolgt. Diese Möglichkeit (Modemverbindung etc.) muss regelmäßig getestet werden (mindestens einmal im Monat). Nach dem Test ist die Verbindung wieder zu deaktivieren.

- Alle notwendigen Kennwörter sind sicher zu hinterlegen, um im Notfall auch bei Abwesenheit des regelmäßig zuständigen Personals Eingriffe vornehmen (lassen) zu können. Alle diesbezüglichen Parameter sind kontinuierlich nachzupflegen (Beispiel: regelmäßige Kennwortänderungen). Es ist sicherzustellen, dass solche Eingriffe nur autorisiert und nachvollziehbar vorgenommen werden können (Beispiel: Hinterlegung der Administratorkennwörter oder Tokens in versiegeltem Umschlag).

Betriebskonzept

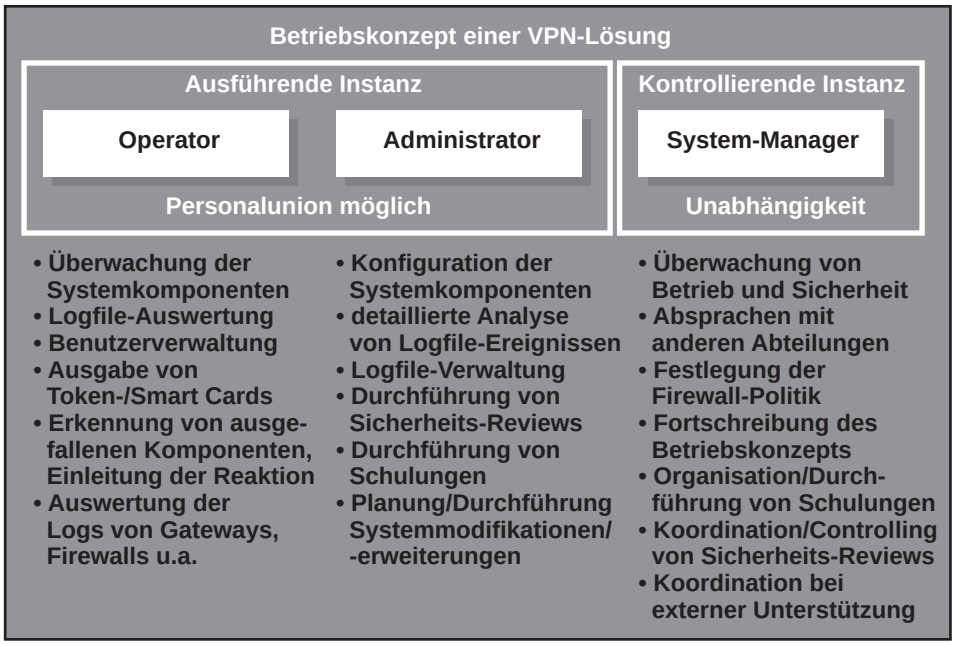
Der Betrieb einer VPN-Lösung muss angesichts der relativ komplexen Architektur und der sicherheitsrelevanten Funktionalität im Rahmen eines Betriebskonzeptes geplant werden. Es empfiehlt sich, folgende Rollen beim Betrieb der VPN-Lösung vorzusehen:

- Operator: Diese Instanz ist für die Überwachung der Systemkomponenten, die regelmäßige Logfile-Auswertung und die Benutzerverwaltung zuständig. Laufende Arbeiten wie die Ausgabe von Token- und Smart Cards, Erkennung von ausgefallenen Komponenten und Einleitung der Reaktion auf solche Ausfälle sowie die durch technische Hilfsmittel unterstützte tägliche Auswertung der Logs der involvierten Komponenten wie Gateways und Firewalls fällt unter die Operator-Zuständigkeit

- Administrator: Der Administrator ist für die Konfiguration der Systemkomponenten, die detaillierte Analyse von Logfile-Ereignissen bei Bedarf und regelmäßig (z. B. auf wöchentlicher Basis), die Logfile-Verwaltung, die Durchführung von Sicherheits-Reviews, Durchführung von Schulungen sowie die Planung und Durchführung von Systemmodifikationen und -erweiterungen zuständig. Operator und Administrator können in kleineren bis mittleren Umgebungen auch durch Mitarbeiter in Personalunion abgebildet werden. In der Regel jedoch müssen unterschiedliche Berechtigungen für Operatoren und Administratoren im System vorgesehen werden.

- System-Manager: Diese Instanz ist für die Überwachung des Betriebs und der Sicherheit (Audit), Absprachen mit anderen Abteilungen, die Festlegung der Firewall-Politik in Abstimmung mit den Firewall-Managern weiterer Administrationsstandorte, die Fortschreibung des Betriebskonzepts, die Organisation und ggf. Durchführung von Schulungen, Koordination und Controlling von Sicherheits-Reviews und Koordination bei Einbeziehung von externer Unterstützungsleistung verantwortlich. Der System-Manager darf nicht in Personalunion die Rolle(n) von Operator und/oder Administrator wahrnehmen, damit die Unabhängigkeit der kontrollierenden von der ausführenden Instanz gewahrt bleibt.

Das Betriebspersonal ist mit entsprechenden Schulungen auf die Wahrnehmung dieser Aufgaben vorzubereiten. Während Administratoren in der Regel eine Schulung durch den Hersteller oder ein qualifiziertes Schulungsinstitut vor Aufnahme ihrer Tätigkeit und bei Release-Wechseln benötigen und darüber hinaus regelmäßig (am besten täglich) gängige Mailing-Listen studieren müssen, kommen Operatoren meistens mit einer Einweisung durch den Administrator oder den Manager bei Aufnahme der Tätigkeit und weiteren Einweisungen bei geänderten Rahmenbedingungen aus. Wöchentliche Informationen für die Operatoren, die aus den Mailing-Listen durch den Administrator zusammengefasst werden, sind ebenfalls sinnvoll. Allen Mitarbeitern muss die Möglichkeit der kontinuierliche Weiterbildung durch Fachzeitschriften, Fachseminare etc. eingeräumt werden.



Das Betriebskonzept muss Regelungen für die automatische Alarmierung vorsehen. Eine solche Alarmierung muss bei Bedarf und technischer Machbarkeit für entsprechend zu definierende Einsatzzwecke und -bereiche erfolgen. Die manuelle Alarmierung, d. h. die gegenseitige Benachrichtigung von Mitarbeitern bei bestimmten Ereignissen, ist insbesondere in folgenden Fällen sinnvoll:

- Operator an Administrator bei Verdacht auf Angriff oder Störung

- Administrator an Manager bei Maßnahmen in Form von Konfigurationsänderungen

- Administrator an Manager bei Verdacht auf erfolgreiche Angriffe

Folgen für das Client-Management

Das Management von Client-Rechnern, die vom Standort des Administrators nur noch über VPN zu erreichen ist, stellt eine besondere Herausforderung dar. Ein entsprechendes Konzept muss erarbeitet werden, das u. a. die Festlegungen in diesen Bereichen beinhaltet:

- Personal Firewalls auf den Clients müssen dafür sorgen, dass der Internetanschluss der Clients nur dem Aufbau der VPN-Verbindung dient und keine ungeschützte Kommunikation des Clients mit dem Internet möglich ist. Die Regeln für diese Personal Firewalls müssen zentral gepflegt und konfiguriert werden. Dazu sind Personal Firewalls auszuwählen, die über eine zugehörige zentrale Serverlösung eine zentrale Administration erlauben. Das Regelwerk für die Firewalls ist zu testen, damit sowohl die Funktionalität der Clients als auch deren Sicherheit gewährleistet wird.

- Beim Virenschutz auf den Clients ist darauf zu achten, dass regelmäßige Updates auch für die VPN Clients möglich bleiben.

- Die Netzeinstellungen der VPN-Clients müssen getestet und standardisiert werden. Dies umfasst vor allem Aspekte der Adressverwaltung und der Namensauflösung.

Somit müssen einige Bereiche des Client-Managements in Anbetracht der VPN-Lösung vollständig überdacht werden.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
- **21.07. - 25.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**

TCP/IP und SNMP
- **21.07. - 25.07.03 in Berlin**
- **22.09. - 26.09.03 in Berlin**

Internetworking
- **30.06. - 04.07.03 in Aachen**
- **06.10. - 10.10.03 in Aachen**

Ethernet Technologien
- **30.06. - 04.07.03 in Aachen**
- **15.09. - 19.09.03 in Aachen**

Paketpreis für alle vier Seminare:
€ 6.690,-- zzgl. MwSt.
(Einzelpreise: € 1.990,-- bis € 2.290,--)

Weitere Termine auf unserer Web-Seite
www.comconsult-akademie.de

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
- **23.06. - 27.06.03 Bonn**
- **21.07. - 25.07.03 Aachen**

Trouble Shooting in geswitchen Ethernet-Umgebungen
- **14.07. - 18.07.03 Aachen**
- **08.09. - 12.09.03 Aachen**

Trouble Shooting für TCP/IP- und Windows-Umgebungen
- **22.09. - 26.09.03 Aachen**

Tool-Ausstattung: Sniffer Basic

Paketpreis für alle drei Seminare mit Sniffer-Lizenz: € 7.500,-- zzgl. MwSt.
(Seminar-Einzelpreise: je € 2.490,--)

Weitere Termine auf unserer Web-Seite
www.comconsult-akademie.de

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I - III:

Von den Einzelbausteinen zur integrierten Lösung
- **23.06. - 27.06.03 Berlin**
- **22.09. - 26.09.03 Bonn**

IP-VPNs, der Kern einer Sicherheits-Infrastruktur
- **08.07. - 10.07.03 Köln**
- **13.10. - 15.10.03 Bonn**

Planung und praktische Konfiguration
- **28.07. - 01.08.03 Aachen**
- **01.12. - 05.12.03 Aachen**

Paketpreis: € 4.990,-- zzgl. MwSt.
(Einzelpreise: € 1.690,-- bis € 2.290,--)

Weitere Termine auf unserer Web-Seite
www.comconsult-akademie.de

Sonderveranstaltung

Umstieg auf Rapid Spanning Tree

14. - 15.07.03 in Aachen

Markus Schaub, der Cisco-Experte der ComConsult Akademie zeigt Ihnen in dieser Sonderveranstaltung wie Rapid Spanning Tree und Multiple Spanning Trees-Verfahren arbeiten und welche Vorteile Sie dadurch haben. Gleichzeitig bereitet Sie das Seminar auf eine Migration aus bestehenden Layer-2 und Layer-3-Netzwerken auf RSTP vor. Zum Abschluss des Seminars konfigurieren Sie praktisch auf der Basis einer Reihe von Layer-2-Switch-Systemen eine Musterlösung und diskutieren dabei die Eigenschaften des Verfahrens und mögliche Fehlkonfigurationen. Testen Sie aktiv in einem laufenden Netzwerk, wie schnell das Verfahren umschaltet.
(Preis: € 1.590,-- zzgl. MwSt.)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Börse

Gebrauchte Netzwerk-Komponenten

Gebote

Adapter IBM Modell: 8228, Anzahl 50, Preis 10 Euro, Mindestabnahme 10 Stück, Anzeigen-Nr. B30410

Ringleitungsverteiler Connectware Modell: 8* RJ45-Buchse+ RI/RO, Anzahl 10, Preis VB 10,00 Euro, Anzeigen-Nr. B30408

Router Cisco Modell: 2504 (TR - ISDN), Anzahl 1, Preis VB 380,00 Euro, Anzeigen-Nr. B30407

Switch/Brücke Olicom WiredSpeedBridge OC3401, Anzahl 3, Preis VB 180,00 Euro, Anzeigen-Nr. B30409

Gesuche

Adapter Nortel Centillion 50 oder 100, Anzahl 2, Preis VB, mit mindestens je 1 ATM OC-3c und 8 Ethernet, Anzeigen-Nr. S30501

Weitere Gebote und Gesuche unter
www.comconsult-akademie.de

Impressum

Verlag:
Dr. Suppan International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland, Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich, 12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der
ComConsult Akademie

Für unverlangt eingesandte Manuskripte
wird keine Haftung übernommen