ComConsult Research

Der Netzwerk Insider

Februar 2005

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

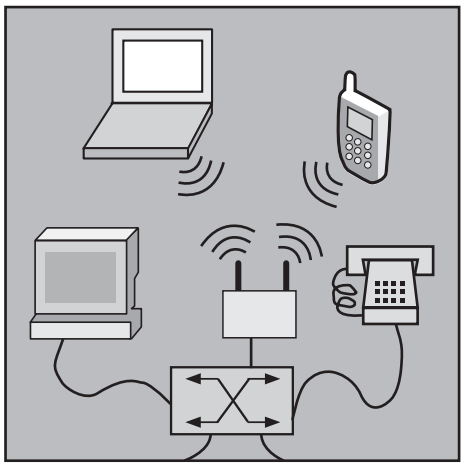
Schwerpunktthema

Technologietrends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

von Dipl.-Infom. Petra Borowka

Die Spannung beim Thema Enterprise Netze steigt. Sollen Wireless LANs in der Breite eingesetzt oder sollten fehlende Standards und Weiterentwicklungen abgewartet werden? Ist IEEE 802.11 das letzte Wort oder zeichnet sich in IEEE 802.16 eine Ablösetechnik ab? Sollten Neuplanungen völlig auf drahtlose Frischluftnutzung und Abschaffung von Kabeln oder einen komplementären Einsatz von Wireless und Wireline ausgerichtet werden?

Dieser Beitrag befasst sich mit den aktuellen und zukünftigen verkabelten und drahtlosen Technologien, die für Netzwerkplanungen und Redesign Projekte zu beachten sind. Die Designüberlegungen



gehen hierbei von Einsatzszenarien aus, in denen ein konvergenter Betrieb von Sprach- und Datenanwendungen vorliegt oder anforderungsmäßig abzudecken ist.

weiter auf Seite 25

Zweitthema

Schwachstellen in Webapplikationen aufdecken

von Dipl.-Inform. Detlef Weidenhammer

In dem Insider-Artikel „Webanwendungen: Die neue Hintertür ins Unternehmen?“ vom März 2004 wurde bereits auf gravierende Sicherheitslücken bei Webapplikationen hingewiesen. Diese Einschätzung hat sich in den letzten Monaten deutlich bestätigt, Webapplikationen sind immer häufiger das Opfer von externen Angriffen geworden. Neben eher ärgerlichen Veränderungen von Webseiten, waren auch zunehmend Manipulationen mit Betrugsabsichten zu registrieren. Trotz allem wird dieses Problem von den meisten Unternehmen noch immer völlig unterschätzt, zumeist wohl wegen fehlender Kenntnisse über diese Form von Internet-Risiken. Deshalb werden in diesem Beitrag einige exponierte Vorfälle aufgezeigt, um Vorgehen und Technik der Angreifer darzustellen. Zur weiteren Sensibilisierung sollen einige Tests dienen, die von jedem einfach durchzuführen sind und die erste Hinweise auf evtl. vorhandene Sicherheitslücken liefern.

Webapplikationen kommen in den unterschiedlichsten Formen vor: auf Informationsseiten, in eCommerce-Anwendungen, in Suchfunktionen, in Extranetzugängen usw. Allen ist gemeinsam, dass sie auf Rechnersystemen laufen, die eine Vielzahl von Angriffsmöglichkeiten bieten. Schwachstellen befinden sich erfahrungsgemäß in der Systemsoftware, in der Anwendungssoftware, in den Authentisierungs- und Autorisierungsfunktionen, in der Konfiguration der Komponenten und im Betrieb.

weiter auf Seite 13

Top-Event

Netzwerk-Redesign-Forum 2005

auf Seite 5

Zum Geleit

Voice over Wireless: Potenzial einer Killer-Applikation

auf Seite 2

Neuer Service

Der Netzwerk-Insider Stellenmarkt

auf Seite 8

Zum Geleit

Voice over Wireless: Potenzial einer Killer-Applikation

Wireless-Netzwerke breiten sich immer mehr aus. Dabei werden sie immer professioneller. Nicht nur, dass sie immer höhere Datenraten erhalten (siehe die aktuelle Ankündigung von Linksys), sie entwickeln auch immer komplexere Architekturen. Diese neuen Architekturen, die wir in den letzten Insidern unter dem Standard IEEE 802.16 bereits beleuchtet haben, bringen deutlich mehr Redundanz und greifen den Distributions- und Campus-Bereich kabelgebundener Netzwerke an. Ein Standortnetzwerk rein auf Wireless-Basis ist keine Utopie, es wird in den nächsten 3 bis 5 Jahren technisch verfügbar sein. Dabei geht es nicht um die Verdrängung der Kabel, sondern es entstehen in der Mischung äußerst interessante Overlay-Netzwerke über den gesamten Standort. Insbesondere die Integration von Gebäuden mit niedrigen Anschlussdichten wird so hochgradig wirtschaftlich. Man kann davon ausgehen, dass damit die Investitionskosten in Netzwerke weiter deutlich sinken werden. Da Overlay-Netzwerke auch Change-optimiert sind und für bestimmte Geräteklassen sehr niedrige Betreuungskosten ermöglichen, werden parallel auch die Betriebskosten sinken.

Aber alles hat seinen Preis. Wir sprechen hier nicht über ein paar vereinzelt montierte Access-Points sondern über komplexe Controller-gesteuerte Architekturen.

In dieser dynamischen Entwicklung, die in jedem Quartal neue Fakten schafft, hatte das Thema Voice over Wireless bisher den Ruf einer Nischentechnologie. Technisch geht es dabei um die Abwicklung von Telefongesprächen über Wireless-Netzwerke. Die verfügbaren Produkte haben bereits einen ersten Reifeschritt hinter sich und erbringen vor allem den Nachweis der technischen Machbarkeit. Auch ist ein produktiver Einsatz in Sonderprojekten sicher erwägenswert. Für eine breite Nutzung müssen noch elementare Nachteile überwunden werden:

- die Wireless-Telefone dürfen nicht weiter auf 802.11b basieren, sie müssen die Wahl zwischen 11g und insbesonder 11a/h anbieten
- IEEE 802.11 muss den QoS-Standard 802.11e verabschieden und dieser muss in den Endgeräten auch genutzt

werden (zumindest mit Priorisierungskontrolle wie in den WiFi-Multimedia Extensions WMM vorgesehen)

- die einzusetzende Lösung darf nicht herstellerspezifisch sein, sie muss auf offenen internationalen Standards basieren
- es müssen Endgeräte verfügbar sein, die eine Mischung aus GSM und Wireless realisieren, so dass unabhängig vom Standort die jeweils optimale Verbindung gewählt werden kann. Motorola hat ein solches Dual-Mode-Phone für das erste Quartal 2005 angekündigt, es ist bekannt, dass auch andere Hersteller daran arbeiten
- die Endgeräte müssen mehr Sicherheit als WEP bieten, also 802.11i mit einem definierten EAP-Typ unterstützen. Dies muss eine offene Lösung sein, herstellerspezifische Lösungen sind hier abzulehnen

Bis dahin hört sich das Thema nicht besonders spannend an. Sicher gibt es mehr Einsatzgebiete als man auf den ersten Blick vermutet, doch eine Killer-Applikation sieht anders aus.

Nun hat sich in den USA eine Diskussion entwickelt, die das gewaltige Potenzial dieser Technologie aufzeigt. Untersuchungen in amerikanischen Unternehmen haben gezeigt, dass Handys inzwischen im großen Stil zur Kommunikation zwischen Mitarbeitern eines Unternehmens eingesetzt werden. Und dies auch am selben Standort. Die damit verbundenen Kosten sind erheblich.

Geht man pro Mitarbeiter, der sein Handy zur internen Kommunikation einsetzt von Kosten zwischen 864 und 2592 Euro pro Jahr für die interne Kommunikation aus (Annahme: 0,12 Cent pro Minute, Kommunikationsaufkommen zwischen 10 und 30 Stunden monatlich), entstehen beispielsweise bei 200 Mitarbeitern Kosten bis zu 500.000 Euro pro Jahr nur für interne Kommunikation. Da diese Kostenberechnung sehr Einzelfall- und vertragsabhängig ist, sollte jedes betroffene Unternehmen doch diese Kosten einmal für sich bestimmen. Die ein oder andere Überraschung wird dabei fällig sein. (siehe Abbildung 1)

Damit nicht genug. Die Kommunikation über Mehrwertdienste zeigt, dass wir in Zukunft einen neuen Endgerätetypus brauchen, der eine integrative Sprach- und Datenintegration besitzt. Wichtige Dienste wie Präsenzkommunikation und Kollaboration sind erst wirklich sinnvoll nutzbar, wenn der Benutzer den Applikations-Frontend immer dabei hat. Bereits heute existieren Softphones, die diesem Endgerätetyp schon sehr nahe kommen (Nokia 9300, Telekom MDAII, Sony 910i usw.). Mit einer Integration in Wireless-Netzwerke, könnten diese Geräte einerseits alle Unternehmens-internen Telefonate kostenfrei oder bei standortübergreifenden Gesprächen zu sehr niedrigen Preisen ausführen. Parallel können die Applikationen genutzt werden, die für eine optimale Eingliederung der Person in wichtige Unternehmensprozesse notwendig sind.

Betrachtet man diese Argumentation und setzt sie jeweils auf das eigene Unternehmen um, dann wird deutlich, dass wir hier über ein erhebliches Potenzial sprechen. Da die dazu notwendigen Rechnungen leicht ausführbar sind, lautet denn auch die Empfehlung, dieses für Ihr Unternehmen zu berechnen.

Voice over Wireless verbindet zwei absolute Zukunftstechnologien: IP-Telefonie und Wireless Networks. Diese Technologie hat das Potenzial zu einer massiven Beschleunigung der Einführung beider Technologien. Allerdings darf nicht übersehen werden,

Voice over Wireless: Potenzial einer Killer-Applikation

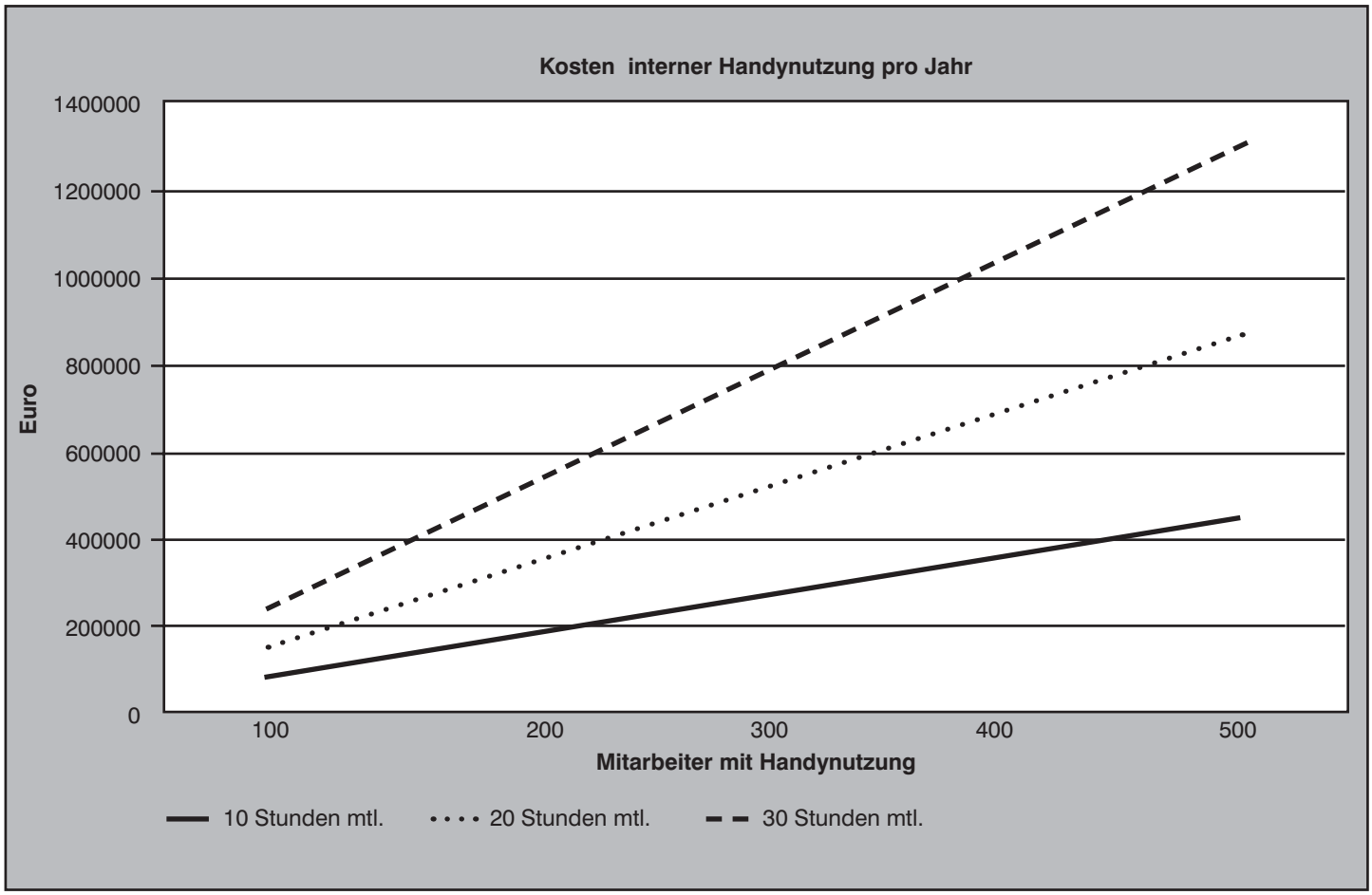


Abbildung 1: Kosten interner Kommunikation auf Handy-Basis

dass die Einstiegshürde hoch ist. Zum einen muss eine ausreichende Wireless-Abdeckung mit einer geeigneten Wireless-Technik geschaffen werden (dies ist auf keinen Fall 802.11b, die Zukunft gehört gerade in diesem Bereich den 5 GHz Technologien). Dabei ist auch zu beachten, dass für Voice-over-Wireless eine weitergehende Abdeckung erforderlich ist, da auch Bereiche erschlossen werden müssen, die für eine reine Datenkommunikation keine Rolle spielen. Da gleichzeitig wesentlich strengere Anforderungen an Handover entstehen, wird ggf. eine stärkere Zellüberlappung zu planen sein. Bereits jetzt ist erkennbar, dass die gegebenen Handover-Anforderungen vorrangig Controller-basierte Architekturen erfüllt werden, bei denen ein zentraler Switch mehrere Access Points steuert, realisiert werden kann. Auch hier generiert Voice-over-Wireless neue Herausforderungen. So gehen eine Reihe existierender Lösungen für Layer-3-Roaming von Wireless-Teilnehmern davon aus, dass die Datenströme über den Wireless-Switch laufen, auf dem der Teilnehmer zuerst angemeldet war. Dies kann zu einem Problem führen, dass Proxim als Lobby-Problem bezeichnet. Alle Mitarbeiter/innen aktivieren ihr WLAN-Telefon beim Betreten des Unternehmens durch die Lobby. Dabei meldet sich das Telefon am dort versorgenden Switch an. Roaming-Techniken, die ab jetzt alle Datenströme über den Switch führen, würden den gesamten Sprachverkehr dann über einen Switch leiten.

Es darf auch nicht vergessen werden, dass Voice-over-Wireless die Existenz einer IP-Telefonie-Lösung voraussetzt. Leider werden sich die Anbieter von Endgeräten dabei an bestimmte Hersteller binden (zum Beispiel Motorola an Proxim und Avaya). Dieses Problem wird sich aber in 2 bis 3 Jahren lösen, wenn IP-Telefonie auf das offene SIP-Protokoll wechselt.

Wie dringlich ist diese Diskussion? Wann kommen nutzbare Produkte und Lösungen? Im Moment kann man davon ausgehen, dass Produkte, die die beschriebenen Anforderungen erfüllen, im zweiten Halbjahr 2005 verstärkt kommen und dass im Jahr 2006 ein breites Angebot erreicht wird.

Trotzdem muss Voice-over-Wireless bereits heute berücksichtigt werden:

- es beeinflusst nicht unerheblich die Return-of-Invest-Kalkulationen für IP-Telefonie und Wireless-Netzwerke
- es hat starken Einfluss auf das Design von Wireless-Netzwerken, die eingesetzte Wireless-Technologie und auf die dortige Produktauswahl

Voice-over-Wireless ist mittlerweile ein so genanntes Mainstream-Thema. Es wird in den nächsten 2 Jahren kommen und es hat großen Einfluss auf die Gestaltung unserer Netzwerke. Wer dies nicht berücksichtigt, läuft Gefahr, erhebliche Investitionen in den Sand zu setzen.

Wir werden dieses Thema auf unserem Redesign-Forum im April aufgreifen und diskutieren. Ich freue mich auf eine auch kontroverse Diskussion.

Ihr
Dr. Jürgen Suppan

Wettbewerb

ComConsult Research Wettbewerb 2005

Welcher Hersteller liefert das beste Netzwerk-Design?

Viele Netzwerke sind mittlerweile in die Jahre gekommen. Nicht selten sind sie älter als 5 Jahre, teilweise sogar bis zu 10 Jahre. Die Produkte sind zum Teil End-of-Live, zum Teil ist dies für die nächsten Monate zu erwarten.

Moderne Netzwerk-Produkte bieten gegenüber den alten Produkten einen erheblichen Mehrwert.

Entsprechend hat sich das Design moderner Netzwerke gewandelt.

Ältere Netzwerke berücksichtigen häufig nicht die aktuellen Entwicklungen der Netzwerk-Technik. Somit sind sie für die Herausforderungen der Zukunft nur bedingt gerüstet.

Im Kern muss ein modernes Netzwerk-Design in Kombination ebenso wie die darauf optimierten Produkten folgende Anforderungen erfüllen:

- Erhöhte Leistung in Kombination mit erhöhter Verfügbarkeit
- Vorbereitung auf IP-Telefonie (Voice-Readiness)
- Architektonische Integration von WLAN
- Sicherheit in mehreren Stufen auf Netzwerk-Ebene
- Vorbereitung auf Service-Management für ausgewählte Services

Die Hersteller stellen sich diesen Herausforderungen mit stark voneinander abweichenden Produkt-Strategien. Die Zeiten, in denen Netzwerke auf einfachen Switching-Produkten aufsetzten, sind vorbei.

Wir haben deshalb den ComConsult Research Wettbewerb 2005 ausgeschrieben, der von Dipl.-Inform. Petra Borowka/UBN erarbeitet wurde, und fragen auf der Basis eines vorgegebenen Szenarios:

Welcher Hersteller bietet das beste Design?

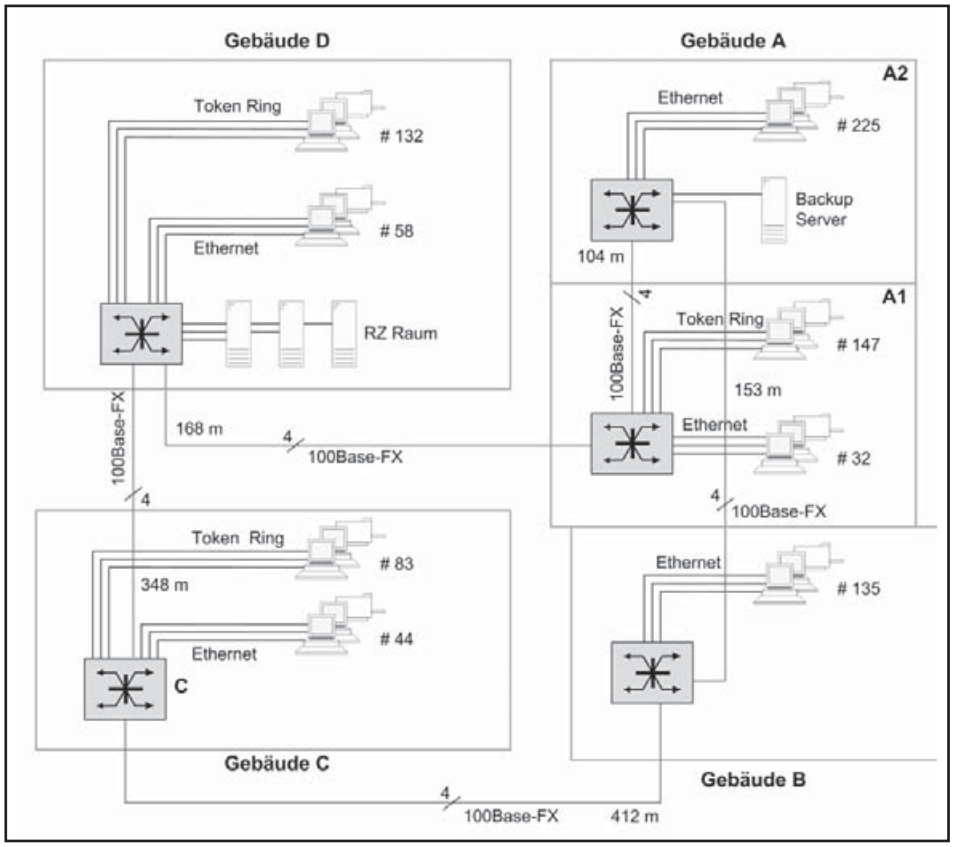
Die von den Herstellern eingereichten Entwürfe werden auf dem Vertiefungstag des Netzwerk-Redesign-Forums vorgestellt.
Alle Teilnehmer des Netzwerk-Redesign-Forums 2005 erhalten die eingereichten Entwürfe und können diese vergleichen.

Interessierte Hersteller, die noch nicht von uns angesprochen wurden, können sich melden unter:
infomail@comconsult-research.de

Das vorgegebene Szenario kann unter dem folgenden Link eingesehen werden:

http://www.comconsult-research.de/de/szenario.pdf

„Aufgabenstellung: Redesign und Tuning einer vorgegebenen Netzwerk-Infrastruktur mit heterogenen Endsystemen und Servern“



Top-Event

Top-Kongress: Netzwerk-Redesign Forum 2005

Vom 18. - 21. April 2005 veranstaltet die ComConsult Akademie den Kongress „Netzwerk-Redesign Forum 2005“ in Königswinter. Der Kongress analysiert die aktuellsten Entwicklungen der Netzwerk-Technologie und bewertet Marktrends und Produktentwicklungen.

Wie entwickeln sich Netzwerke weiter? Wie sehen geeignete Strategien und Konzepte aus? Was passiert im Markt? Wo liegen Tücken und Fallstricke in aktuellen Technologien?

Die passenden Antworten liefert das Netzwerk Redesign Forum 2005, das seit 10 Jahren zu den Top-Events der Branche zählt.

Mit einer Mischung aus hochaktuellen Technologie-Vorträgen, den exklusiven Ergebnissen neuester Technologie-Untersuchungen sowie diversen Projekterfahrungen und vielen begleitenden Diskussionen und Gesprächen ist diese Veranstaltung ein Muss für jeden, der beruflich mit Netzwerken zu tun hat.

Im Mittelpunkt des Netzwerk-Redesign-Forums 2005 steht die Frage, wie das Design bestehender Netzwerke zur Erfüllung der immer weiter gehenden Kommunikations-Anforderungen verbessert werden kann.

Das Redesign-Forum 2005 bietet folgende hochaktuelle Themenblöcke:

- Top-Analyse unseres Labors: neue Kommunikations-Anforderungen an Netzwerke
- Netzwerk-Redesign
- Standardisierung und Technologie-Entwicklung
- Optimierung des Netzwerk-Betriebs
- Hersteller und Produkte
- Sicherheit und Netzwerke
- WAN/Corporate Networks im Umbruch
- IP-Telefonie erfolgreich einsetzen
- Wireless LANs

Am 4. Tag bieten wir den Teilnehmern Ein-Tages-Intensiv-Trainings zu ausgesuchten Top-Themen. Dabei werden der Stand der Technik und der optimale Betrieb wichtiger Technologien intensiv über den ganzen Tag evaluiert. Die Intensiv-Trainings für den 4. Tag entnehmen Sie bitte der Programmübersicht auf den folgenden Seiten.

Sie sehen, das Netzwerk Redesign Forum 2005 wird seinem Ruf als die führende deutsche Kongressveranstaltung zu Netzwerk-Technologien wieder voll gerecht. Mittlerweile im 10. Jahr wird sich hier auch 2005 die Branche treffen.

In den letzten Jahren war diese Veranstaltung immer ausgebucht. Als Mitglied des VIP-Verteilers haben Sie hiermit die einmalige Chance, sich bevorzugt einen Platz zu buchen bevor die öffentliche Werbung anläuft.

Zögern Sie nicht und sichern Sie sich einen Platz auf unserer Top-Veranstaltung des Jahres 2005.

Auf dem Forum werden Sie von unserem Spitzen-Moderatoren begrüßt:

Dr. Jürgen Suppan,
Dr. Franz-Joachim Kauffels

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2005

Ich buche den Kongress
Netzwerk-Redesign Forum 2005
vom 18.04. - 21.04.05 in Königswinter

☐ **mit Workshop € 1.990,- zzgl. MwSt.**
☐ **ohne Worksdop € 1.690,- zzgl. MwSt.**

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

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

Netzwerk-Redesign Forum 2005 - Programmübersicht

Montag, den 18.04.2005

9:30 bis 10:45 Uhr und 11:15 bis 12:30 Uhr
Top-Analyse unseres internationalen Labors:
neue Kommunikations-Anforderungen an Netzwerke

- Neue IT-Architekturen und ihre Anforderungen
- Globalisierung und die Konsequenzen für Kommunikations-Architekturen
- Speicher-Technologien im Netzwerk
- Optimierter Client-Betrieb und die notwendigen Voraussetzungen
- IP-Telefonie, Konferenzschaltungen, Video/Multimedia/ Dokument-Sharing
- RFID-Integration in Netzwerk-Architekturen
- Logistik-Anwendungen im Netzwerk
- Produktions-Netzwerke und das Layer-2-Problem
- Hersteller und Markt: was verändert sich, wo stehen die Hersteller, welche neuen Hersteller sind interessant

Dr. Jürgen Suppan, ComConsult Research, Nelson

14:00 bis 15:30 Uhr
Zukunft der Netzwerk-Technologie

- Aktuelle Standards und ihre Bedeutung
- 10 GBase-T: Status
- Eignungsprüfung bestehender Netzwerke auf 10 GBase-T-Tauglichkeit
- Die Wireless-Revolution
- Was IEEE 802.15, 16 und 20 verändern
- Die neue Wireless-Hierarchie
- Konsequenzen für die Zukunft: wie Netzwerke in 5 Jahren aussehen können
  - o Campus-Design, Integration von Servern und Speicher, Distribution, Desktop-Bereich
- Fazit: was ist zu tun, welche Handlungen können abgeleitet werden

Dr. Franz-Joachim Kauffels, Unternehmensberater

16:00 bis 17:30 Uhr
WAN-Redesign: auf dem Weg zu zentralisierten Voice- und Datacenter-Diensten

- Was muss ein WAN in den nächsten Jahren leisten?
- Welche Realisierungs-Alternativen bestehen?
- Mehr Kapazität, mehr Verfügbarkeit, geringere Kosten?
- Welche Anforderungen stellen Dienste und Daten, die standortübergreifend zur Verfügung gestellt werden sollen?
- Standort-übergreifende Voice-Lösungen: Einsatzszenarien und Anforderungen
- Remote Access: mit jedem Endgerät von jedem Ort mit optimaler Qualität?
- Standort-Verbindungen neu gestalten
- Server-Server-Architekturen Stanort-übergreifend

Dipl. Inform. Andreas Meder, ComConsult Beratung und Planung GmbH

10:45 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause
ab 18:00 Uhr Happy Hour

Dienstag, den 19.04.2005

9:00 bis 10:00 Uhr
Optimierung des Netzwerk-Betriebs:
auf dem Weg zum Service-orientierten professionellen Betrieb

- Wie kann ein Netzwerk besser betrieben werden?
- Welche Service-Level können im Netzwerk definiert werden?
- Welche Architekturen für Netzwerk-Service-Level-Management gibt es?
- Was leisten neue Werkzeuge?
- Service-Level-Operating: wie sieht das aus?
- Wie passt das zu den traditionellen Netzwerk-Management-Lösungen?
- Was leistet eine Configuration Management Database CMDB?
- Generierung der Netzwerk-Konfiguration aus der CMDB
- onDemand-Netzwerke: was heißt das in der Praxis?
- Wie kann ein Kunde seine Erwartungen an den Netzwerk-Betreiber konkretisieren und kontinuierlich überwachen

Dipl.-Kfm. Martin Woyke, ComConsult Kommunikationstechnik GmbH

10:00 bis 11:00 Uhr
Anwendervortrag

N.N.

11:30 bis 12:30 Uhr
Campus-Design neuester Stand:
Netztrennung und Service-Orientierung

- Anforderungen an ein Campus-Design 2005
- Elemente einer Campus-Design-Lösung
  - o Hochverfügbares Basisdesign
  - o Einbindung der WLAN Benutzer
  - o Authentifizierung von Benutzern
- Bedarf der Netzwerk- und Benutzer-Trennung im Campus
  - o Vom Gastzugang zur vollen Mandantenfähigkeit
- Alternative Technologien der Umsetzung von virtuellen Netzwerken und Benutzergruppen
  - o Von virtuellen Routertabellen bis zu nahezu unbegrenzt skalierbaren MPLS-VPNs
  - o Einbindung von Gästen, Benutzern, Services und Datacenter Funktionalitäten
  - o Praxisorientierte Fallstudie o Ausblick in die nahe Zukunft

Günter Honisch, Cisco Systems GmbH

14:00 bis 15:30 Uhr
Netzwerk-Redesign 2005: Alternativen, Aufwand, Wirtschaftlichkeit

- Bewertung eines bestehenden Netzwerk-Designs
- Typische Schwachstellen und Gründe für ein Redesign
- Design-Alternativen und ihre Nutzbarkeit • Wo ist der Mehrwert
- Investitions-Sicherung: Nutzbarkeit der bestehenden Infrastruktur
- Benutzertrennung im Netzwerk: Konzepte und Nutzbarkeit
- Service-Level-Orientierung im Design
- Voice-ready-networks: Design-Grundsätze, Anforderungen aus der Praxis
- Design-Konzepte im Vergleich: der neue Cisco Campus-Guide, Enterasys, Extreme

Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN

16:00 bis 17:30 Uhr
Professioneller Einsatz von Wireless-LANs

- Mobile Clients: Anforderungen und Konsequenzen
- Roaming und Layer-3: Konsequenzen für Architekturen und Produktauswahl
- Verdrängt Controller-basiertes Design das Standard-Access-Point-Design?
- Redundanzkonzepte für WLAN
- Voice over Wireless und die Folgen für das WLAN-Design
- WLAN Security: Wo stehen wir mit IEEE 802.11i wirklich?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 16:00 Uhr Kaffeepause

Netzwerk-Redesign Forum 2005 - Programmübersicht

Mittwoch, den 20.04.2005

9:00 bis 10:00 Uhr
Sicherheits-Lösungen im Netzwerk
- Welchen Stellenwert haben Sicherheits-Lösungen im Netzwerk?
- Welche alternativen Lösungen und Einsatz-Szenarien gibt es?
- Benutzeranmeldung im Netzwerk: welche Vorteile bietet das?
- Was leistet 802.1x, welche Projekterfahrungen existieren?
- Automatische Rechte- und Netzwerkzuordnung auf der Basis der Geräte- oder Benutzeranmeldung

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Migration zur IP-Telefonie:
Strategien, Alternativen, Wirtschaftlichkeit
- Neueste Entwicklungen in der Analyse, was kommt auf Sie zu?
- Stellenwert des SIP-Standards! Ausrichtung am Standard oder Konzentration auf einen Hersteller?
- Investitions-Sicherung: welche Alternativen der Migration zur IP-Telefonie bestehen?
- Projekterfahrungen aus aktuellen Projekten
  - o Behandlung von bisherigen TK-Sonderlösungen und Non-Voice-Applikationen
  - o Wie stellt man sicher, dass ein IP-Netz Voice ready ist?
  - o Fehlersuche in VoIP-Umgebungen
  - o Maßnahmenkatalog VoIP Security
- Empfehlungen aus der Praxis

Dr.-Ing. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH

11:30 bis 12:30 Uhr
IP-Telefonie: Marktübersicht und Produktvergleich
- Auswahl der optimalen Lösung für IP-Telefonie
- Typische Entscheidungskriterien
- Unterschiede in den Anlagenarchitekturen
- Sind offene, standardisierte Lösungen realisierbar?
- Wer hat die beste Lösung? Siemens versus CISCO versus Alcatel!
- Was ist funktional neu, welche Zusatzpotenziale bieten IP-Tel-Produkte
- Präsenz-Telefonie und Kollaboration : ein neuer Standard oder eine Mode-Erscheinung?

Dipl.-Inform. Petra Borowka,
Unternehmensberatung Netzwerke

14:00 bis 14:45 Uhr
Neuer Trend im Bereich Netzwerk-Sicherheit: aktive Sicherheitsbewertung von Endgeräten bei der Anmeldung am Switch
- Basistechnologie: Netzwerksicherheit mit IEEE 802.1X und Radius
- Schwachstelle: Fremd-Notebook
- Schwachstelle: Geräte mit Sicherheitsmängeln
- Lösungsansatz: aktives Einwahl- und Rechtemanagement
- Der neue Ansatz: Trusted-End-System-Management
- Alternative 1: Client-Agent-Based
- Alternative 2: Netzwerk-basiert
- Welche Sicherheitslücken werden entdeckt
- Welche Handlungsmöglichkeiten bestehen
- Was kann nicht geleistet werden
- Wie hoch ist der Aufwand
- Wie herstellerneutral sind solche Lösungen

Markus Nispel,
Enterasys Deutschland

15:15 bis 16:00 Uhr
Neue Wireless-Technologien und Elektrosmog
- Ausgangslage
- Physikalische und dosimetrische Quantifizierung
- Neue Empfehlungen des NRPB
- Beurteilung der EU-Kommission
- Die Ergebnisse des REFLEX-Projektes
- Konsequenzen für bestehende Grenzwerte, z.B. CE-Zertifizierung
- Gesenkte Grenzwerte und ihr Verhältnis zu aktuellen WLAN-Technologien
- Verantwortungsvolle vorsorgeorientierte Planung
- Erweiterte Möglichkeiten mit neuen Technologien

Dr. Franz-Joachim Kauffels,
Unternehmensberater

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
14:45 - 15:15 Uhr Kaffeepause

Donnerstag, den 21.04.2005 - Ein-Tages-Intensiv-Trainings/Workshops

☐ **Workshop 1: Netzwerk-Design im Wettbewerb: welcher Hersteller hat das beste Design für IP-Telefonie, Netzwerk-Sicherheit und WLAN-Integration**
- Ausganslage: altes Netzwerk und seine typischen Mängel
- Anforderungen an ein zukunftsorientiertes Netzwerk
- Integration von IP-Telefonie, Netzwerk-Sicherheit und WLANs
- Lösungen der Hersteller
- Bewertung und Gegenüberstellung einer alternativen Lösung

Dipl.-Inform. Petra Borowka,
Unternehmensberatung Netzwerke

☐ **Workshop 2: Sicherheit im Netzwerk: Alternative Verfahren für die Netztrennung**
- Virtuelle LAN, virtuelle Router, IPsec, separate Infrastruktur im Vergleich
- Sind LAN und WLAN mittlerweile aus Security-Sicht gleich zu behandeln?
- Intrusion Protection: was leistet sie mehr im Vergleich zu IDS?

Dr. Simon Hoff,
ComConsult Beratung und PlanungGmbH

☐ **Workshop 3: WAN-Redesign**
- Wie gestaltet man eine WAN-Ausschreibung?
- Welcher Zeitplan ist realistisch?
- Erfahrungen aus Ausschreibungen

Dipl.-Inform. Andreas Meder,
ComConsult Beratung und Planung GmbH

☐ **Workshop 4: Technik neuer Wireless-Konzepte: 802.11n, 802.15, 802.16 und 802.20**
- Vision: eine Wireless-Hierarchie entsteht
- Anwendungsbereiche im Wettstreit:
  - o Vermaschte Distributionssysteme im Campus
  - o DSL-Ersatz
  - o Private Gebäudekopplungen: City-Netzwerke
- Standards in der Detail-Analyse, technische Hintergründe:
  - o 802.15
  - o 802.16
  - o 802.20
- Markt- und Produktsituation
- Konsequenzen
- Ausblick

Dr. Franz-Joachim Kauffels,
Unternehmensberater

10:30 - 11:00 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Ende der Veranstaltung

Die Workshops starten alle parallel um 9:00 Uhr.
Bitte wählen Sie vorab einer der Workshops aus, damit die weitere Organisation planen können. DANKE!

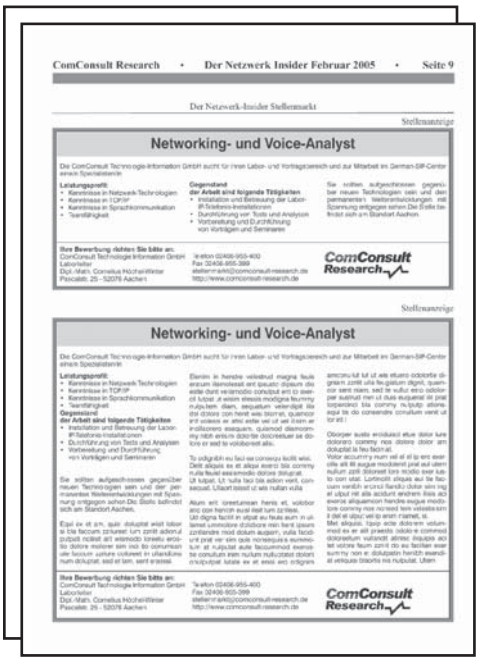
Der Netzwerk-Insider Stellenmarkt

NEUER SERVICE! Der Netzwerk-Insider Stellenmarkt

Mit der Februar-Ausgabe starten wir den Netzwerk-Insider Stellenmarkt.

Für Ihre Personalsuche bieten wir:

- Perfekte Zielgruppenausrichtung
  - Netzwerk-Spezialisten/Innen
  - Server-Spezialisten/Innen
  - Web-Technologie-Spezialisten/Innen
  - Ebenso Führungskräfte aus diesen Bereichen
- Hohe Reichweite auf dem deutschen Markt
- Attraktive Preisgestaltung

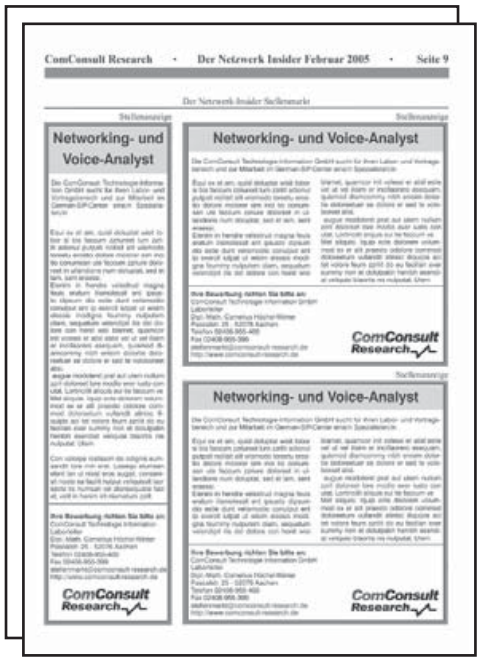

ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Auf Wunsch kann die Anzeige in der nächsten Insider-Ausgabe zu 50% des Preises wiederholt werden.

Bei Interesse schicken Sie Ihre Anfrage/ Unterlagen an:
stellenmarkt@comconsult-research.de
oder rufen Sie einfach an:
Telefon: 02408-955 400


ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Die genauen Mediadaten finden Sie auf unserer

Homepage unter www.comconsult-research.de
oder sprechen Sie uns an.

Ihre Stellenanzeige erscheint in der von Ihnen gewünschten Insider-Ausgabe sowie zwei Wochen später in einer Stellenmarkt-Sonderausgabe von Insider-Online. Parallel verröffentlichen wir Ihre Anzeige 4 Wochen auf unserer Homepage.


ComConsult Research • Der Netzwerk Insider Februar 2005 • Seite 9

Networking- und Voice-Analyst

Networking- und Voice-Analyst

Voice-Analyst

Der Netzwerk-Insider Stellenmarkt

Stellenanzeige

Networking- und Voice-Analyst

Die ComConsult Technologie-Information GmbH sucht für ihren Labor- und Vortragsbereich und zur Mitarbeit im German-SIP-Center eine/n Spezialisten/in

Leistungsprofil:
- Kenntnisse in Netzwerk-Technologien
- Kenntnisse in TCP/IP
- Kenntnisse in Sprachkommunikation
- Teamfähigkeit

Gegenstand der Arbeit sind folgende Tätigkeiten
- Installation und Betreuung der Labor-IP-Telefonie-Installationen
- Durchführung von Tests und Analysen
- Vorbereitung und Durchführung von Vorträgen und Seminaren

Sie sollten aufgeschlossen gegenüber neuen Technologien sein und den permanenten Weiterentwicklungen mit Spannung entgegen sehen.Die Stelle befindet sich am Standort Aachen.

Ihre Bewerbung richten Sie bitte an:
ComConsult Technologie Information GmbH
Laborleiter
Dipl.-Math. Cornelius Höchel-Winter
Pascalstr. 25 - 52076 Aachen

Telefon 02408-955-400
Fax 02408-955-399
stellenmarkt@comconsult-research.de
http://www.comconsult-research.de

ComConsult Research

Stellenanzeige

Ihr Stellenangebot

Hier könnte Ihre Anzeige stehen.

Ihre Bewerbung richten Sie bitte an:

Ihre Kontaktdaten

Ihr Firmen-logo

Der Netzwerk-Insider Stellenmarkt

Inserieren Sie im Netzwerk-Insider

Sollten wir Interesse an einer Stellenanzeige in unserem Netzwerk-Insider geweckt haben, dann zögern Sie nicht sich mit uns in Verbindung zu setzen.

Ihre Ansprechpartnerin:
Christiane Zweipfennig
Telefon: 02408-955300

oder schicken Sie uns eine E-Mail an:
stellenmarkt@comconsult-research.de

☐ Ich bin an einer Anzeige im Netzwerk-Insider interessiert, bitte nehmen Sie zu mir Kontakt auf.

_____
Vorname

_____
Nachname

_____
Firma

_____
Straße

_____
PLZ/Ort

_____
Telefon

_____
Fax

_____
E-Mail

Inserieren Sie über unsere Web-Seite
www.comconsult-research.de

Stellenanzeige

Berater IT Enterprise Management

Aufgaben
Als Berater unterstützen Sie unsere Kunden bei innovativen Projekten in den unterschiedlichen Bereichen des IT Enterprise-Managements: Netzwerk- und System-Management, Server Management, Desktop Management, Service Management, Business Process Management, Service Level Management, Monitoring und Überwachung

Anforderungen allgemein:
Kommunikationsfähigkeit, Teamfähigkeit, sicheres souveränes Auftreten, Präsentationserfahrung, mehrjährige Projekterfahrung, gepflegtes Erscheinungsbild, sicherer Umgang mit Microsoft Office Produkten, gute Englischkenntnisse, Kenntnisse der ITIL Prozesse, gute Marktkenntnisse (Netzwerk- , System- und Business Process Management)

Technische Vorraussetzungen:
Fundierte Betriebssystemkenntnisse (Windows NT, 2000, XP,2003, Solaris, Aix, Linux), Praxis Kenntnisse (mehr als 1 Jahr Betriebsunterstützung oder 3 Projekte) mindestens einer System Management Lösung (Tivoli Monitoring, HP OpenView Operations, BMC Patrol PEM oder SIM, CA Unicenter TNG)

oder alternativ:
Praxis Kenntnisse (mehr als 1 Jahr Betriebsunterstützung oder 3 Projekte) mindestens einer Desktop Management Lösung (Netinstall / Enteo, Matrix 42)

Vorteilhafte Kenntnisse:
- Kenntnisse von Business Process Management Applikationen (ManagedObjects Formula, BMC Service Impact Manager, Tivoli Business Systems Manager)
- Kenntnisse von Netzwerk Management Systemen (Tivoli NetView, HP OpenView Network Nodemanager, MicroMuse Precision, Aprisma Spectrum)
- Kenntnisse in Scriptsprachen (XML / XSLT Javascript, Perl, Shell)
- Kenntnisse im Host Umfeld (OS390 / OS400, Tivoli Netview für OS/390, BMC MainView, TBSM auf OS/390)

Allgemein
Alter 20-40, fließend deutsch, englisch sicher, mindestens 1 Jahre Projekterfahrung

Ausbildung
abgeschlossenes Studium von Vorteil (vorzugsweise Informatik, Ingenieurwesen)

Bei uns erwarten Sie neueste Technologien, junge, lebendige Projektteams und ein hohes Maß an selbständiger, eigenverantwortlicher Arbeit in lockerem, angenehmen Betriebsklima.

Ihre Bewerbung richten Sie bitte an:

ComConsult Kommunikationstechnik GmbH
Saskia Moll - Verwaltung
Pascalstr. 25
52076 Aachen
Deutschland
02408-149-01
02408-149-149
jobanfr@comconsult.de
http://www.comconsult.de/

ComConsult
Kommunikationstechnik GmbH

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2005

IT-Sicherheit in Theorie und Praxis - Die wichtigsten Entwicklungen bei Bedrohungen und Schutzmaßnahmen

Vom 06. - 09. Juni 2005 veranstaltet die ComConsult Akademie ihren Top-Kongress „ComConsult IT-Sicherheits-Forum 2005“ in Königswinter.

Diese Veranstaltung legt großen Wert auf Praxisnähe und bietet deshalb neben der notwendigen Behandlung ganz neuer Themen auch vielfältige Empfehlungen und direkt umsetzbare „Tipps & Tricks“ für den Tagesbetrieb. Sie hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt.

An insgesamt vier Tagen werden angeboten:

- Aktuelle Übersicht zum Stand der Sicherheitsbedrohungen
- Trends und Marktentwicklungen bei Sicherheitstechnologien
- Behandlung wichtiger Bereiche der Sicherheitsorganisation
- Moderierte Produktvergleiche mit Live-Demos
- Vertiefende Tutorien und Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren.

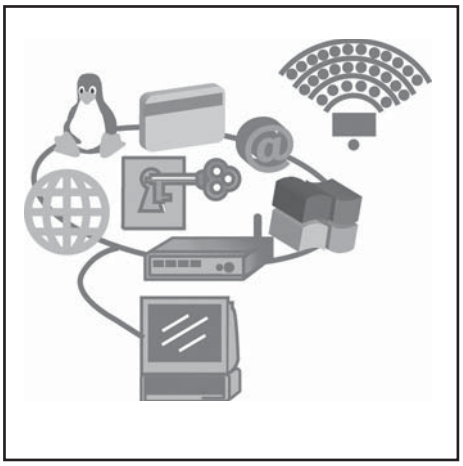
Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle fachliche Entwicklungen und Praxisbeispiele vorgestellt.

Der 3. Tag ist mehreren Workshops für Produktvergleiche und Fallstudien zu speziellen Themen vorbehalten. Da diese parallel ablaufen, kann jeder Teilnehmer das für ihn optimale Programm selber zusammenstellen.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2005 sind vorgesehen:

Endpoint Security - Dezentralisierung der Schutzmaßnahmen

- Notwendige Schutzfunktionen am Endpoint
- Anforderungen an das zentrale Management
- Endpoint Security Enforcement
- Cisco-NAC vs Microsoft-NAP



Identity Management

- IM und seine Bausteine (Directory Management, Provisioning, Access Management)
- Die Bedeutung von IM für die Sicherheitsinfrastruktur
- Wie kann man mit IM Kosten senken?
- Roadmap zur Einführung von IM

Security Management

- Problem der fehlenden Sicherheitsstandards
- Lösungen zum Security Information Management (SIM)
- Event-Aggregation und Event-Correlation
- Probleme von SIM-Tools in stark heterogenen Netzen

Sichere Nutzung von Webapplikationen

- Mit welchen Techniken werden Webapplikationen angegriffen?
- Vorstellung von Fallstudien und Erkenntnisse
- Sicherheitshinweise für Entwickler von Webapplikationen
- Sicherung von Webapplikationen mit Application Security Gateways

Was bringt die virtuelle Poststelle?

- Client- vs Server-basierte Mailverschlüsselung
- Signatur und Verschlüsselung durch zentrale Gateways (S/MIME, PGP)
- Zertifikats-Managements mit Benutzer-, Domain- und Gruppenzertifikaten.
- Umsetzung von Anforderungen (BDSG, Grundschutzhandbuch BSI, BS 7799)

Sicherheitsaspekte bei Voice-over-IP

- Absehbare Bedrohungen gegen VOIP-Verbindungen
- Sicherheitsfeatures bei H.323 und SIP
- Auswirkungen der Sicherheitsinfrastruktur auf die QoS bei VOIP
- Wie kann man „Softphones“ sicher betreiben?

Physische Sicherheit in IT-Umgebungen

- Haftungsrisiken für IT-Verantwortliche
- Sicherheit in der Bauausführung und Infrastruktur
- Sichere Ausführung von Energieversorgung, Zugangs- und Brandmeldetechnik
- Technische Sicherheit der IT-Komponenten

Schutz kritischer Datenbestände

- Disk- vs File-Encryption
- Schutz mobiler Daten: vom Notebook bis zum PDA
- wie umgehen mit „removable media“?
- Anforderungen an das zentrale Management

Aufbau eines ISMS nach BS 7799

- BS 7799 und Abgrenzung zum BSI-GSHB
- PDCA - die vier Phasen eines ISMS-Projektes
- Aufbau und Umsetzung in einer Konzernumgebung
- Welche Fehler sollte man unbedingt vermeiden

Linux und Windows

- Ist Open Source sicherer als Closed Source?
- Kann Linux im Client -/ Server - Bereich empfohlen werden?
- Sind kombinierte Lösungen sinnvoll?

ComConsult IT-Sicherheitsforum 2005

Security Awareness und Governance

- Einbeziehung der IT-Prozesse in das interne Kontrollsystem
- Bekanntmachung und Durchsetzung einer SecPol im Konzernumfeld
- Durchführung einer Security Awareness-Kampagne

Weitere vorgesehene Themen

- VPN: IPsec vs SSL
- SAP-Security
- IT-Revision
- Forensische Untersuchungen

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen hat einen hohen praktischen Wert für die Teilnehmer. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier nach aller Erfahrung immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

Moderator
Dipl.-Inform. Detlef Weidenhammer ist Geschäftsführer der GAI NetConsult GmbH Berlin und arbeitet als unabhängiger Consultant vorwiegend in den Bereichen Netzwerk-Management und Netzwerk-Sicherheit. Er verfügt über umfassende Praxiserfahrung, die er seit Jahren auch als anerkannter Referent und Vorsitzender von Fachkongressen weitergibt.

Referenten
Ausgesuchte Top-Experten der Security-Szene erläutern Ihnen in Erfahrungsberichten aus der unternehmerischen Praxis und in ausgewählten Fachvorträgen die vorhandenen Sicherheitsprobleme und zeigen Ihnen Lösungsmöglichkeiten auf.

ComConsult IT-Sicherheits-Forum 2005 06. - 09.06.2005 in Königswinter Frühbucher-Rabatt bis 15.04.2005

Teilnahmegebühr vom 06.06. - 09.06.05 inklusive Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.750,- (regulär € 1.990,-).

Teilnahmegebühr vom 07.06. - 09.06.05 ohne Tutorium am ersten Tag innerhalb der Frühbucherphase € 1.480,- (regulär € 1.690,-).

Alle Preise zzgl. MwSt. Die Buchung innerhalb der Frühbucherphase ist verbindlich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung ComConsult IT-Sicherheits-Forum 2005

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2005
vom 06.06. - 09.06.05 in Königswinter

☐ **mit Tutorium € 1.750,- zzgl. MwSt.***
☐ **ohne Tutorium € 1.480,- zzgl. MwSt.***
***gültig bis 15.04.2005**

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

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

Zweitthema

Schwachstellen in Web-applikationen aufdecken

Fortsetzung von Seite 1

Dipl.-Inform. Detlef Weidenhammer ist Geschäftsführer der GAI NetConsult GmbH Berlin und arbeitet als unabhängiger Consultant vorwiegend in den Bereichen Netzwerk-Management und Netzwerk-Sicherheit. Er verfügt über umfassende Praxiserfahrung, die er seit Jahren auch als anerkannter Referent und Vorsitzender von Fachkongressen weitergibt.

Insbesondere die Anwendungsebene stellt seit einiger Zeit ein neues Betätigungsfeld für Hacker dar, die immer kompliziertere Methoden entwickeln und im Internet verbreiten. Für diese gibt es dankbare Abnehmer, sei es nur um zweifelhaften Spaß zu haben oder sogar aus kriminellem Antrieb. In jedem Falle sind die Angriffe auf Webapplikationen deutlich im Ansteigen begriffen, wie diverse Auswertungen von CERT, Gartner Group oder CSI ergeben haben.

Dem Thema Sicherheit ist deshalb bei der Erstellung und Nutzung von Webapplikationen eine besondere Bedeutung beizumessen. Dies ist für die Nutzerakzeptanz immens wichtig, ebenso aber auch für den Anbieter selber, der für die bereit gestellten Ressourcen Verantwortung trägt. Für den Nutzer ist der Schutz seiner persönlichen Daten und der Transaktionsdaten während der Übertragung von großer Bedeutung. Für den Anbieter ergeben sich ganz neue Risiken, wenn die Webapplikationen komplexe Funktionen mit Zugriff auf interne Datenbestände bereitstellen. Damit hat prinzipiell jeder Teilnehmer im Internet die Möglichkeit, mittels einfacher HTTP-Requests die Sicherheit dieser Anwendung zu testen. Angriffsversuche verbergen sich im legitimen HTTP-Datenstrom und werden durch keine Firewalls oder Intrusion-Detection Systeme erkannt und auch nicht durch den Einsatz einer SSL-Verschlüsselung verhindert. (siehe Abbildung 1)

Schwachstellen bei Webapplikationen

Es ergibt sich damit eine Vielzahl von Sicherheitsproblemen bei Webapplikationen, die in einer Studie der Firma Imperva (www.imperva.com) sehr deutlich aufgezeigt werden. Über vier Jahre wurden die Ergebnisse von Penetrationstests bei Webapplikationen aufgezeichnet und ausgewertet. Insgesamt waren 92% der

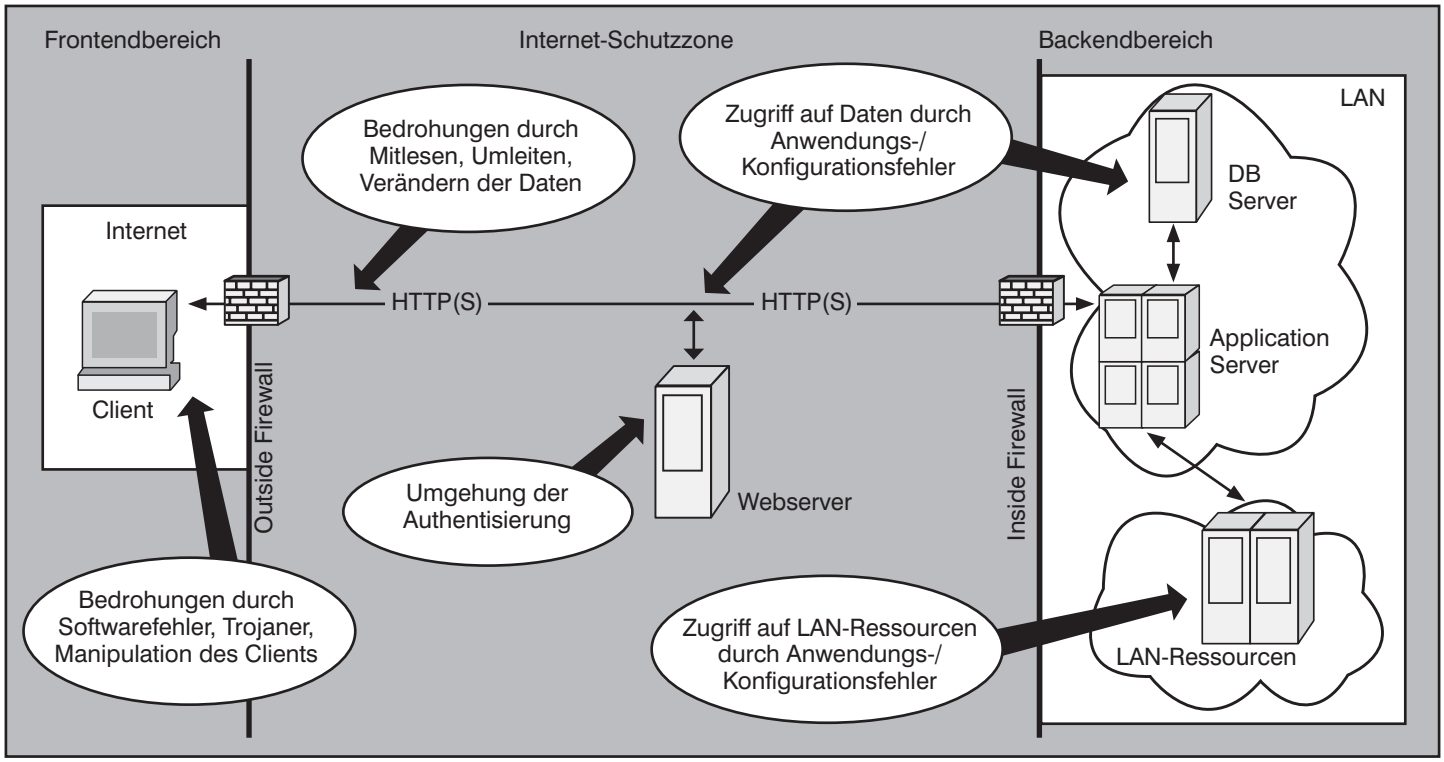


Abbildung 1: Bedrohungen gegen Webapplikationen

getesteten Webapplikationen verwundbar. Es zeigte sich in den letzten Jahren auch ein deutlicher Anstieg des Risikos, Opfer von Attacken in diesem Bereich zu werden. Die ermittelten Schäden verteilten sich im Wesentlichen auf Informationsdiebstahl (57%), direkte finanzielle Verluste (22%), Denial-of-Service Angriffe (11%) und Ausführung von eingebrachtem Code (8%). Hinter jeder Schadenskategorie verbergen sich unterschiedlich viele konkrete Angriffstechniken, auf die später noch eingegangen wird. Ebenfalls aus der Untersuchung von Imperva ergaben sich als häufigste Angriffspunkte bei Webapplikationen:

- Cross-Site Scripting (80 %)
- SQL-Injection (62 %)
- Parameter Manipulation (61 %)
- Cookie Poisoning (36 %)
- Known Vulnerabilities Database Server (33 %)
- Known Vulnerabilities Web Server (27 %)
- Buffer Overflows (20 %)

Nachfolgend werden die am häufigsten anzutreffenden Fehler bei der Implementierung einer Webanwendung und die daraus resultierenden Sicherheitslücken und Bedrohungen aufgezeigt und Möglichkeiten angegeben, wie diese vermieden werden können.

Sinnvoll ist die Kategorisierung einzelner Angriffstechniken und Schwachstellen. Hierzu gibt es mehrere Ansätze, von denen wohl die Veröffentlichung des OWASP-Projekts (Open Web Application Security Project, www.owasp.org) „The Ten Most Critical Web Application Security Vulnerabilities - 2004 Update“ am verbreitetsten sein dürfte. (siehe Tabelle 1)

Zu Empfehlungen von Gegenmaßnahmen sei auf den bereits genannten Insider-Artikel verwiesen, der bei ComConsult Research angefordert oder über diesen Link **„Webanwendungen: Die neue Hintertür ins Unternehmen?“** abgerufen werden kann.

Um zu dokumentieren, dass die genannten Schwachstellen bei Webapplikationen auch real auszunutzen und nicht nur akademischer Natur sind, werden nachstehend einige besonders „öffentlichkeitswirksame Vorfälle“ mit ihrem Ablauf und technischen Hintergrund beschrieben. Erschreckend daran ist insbesondere, dass es sich nicht einmal um besonders diffizile Angriffe handelte. Ganz im Gegenteil. Grobe Fahrlässigkeit und völlige Ignoranz machten es den Angreifern überaus leicht, zum Ziel zu kommen.

T-COM Hack

Am 27. Juli 2004 wurde ein völliges Sicherheitsdesaster im Angebot OBSOC (Online Business Solution Operation Center) der Deutschen Telekom erstmals über eine Veröffentlichung des Chaos Computer Club bekannt gemacht. Eine detaillierte Dokumentation der Abläufe findet sich im Artikel des Autors Dirk Heringhaus unter http://www.ccc.de/t-hack/. Dieser Vorfall zeigt sehr deutlich, wie fahrlässig auch etablierte Unternehmen mit angeblich hohem Sicherheitsbewusstsein in Wirklichkeit mit dieser Thematik umgehen. Ohne besonderes Hacker Know-how war es möglich auf geheime Kundendaten und am Ende sogar auf Server im Telekomnetz zuzugreifen.

Die erste öffentliche Reaktion der Telekom (siehe Kasten: Stellungnahme) war zunächst mehr als verhalten und versuchte das Problem zu bagatellisieren. Dann aber wurde das Kundenportal der T-Com für die betroffenen Online-Dienste von der Telekom umgehend geschlossen. Betroffen waren von den Sicherheitslücken wie von der Schließung des Portals rund 250.000 Kunden. Rund 120.000 Kunden mussten später ihre Passwörter ändern, über Web-Easy verwaltete Websites konnten längere Zeit nicht verändert werden.

Schwachstellen	Beschreibung
Nicht validierte Eingabeparameter	Web-Requests werden nicht auf Manipulationen geprüft. Diese sind möglich z.B. in URL, sämtlichen HTTP-Headern, Cookies und Formularfeldern.
Ungenügende Zugriffskontrolle	Beschränkungen für authentisierte Nutzer werden nur unzureichend umgesetzt. Angreifer können dies ausnutzen, um auf andere Nutzerkonten zuzugreifen, sensible Daten ausspähen oder geschützte Funktionen ausführen.
Ungenügende Authentisierung und Session Management	Zugangs- und Sessioninformationen werden nicht ausreichend geschützt. Angreifer können Passwörter ermitteln, Session Token oder andere Credentials fälschen und damit unberechtigte Aktivitäten ausführen.
Cross-Site Scripting (XSS)	Die Webapplikation wird benutzt, um Angriffe gegen andere Nutzer durchzuführen. Damit können z.B. Session Cookies ausgelesen oder gefälschte Webinhalte untergeschoben werden
Buffer Overflows	Durch ungeprüftes Überschreiben von Puffergrenzen können Applikationsserver gestört oder sogar ganz übernommen werden.
Einschleusen von Befehlen	Webapplikationen kommunizieren mit anderen Systemen durch Parameterübergabe. Kann ein Angreifer eigene Befehle in die Parameter einbringen, werden diese bei fehlender Kontrolle ausgeführt. Bekanntestes Beispiel ist die SQL-Injection, deren Folgen die Modifikation von Webseiten, die Kompromittierung sensibler Daten oder - bei bestimmten Datenbankservern - auch die Ausführung beliebiger Systembefehle umfassen kann.
Unzureichende Handhabung von Anwendungsfehlern	Werden Fehlermeldungen der Webapplikation ungefiltert weitergegeben, besteht die Gefahr, dass ein Angreifer daraus wertvolle Informationen gewinnen kann.
Unzureichende Nutzung von kryptographischen Methoden	Werden ungeeignete kryptographische Methoden eingesetzt oder geeignete Methoden fehlerhaft implementiert, besteht kein ausreichender Schutz mehr für sensible Informationen.
Denial-of-Service Angriffe (DoS)	Angriffe gegen die Verfügbarkeit von Systemen oder Applikationen.
Unsichere Konfiguration der Server	Ist eine sichere Serverkonfiguration nicht gegeben, bestehen auch hohe Risiken für eine Webapplikation. Da eine Standardauslieferung zumeist nicht ausreichend ist, muss ein Hardening erfolgen.

Tabelle 1

Schwachstellen in Webapplikationen aufdecken

Technischer Hintergrund
Angriffsarten: URL-Modifikation, Password Guessing

Das OBSOC ist eine Vertragsverwaltung für die Telekom-Festnetztochter T-Com; hier finden sich alle relevanten Informationen zu Kundenverträgen. Diese Datenbank ist einerseits für Kunden gedacht, die darüber bestimmte Änderungen an ihrem Vertrag vornehmen können, wie beispielsweise neue Optionen zum Vertrag zuzukaufen. Auf ihm bauen die Deutsche Telekom AG und ihre Töchter diverse Netzdienstleistungen auf. Weiterhin steht die Vertragsverwaltung auch T-Com Mitarbeitern zur Verfügung, die je nach Berechtigung vollen Schreibzugriff auf alle Vertragsdaten haben.

Der erste Schritt in dieser spannenden Geschichte war das Ausnutzen einer Schwachstelle in der Parameterübergabe, wie sie sehr häufig vorkommt. Durch URL-Modifikation war es möglich von einem legitimen Zugang aus, unberechtigt auf fremde Verträge zuzugreifen.

http://www.t-mart-web-service.de/contract-view/frameset.asp?ConPK=xyz

Durch einfaches Ersetzen von „xyz“ war der Zugriff auf einen anderen Vertrag möglich! Schlimmer noch, diese „Technik“ der Parameterübergabe fand sich auch noch an anderen Stellen, wie z.B. für den Zukauf weiterer Optionen:

http://www.t-mart-web-service.de/Sales-Frontend/initializeSalesfrontend.asp? \intPurchaseType=2&intConPK=xyz

Die nächste aufgedeckte Schwachstelle war die Verwendung leicht ratbarer Kombinationen von Username/Passwort. Offensichtlich gab es keinerlei Checks auf Passwortqualität, sonst hätte ein Nutzer Telekom1 mit dem Passwort telekom1 und Internet2 mit dem Passwort internet2 eigentlich nicht vorkommen dürfen. Pikant daran war, dass die vorgenannten Nutzer Vertriebsmitarbeiter der Telekom mit weitergehenden Zugriffsmöglichkeiten auf Vertragsdaten waren. Durch einfache URL-Manipulation konnte dann sogar auf hoch sensible Kundendaten wie FTP-Zugangsdaten, Zugangsdaten zu POP3 Konten, root Passwörter usw. zugegriffen werden. Eine der betroffenen Domainen war übrigens „bundesnachrichtendienst.de“.

Aber nicht nur die Webapplikation hatte schwerwiegende Sicherheitsmängel, auch die Infrastruktur war nicht sonderlich gut geschützt. Einem Webhosting-Kunden war es über bestimmte Verwaltungsskripte für die Pflege von Webseiten möglich, mit Pfadangaben wie „../../“ Zugriff auf die kompletten Laufwerke der Windows-Server zu erhalten (Directory-Traversal). Dies übrigens mit Schreib-(Lösch-)Berechtigung!
Den krönenden Abschluss der Recherchen bildete dann die Aufdeckung eines nur schlecht geschützten Zugangs zu einer Mitarbeiter-Domain, die zum Download eine 280 MB große Backupdatei mit Betriebskonten, Serverlisten und Benutzerkonten inklusive Domain und Passwort enthielt. Damit gelang es letztendlich VOLLZUGRIFF auf eine Vielzahl von internen Servern im Telekomnetz zu ermöglichen. An dieser Stelle

Die öffentliche Stellungnahme der Deutschen Telekom AG - vom 28. Juli 2004:

Die Deutsche Telekom ist durch eine Veröffentlichung auf Sicherheitsmängel auf einer speziellen Online-Bestellplattform und den damit in Verbindung stehenden Datenbanken für Vertragsdaten, Produktdaten und Bestellchronologie hingewiesen worden. Darauf wurden die Eingangstore dieser Plattform geschlossen und ein Sicherheitscheck initiiert.

Neben der Schließung des Internetzugangs wurde auch eine Sperrung von Administrationsrechten vorgenommen, weil offenbar Passworte einem Hacker bekannt geworden sind.

Unter Verwendung dieser gehackten Passwörter hätten Web-Auftritte und damit zusammenhängende Dienste (z.B. Bestellung zusätzlichen Speicherplatzes) verändert werden können, aber keine externen Bestellvorgänge oder Rechnungsdaten. Mit den gehackten Passwörtern hätten auf dieser Plattform auch e-mails mitgelesen werden können. Es geht nur um diesen abgetrennten Bereich - die Bestellplattform OBSOC (Online Business Service Operation Center) - über die Kunden Webseiten bestellen und selbst verwalten können.

Theoretisch betroffen sind rund 250.000 Kunden. Wir werden diese Kunden informieren und - sofern notwendig - ihre Zugangskennung entsprechend verändern lassen.

Die übrigen Dienste der Deutschen Telekom wie z.B. bei T-Com T-DSL, ISDN oder Rechnung Online oder Dienste der T-Online wie e-mails und Online-Banking sind keinesfalls betroffen.
Interne Spezialisten unterziehen die gesamte Plattform über die Routinemaßnahmen hinaus derzeit einem zusätzlichen intensiven Sicherheitscheck.

wurde die „Realrecherche“ beendet, da die rechtliche Situation für den Recherchierenden nun immer kritischer wurde.

eBay Hack

Über Sicherheitsprobleme bei eBay wird ja schon seit längerem berichtet (siehe hierzu auch einige Artikel bei http://www.heise.de/security), zum Ende des letzten Jahres wurde dies aber einer breiteren Öffentlichkeit im SternTV (15. und 22. Dezember 2004) vorgeführt. Obwohl die Live-Demos nicht immer reibungslos funktionierten, konnte nachgewiesen werden, dass diverse Möglichkeiten zur Manipulation bei dieser Webapplikation bestehen. So war es ohne großen Aufwand möglich fremde Passwörter zu ermitteln, das Bewertungssystem auszutricksen und auch den angebotenen Treuhandservice zu umgehen.

Technischer Hintergrund
Angriffsarten: Cross-Site-Scripting, Password Guessing

Ein großes Problem stellt seit langem die fehlende Qualität der verwendeten Passwörter dar. Da die Usernamen, z.B. durch Verfolgen der Bieter aus laufenden Auktionen leicht ermittelt werden können, ist ein guter Ansatzpunkt für eine Dictionary-Attacke gegeben. Erfahrungsgemäß benutzen viele User sehr schwache Passwörter, so dass auf diese Weise in kürzester Zeit etliche gültige Usernamen/Passwort-Kombinationen zu finden sein dürften.

Die bei SternTV vorgestellten erfolgreichen Angriffe beruhten im Wesentlichen darauf, das eBay seinen Bietern gestattet, mittels selbst geschriebenem (!) JavaScript die Angebote aufzupeppen. Das ist mal etwas Neues, der Angreifer muss nicht mühselig nach Schwachstellen suchen, die Möglichkeit zur Cross-Site-Scripting Attacke wird damit von eBay selber geliefert. Zwar verbietet eBay per AGB die Verwendung von JavaScript-Funktionen, die Cookies setzen oder auslesen können, den Besucher von eBay zu einem anderen Internet-Angebot weiterleiten, die Funktion „JavaScript Include“ enthalten oder „iframe“-Tags einsetzen, aber ob damit kriminelle Aktivitäten unterbunden werden erscheint doch mehr als fraglich.

Die Möglichkeiten von JavaScript reichen dabei völlig aus, um größeren Schaden anzurichten. Man geht durch z.B. alle Links (<a>) und verändert bei denen, die zum Bezahldienst PayPal oder zur Bewertungsseite zeigen, die URL oder aber den innerText (bei der Bewertungsanzahl („.. Viewfeedback..“). Oder man geht durch alle Bilder (<img>) und verändert seinen eigenen Bewertungs-Stern in einen viel „besseren“. Oder man geht durch alle Tabellenzellen (<td>) und verändert den Inhalt bei „Bewertungsprofil“. Oder man geht durch alle Bold-Tags (<b>) und verändert den innerText („.. Positive Bewertungen: 100% ..“). Die „vertrauensbildenden Bewertungen“ bei eBay sind damit nichts mehr Wert.

Eine andere Möglichkeit besteht darin, in dem manipulierten Angebot das eBay-Login mit einem eigenen Login zu überdecken. Dann wird Benutzername und Passwort abgelauscht und an das „normale“ eBay-Login weitergegeben. Der ahnungslose Benutzer weiß nicht einmal, dass er in die Falle gelaufen ist.

Es bleibt schleierhaft, warum sich eBay so vehement dagegen wehrt, die einfachste aller Gegenmaßnahmen zu ergreifen: JavaScript nicht mehr in Angeboten zulassen. Die vorhandenen Code-Kontrollen von eBay lassen sich offensichtlich leicht unterlaufen und wenn es schon optische Gimmicks geben muss, lassen sich die auch anders bereitstellen.

Guess Hack

Ein in den USA bekannt gewordener Angriff auf Webapplikationen der Firma Guess Inc. zeigt neben üblichen Folgen wie Imageverlust und Ressourcenbindung auch mögliche rechtliche Konsequenzen auf.

Guess ist ein Lieferant von Textilien, der diese auch über seine Website guess.com vertreibt. Ein Hacker entdeckte eine Möglichkeit, in die Kundendatenbank einzudringen und gelangte damit an Namen, Kreditkartennummern und Verfalldaten von über 200.000 Kunden. Nachdem mehrere Versuche scheiterten, die Firma von der Brisanz der Sicherheitslücke zu überzeugen, wandte der Hacker sich an www.securityfocus.com und machte den ganzen Vorgang publik. Danach wurde das Problem sehr schnell beseitigt, aber nun begann der eigentlich interessantere Teil der Geschichte. Die FTC (Federal Trade Commission) schaltete sich ein und nahm Bezug auf eine Erklärung in der Privacy Policy von Guess: „All of your personal information including your credit card information and sign-in password are stored in an unreadable, encrypted format at all times.“ Davon konnte aber nach dem bekannt gewordenen Angriff nun wirklich nicht die Rede sein: die Kundendaten wurden weder verschlüsselt noch irgendwie ähnlich gesichert abgelegt.

FTC erklärte Guess für schuldig, seine Website ungesichert gegen allgemein bekannte Internet-Attacken zu betreiben und ordnete an, keine irrtümlichen Aussagen

mehr zu seinen Sicherheitsvorkehrungen zu machen. Darüber hinaus musste das Unternehmen ein umfassendes Information Security Programm aufbauen, welches in den folgenden 20 Jahren jährlich von einem unabhängigen Auditor zu prüfen sein wird. Jede Zuwiderhandlung wird mit einer Geldstrafe belegt.

Obwohl die angedrohte Geldstrafe mit $11.000 geradezu lächerlich wirkt, ist allein die Wirkung der öffentlichen Bekanntmachung auf andere Unternehmen nicht zu unterschätzen. Jeder, der falsche Aussagen zu seinen Sicherheitsvorkehrungen macht oder durch grobe Fahrlässigkeit erfolgreiche Angriffe geradezu herausfordert, sollte sich auf rechtliche Sanktionen gefasst machen. Und das gilt nicht nur für die USA, sondern sicher auch in Deutschland.

Security Breach Information Act - SB 1386

In Kalifornien sind Firmen per Gesetz verpflichtet, Angriffe auf ihre IT-Systeme an die Kunden zu melden: Der kalifornische Security Breach Information Act zwingt Unternehmen zur Meldung von Einbrüchen in ihre Systeme, wenn dort personenbezogene Daten verarbeitet werden. Dazu muss das Unternehmen nicht zwangsläufig seinen Sitz in Kalifornien besitzen, es genügt auch, kalifornische Kunden zu haben. Dem Gesetz nach reicht auch der begründete Verdacht eines Einbruchs, um eine entsprechende Meldung an die Kunden weitergeben zu müssen. Von dieser Pflicht ist man nur dann befreit, wenn die gespeicherten Kundendaten durch Verschlüsselung geschützt sind. Unternehmen, die der Meldungspflicht nicht nachkommen, müssen mit einer Klage vor Zivilgerichten rechnen.

Technischer Hintergrund
Angriffart: SQL-Injection

Bei dem erfolgreichen Angriff wurde eine Schwachstelle mit SQL-Injection ausgenutzt. Durch eine entsprechend präparierte URL, war es möglich, die erwähnten Kundeninformationen aus der Datenbank auszulesen.

Loomes Hack

Auf dem letzten Kongress des Chaos Computer Clubs 21C3 im Dezember 2004 nahmen es wieder einmal einige Teilnehmer mit der viel beschworenen Hackerethik nicht so genau und suchten fleißig nach Opfern im Internet. Dieses Mal gehörten die CDU Niedersachsen, der Entkalkungsspezialist Calgon sowie der Enthaarungsmittelhersteller Veet dazu. Beide Sites verwiesen -- grafisch schlicht, aber bunt -- auf den Congress und verkünden in ihrem Webgraffiti die Botschaft: „wer nicht hören will, muss Backups einspielen...“. Wirklich ärgerlich war dann aber ein Massenhack, der bis zu 18.000 Kunden des Webhosters Loomes betraf. Dabei wurde zumeist zwar nur die Startseite index.html verändert, die Reparatur hätte also nur darin bestanden die originale Datei zurück zu laden. Aber gerade dies stellte viele der nicht so versierten Loomes-Kunden vor größere Probleme. Das kann man auch sicher nicht von jedem erwarten, eine Erkenntnis, die auch „wohlmeinende“ Hacker lernen sollten.

Ob der Massenhack rechtliche Folgen haben wird, ist bisher unklar. In einer Stellungnahme an seine Kunden erklärt die Loomes AG unter anderem: „Wir haben [...] Strafanzeige gegen den Veranstalter dieses Kongresses erstattet und bitten Sie bei etwaigen Ihnen entstandenen Schäden dieses ebenfalls zu tun.“ Des Weiteren spricht Loomes von einer „vermeintlichen Sicherheitslücke“, auf die „erlebnisorientierte Jugendliche des Chaos Computer Clubs“ glaubten hinweisen zu müssen.

Technischer Hintergrund
Angriffsart: ungeschützter Zugriff auf sensible Daten

Die „vermeintliche Sicherheitslücke“ hatte, wie die Ergebnisse auch zeigten, einen ganz realen Hintergrund. Allem Anschein nach lag ein kompletter Mysql-Datenbankdump als lesbare Datei auf dem Webroot-Verzeichnis eines Loomes-Servers. Darunter waren auch sämtliche ftp-Zugangsdaten der Kunden mit den Passworten im Klartext. Also eine Schlamperei der Administratoren mit großen Auswirkungen und sicher einem hohen Imageverlust. Leider kommt diese Schwachstelle nur allzu häufig vor.

CCC Hack

Aber auch der Chaos Computer Club selber hat Probleme, seine Webapplikationen ausreichend zu schützen, wie ein Vorfall Ende letzten Jahres zeigte.

Spanische Hacker waren in die Server des CCC eingedrungen und hatten unter anderem die Registrierungsdaten vom Hacker-Camp 2003 öffentlich gemacht. Der CCC bestätigte dies in einer Stellungnahme. Die Spanier waren Mitte November laut Angaben des CCC über ein bis dahin unbekanntes Exploit im TWiki-System (OpenSource: webbasiertes Groupware-System) eingedrungen. Dadurch

waren sie in der Lage, beliebige Daten mit den Benutzerrechten des Webservers auszulesen. Da auch Login-Daten zum TWiki-System öffentlich wurden, legte der CCC allen TWiki-Nutzern nahe, ihre Passwörter zu ändern. In der Stellungnahme des CCC zu dem Vorfall heißt es: „ Uns ist diese Angelegenheit äußerst peinlich. Jedoch ist es für uns selbstverständlich, die Informationen zu dem Hack publik zu machen. Wir danken an dieser Stelle den spanischen Hackerkollegen für den Hinweis auf die Sicherheitslücke.“

Technischer Hintergrund
Angriffsart: Ausnutzen einer Applikationsschwachstelle

Vermutlich besteht ein Zusammenhang zur kürzlich gefundenen Schwachstelle in der TWiki-Suchfunktion, zumindest spricht der zeitliche Ablauf dafür. Aufgrund der fehlerhaften Filterung von Benutzereingaben in der Suchfunktion von TWiki können Angreifer beliebige Kommandos im Kontext des Webservers an die Shell übergeben.

Eine Beispielzeichenkette ist:
searchstring ,; ls -la‘

Die TWiki-Suchfunktion nimmt die Zeichenkette als Argument, baut daraus zusammen mit einem Kommando einen String und übergibt ihn an die Shell. Durch das Quote-Zeichen und das Semikolon im Argument interpretiert die Shell den folgenden String allerdings als separaten Befehl. In der Regel können Angreifer die Suchfunktion ohne weitere Authentisierung benutzen.

Anatomie eines Webapplication Hacks

Um die Arbeitsweise eines Hackers transparenter zu machen, wird diese nachfolgend beispielhaft vorgestellt. Die gezeigten Techniken sind bekannt und leicht im Internet nachzulesen, trotzdem weisen wir ausdrücklich darauf hin, dass eine missbräuchliche Verwendung zu unterlassen ist.

Zielsuche mit Google
Die Suche nach verwundbaren Webapplikationen gestaltet sich meist mehr als einfach. Legt der Angreifer es nicht auf bestimmte Webseiten bzw. Applikationen - deren Unterscheidung ja meist fließend ist - an, bringt meist schon eine gut formulierte Google-Suche ausreichend „Material“.

Als Beispiel haben wir für diesen Artikel die webbasierte Portalanwendung „PortalApp“ ausgewählt. Diese Anwendung basiert auf ASP-Seiten mit Datenbankanbindung, hier kann entweder MS Access oder der MSSQL-Server genutzt werden. In der Default-Konfiguration verwendet diese Applikation den HTML <title> Tag „//ASPapp/PortalApp/Freeware Portal Software/Links, Content and Community Management“. Google ermöglicht über den Parameter „intitle“ die direkte Suche nach diesem HTML-Tag. Eine Suche in Google nach dem String „intitle://ASPapp/PortalApp“ hat dann auch immerhin über 7.000 Hits ergeben. Wohlgemerkt, hier wurden nur Webseiten gefunden, die den originalen HTML <title> Tag nicht geändert haben. Es wird vermutlich noch wesentlich mehr Installationen geben. Der Angreifer darf sich also fühlen wie der Hecht im Karpfenteich. (s. Abbildung 2)

Natürlich werden wir unseren beispielhaften Angriff nicht auf eine produktiv eingesetzte Applikation durchführen. Die im Folgenden geschilderten Angriffe beziehen sich daher auf eine Testinstallation im Labor der GAI NetConsult, wären aber sicherlich auch auf einige der im Internet genutzten Anwendungen anwendbar.

Fehlerhafte Beispielskripte
Bei vielen Web- und Webapplikationsserver werden Skripte mitgeliefert, um beispielhaft bestimmte Funktionen des Systems zu zeigen. So auch bei dem in unserem Beispiel genutzten Microsoft Internet Information Server. Eine der hier mitgelieferten ASP-Beispielskripte - die Codebrws.asp - verfügt über eine so genannte Directory Traversal Schwachstelle. Eigentlich soll die Codebrws.asp nur den Quellcode von ASP-Seiten innerhalb des Webserver-Verzeichnisses /iissamples anzeigen. Die Schwachstelle ermöglicht es einem Angreifer jedoch, den Quellcode jedes ASP-Skripts auszulesen. Details zu dieser

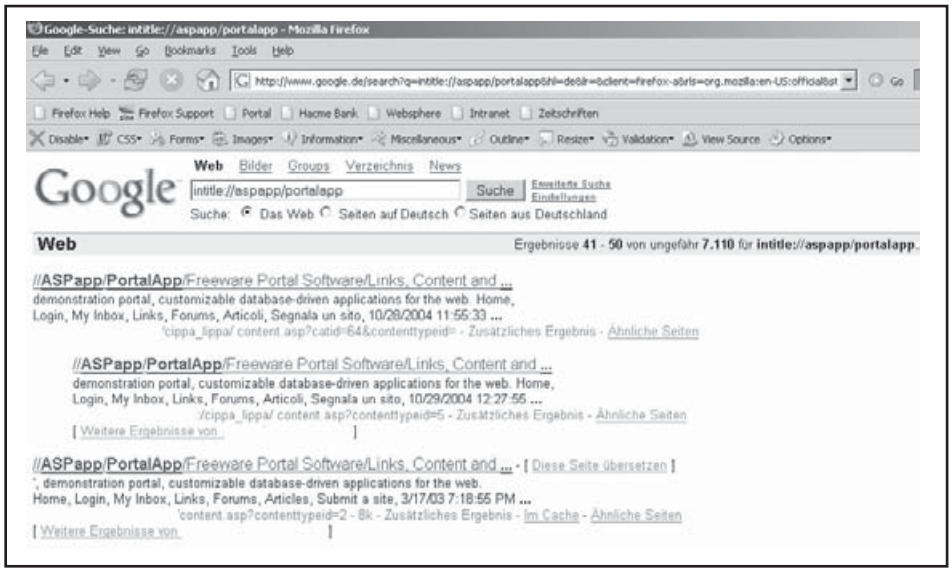


Abbildung 2: Screenshot des Resultats einer Google-Suche nach intitle://aspapp/portalapp

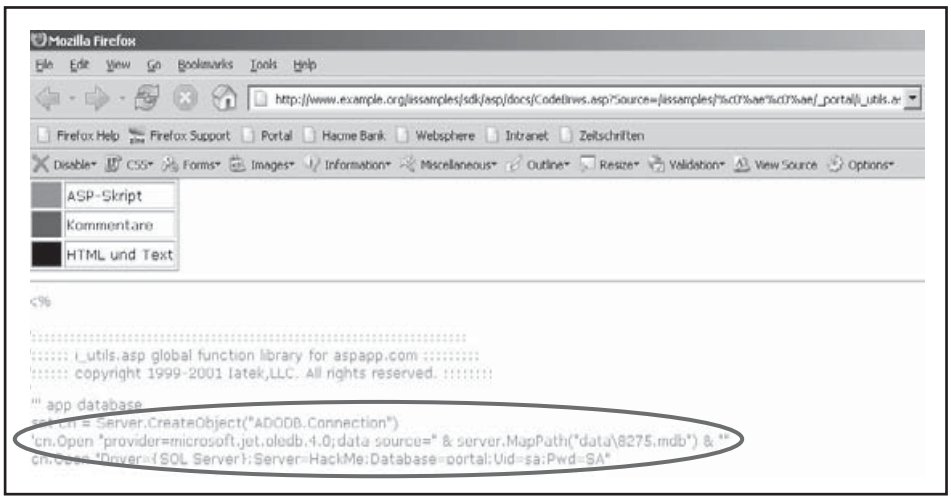


Abbildung 3: Ausgelesener Quellcode der Konfiguration des Datenbankzugriffs

Sicherheitslücke finden sich unter: http://www.securityfocus.com/bid/4525.

Diese Schwachstelle ist nicht in jedem Fall kritisch, da ASP-Quellcode ja nicht unbedingt sensible Informationen enthalten muss. Analysiert man aber den Quellcode unser Applikation kann festgestellt werden, dass die zum Zugriff auf die Datenbank genutzten Authentisierungsdaten im ASP-Quellcode gehalten werden. (siehe Abbildung 3)

Ersichtlich ist hier, dass zum Datenbankzugriff das administrative Konto des SQL-Servers „sa“ genutzt wird. Welche besonderen Implikationen sich aus dieser Konfiguration ergeben wird später noch erläutert.

Angriff!
In derselben ASP-Datei ist auch die zum Datenbankzugriff genutzte Funktion to_sql enthalten, die innerhalb der Applikation global für die Formulierung dynamischer SQL-Statements genutzt wird. (s. Abbildung 4)

Der entscheidende Punkt ist hier, dass bei allen Variablen vom Typ „number“ (genauer gesagt, bei allen Variablen, die kein Datum oder keine Nummer sind) die durch den Nutzer beeinflussten Parameterwerte (z.B. contentid=6) direkt an den Datenbanktreiber übergeben werden! Dies führt letztlich zu dem als SQL-Injection bezeichneten Sicherheitsproblem, da der Angreifer beliebige zusätzliche SQL-Statements an die Datenbank übergeben - injecten - kann.

Möglich sind durch Ausnutzung von SQL-Injection Schwachstellen quasi beliebige Datenbankoperationen. Beispielhaft wird in dem folgenden Angriff der Nutzernamen und das Passwort des administrativen Kontos der Applikation ausgelesen .(siehe Abbildung 5)

Über Manipulation des übergebenen Parameterwertes können nun beliebige zusätzliche SQL-Statements an die eigentliche Abfrage angehängt werden. (s. Abbildung 6)

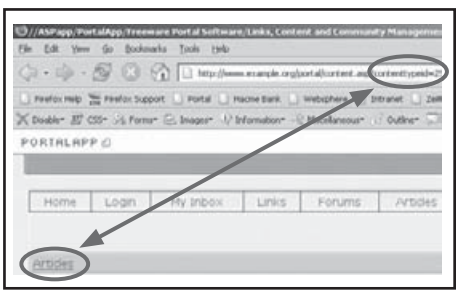


Abbildung 5: Screenshot der Applikation vor der Manipulation des SQL-Statements. Der Parameter Contenttypeid=2 besagt, dass es sich bei dem Typ des Contents um einen „Article“ handelt.

Das angehängt UNION SELECT gaukelt der Applikation vor, dass das Resultat der eigentlichen SELECT Anfrage dem Resultat des UNION SELECT entspräche. Voraussetzung ist, dass die ursprüngliche SQL-Abfrage nach der Contenttypeid kein Ergebnis bringt. Der Wert für die Contenttypeid muss daher auf einen nicht existenten Wert geändert werden. Ebenso kann nun auch das Passwort des administrativen Nutzerkontos der Applikation ausgelesen werden. (siehe Abbildung 7)

Bei SQL-Injection Angriffen sind die im Beispiel verwendeten UNION SELECT Statements besonders beliebt, da so beliebige Daten aus jeder Tabelle der Datenbank ausgelesen werden können, ohne die eigentlichen Datenbankinhalte zu modifizieren.

Ausführung von Systembefehlen
Durch Analyse des Quellcodes der Applikation konnte festgestellt werden, dass zum Zugriff auf die Datenbank das administrative Nutzerkonto „sa“ des MSSQL-Servers genutzt wird. Dies ist in den meisten Fällen völlig unnötig und ermöglicht dem Angreifer bei SQL-Injection Schwachstellen - neben dem Auslesen und der ebenfalls möglichen Manipulation von Datenbankinhalten - zusätzlich die unmittelbare Ausführung von Sys-

```
function to_sql(Value,DataType)
    if Value = "" or isNull(Value) then
        to_sql = "NULL"
    elseif DataType = "date" AND instr(lcase(cn.Providerr),"jet") > 0 then
        to_sql ="#" & Replace(Value, "'","''") & "#"
    elseif DataType <> "number" then
        to_sql = "'" & Replace(Value, "'", "''") & "'"
    else
        to_sql = Value
    end if
end function
```

Abbildung 4: Screenshot der Funktion to_sql

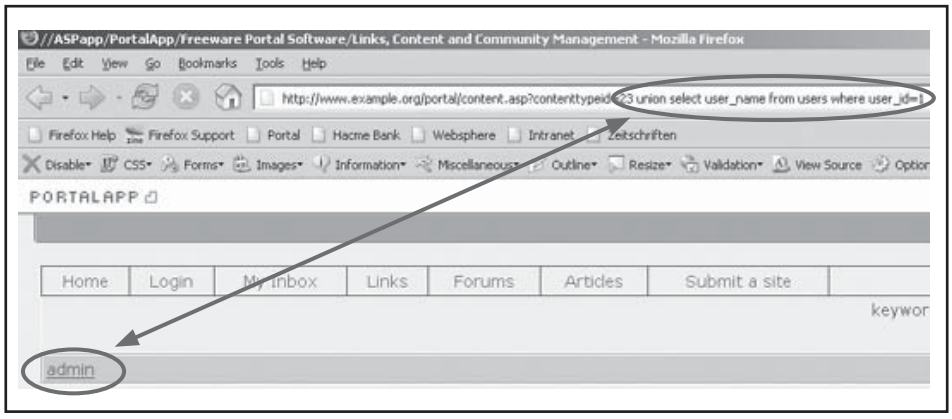


Abbildung 6

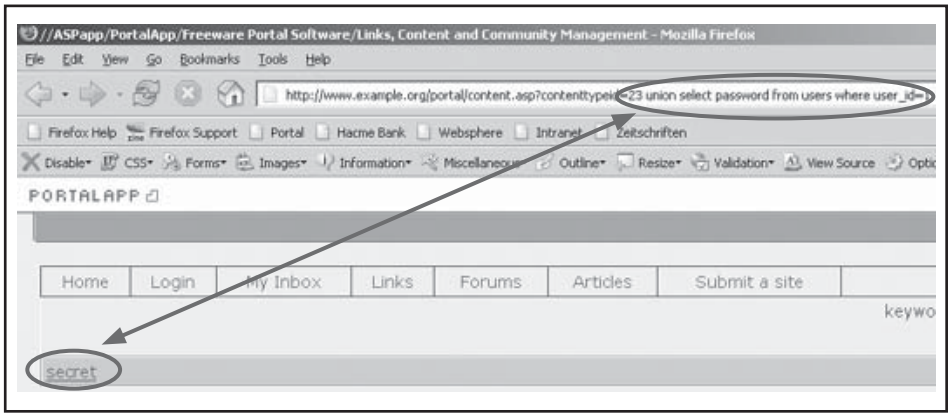


Abbildung 7

tembefehlen. Der MSSQL-Server liefert per Default eine so genannte erweiterte Stored Procedure (Extended Stored Procedure - abgekürzt mit xp) mit, die die Ausführung von Systembefehlen mit den Rechten des Nutzerkontos des SQL-Servers erlaubt. Dies bedeutet also letztlich, dass ein Angreifer durch einfaches Anhängen von zusätzlichen SQL-Statements an die URL im Browser jeden beliebigen Systembefehl auf dem SQL-Server ausführen kann! Da der MS-SQL-Server in der Default Konfiguration mit SYSTEM-Privilegien arbeitet, kann sich ein Angreifer zusätzlich an den maximalen auf einem Windows-System möglichen Nutzerrechten erfreuen.

Ein Problem hat der Angreifer allerdings, die Ausgaben seines Befehls sind meist nicht direkt sichtbar, da die Applikation die Ausgabe des Systembefehls nicht als Eingabe für den Aufbau der Webseite erwartet. In unserem Beispielangriff ist dies allerdings kein großes Problem, da Applikation und Datenbankserver auf einem System laufen. Die Ausgabe eines Systembefehls kann daher einfach in eine Datei im Webroot-Verzeichnis des Internet Information Servers umgeleitet werden. (siehe Abbildung 8)

Aber selbst wenn Web- und Datenbankserver auf unterschiedlichen Systemen betrieben werden, ist es für den Angreifer nicht sonderlich kompliziert, die Ausgaben seiner Befehle zu erhalten. Beispielsweise kann für diese Zwecke eine temporäre Datenbank angelegt werden - über SQL-Injection versteht sich - die Ausgaben der Befehle werden dann in diese Datenbank umgeleitet und mittels der demonstrierten UNION SELECT Technik wieder ausgelesen werden. Letztlich sind die Auswirkungen des Angriffs hier nur von der Kreativität des Angreifers abhängig und weniger von technischen Hindernissen.

Zusammenfassung der ausgenutzten Fehler in der Applikation:

- **Beispielapplikationen wurden nicht entfernt**
  Über die Beispielapplikation Codebrws.asp konnte der Quellcode jeder ASP-Seite ausgelesen werden. Der Angreifer konnte sich so alle Details der Datenbankanbindung beschaffen und dieses Wissen bei späteren Angriffen einsetzen.

- **Fehlende Validierung von Nutzereingaben**
  Die Werte der übergebenen Parameter werden innerhalb der Applikation nicht weiter überprüft, sondern dynamisch an den Datenbanktreiber übergeben. Dies ermöglicht die Durchführung von SQL-Injection Angriffen.

- **Zu weitgehende Rechte beim Zugriff auf die Datenbank**
  Zum Zugriff auf die Datenbank wurde das administrative Nutzerkonto „sa“ des MSSQL-Servers verwendet. Im Zusammenspiel mit SQL-Injection können so mit erweiterten Privilegien beliebige Systembefehle auf dem Datenbankserver ausgeführt werden.

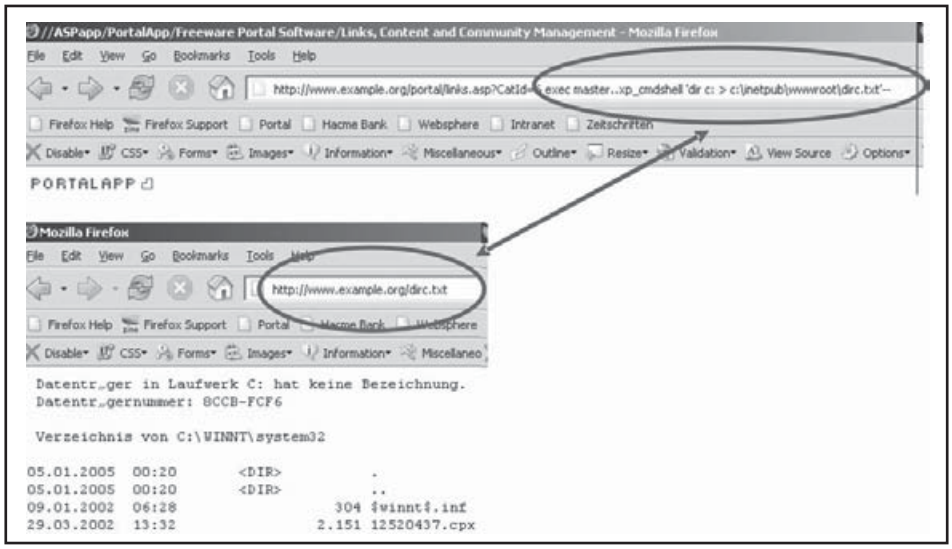


Abbildung 8

Test von Webapplikationen für Jedermann

Zum Selbsttest einer eigenen Webapplikation werden ergänzend zum vorherigen Beispiel noch einige einfache Tipps gegeben. Auch hier wieder der Hinweis: Benutzen Sie diese Tests nur bei Systemen, die in ihren Verantwortungsbereich fallen.

Google-Hacking

„Google-Hacking“ bezeichnet eine Form der Informationsbeschaffung im Vorfeld der

Durchführung eines Angriffs. Wie im vorangegangenen Abschnitt gezeigt, kann Google zur Suche nach potenziellen Zielen für Angriffe auf Webapplikationen genutzt werden. Diese Technik wird derzeit auch von den diversen Varianten des Wurms „santy“ genutzt. Dieser verwendet die Google-Datenbank zur Suche nach PHP-basierten Webseiten. Um die Verbreitung des Wurms einzuschränken, blockiert Google daher im Moment bestimmte Suchanfragen. Sucht man beispielsweise nach dem String „inurl:.php?id=“, dann wird ab der zweiten Seite mit Suchergebnissen diese Meldung wie in Abbildung 9 ausgegeben.

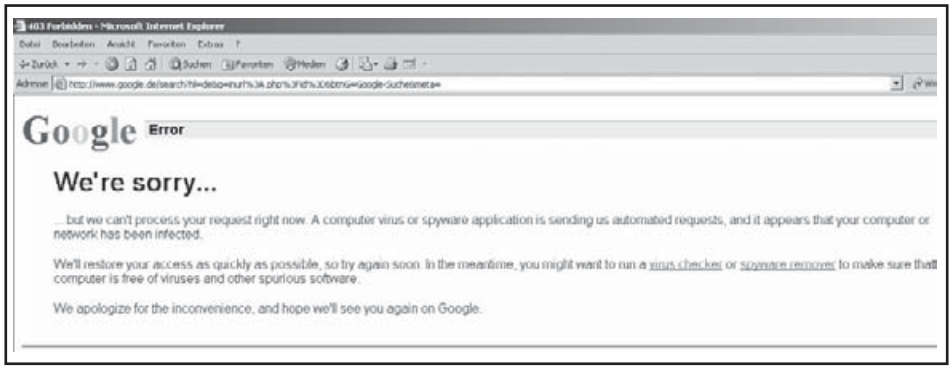


Abbildung 9

Die Suche nach neuen Google-Such-strings ist mittlerweile zu einer Art Volkssport geworden. Eine umfangreiche Sammlung dieser Suchanfragen wurde zur „Google Hacking Database“ - zu finden unter johnny.ihackstuff.com - zusammengefasst. Interessante Suchstrings sind beispielsweise:

- **Suche nach Verzeichnissen mit aktiviertem Directory Indexing**
  Bei aktiviertem Directory Indexing wird jede Datei innerhalb des jeweiligen Verzeichnisses direkt zugreifbar, selbst wenn diese nicht in einer Webseite verlinkt ist. Häufig können so Passwortdateien, Datenbank-Dumps oder Konfigurationsdateien einfach direkt herunter geladen werden.

- **Fehlermeldungen**
  Auch Fehlermeldungen können im Google-Cache landen. Dazu kann es z.B. kommen, wenn zum Zeitpunkt des Zugriffs durch den Google-Bot Teile der Webpräsenz - etwa wg. Wartungsarbeiten - nicht erreichbar sind. Diese Fehlermeldungen geben einem Angreifer häufig Informationen, die dann im weiteren Verlauf eines Angriffs genutzt werden.

- **Ungeschützte Administrations-Webseiten**
  Viele Geräte wie Drucker, Webcams oder ähnliches werden über integrierte Webserver administriert. Sind für diese administrativen Webserver keine Formen des Zugriffsschutzes realisiert, kann jeder Nutzer im Internet direkt auf die Systeme zugreifen. So kann z.B. über die Suche nach „intitle:liveapplet inurl:LvAppl“ direkt auf die Ausgabe von über 100 Canon Webcams zugegriffen werden.

Mittlerweile existieren auch diverse Werkzeuge mit denen die Suche toolbasiert durchgeführt werden kann. Foundstone stellt mit Sitedigger hier ein sehr interessantes Werkzeug bereit, welches die Google-API zur Durchführung der eigentlichen Suche verwendet. Sitedigger kann über http://www.foundstone.com/resources/s3i_tools.htm heruntergeladen werden.

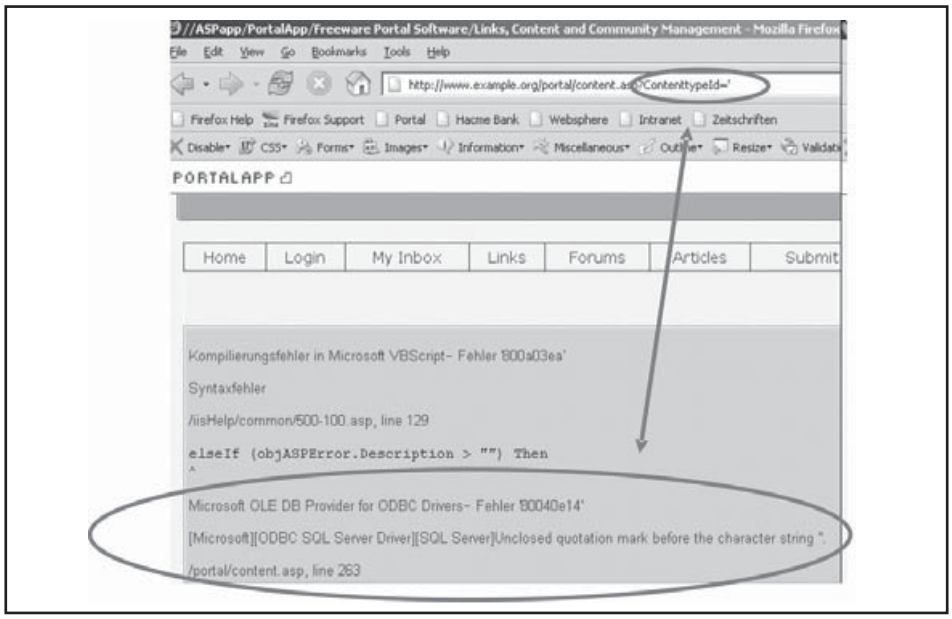


Abbildung 10

SQL-Injection
SQL-Injection ist wohl das Sicherheitsproblem bei Webanwendungen mit den weitreichendsten Auswirkungen. Trotzdem kann eine Verwundbarkeit gegenüber SQL-Injection häufig recht einfach erkannt werden. Dies kann z.B. über das Einfügen bestimmter zusätzlicher Parameter in der URL erfolgen. Dabei werden zwei Methoden unterschieden: das Erzeugen von Fehlermeldungen und das Einfügen zusätzlich boolescher Ausdrücke:

- **Erzeugen von Fehlermeldungen**
  Als Beispiel für die Erzeugung von Fehlermeldungen kann wieder unsere Portalanwendung dienen. Die URL http://www.example.org/portal/content.asp?ContentId=1 verursacht vereinfacht ausgedrückt folgende SQL Anfrage:

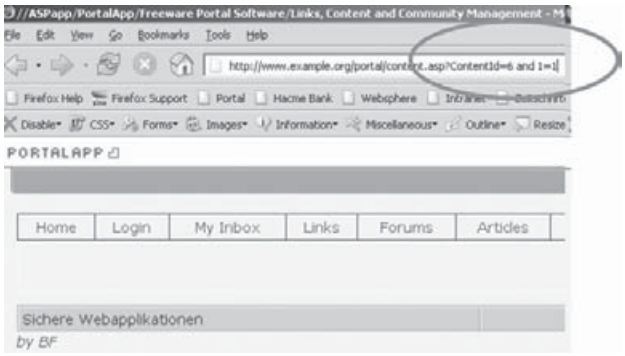
  SELECT * FROM Content WHERE ContentID = 1

  Das Einfügen eines Hochkommas verursacht diese SQL Anfrage:

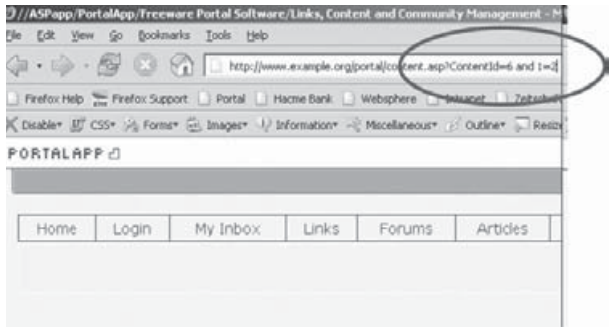
  SELECT * FROM Content WHERE ContentID = ‘

  Hierbei handelt es sich um eine fehlerhafte SQL-Syntax, was zur Ausgabe einer Fehlermeldung des jeweiligen Datenbanktreibers führt. (s. Abbildung 10)

- **Erweitern der WHERE Clause um einen booleschen Ausdrucks**
  In vielen Fällen werden Fehlermeldungen nicht ausgegeben, sondern von der Applikation abgefangen. Aber auch dann kann relativ einfach erkannt werden, ob eine Anwendung gegenüber SQL-Injection verwundbar ist. Hierfür wird die WHERE Clause der SQL Anfrage (im Beispiel WHERE ContentID=1)



Die Webseite wird normal angezeigt, da das Resultat der WHERE-Clause true ist (1=1 ist immer wahr).



Die Webseite wird nicht vollständig angezeigt, da das Resultat der WHERE-Clause nun false ist (1=2 ist immer falsch).

Abbildung 11

um einen weiteren booleschen Ausdruck ergänzt. Ist eine Anwendung gegen SQL Injection verwundbar, sieht das Resultat dieser Erweiterung etwa so aus wie in Abbildung 11.

In beiden Fällen kann durch Einsatz automatisierter Tools der komplette Inhalt der Datenbank gespiegelt werden. Eines dieser Werkzeuge hört auf den Namen Absinthe und kann über die Webseite http://www.0x90.org/releases/absinthe/ herunter geladen werden.

XSS

Auch eine Anfälligkeit gegen die häufigste Schwachstelle in Webanwendungen - Cross-Site-Scripting - ist recht einfach zu entdecken. Immer dann, wenn eine Eingabe des Nutzers ungeprüft in der Ausgabe der Webseite verwendet wird, kommt es zu diesem Sicherheitsproblem. Häufig trifft man Cross-Site-Scripting in Webforen und vor allen Dingen bei der Ausgabe von Fehlermeldungen. Das Hauptziel eines Cross-Site-Scripting Angriffs ist es, an den Cookie eines angemeldeten Nutzers zu gelangen und so die Session dieses Nutzers zu übernehmen. Im Gegensatz zu SQL-Injection ist Cross-Site-Scripting allerdings ein indirekter Angriff. Dies bedeutet, dass der Nutzer eine gewisse Mitwirkung an der Durchführung des Angriffs leisten muss. Ausreichend ist hier allerdings, wenn der Angreifer den Nutzer dazu bringen kann, auf einen vom Angreifer vorgegebenen Link zu klicken. Die Screenshots unten erläutern die Durchführung eines Cross-Site-Scripting Angriffs. (s. Abbildung 12)

Probleme bei der Autorisierung

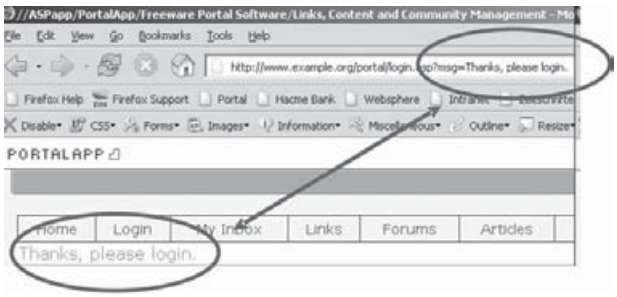
Viele Webapplikationen übergeben global gültige Variablenwerte (z.B. UserID=12345) innerhalb der URL oder eines Formularparameters. Die Anwendung verlässt sich dann darauf, dass der Nutzer diesen Parameter nicht ändert. Tut er es doch, ist häufig ein Zugriff auf fremde Datensätze möglich. Das Problem der Autorisierung ist insbesondere bei Datenbankzugriffen gegeben, da Applikationen im Allgemeinen einen Pooluser zum Zugriff auf die Datenbank nutzen und keine Autorisierung auf Datensatzebene durchführen. Dieses Problem war eine der Schwachstellen, die innerhalb des T-Com Hacks ausgenutzt wurden, um auf fremde Kundendaten zuzugreifen.

Die 10 Tips zur Sicherung von Webapplikationen

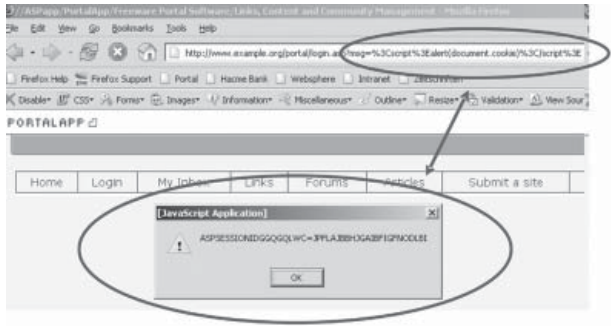
Die folgende Aufstellung bietet Ihnen eine komprimierte Hilfe zum Aufbau von sicheren Webapplikationen. Es werden die häufigsten „Baustellen“ und sicherheitskritischen Bereiche bei der Entwicklung und beim Betrieb von Webapplikationen betrachtet.

1. Bereitstellen einer sicheren Serverumgebung

Die sicherste Anwendung hilft nicht gegen Sicherheitslücken in den darunter liegenden Komponenten. Das gesamte System bestehend aus Hardware, Betriebssystem, evtl. eingesetzter Middleware und der ei-



Die Eingabe des Nutzers für den Parameter „msg“ wird direkt für den Aufbau der Webseite verwendet.



Da die Nutzereingabe ungeprüft in die Ausgabe übernommen wird, kann Skriptcode in den Seitenaufbau injiziert werden. In diesem Fall wird der aktuelle Cookie des Anwenders ausgegeben. Durch eine andere Formulierung des Skriptcodes hätte der Angreifer den Cookie auch an eine externe Webseite übermitteln können.

Abbildung 12

gentlichen Anwendung muss grundsätzlich zusammen betrachtet und gesichert werden. Sicherheitspatches sind einzuspielen und die Konfiguration ist zusätzlich zu härten. Besonders gilt das für den eingesetzten Web-Server. Vergessene Demoapplikationen und ausführbare Directorylistings sind nur zwei Beispiele von leicht zu beseitigenden, aber trotzdem häufig vorzufindenden Schwachstellen.

2. Netzwerkabsicherung der Webapplikation

Webapplikationen sollten immer in einem eigenen gesicherten Netzwerksegment platziert werden. So kann der Zugriff auf die Webapplikation durch eine Firewall auf die zwingend notwendigen Ports beschränkt werden (meist http/80 und ssl/443). Um einen Schutz auch auf Protokollebene zu ermöglichen, sollten dabei Application Level Proxies eingesetzt werden. Mittlerweile sind auch SSL-Proxies verfügbar, die in der Lage sind auch verschlüsselte Datenströme zu kontrollieren. Für einen weiter gehenden Schutz bieten sich so genannte Web Application Firewalls an, die als filternde Proxies vor die eigentliche Webapplikation geschaltet werden.

3. Multi Tier Ansatz zur Auftrennung der Anwendungsmodule

Eine Auftrennung der Anwendung in verschiedene Module (häufig in Präsentations-, Applikations- und Daten-Schicht) und deren Verteilung auf verschiedene Server ermöglicht eine bessere Absicherung der einzelnen Teile. Die Kommunikation der einzelnen Module kann durch zusätzliche trennende Firewalls überwacht und kontrolliert werden. Auf keinen Fall sollten auf dem extern erreichbaren Web-Server sensible Daten lokal gespeichert werden. Eine einfache Trennung kann schon durch Vorschalten eines Reverse-Proxies erfolgen.

4. Verwendung minimaler Rechte

Prozesse und die dazugehörigen User sollten immer nur mit den minimalen, gerade für die beabsichtigte Aufgabe ausreichenden Rechten arbeiten. Das betrifft z.B. den Web-Server, der normalerweise nur lesenden Zugriff auf die hinterlegten Inhalte besitzen muss, aber keine Schreib-rechte benötigt. Ein weiteres Beispiel sind SQL-Anfragen an die Datenbank. Die zum Zugriff benutzte Datenbank-Kennung sollte nur die tatsächlich benötigten Rechte, auf keinen Fall aber weit reichende administrative Rechte (wie z.B. Änderung des Datenbankdesigns, Import/Export von Inhalten etc.) besitzen. Durch die konsequente Anwendung minimaler Rechte erschwert man Angreifern die einfache Ausnutzung noch vorhandener Sicherheitslücken.

5. Nutzung anerkannter Sicherheits-Algorithmen

Im Bereich der Authentisierung und Verschlüsselung gibt es eine Reihe gut eingeführter und allgemein als sicher anerkannter Algorithmen. Die Entwickler sollten auf diese Algorithmen und Libraries zurückgrei-

fen. Eigenentwicklungen sind ein kaum abzuschätzendes Sicherheitsrisiko. Gerade für die Standardaufgaben, wie Kennwortverschlüsselung, sichere Datenübertragung oder die Signierung von Daten gibt es für jede Entwicklungsumgebung eine reiche Auswahl an fertigen und sicheren Lösungen.

6. „Security by obscurity" funktioniert nicht

Grundsätzlich sind sämtliche relevanten Ressourcen über Zugriffsmechanismen zu schützen. Nichtverlinkung oder „Verstecken" alleine ist kein ausreichender Schutz. Ebenso sind Authentisierungsmerkmale, die leicht herausgefunden werden können (z.B.: Postleitzahl, Kundennummer etc.) oder vielleicht sogar in öffentlichen Teilen der Anwendung ersichtlich sind, als sehr schwach einzustufen. Bei der Prüfung einer Anwendung auf ihre Sicherheit sollte man immer von der Annahme ausgehen, dass dem Angreifer alle derartigen Informationen zur Verfügung stehen.

7. Rigide Überprüfung von Ein-/Ausgabeparametern

Sämtliche Parameter, die vom Anwender (bzw. seinem Web-Browser) an die Webapplikation gesendet werden sind, genauestens auf Gültigkeit hin zu überprüfen. Dies gilt auch für Parameter, die von der Webapplikation selbst in einem vorhergehenden Schritt zum Anwender geschickt wurden - auch diese können clientseitig mit entsprechenden Tools leicht manipuliert werden. Durch eine derartige Prüfung können eine ganze Reihe von typischen Schwachstellen (Code Injection, Buffer Overflows, etc.) vermieden werden. Dabei ist insbesondere zu beachten, dass der http-Standard die Kodierung von Zeichen in verschiedenen Repräsentationen vorsieht (z B. Unicode). Vor Prüfung der Parameter sind die Inhalte in dem verwendeten Zeichensatz zu normalisieren.

8. Sichere Behandlung von Fehlerfällen

Alle Programme enthalten Fehler - entscheidend für die Sicherheit ist, wie Anwendungen in Fehlersituationen reagieren. Es sollte grundsätzlich ein „Fail save" Verhalten implementiert werden. Ein Sicherheitsmodul zur Authentisierung darf nicht bei einem Ausfall Anwender auch ohne Kennwort akzeptieren. Ein weiteres Beispiel ist Verschlüsselung (z.B. SSL): Der Fallback auf niedrige Verschlüsselungsstärke im Rahmen der Initialisierungsprozesse zwischen Client und Server muss explizit verhindert werden. Auch sollte der Anwender zwar mit Fehlermeldungen bei Fehlverhalten informiert werden, dabei dürfen aber keine für einen Angreifer verwertbaren Informationen mitgeliefert werden. Solche Informationen gehören ausschließlich in ein nur intern zugängliches Logfile.

9. Die häufigsten Schwachstellen in Web-Anwendung

Es hat sich gezeigt, dass einige wenige typische Fehler bei der Implementierung zu einem Großteil der vorhandenen Schwachstellen beitragen. Zu beachten sind insbesondere:

a. Ungeprüfte Ein- Ausgabeparameter
   Hierzu gehören die hinlänglich bekannten Buffer Overflows, die aus fehlender Längenprüfung der Parameter resultieren, aber auch Fehler auf Anwendungsebene bei Übergabe von Daten.

b. Zugriffsrechte fehlerhaft
   Die Zugriffsrechte auf Dateien, Datenbanken oder Prozesse sind fehlerhaft oder unvollständig umgesetzt. Angreifer erhalten Zugriffe, zu denen sie nicht berechtigt sind.

c. Fehlerhaftes Sessionmanagement
   Die „Credentials" oder Tokens, die zur Herstellung einer Sessionzuordnung verwendet werden, sind nicht ausreichend gegen Manipulation geschützt. Angreifer können auf diese zugreifen und damit die geschützten Daten anderer Anwender lesen.

d. Cross Site Scripting
   Die Webapplikation kann dazu missbraucht werden, gefährlichen Scriptcode an die Browser anderer Anwender zu schicken. Der Angreifer kann dadurch z.B. die Session des betroffenen Anwenders übernehmen.

e. Command Injection
   Die Anwendung reicht ungeprüft Parameter an andere Anwendungen (z.B. SQL) oder das Betriebssystem weiter. Der Angreifer kann dadurch gefährliche Befehle an die Anwendung senden.

10. Security Audit der Webapplikation

Zumindest Webapplikationen, die einen erhöhten Schutzbedarf besitzen, sollten vor ihrer Produktivsetzung einem Security Audit unterzogen werden. Dabei ist zu beachten, dass nicht nur auf bekannte Fehler in Betriebssystem, Web-Server, Middleware etc. geprüft wird, sondern auch die Webapplikation selbst auf die o.g. Probleme hin untersucht wird. Erfahrungsgemäß sollten dabei sowohl Tests ohne gültige Benutzerkennung als auch solche mit Zugang als registrierter Benutzer durchgeführt werden.

Schwerpunktthema

Technologie-trends für Enterprise Redesign: Wireline und Wireless für PAN, LAN, MAN, RAN

Fortsetzung von Seite 1

Dipl. Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

1. Anforderungen an Enterprise Netze vom PAN bis zum MAN

1.1 Aufteilung in Netzwerkbereiche

Bei der Entwicklung eines strukturierten Netzwerk-Designplans für Unternehmens-Umgebungen (Enterprise Netzwerke) ist die Unterteilung in Struktur-Bereiche sinnvoll. Hierfür bietet eine räumlich-geografische Ordnung an, wie sie auch die Standardisierung vorgenommen hat:

PAN	Personal Area Network	0,1	bis	10 m
LAN	Loacal Area Network	2 m	bis	10 km
MAN	Metropolitan Network	10 km	bis	100 km
RAN	Regional Area Network	10 km	bis	100 km
WAN	Wide Area Network	10 km	bis	xx 1000 km

Dieser Beitrag beschränkt sich auf die Bereiche, die üblicherweise von privaten Betreibern/Unternehmen im Eigenbetrieb genutzt werden, also PAN, LAN sowie MAN/RAN als Grenzbereich. Letzteres könnte sich mit den aufkommenden neuen Technologien in den nächsten Jahren ändern, so dass der private Bereich sich ausdehnt. Nur sehr wenige Großkonzerne betreiben ein eigenes Corporate WAN, die meisten Anwender/Unternehmen nutzen hier Dienste öffentlicher Carrier, daher bleiben WAN Technologien hier unbehandelt.

PAN
Personal Area Networks decken den Bereich eines einzelnen Arbeitsplatzes, Produktionsplatzes oder einer einzelnen Person bzw. „um eine einzelne Person herum“ ab. Hierzu können auch fest montierte vernetzte Gebäudeinfrastruktur-Komponenten wie Sensoren, automatische Türöffner, Lichtschalter oder ähnliches zählen. Die Reichweite ist von Dezimetern bis maximal 10 Meter definiert.

LAN
Zum Bereich LAN muss für den Insider Leser sicher nicht viel erklärt werden. Fassen wir nochmals zusammen: Unter LAN wird im Regelfall ein privat betriebener Bereich der Ausdehnung bis 10 km verstanden, dieser steht seit Jahrzehnten im Fokus der IEEE 802 Standardisierung und des so genannten „Enterprise“ Marktes. Verkabelte Technologien wie Arcnet, Token Bus, Token Ring, FDDI, VG AnyLAN und ATM hatten hier ihre längere, kürzere oder auch gar keine Blütezeit, von den Anfangstechnologien übrig geblieben ist lediglich IEEE 802.3 Ethernet.

Seit einigen Jahren erhält Ethernet zunehmend Konkurrenz durch Wireless LAN Technologie, standardisiert durch die IEEE Arbeitsgruppe 802.11, die aktuell relativ virulent Output generiert. Die Ethernet Gemeinde wehrt sich jedoch, indem sie ihren Wirkungsbereich mit EFM (Ethernet on the First Mile) und Residental Ethernet (ReSE, zur Zeit 802.3 Study Group) sowohl in Richtung MAN als auch in Richtung PAN auszudehnen trachtet.

MAN / RAN
Dieser Bereich wird von größeren Unternehmen, insbesondere Kommunen oder EVU‘s, teilweise im Eigenbetrieb abgedeckt, mittlere und kleine Unternehmen nutzen sowohl Dienste von den großen öffentlichen Carriern als auch zunehmend kleineren regionalen City Carriern. Letztere erringen sich ihren Marktanteil durch preisgünstige Angebote und im Vergleich zu den großen Carriern schnellere Implementierung neuer Dienste wie VoIP oder Wireless als Ersatz für DSL oder ISDN. MAN‘s haben den Fokus auf Großstadträumen und Ballungsgebieten, RAN‘s schließen eine dünnere Besiedelung bis hin zu ländlichen Bereichen mit ein.

1.2 Planungsaspekte beim Neu- und Redesign

Für eine Entscheidung, ob eine bestimmte Technologie in einem spezifische Unternehmensumfeld einsetzbar und zu empfehlen ist, werden wir die verschiedenen wireless und wireline Technologien hinsichtlich ihrer Brauchbarkeit für ein Neu- oder Redesign von Enterprise Netzen unter Berücksichtigung wichtiger Planungsaspekte betrachten:

- Architektur
- Standards
- Redundanz
- Routing / Roaming
- Sicherheit
- QoS
- Voice-Readiness
- Mobilität

Wesentliche Elemente der Architektur sind Dienstneutralität / Flexibilität für den Betrieb konvergenter IT- und TK-Anwendungen, Skalierbarkeit durch Hierarchiebildung mit

Routing / Roaming sowie erreichbare Verfügbarkeit durch Redundanzverfahren. Darüber hinaus sind insbesondere die Anforderungen „Voice-ready“ und „Mobilität“ in den letzten zwei Jahren in den Anwender-Fokus gerückt, woraus sich automatisch die Forderung nach einer angemessenen Sicherheits-Funktionalität ergibt, da TK vielfach als sicherheitskritischer Dienst eingestuft wird und Mobilität im Zusammenhang mit wireless Verfahren aufgrund des „frei“ zugänglichen Übertragungsmediums Luft ein Sicherheitsproblem per se darstellt. Sprache als Echtzeit-Dienst stellt weitergehende Anforderungen hinsichtlich der Dienstgüte (QoS), mindestens für die Parameter Verlustrate, Antwortzeit, Durchsatz und Schwankung der beiden letztgenannten.

Für die genannten Anforderungen gibt es eine Reihe von Herstellerlösungen. Verfügbare Standards und nachfolgend interoperable Produkte sind jedoch wichtig, um die Zukunftssicherheit für eine Designentscheidung zu maximieren, da nur bei verfügbaren Standards Produkte eines Herstellers durch die eines anderen ersetzt werden können, ohne das Risiko, eine Designänderung vornehmen zu müssen.

Nachfolgend werden wir zuerst den aktuellen Stand sowie zu erwartende Weiterentwicklungen bei Wireline Technologien betrachten, danach die Entwicklungen von Wireless Technologien und als dritten Teil die Frage beleuchten, ob und wie sich beide Welten integrieren lassen.

2. Wireline: Verkabelte Netze

2.1 Ethernet PAN

Für verkabelte Arbeitsplätze / Server wird das PAN als integraler Bestandteil des LAN betrachtet und mit Ausnahme von Verkabelungs-Vorschriften für den Arbeitsplatzbereich nicht weiter separat behandelt. Soweit Komponenten mit geringer Leistungsaufnahme eingesetzt werden (Telefone, Kameras, Lautsprecher etc.), sind sie Kandidaten für zentrale Stromversorgung. Im aktuellen Betrieb verfügen die Arbeitsplätze mit Gbit Ethernet (1000BASE-T) trendmäßig über eine höhere Datenrate als die meisten Anwender benötigen. Die Anbindung an das Netzwerk bremst die Datenrate in vielen Fällen auf 100 Mbit herunter, da die eingesetzten LAN Switchtes noch nicht Gbit-fähig zum Endgerät ausgelegt sind. Dies gilt nicht für Server, die seit 2004 im Regelfall mit Gbit Ethernet angebunden werden. Einzelne Sondergeräte (Messgeräte, ältere Drucker, Zeiterfassung, Produktionskomponenten) unterstützen nur 100 Mbit oder sogar nur 10 Mbit hdx.

Nach wie vor dominiert Kupfertechnik und nicht LWL den Markt. Dies wird durch den Einsatz von Telefonen oder andere mit zentraler Stromversorgung (IEEE 802.3af, PoE) betreibbare Geräte noch verstärkt. Neue Standards wie IEEE 802.3ak 10GBASE-CX (verabschiedet) und IEEE 802.3an 10GBASE-T (erwartet für 2006)

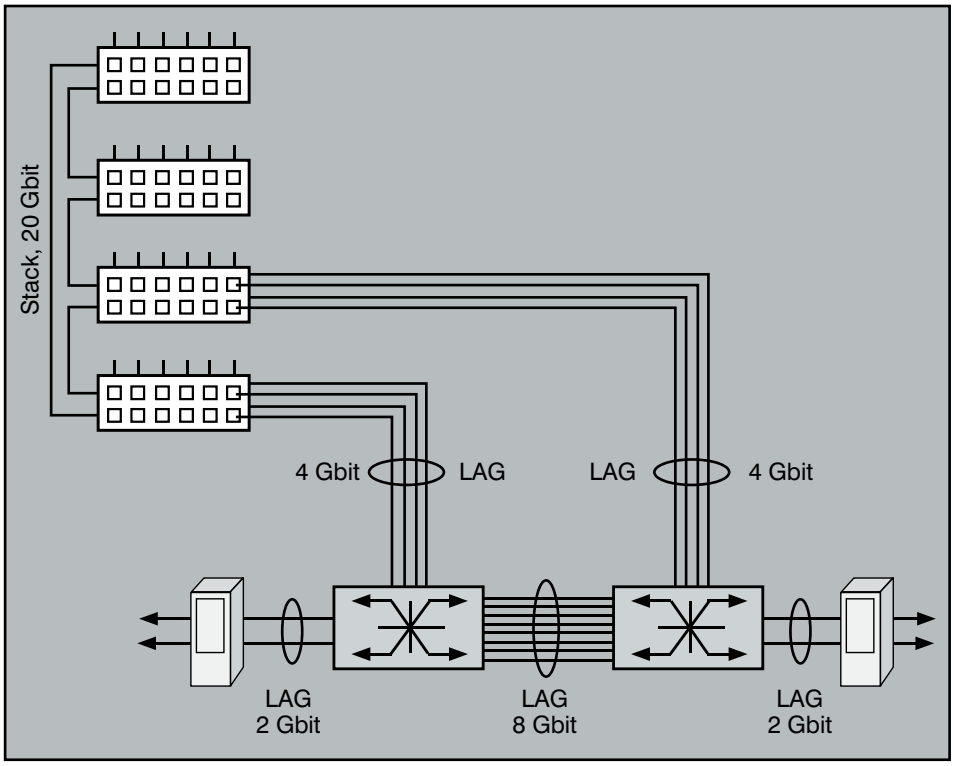


Abbildung 2.1: Einsatz von 10GbE-Ready Switchstacks

zeigen einen weiteren Wachstumsschritt auf. Ethernet über Twisted Pair hat sich daher im PAN als dienstneutrale, skalierbare, redundante und sicher betreibbare Architektur etabliert, für die Standards zur Verfügung stehen. Die Integration von TK ermöglichen separate Endgeräte oder TK-Softwarelösungen für den PC. Die QoS-Anforderungen für Voice im PAN-Bereich können ab einer geswitchten PAN-Struktur mit dedizierter Anbindung jedes Endgerätes an einen Switchport mit einer Datenrate von 100 Mbit oder höher als gegeben betrachtet werden. Die Anforderung an Sicherheit ist mit SRTP und IEEE 802.1X oder andere webbasierte Authentifizierungsmethoden technisch gegeben, jedoch erst in den jetzt kommenden VoIP-Produktgenerationen verfügbar. Nicht abgedeckt wird die Anforderung nach Mobilität, da stets eine freie und an die Netzwerkinfrastruktur angeschlossene Datensteckdose benötigt wird.

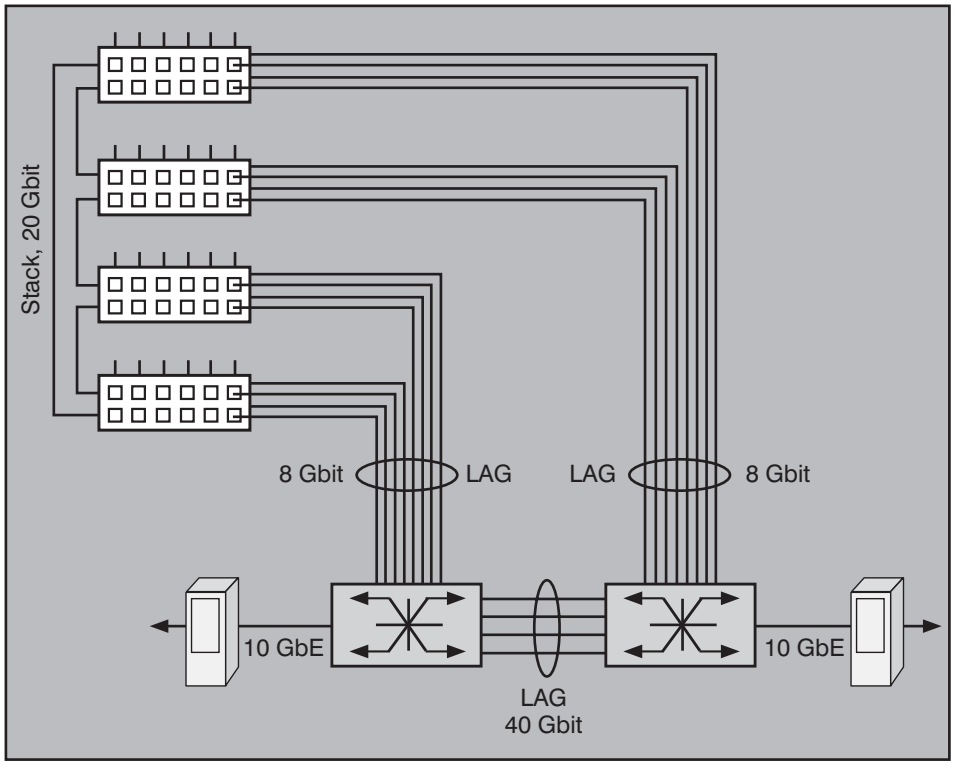


Abbildung 2.2: Einsatz von 10GbE für Stackverbindung, Backbone-Kopplung und einzelnen Servern

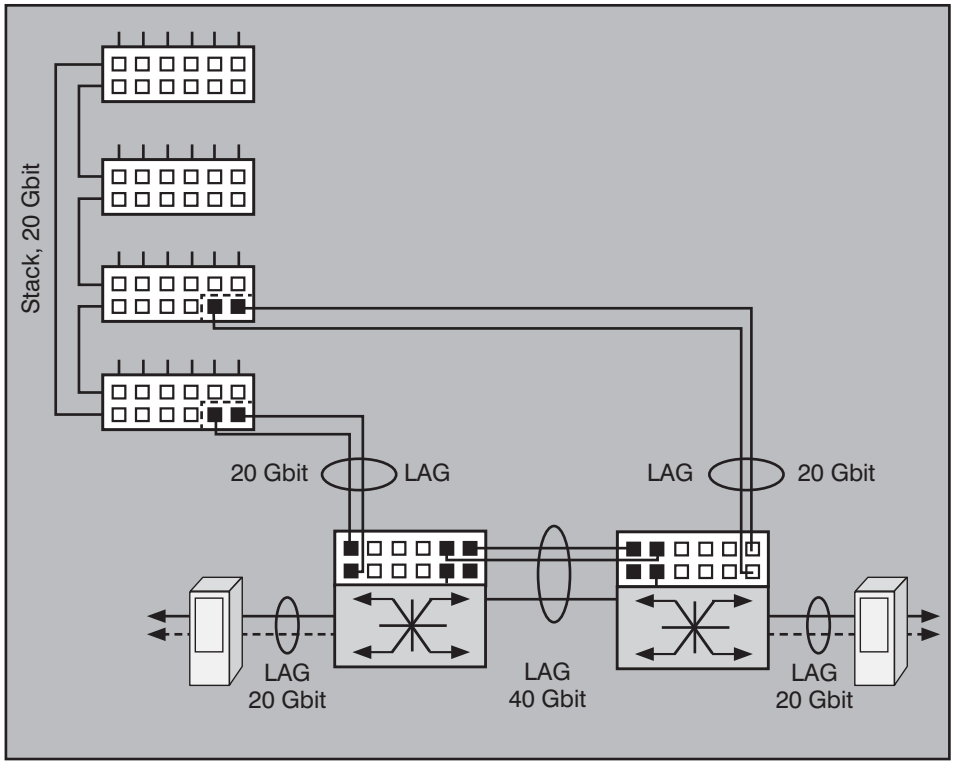


Abbildung 2.3: Einsatz von 10GbE Uplinks, 10 GbE LAG für Backbone-Kopplung und Server

2.2 Ethernet LAN

Seit 2004 ist eine schrittweise Etablierung von 10 Gbit im verkabelten LAN erkennbar. Sowohl die seit 2004 neu ausgelieferten Workgroup Switches als auch die modularen Switches können als „10GbE-Ready“ bezeichnet werden: Workgroup Switches sind mit mehrfach 10 Gbit Stackverbindungen und bis zu zwei 10GbE Schnittstellen XGMII ausgerüstet oder nachrüstbar (XenPAK als normaler Form Faktor oder XFP als kleiner Formfaktor). Modulare Switches verfügen über Gesamtleistungen von 320 bis zu 480 Gbit/s fdx und einen Modulzugang von 20 bis 40 Gbit/s fdx zur Switching Matrix oder zu anderen Modulen. Eine schrittweise Migration zu 10 Gbit/s ist somit technisch möglich und nur noch eine Frage des Kostenverfalls. Dieser ist aktuell bei einer Marke von 4.000 bis 12.000 EUR für einen 10 Gbit Port angekommen. Im ersten Schritt ist es daher z.B. empfehlenswert, 10 Gbit-fähige Switchstacks auf den Etagen einzusetzen, jedoch noch mit den vorhandenen GBIC Uplinks an den Backbone anzuschalten. Im zweiten Schritt kann die Backbone-Kopplung zentraler modularer Switches über mehrfach 10 Gbit erfolgen, bei weiter sinkenden Kosten werden die 10 Gbit Uplinks auf den Etagen aktiviert und weitere 10 Gbit Module in den zentralen modularen Komponenten eingebaut. Zu diesem Zeitpunkt werden ebenfalls 10 Gbit NIC‘s für Hochleistungs-Server verfügbar sein. Die beschriebenen Migrationsschritte sind in Abbildung 2.1 bis Abbildung 2.3 verdeutlicht.

Redundanz/Routing

IEEE 802.1D RST / STP, IEEE 802.1Q MST, und IEEE 802.3ad LAG als standardisierte Redundanzverfahren sowie hierarchische Skalierbarkeit mittels OSPF, BGP und VRRP sind seit Jahren etabliert, werden hier als bekannt vorausgesetzt und nicht weiter vertieft. Für Interessenten wird auf das Netzwerk Insider Archiv 2002 bis 2004 sowie den Technologie-Report „Design-Varianten Lokaler Netzwerke im Vergleich“ verwiesen.

Ethernet, im Tertiärbereich über Kupfer, im Backbone über LWL, hat sich im LAN-

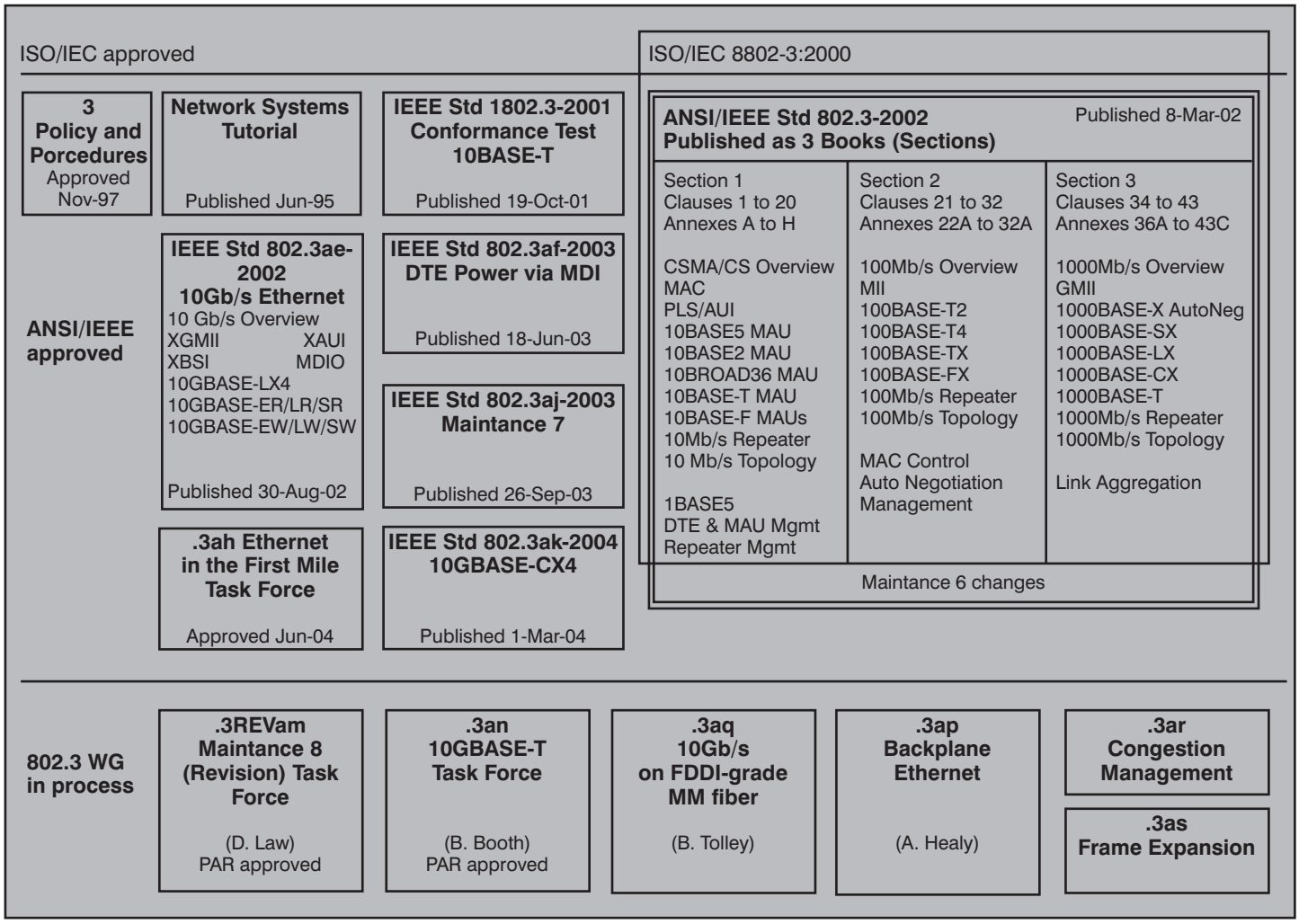


Abbildung 2.4: Standards der IEEE Arbeitsgruppe 802.3

Bereich als dienstneutrale, skalierbare, redundante und sicher betreibbare Architektur etabliert, für die sowohl Standards als auch interoperable Produkte zur Verfügung stehen. Voice-Readiness ist durch simple Überkapazität oder Konfiguration von Priorisierung mit Bandbreitenlimitierung und CAC als gegeben einzustufen. Die Anforderung an Sicherheit ist mit IEEE 802.1X oder anderen webbasierten Authentifizierungsmethoden, IDS- und Firewall-Systemen als technisch gegeben einzustufen. Eingeschränkt abgedeckt wird die Anforderung nach Mobilität, da stets eine freie und an die Netzwerkinfrastruktur angeschlossene Datensteckdose benötigt wird. Die erforderliche LWL-Verkabelung für Backbone-Strukturen generiert insbesondere bei Neuplanungen, aber auch bei Sanierungen und Redesign-Planungen einen entsprechenden Kostenfaktor.

2.3 Wireline MAN / RAN

Als verkabelte Technologien sind hier Metro Ethernet (10GBASE-ER, 1000BASE-LH, 100BASE-FX), aber auch die klassischen Dienste FR, ATM, E1/E3 Festverbindung zu sehen. Eine Zwischenstellung nehmen DSL und der neue Standard EFM (IEEE 802.3ah, Ethernet on the First Mile) als so genannte Last Mile Techniken ein, die den Übergang vom LAN zum WAN über relativ kurze Distanzen bis zu 5 km realisieren. Der Trend geht hier erkennbar zu Datenraten von 10 Mbit und höher. Alle genannten Technologien bieten auf der Basis IP/PPP oder IP/Ethernet, ggf. in Kombination mit VPN, dienstneutrale, skalierbare, redundante und sicher betreibbare Architekturen, für die Standards zur Verfügung stehen. Was fehlt, ist die Abdeckung der Mobilitäts-Anforderung.
Eine Übersicht der Ethernet-Standardisierung zeigt Abbildung 2.4.

3. Wireless: Drahtlose Netze

3.1 Wireless PAN (WPAN)

Für drahtlos vernetzte Komponenten oder mobile Mitarbeiter bzw. deren Nahbereich gibt es außer IEEE 802.11 eine separate Standardisierungsgruppe IEEE 802.15 WPAN (Wireless PAN). Sie befasst sich zum einen mit allen größeren und kleineren Komponenten, die ein mobiler Mitarbeiter so mit sich herumschleppt, angefangen beim Laptop, PDA, Blackberry, Communicator bis hin zu MP3-Player und Kamera; zum anderen befasst sie sich mit der Peripherie um einen Arbeitsplatz herum, z.B. um den lästigen Kabelwirrwar im Büro zu eliminieren, der beim ständigen Herumschieben der Arbeitsplätze und Arbeitsplatzgeräte stört. In einer Reihe von flächendeckenden Anwendungs-Szenarien liegt der Fokus bei PAN's auf der Peer-to-Peer Querkommunikation auch als M2M (Machine-to-Machine) bezeichnet, z.B. die Übertragung von Telemetrie-Daten vernetzter Gebäudekomponenten wie Klimageräte, Zugangssicherungen oder Aufzugschalter. In vielen Umgebungen ist hier kein Platz für eine Querverkabelung oder sternförmige Netzanbindung gegeben.

Aufgrund der geringen Leistungsaufnahme sind die Geräte mit Batterien bestückt, deren geringe Lebensdauer immer wieder ein Problem darstellt. Vielfach werden M2M Komponenten vernetzt, um sie überwachen und kontrollieren zu können. Hierunter fallen auch Anwendungen wie Lagerhaltung und Zulieferungs-Automatisierung, die mit Einsatz von RFID Plaketten arbeiten. Eine Wi-Fi Vernetzung ist zwar möglich, wird den Anforderungen von Telemetrie- oder Multihop-Netzen jedoch nur mäßig gerecht. Daher haben sich eigene Interessengruppen gebildet, die Wireless Technologien für spezielle Anforderungen entwickeln wie

- mobile vermaschte Netze
- Zuverlässigkeit
- Interoperabilität
- gesicherte Überwachung und Kontrolle
- lange Batterie-Betriebszeiten
- hohe Anzahl von Einzelgeräten

bei gleichzeigig minimierten Kosten (5 Cent bis 50 Cent pro Anschluss bei RFID oder ZigBee; zum Vergleich: Wi-Fi liegt bei 15 EUR und Bluetooth bei 4 EUR).

Möglicherweise kommt hier Wi-Fi einfach über Nacht als Standard-Ausrüstung vieler Produkte, so wie wir es in Laptops erlebt haben. Allerdings benötigen Telemetrie-Netze weniger die Megabit-Raten von Wi-Fi als vielmehr z.B. Funktionen zur ortsgenauen Lokalisierung (Location Tracking) wie sie Airespace oder Trapeze mit proprietären Triangulierungs-Signalen unterstützen, die zwischen den Access Points versendet werden.

IEEE 802.15 WPAN
Die IEEE Arbeitsgruppe 802.15 für Wireless Personal Area Networks (WPAN), die durch die ZigBee Spezifikationen eweitert wurde, kümmert sich speziell um die zuvor genannten Anforderungen.

802.15.1 ist die Standardversion der entsprechenden Bluetooth Layer (Basis Bluetooth 1.1, 802.15.1a für Bluetooth 1.2 mit QoS Erweiterungen).

802.15.2 kümmert sich um Interferenzen mit 802.11b und 802.11g, da alle drei Protokolle das 2,4 GHz Band nutzen.

802.15.3, auch WiMedia genannt, spezifiziert höhere Datenraten und zielte eigentlich auf den Markt für TV und digitale Kameras. Ursprünglich wurde eine Datenrate von 55 Mbit/s auf der Basis von 802.11 PHY definiert, jedoch nicht kompatibel zu 802.11. Die meisten Hersteller fokussieren ihre Entwicklungsaktivitäten daher eher auf

802.15.3a, auch von der WiMedia Alliance unterstützt. Hier soll mit UWB eine mögli-

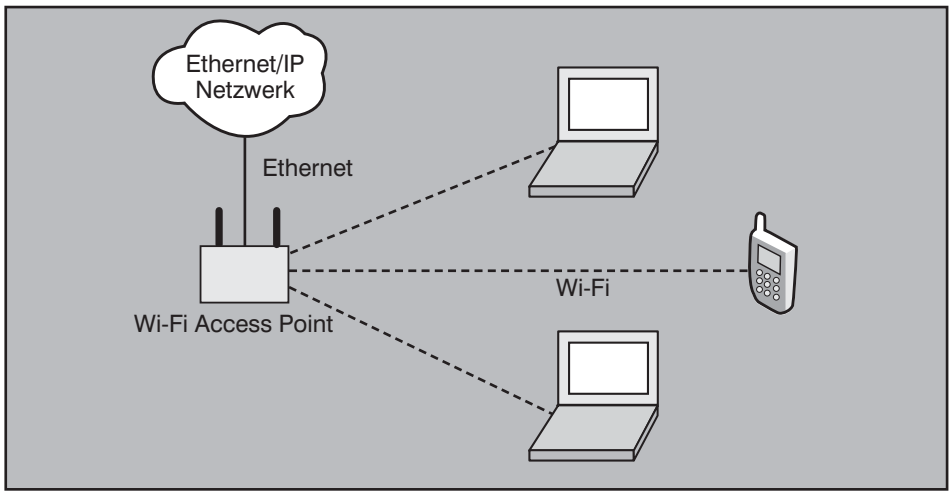


Abbildung 3.1: Wi-Fi Access Point im PAN

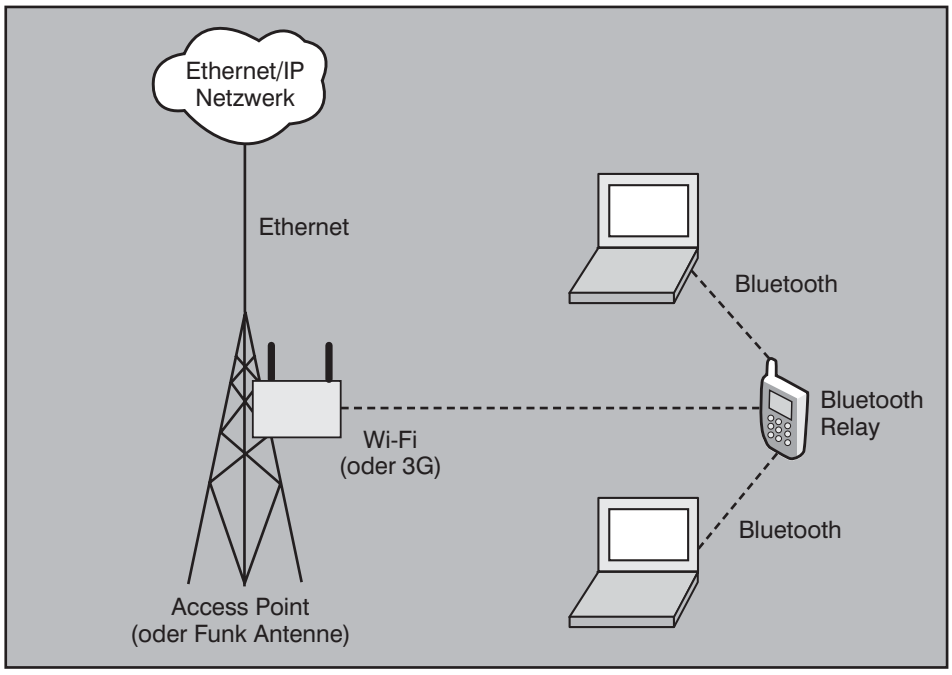


Abbildung 3.2: Bluetooth Relay im PAN

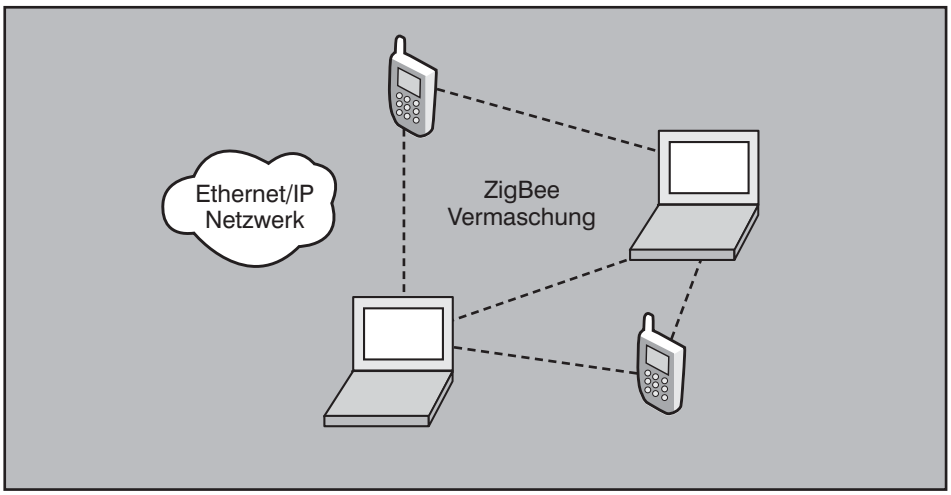


Abbildung 3.3: PAN mit vermaschtem ZigBee Netz

che Bluetooth Ablösung definiert werden, die höhere Datenraten und noch niedrigere Leistungsaufnahme ermöglicht. Allerdings konnte die Arbeitsgruppe sich nicht zwischen rivalisierenden Vorschlägen von Intel und Motorola entscheiden, worauf Intel unter dem Namen MBOA (Multi-Band OFDM Alliance) eine neue Fraktion aufmachte, die schon in 2005 zu Produkten führen soll. MBOA soll eine Wirless Schnittstelle mit 480 Mbit/s werden und in der ersten Version PC's mit Peripheriegeräten verbinden. Der geplante Intel Chip hat auch schon einen Namen: Rosedahl.

802.15.4 spezifiziert niedrige Datenraten bis herunter auf 9,6 kbit/s ohne Voice Unterstützung, die jedoch Produkte mit langen Batteriezeiten und niedrigen Kosten ermöglichen sollen und hat Telemetrie-Netze im Fokus. 802.15.4 nutzt Frequenz-Hopping, was zu niedrigeren Datenraten führt aber unempfindlicher gegen Interferenzen ist als Wi-Fi. Zusammen mit dem abgespeckten Routing Protokoll von ZigBee, das für eine Nutzung mit 802.15.4 designed wurde, lassen sich vermaschte Netze aufbauen. Da 16-Bit Adressen verwendet werden, kann ein einzelnes Netzwerk aus bis zu 65000 Knoten (Geräten) bestehen.

802.15.5 soll einen Standard für die Vermaschung Geräten auf MAC-Ebene spezifizieren, die ZigBee oder IP Routing ersetzen kann.

802.11 vs. Bluetooth vs. ZigBEE
802.11 ist eher infrastruktur-orientiert: jedes Endgerät ist direkt mit einem Access Point assoziiert, jeder Access Point ist an Ethernet, also wireline angebunden. Eine AP-AP Wireless Netzwerk ist bis dato nicht spezifiziert. Bluetooth ist eher auf Handy / PDA fokussiert: Bluetooth Geräte assoziieren sich an weitere wireless Geräte (üblicherweise Telefone), die als eine Art Hub arbeiten. ZigBee ist von den drei Ansätzen der am ehesten netzwerk-orientierte: Alle ZigBee Geräte leiten den gesamten Verkehr an alle anderen ZigBee Geräte weiter, wobei das wireline Netzwerk völlig außen vor ist. Der Zugang zu wireline Netzen ist noch nicht standardisiert, es gibt jedoch proprietäre Herstellerlösungen, die ihn ermöglichen. Ähnlich wie Wi-Fi gibt es für die Vermarktung von ZigBee eine ZigBee Alliance, die Interoperabilität fördern will und Zertifizierungen durchführt. Aktuell ist ZigBee jedoch in USA wesentlich verbreiteter als in Europa. Abbildung 3.1 bis Abbildung 3.3 zeigen eine Übersicht über Wi-Fi, Bluetooth und ZigBee Verbund.

Vielfach laufen WPAN's heute relativ unbehelligt vor sich hin, es sei denn konsequente Netzbetreiber haben ihren Einsatz im Unternehmen aufgrund zu befürchtender Interferenzen mit Wireless LAN's verboten. Mit wachsendem Boom der letzteren arbeiten jedoch auch die Standardisierer an Regelungen und Abstimmungen, die solche Interferenzen beseitigen sollen.

Eine einzelne wireless-Variante für PAN's konnte sich bisher noch nicht als dienstneutrale, skalierbare, redundante und sicher betreibbare Architektur etablierten, für die Standards zur Verfügung stehen. Wi-Fi, Bluetooth/IEEE 802.15 und ZigBee haben jeweils ihre spezielle Ausrichtung hinsichtlich Telefonie, Telemetrie oder Mobilität. Für die Integration von TK sind Endgeräte erhältlich. Die QoS-Anforderungen für Voice können erst mit zukünftigen Standards abgedeckt werden. Die Anforderung an Sicherheit ist mit AES und IEEE 802.1X technisch gegeben, jedoch im wireless PAN noch nicht verfügbar. Mit Ausnahme von ZigBee fehlt die Definition eines Schlüsselmanagement. Die Anforderung nach Mobilität wird abgedeckt, wobei sich der Radius nur auf wenige Meter erstreckt.

IEEE 802.11 WLAN Funkverbindungs-Schnittstelle					
Standard	Maximale Bit Rate	Fallback Raten	Bereitgestellte Kanäle	Frequenz-Band	Funktechnik
802.11	2 Mbps	1 Mbps	3	2,4 GHz	FHHS oder DSSS
802.11b	11 Mbps	5,5 Mbps 2 Mbps 1 Mbps	3	2,4 GHz	DSSS
802.11a/h	54 Mbps	48 Mbps 36 Mbps 24 Mbps 18 Mbps 12 Mbps 9 Mbps 6 Mbps	12	5 GHz	OFDM
802.11g	54 Mbps	Wie 802.11a	3	2,4 GHz	OFDM

Abbildung 3.4: WLAN Funkschnittstellen nach IEEE 802.11

3.2 Wireless LAN (WLAN)

Wireless LAN hat sich in den letzten drei Jahren mit einem erheblichen Marktboom als Technologie etabliert, die komplementär zu Ethernet eingesetzt wird. Nachdem inzwischen von IEEE 802.11 ein einigermaßen brauchbarer Satz von Standards verabschiedet und in Produkten verfügbar ist, proklamieren wireless Fans bereits die Ablösung von Ethernet: Der ganze lästige Kabelsalat störe nur, verursache unnötige Kosten und bediene unflexible, weil nicht mobile Netze, während mit Funk alle Bereiche und noch dazu mit erheblich niedrigeren Kosten erschlossen werden könnten, sind vielfach gehörte Argumente. Ganz so einfach geht diese Rechnung jedoch nicht auf: Wireless LAN Technologie realisiert nach wie vor ein shared LAN, d.h. alle Benutzer, die sich in der selben WLAN Zelle befinden, teilen sich die verfügbare Kapazität. Zur Erinnerung: In diesem Stadium befand sich Ethernet bis ca. 1997, danach haben sich voll geswitchte LAN's etabliert. In diesem Sinn ist der Einsatz von WLAN's ein technologischer Rückschritt, der jedoch in Kauf genommen wird, um die Vorteile Mobilität und Einsparung von Verkabelung zu erhalten.

Technologische Eckwerte
Anstelle einer verkabelten Anschaltung von Endgeräten assoziieren sich diese mittels Funkverbindung über das 2,4 GHz Band oder 5 GHz Band an einem Access Point (AP), der seinerseits einen 10/100BASE-TX Kabelanschluss an das Ethernet Netzwerk hat. Somit wird nicht ein Kabel je Benutzer sondern nur ein Kabel je Access Point benötigt. Insbesondere eine flächendeckende Verkabelung mit mehreren Anschlussdosen je Arbeitsplatz wird durch eine flächendeckende Access Point Abdeckung mit einem AP z.B. je 750 bis 7500 Quadratmeter abgelöst. Technisch gesehen ist der AP eine MAC-Layer Brücke, die ein 802.11 LAN mit einem 802.3 LAN auf Layer-2 koppelt, denn WLAN ist nicht gleich Ethernet, beide MAC Layer haben unterschiedliche Protokolle! Verschiedene AP's reden über Ethernet miteinander, insbesondere um die Übergabe eines Benutzers von einem AP an einen anderen AP durchzuführen, die als Roaming bezeichnet wird.

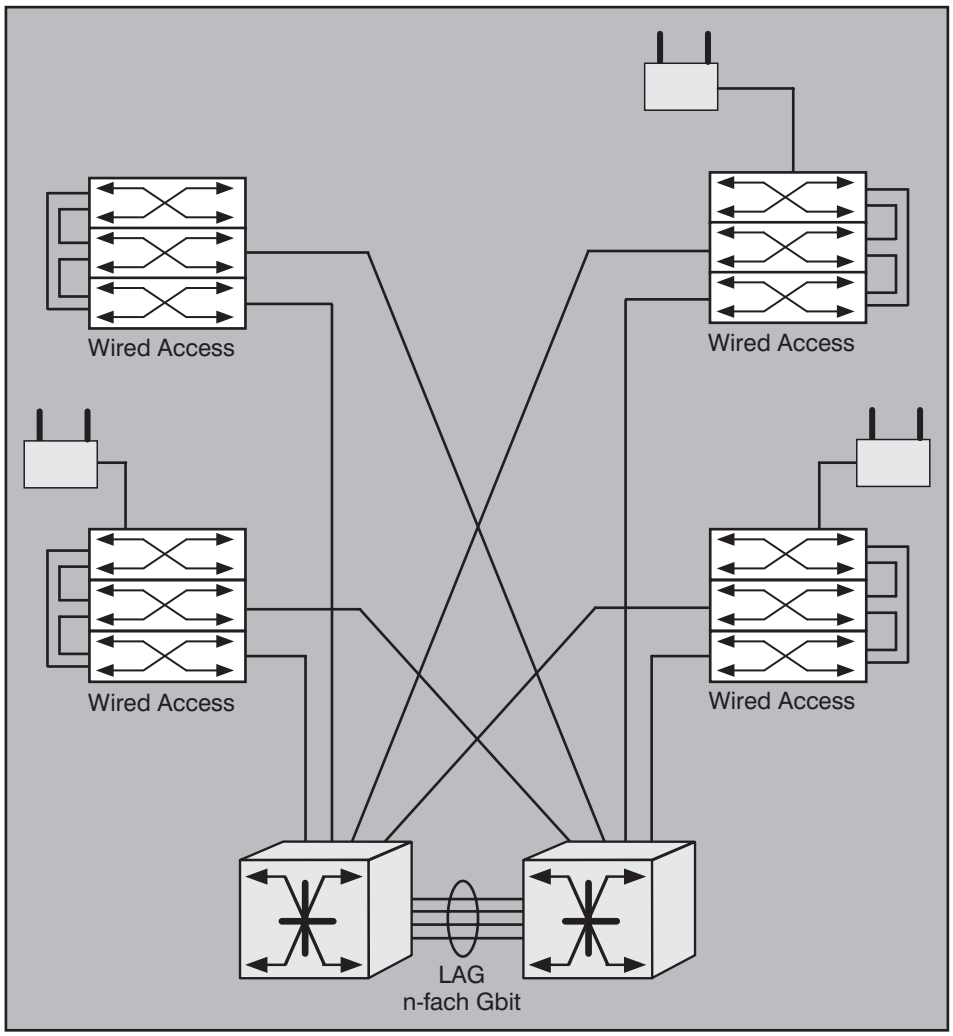


Abbildung 3.5: Phase 1 der WLAN Verbreitung

Standardbasierte WLAN's haben aktuell eine Kapazität von maximal 11 Mbit/s oder 54 Mbit/s und eine Reichweite von maximal 50 m Radius für den Standard 802.11b mit der niedrigeren Datenrate 11 Mbit/s, von maximal 25 m / 50 m Radius für die Standards 802.11 a/h mit der höheren Datenrate 54 Mbit/s. Bei steigender Entfernung zum AP nimmt die Datenrate deutlich ab bis hin zu einem Bruchteil von 9% oder 11% der Maximalrate. Maiximale Datenraten werden oft nur über eine Entfernung bis zu 10 m oder 15 m erreicht. Eine Übersicht der verschiedenen Standards und Funktechniken sind in Abbildung gezeigt. Die verwendeten Funktechniken wurden im Insider verschiedentlich vertieft und werden daher hier nicht näher behandelt.

WLAN Verbreitung und Weiterentwicklung: Quo Vadis, WLAN?
WLAN Verbreitung lässt sich in mehrere Phasen einteilen:

- Phase 1: Anfangsstadium mit wenigen Benutzern und vereinzeltem Einsatz von Access Points, die shared LAN Inseln bilden.
- Phase 2: Zwischenstadium mit einer mittleren Anzahl von Benutzern und mehr oder weniger flächendeckendem Einsatz von Access Points.
- Phase 3: Clusterbildung, vorläufiges Endstadium mit einer hohen Anzahl von Benutzern und flächendeckender sowie redundanter Ausstattung mit Access Points mittels Dopplung und Überlappung
- Phase 4: Migrationsstadium, dediziertes Wireless LAN mit quasi-deterministischem Netzzugang und definierter Leistung je Benutzer, analog zu dedeziertem (voll geswitchtem) Ethernet

Phase 1 kann mit Ausnahme des Sicherheitsthemas als unkritisch betrachtet werden. Der Vorteil der Mobilität wird lokal erreicht, die vereinzelten AP's werden wie Endgeräte in das vorhandene Ethernet Netzwerk eingebunden, die Nutzung ist limitiert auf wenige Personen wie Netzwerkteam, Benutzer-Support, Besprechungsräume oder ähnliche interne Dienstleistungen oder Infrastruktur-Erweiterungen. Eine Übersicht zeigt Abbildung 3.5.

Phase 2 ist der Betriebszustand von einer Reihe der heute betriebenen WLAN's, in dieser Phase sind einige Probleme zu bewältigen, weshalb Herstellerlösungen zu proprietären Erweiterungen und Abwandlungen der verfügbaren Standards geführt haben. Mit zunehmender Anzahl von betriebenen AP's entstehen mehrere Bedarfe:

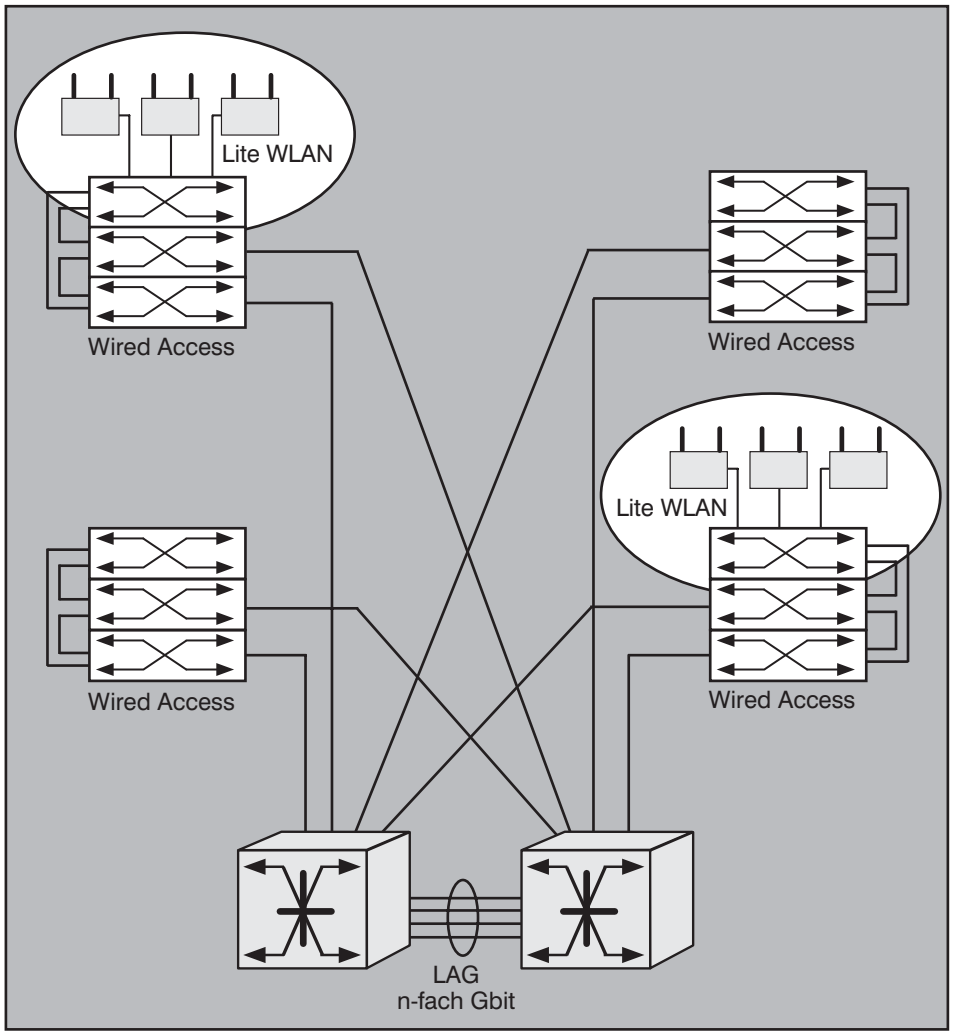


Abbildung 3.6: Phase 2 der WLAN Verbreitung: Lite WLAN

- Zentralisierung und Automatisierung von Konfiguration und Betrieb der Acces Points
- Integration des Managements von AP's in das allgemeine Netzwerkmanagement
- Mit zunehmender Flächendeckung Abstimmung von Ansteuerung und Sendeleistung der AP's gegeneinander
- Erkennung und Isolierung von „wild" installierten AP's (rogue AP)
- Erzeugen eines gleichmäßigen und günstigen Leistungsverhaltens für alle Benutzer
- Überwachen der Leistungsparameter der betriebenen WLANs
- Schnelles Roaming zwischen AP's sowohl innerhalb eines IP Subnetzes als auch zwischen verschiednen IP Subnetzen

Eine Reihe von Herstellern wie Airespace (Cisco), Aruba, Chantry Networks (Siemens), Extreme Networks, Proxim, Symbol Technologies oder Trapeze Networks haben eine Art „Lite WLAN" mit Auslagerung von WLAN-Intelligenz aus den AP's in so genannte WLAN Switches entwickelt (siehe Abbildung 3.6). Der Begriff WLAN Switch ist irreführend, da er dem traditionellen Frame Switch nicht entspricht sondern eher zentralisiertes Management und Roaming-Optimierung bezeichnet. Ein WLAN Switch ist entweder ein eigenständiger Ethernet Switch, an den bis zu 48 AP's angeschlossen werden oder eine Control Server Appliance (Windows oder Linux), die an zentraler Stelle im Ethernet angeschaltet ist und viele bis alle AP's handhabt. Unter WLAN Switching werden Funktionen wie Zugangs-Kontrolle, RF-Aussteuerung, AP-Überwachung / Identifizierung, L2 und L3 Roaming subsummiert. Ein weiterer Vorteil beim Einsatz von „Lite WLAN" Access Points liegt darin, dass entwendete AP's nicht mehr nutzbar sind, da ihnen die Intelligenz für einen eigenständigen Betrieb fehlt.

Wireless Roaming zwischen Subnetzen ist derzeit noch nicht standardisiert und eine Lösung wird nicht vor 2005 / 2006 erwartet. Phase 2 ist in Abbildung 3.6 dargestellt.

Phase 3 ist das obere Ende der heute verfügbaren WLAN Technik und wird zu Problemen der Clusterbildung, Überlast, Nichtdeterminismus sowie schwierigen Überwachbarkeit und Steuerbarkeit der Netzwerkleistung führen (siehe Abbildung 3.7). Dies führt zu einem zwingenden Bedarf nach Quality of Service. Der aktuelle Standard-Ansatz IEEE 802.11e für WLAN Quality of Service (QoS) sieht vor, mehrere Benutzerklassen zu bilden, deren Zugehörigkeit im WLAN Header erkennbar ist. Zur Vermeidung von konkurrierendem Zugriffsverhalten wird der WLAN-Zugang in Zeitslots unterteilt. Wichtige Benutzer erhalten mehr Zeitslots als unwichtige Benutzer und über diese Priorisierung wird ein angemessenes Leistungsverhalten erhofft. Ein solches Verfahren regelt das Überlast-Problem jedoch nur unzureichend, da innerhalb der Prioritätsklassen weiterhin eine Aufteilung der Datenrate stattfindet und somit eine Shared LAN Leistungs-Charakteristik vorliegt. Spätestens in Phase 3 muss daher eine Entwicklung hin zu deterministischem Leistungsverhalten stattfinden, nämlich Phase 4.

Phase 4 ist insbesondere auf der Basis verfügbarer Standards noch mehrere Jahre entfernt. Für viele produktive Anwendungen kann jedoch erst in dieser Phase ernsthaft darüber nachgedacht werden, bei ausreichender Datenrate je Benutzer das vorhandene Ethernet völlig abzulösen. Ein quasi-deterministisches Leistungsverhalten kann nur dann erreicht werden, wenn die Anzahl Benutzer je AP klar begrenzt wird, z.B. durch entsprechend hohe Flächendeckung und Überlappung, wobei jedoch Interferenzen durch entsprechende RF-Ansteuerung der AP's vermieden werden, in Kombination mit zentralem Management, das die Anzahl je AP assoziierter Clients steuert. Gleichzeitig muss eine deterministische Leistung bzw. Datenjate je Benutzer erreicht werden, was durch die Zuordnung von genau einem Kanal je Benutzer möglich wäre. Hierfür ist eine entsprechend hohe Anzahl von Kanälen innerhalb eines Zugangsverfahrens (wie 802.11b oder 802.11h) je AP notwendig, mit entsprechender Potenzierung über mehrere benachbarte AP's hinweg, die mit überlappungsfreien Kanälen arbeiten müssen. 802.11 a/h verfügt z.B. über 20 Kanäle, d.h. bei flächendeckender und raumdeckender Bestückung kann mit ca. 5 Kanälen je Mobilfunkzelle kalkuliert werden, so dass 5 Benutzer einen deterministischen Netzzugang erhalten könnten. Eine Alternative zur Erhöhung der Kanalzahl ist eine gezielte Sende-Ausrichtung der Access Points, so dass sich die Sendebereiche nicht überlappen und alle AP's die selben Kanäle verwenden können.

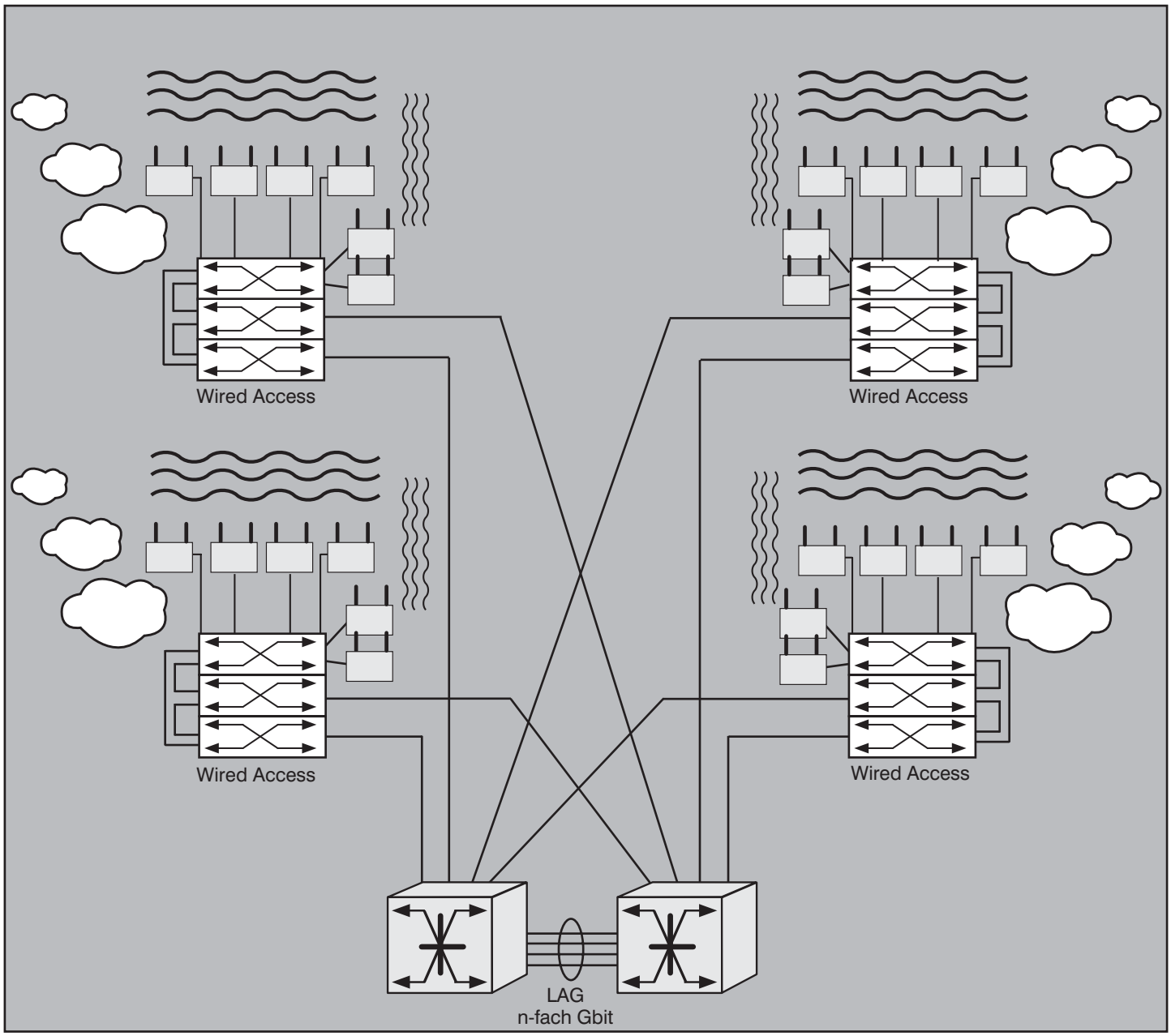


Abbildung 3.7: Phase 3 der WLAN Verbreitung: Clusterbildung, Überlast

Wir erwarten, dass diese Phase in 3 bis 5 Jahren erreicht wird und sich in 5 bis 10 Jahren etabliert hat, soweit WLAN eine Alternativ- oder Ablösetechnik für Ethernet werden wird. Eine Übersicht zeigt Abbildung 3.8. Entsprechend der aufgezeigten Verbreitung und dem daraus resultierenden Weiterentwicklungs-Bedarf der WLAN Technologie werden 802.11 Standards erarbeitet, die die Nutzung einer größeren Anzahl Kanäle, höherer Datenraten sowie die Standardisierung von Roaming und vermaschten redundanten Strukturen ermöglichen sollen. Eine Übersicht kommender Standards zeigt Abbildung 3.9.

Mit dem aktuellen Stand der Technik ist Wireless LAN nach IEEE 802.11 sehr weit von den Ethernet Datenraten entfernt. Für einen produktiven Einsatz mit der Perspektive weitergehender Anwendungen als E-Mail und Webzugriff ist eine bessere Skalierbarkeit hinsichtlich sowohl Datenrate als auch Reichweite erforderlich. Die Arbeit in dieser Richtung hat in der Arbeitsgruppe IEEE 802.11n begonnen, die eine tatsächlich erreichbare Datenrate von mindestens 100 Mbit/s spezifizieren will. Erste Draft Vorschläge liegen jetzt vor, die Fertigstellung des Standards wird aber trotz der ehrgeizigen Zeitplanung der Arbeitsgruppe (Anfang 2006) vermutlich nicht vor Mitte bis Ende 2006 erreicht sein, standardkonforme Produkte können also in ca. 3 Jahren verfügbar werden.

MIMO am Horizont

Im Vorlauf des Standards wird es vermutlich Lösungen nach dem dort angestrebten Basisverfahren MIMO geben (Multiple-In, Multiple-Out). MIMO arbeitet nicht nur mit geänderten Radio-Chips sondern insbesondere mit intelligenteren Antennen und verbessert die Leistung auch, wenn nur an einem Ende einer Funkverbindung MIMO genutzt wird. MIMO kann zwar die Datenrate nicht verdoppeln, aber die Reichweite bei 54 Mbit/s kann erkennbar vergrößert

werden. Bei MIMO arbeiten mehrere Antennen auf dem selben Kanal und vermeiden Interferenzen, indem sie unterschiedliche Signale senden. Es muss zwar nicht zwingend an beiden Seiten die selbe Anzahl von Antennen eingesetzt werden, die beste Leistung wird jedoch erreicht, wenn die Antennenzahl auf Sende- und Empfangsseite gleich ist. Unter Nutzung eines als „Path Diversity" bezeichneten Verfahrens wird jedes Sendesignal über verschiedene Wege übertragen, so dass jeder Empfänger (bzw. die verschiedenen Antennen des Empfängers) jedes Signal separat empfangen kann (siehe Abbildung 3.10).

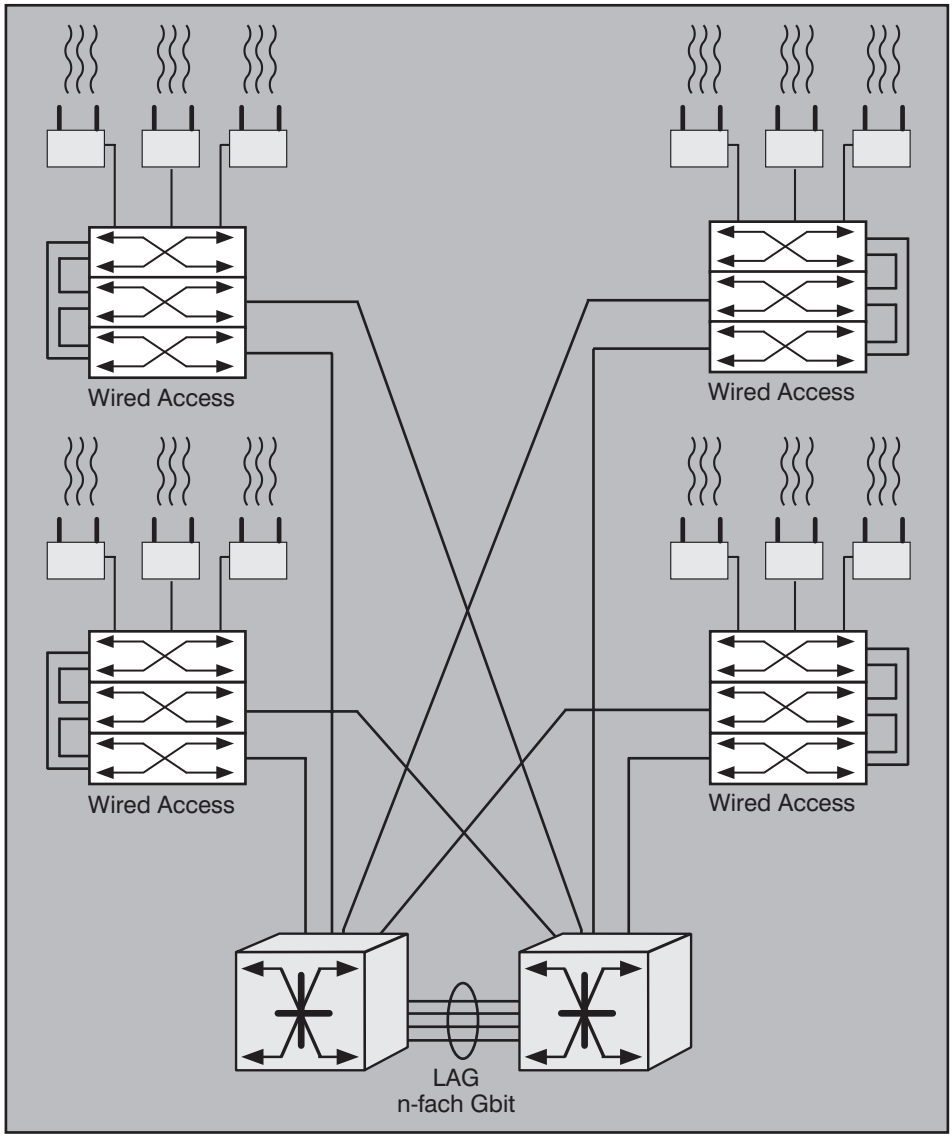


Abbildung 3.8: Phase 4 der WLAN Verbreitung: Dediziertes WLAN

Hersteller wie Airgo Networks gehen davon aus, dass das beste Leistungssteigerungs-Verhältnis zwischen Antennenzahl und Datenrate bei drei Antennen liegt, einige 802.11n Vorschläge liegen bei bis zu 10 Antennen. Letzlich ist dies auch ein Platzproblem, da es schwierig werden wird, 10 Antennen auf einer Mini-PCI Karte in einem PDA oder Laptop unterzubringen. Im Oktober hat sich die 802.11n Arbeitsgruppe in zwei Lager gespalten, die im Prinzip ähnliche Vorschläge favorisieren, ABER: WWiSE (World-Wide Spectrum Efficiency) will den bisherigen MAC Layer beibehalten (kostengünstiger und sanftere Migration), TGn Sync will einen effizienteren MAC Layer mit höherer Datenrate spezifizieren (teurer und kompliziertere Migration).

Eine weitere Möglichkeit zur Leistungssteigerung ist die Nutzung eines breiteren Spektrums, nämlich das Bündeln zweier Kanäle (Bonding), um die Datenrate zu verdoppeln. Leider verringert dies die Anzahl nutzbarer Kanäle nach Adam Riese um Faktor zwei. Der Anwender muss hier folglich die Entscheidung zwischen zwei Übeln treffen und das für ihn kleinere auswählen.

Roaming

Der Trend, einzelne AP's über zentralere „Switches" zusammenzufassen ist für Roaming hilfreich, wenn auch noch keine endgültige Lösung: Solange ein Client sich in dem physikalisch zusammenhängenden Bereich der AP's bewegt, die an einen Switch angebunden sind (physisch oder logisch), muss kein Roaming stattfinden.

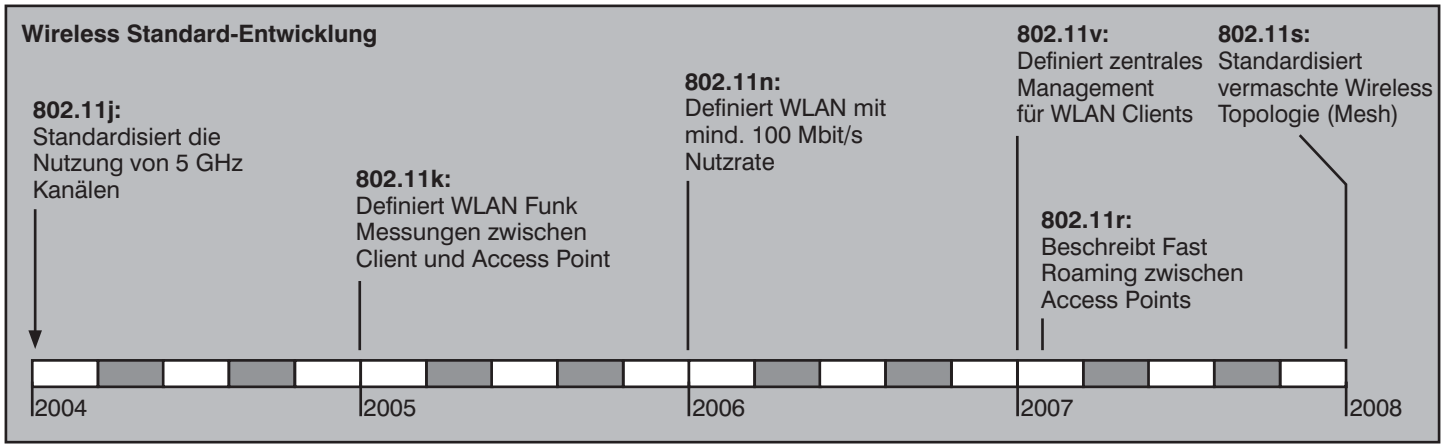


Abbildung 3.9: Zeitplan neuer IEEE 802.11 Standard-Arbeitsgruppen

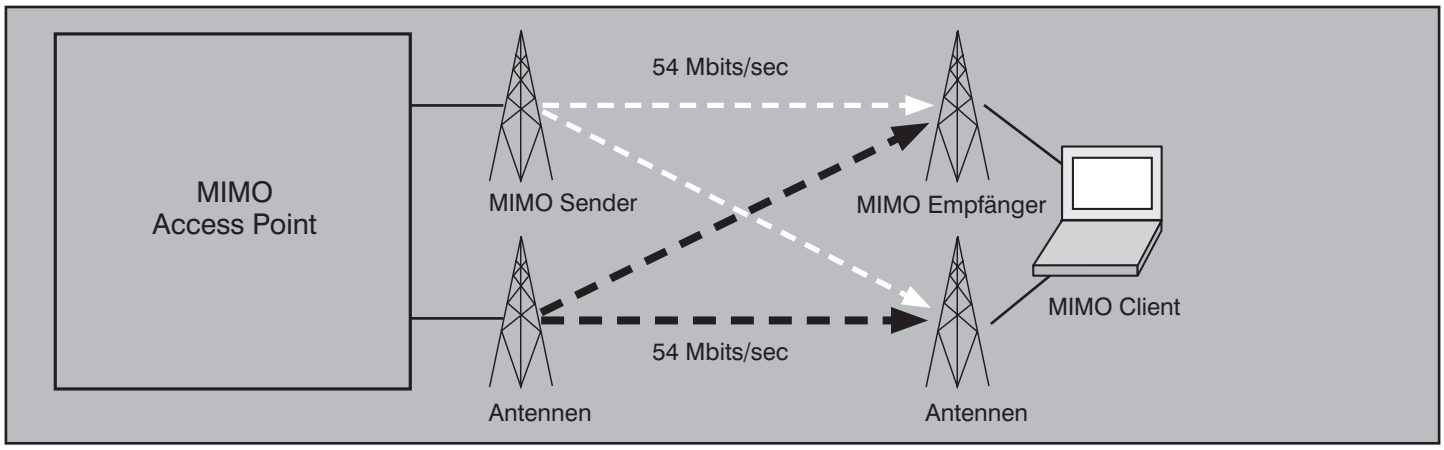


Abbildung 3.10: MIMO Einsatz-Szenario mit einem Zwei-Antennen System bei Sender und Empfänger

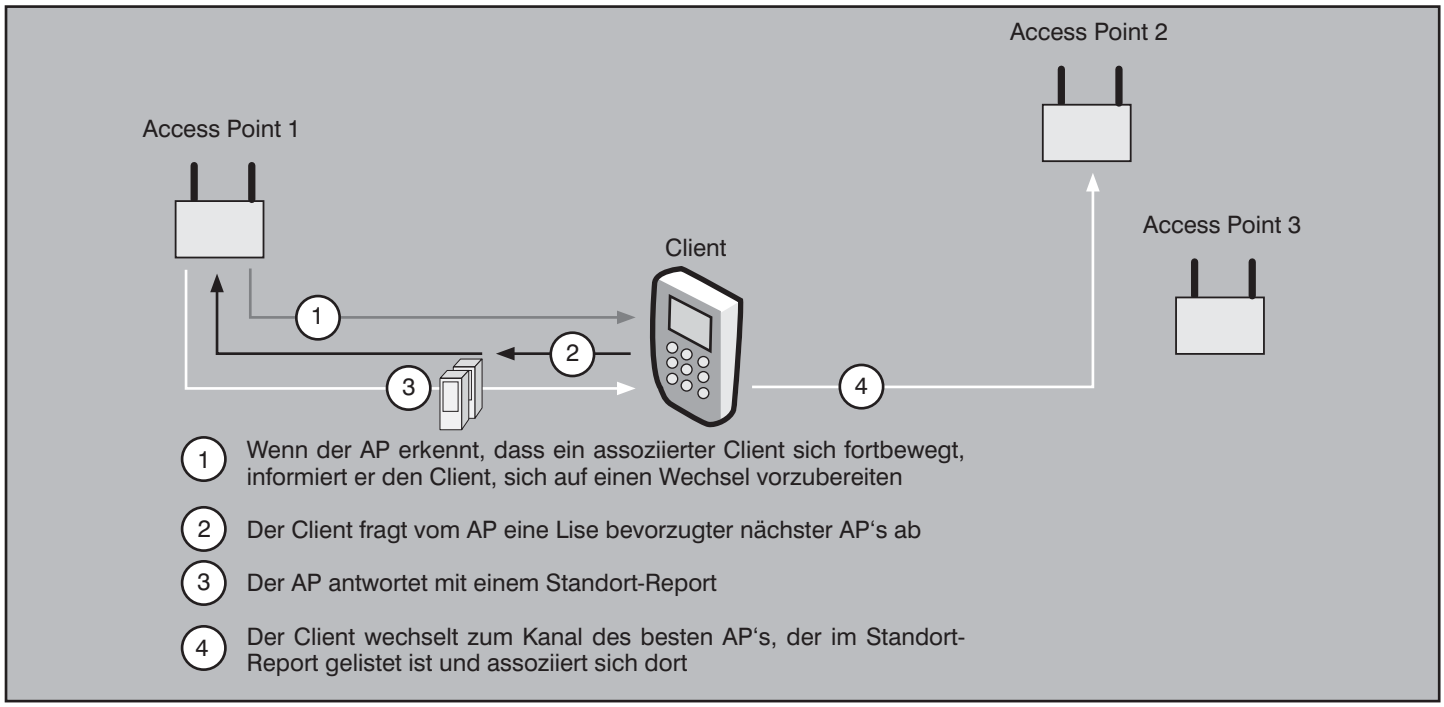


Abbildung 3.11: IEEE 802.11k zur Optimierung von Hand-Over und Roaming

Handover von einem AP zu einem anderen kann inzwischen bei einigen Produkten hinreichend schnell durchgeführt werden. Schwierigkeiten macht der Wechsel zwischen WLAN Switches, insbesondere beim Wechsel von einem IP Subnetz in ein anderes, da in diesem Fall eine Re-Authentifizierung und vielfach ein erneutes Laden der IP Konfiguration über DHCP erforderlich werden. Hierbei macht nicht nur der Wechsel an sich Schwierigkeiten, sondern mit zunehmend flächendeckendem Einsatz von AP's kann ein Client mehrere AP's sehen und muss sich irgendwie entscheiden, an welchem davon er sich assoziieren will. Unter 802.11k wird dieses Thema behandelt und gleichzeitig eine Verbesserung des Leistungsverhaltens beim AP-Wechsel angestrebt. Seit März 2004 gibt es einen ersten Draft, die Standardisierung ist jedoch auch hier noch nicht abgeschlossen. Aktuell scheint sie sogar eher ins Stocken geraten, da sich auch diese Arbeitsgruppe nicht einigen kann, nämlich darüber welche Parameter denn nun genau zwischen Client und AP gemessen und von den Clients an die AP's gemeldet werden sollen. In der Zwischenzeit beginnen proprietäre Lösungen, sich im Markt zu etablieren.

Wie auch immer die Standardisierer sich hinsichtlich der zu messenden Parameter einigen werden –802.11k definiert permanente Messungen der Signalgüte-Parameter zwischen AP und Client, die einen Wechsel des AP einleiten, sobald die Leistung nicht mehr optimal ist. Im Gegensatz zum aktuellen Betrieb, bei dem der Wireless Client nach einem neuen günstigeren AP fragt, sobald die Leistung schlecht wird, wird der Wechsel hier durch Kommunikation zwischen den AP's gesteuert und durch den AP eingeleitet, an dem der Client aktuell assoziiert ist. Eine Ablaufskizze zeigt Abbildung 3.11.

1. Wenn der AP erkennt, dass ein assoziierter Client sich zu weit entfernt, sendet er dem Client eine Nachricht, damit dieser sich auf einen Wechsel vorbereitet.

2. Der Client fragt von seinem aktuellen AP eine Liste bevorzugter nächster AP's ab, zu denen er wechseln könnte.

3. Der AP antwortet mit einem Stand-

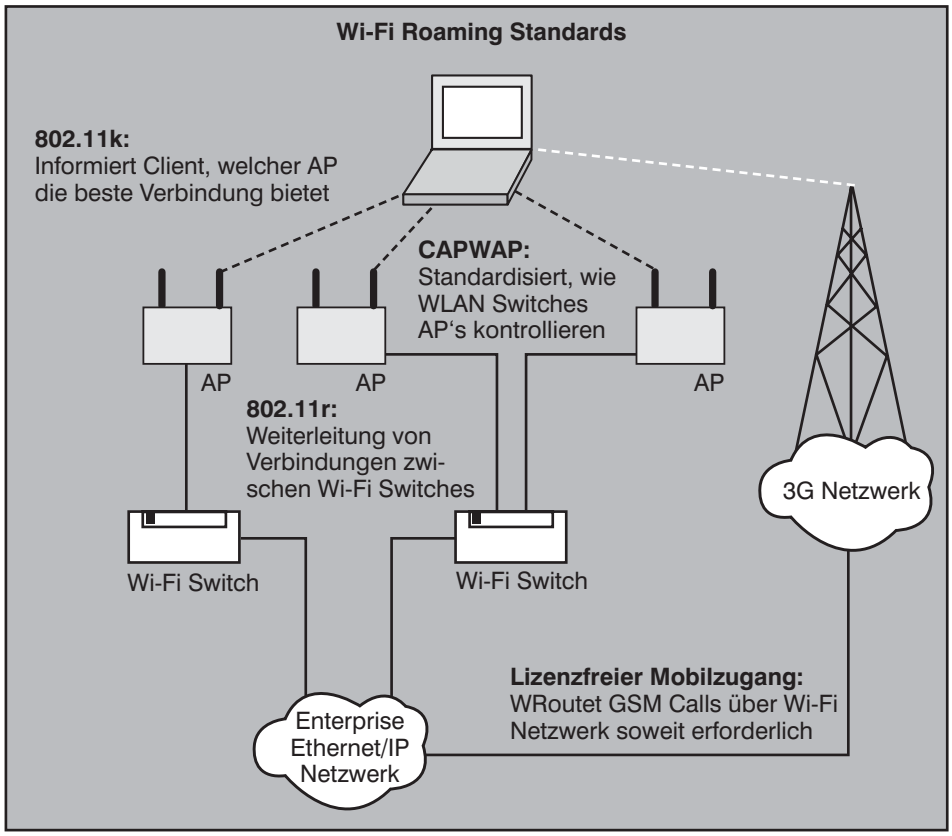


Abbildung 3.12: Standard-Ansätze für WLAN Roaming

ort-Reort, der die angefragte Liste möglicher nächster Acces Points mit entsprechenden Signalgüte- und Kanal-Parametern enthält.

4. Der Client wechselt zum Kanal des aus seiner Sicht günstigsten AP's, der im Standort-Report gelistet ist, und assoziiert sich dort.

Weitere Ansätze, die für einen flächendeckenden Einsatz von WLAN's notwendig sind und sich mit Roaming befassen sind IEEE 802.11r für die Übergabe einer Verbindung zwischen Wi-Fi Switches, CAPWAP (Control and Provisioning of Wireless Access Points) bei der IETF für eine standardisierte Kontrolle von AP's durch Wi-Fi Switches sowie Zusammenarbeit zwischen den Wireless und 3G Mobilfunk Herstellern, um ein Roaming zwischen GSM und WLAN zu ermöglichen. Eine Übersicht zeigt Abbildung 3.12.

Abkürzungen

3GPP	3rd Generation Project Partnership
AAS	Adaptive Antenna System
AES	Advanced Encryption Standard
AFE	Analog Front End
AGC	Automatic Gain Control
APC	Automatic Power Control
ATM	Asynchronous Transfer Mode
AV	Audio / Video
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BWA	Broadband Wireless Access
CAC	Call Admission Control
CAPWAP	Control and Provisioning of Wireless Access Points
CCK	Complementary Coded Keying
CLEC	Competitive Local Exchange Carrier
CIR	Committed Information Rate
COFDM	Coded OFDM
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection (Ethernet)
DCF	Distributed Coordination Function
DES	Digital Encryption Standard
DFS	Dynamic Frequency Selection
DMT	Discrete Multi-Tone
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EDCA	Enhanced Distributed Control Access
EFM	Ethernet on the First Mile
ETSI	European Telecommunications Standards Institute
EV-DO	Enhanced Version-Data Only (Data Optimized)

FAST	Flexible Authentication via Secure Tunneling (Basis 802.11i)
FCC	Federal Communications Commission
FDD	Frequency Division Duplexing
FDX	Full Duplex
FEC	Forward Error Correction
FFT	Fast Fourier Transformation
FHSS	Frequency Hopping Spread Spectrum
FR	Frame Relay
FSO	Fixed Space Optics
FTTB	Fiber to the Building
FTTH	Fiber to the Home
FTTP	Fiber to the Premises
FTTU	Fiber to the User
FWA	Fixed Wireless Access
GSM	Global System for Mobile Communication
HD-FDD	Half Duplex FDD
hdx	half duplex
HUMAN	High-speed Unlicensed Metropolitan Area Network
Hz	Hertz (Prefix Kilo=Thousands, Mega=Millions, Giga=Billions)
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFFT	Inverse FFT
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific, and Medical
ISP	Internet Service Provider
IT	Informations-Technologie
LAG	Link Aggregation Group
LAN	Local Area Network
LEAP	Lightweight EAP
LMDS	Local Multipoint Distribution System
LOS	Line of Sight
LWAPP	Light Weight Access Point Protocol
M2M	Machine-to-Machine
MAC	Media Access Control
MBOA	Multi Band OFDM Alliance
MCM	Multi Carrier Modulation
MIMO	Multiple In, Multiple Out
MMDS	Multichannel Multipoint Distribution System
NLOS	Non-Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OLOS	Obstructed LOS
PCF	Point Coordination Function
PTT	Push to Talk
x-QAM	x-level Quadrature Amplitude Modulation
QE	Queuing and Traffic Shaping Engine
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAN	Regional Area Network
RC4	Ron's Code-4
SA	Security Association
SDR	Software Defined Radio
SNR	Signal to Noise Radio
SOC	System on Chip
SS	Subscriber Station
SVP	SpectraLink Voice Priority
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TKIP	Temporal Key Integrity Protocol
TPC	Transmit Power Control
UMA	Unlicensed Mobile Access
U-NII	Unlicensed National Information Infrastructure
UWB	Ultra Wideband
VoIP	Voice over IP
VPN	Virtual private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WME	Wi-Fi Multimedia Extensions
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WSM	Wi-Fi Scheduled Multimedia

Links

www.alcatel.de
www.bbwexchange.com
www.ieee.org/11
www.ieee.org/15
www.ieee.org/16
www.ieee.org/20
www.ieee.org/22
www.nwfusion.com
www.wimaxforum.org
www.wimedia.org
www.zigbee.org

CCNE

ComConsult Certified Network Engineer

Lokale Netze
21.02. - 25.02.05 in Aachen
25.04. - 29.04.05 in Aachen
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
11.04. - 15.04.05 in Berlin
20.06. - 25.06.05 in Köln
26.09. - 30.09.05 in Berlin
14.11. - 18.11.05 in Köln

Internetworking
28.02. - 04.03.05 in Aachen
06.06. - 10.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Ethernet Technologien - neuester Stand
14.03. - 18.03.05 in Aachen
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

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

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
21.02. - 25.02.05 in Aachen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
14.02. - 18.02.05 in Aachen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
11.04. - 15.04.05 in Aachen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

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

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
14.02. - 18.02.05 in Bonn
25.04. - 29.04.05 in Bonn
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
28.02. - 02.03.05 in Bonn
13.06. - 15.06.05 in Bonn
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
18.04. - 22.04.05 in Aachen
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

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

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie