

## SAN

### Fibre Channel contra Gigabit Ethernet

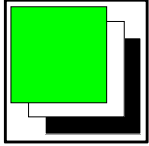
Ähnlich wie beim Telefonie-Markt, bei dem diskutiert wird die Telefonie zukünftig über IP (VoIP) zu übertragen, wird derzeit in Unternehmen darüber nachgedacht, das Speicherdesign nicht über separate SAN-Inseln und Fibre Channel, sondern über das „preiswerte und in Massenware“ verfügbare Ethernet zu realisieren.

Der Anwender ist also aufgefordert zu prüfen, ob er sich für eine etablierte und im Speicherumfeld renommierte Technologie oder für eine „revolutionäre“ Technologie, die auf TCP/IP basiert, entscheidet.

Bevor diese Entscheidung getroffen werden kann, sollte ein Anforderungsprofil zu den Speicherbedürfnissen des Unternehmens erstellt werden. Zwei Hauptanforderungen sind hierbei meist zuerst genannt. Die eine ist die **Verfügbarkeit** und die andere die **Skalierbarkeit**. Die Verfügbarkeit wird mit Produkten gewährleistet, die am Markt eingeführt und hinreichend verfügbar sind. Hier hat Fibre Channel einen entscheidenden Vorteil. Es sind Produkte, die auf manifestierten Standards aufbauen und sich in der Praxis mehrfach bewährt haben. Dies haben auch die „Gegenparteien“ eingesehen. Man kann beobachten, dass auch designierte „IP-Verfechter“ oder „NAS-Anbieter“ (fileorientierte Übertragung) mittlerweile Fibre Channel-Technologien und somit FC-Produkte entwickeln bzw. anbieten. Auch der „teuer“ angesehene Fibre Channel-Markt hat aufgrund der installierten Basis die Möglichkeit nun die Preise zu relativieren und wird dies voraussichtlich auch tun – zumindest sei dies den Herstellern der Fibre Channel-Technologie angeraten.

Betrachtet man die Alternativen am Markt und geht auf die andere Seite zur „Ethernet-Fraktion“, so ist sofort der Standard iSCSI näher zu beleuchten. Anfang 2003 wurde dieser Standard in einer ratifizierten Form frei gegeben. Es wurden einige Anpassungen an das TCP/IP-Protokoll gefordert und realisiert. Es wird gemunkelt, dass so mancher Administrator sein „bewährtes TCP/IP“ nicht mehr so schnell erkennt. Fakt ist, dass die Verbindung der beiden Protokolle iSCSI und IP einen gewissen Protokoll-Overhead erzeugt und dieser sich auf die Verfügbarkeit nicht sonderlich positiv auswirkt.

Durch entsprechende Hardwarebeschleunigungsmaßnahmen sollen über Transport Offload Engines (TOE), welche in den Controllern installiert sind, diese zusätzlichen Zeitaufwände kompensiert werden. Jedoch kosten auch diese Maßnahmen ihr Geld und es ist abzuwarten, ob hierdurch die iSCSI-Controller viel günstiger werden, als die FC-Controller. Betrachtet man die technische Seite, sollte beachtet werden, dass iSCSI z. B. bestimmte Kriterien, wie Serverless Betrieb (z. B. Datenverkehr zwischen Band und Platte), nicht bzw. bedingt unterstützt. Sollte man z. B. dieses Feature als unumgänglich im Unternehmen deklarieren, so muss man sich klar machen, dass die Fibre Channel-Alternative eventuell die sinnvollere ist.



**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

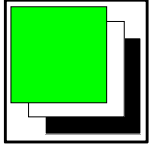
Auch hinsichtlich der Performance muss iSCSI wegen der oben genannten Protokollumsetzung deutliche Abstriche gegenüber der Fibre Channel-Technik machen.

Aus organisatorischer Sicht kann sich folgende Philosophie ableiten lassen. Ein SAN, welches meist in der Obhut des Rechenzentrums liegt, wird auch meist getrennt zum LAN administriert. Auch in kleineren Unternehmen sind hierfür oft getrennte Abteilungen verantwortlich. Es stellt sich die Frage, ob es notwendig ist, dass LAN und SAN über eine einzige Technologie abgedeckt werden muss.

Das primär Wichtigste ist die Anforderung des Kunden. Bei der Speicherung und Sicherung von Daten, wo aufgrund der Bewertung großer Datenmengen die Blockübertragung offensichtlich Vorteile besitzt, sollte die entsprechende Technologie auch eingesetzt werden. Die Zukunft abzuwarten und schauen was diese bringt, ist für einige Unternehmen nicht mehr möglich, da die Zeitfenster für die Speicherung der Daten über das LAN nicht mehr gegeben sind. Es empfiehlt sich daher nicht auf teilstandardisierte Lösungen mit proprietären Produkten zurückzugreifen. Im Einzelfall kann durchaus ein Kompromiss entscheiden, d. h. es muss nicht das größte Fibre Channel-System angeschafft werden, welches unendlich skalierbar und unendlich teuer ist und vielleicht in der Zukunft nie ausgelastet wird. Meist genügt ein SAN, das mit kleineren kostengünstigen Fibre Channel-Switchen im Herzen funktioniert. In der Zukunft (Horizont 3-5 Jahre) hat man dann aufgrund des angemessenen und „amortisierten“ Invests immer noch die Möglichkeit, eine Migration zu den „vermeidlichen“ Zukunftstechnologien durchzuführen.

**Zusammenfassung (Kernaussage)**

SANs sollten mit der Technologie installiert werden, die eine standardisierte und zuverlässige „Konsolidierung“ verspricht – dies ist Stand heute Fibre Channel.



**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

## VoIP

**SIP ist ein „easy to handle“-Protokoll für den Aufbau von VoIP-Kommunikationsbeziehungen in Netzwerken (mit Abstrichen).**

Im Gegensatz zu den anderen Protokollen wird durch das „schlanke“ SIP die Steuerung von VoIP-Endgeräten in Netzwerken im Endeffekt nur einfacher. Die hohe Komplexität des H.323-Protokolls erschwert dessen Anwendung. Für die Übertragung in IP-Netzen ist SIP einfach die bessere Wahl, da es speziell hierfür entwickelt wurde und auf HTTP-Elementen aufsetzt. Dies macht Adressierungsmöglichkeiten in jede Richtung offener, als aufwendige Umsetzungen von Binärinformationen des H.323-Protokolls.

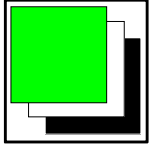
In Bezug auf Sicherheit der Protokolle muss auch angemerkt werden, dass das H.323-Protokoll dynamisch auf Ports im Netzwerk zugreift. Beim SIP-Protokoll gibt es hingegen definierte Ports, die wesentlich einfacher zu überwachen sind.

MGCP - um es nicht außen vor zu lassen - dient hauptsächlich der Initialisierung von Gateways und zur Umsetzung klassischer Telefonie auf Paket-Übertragungen. Für eine reine Paket-Übertragung ist MGCP nicht designed worden und so macht es auch keinen Sinn, dieses als zukunftsträchtiges Protokoll in der reinen VoIP-Welt zu sehen.

Trotz aller Vorteile von SIP gibt es hier auch einige Nachteile. Problematisch kann SIP beim Einsatz von Billing-Funktionen werden. Im Gegensatz zum H.323, wo alle Verbindungsinformationen während der Übertragung gespeichert bzw. mit transportiert werden, kann beim SIP-Protokoll ein Billing nur dann erfolgen, wenn die bestehende Verbindung direkt vom SIP-Proxy überwacht wird. Auch die Umsetzung einer klassischen Telefonverbindung zu einer IP-Verbindung muss mit viel Aufwand betrieben werden. Informationen die zum Beispiel H.323 aus dem ISDN auslesen könnte, müssen bei SIP nachträglich wieder hinzugefügt werden.

### **Zusammenfassung: (Kernaussage)**

Das SIP-Protokoll hat gute Chancen das führende VoIP-Protokoll zu werden, da es einfach anzuwenden ist. Allerdings müssen die Kontrollmechanismen verbessert werden, ohne SIP zu einem trägen „Kommunikator“ werden zu lassen.



## W-LAN

### Ersetzt Wireless LAN - Kabelinfrastrukturen?

Seit Jahren erhöhen sich die Frequenzen, die auf modernen Kabelinfrastrukturen nach Link D, E oder F, mit jeweils 100, 250 oder 600 MHz, übertragen werden. Parallel hierzu entwickeln sich immer mehr neue Technologien im IEEE 802.3 Ethernetumfeld, die heute von üblichen 10 oder 100 Mbit/s über 1000 Mbit/s bis hin zu 10 Gbit/s Ethernet im Backbone reichen. Kabelinfrastrukturen und Übertragungstechnologien bieten somit gemeinsam die Möglichkeit, sehr schnelle Netzwerke im Backbone bis zum Desktop des Endanwenders zu übertragen.

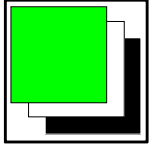
All dies resultiert aus der Nachfrage des Marktes, immer aufwendigere Applikationen in immer kürzeren Zeitintervallen bedienen zu können. Diese Tendenz wird, wenn auch nicht im vollen Umfang und der kompletten Dimension, im Rückblick der letzten Jahre bestätigt. Bei einem unserer Kunden konnten wir über periodische Messungen nachweisen, dass sich binnen fünf Jahren das Datenübertragungsvolumen verzehnfachte. Hinzu kommen Anforderungen an die Echtzeitfähigkeit, insbesondere wenn Multimedia-Signale oder auch Voice over IP-Übertragungen stattfinden sollen. Soweit zu diesem ungebrochenen Trend zu höheren Bandbreiten.

Parallel hierzu entwickelt sich eine Argumentation, die der oben dargestellten vollkommen konträr ausgerichtet ist. Es geht um die Einführung von Wireless LAN-Infrastrukturen als Ersatz von Kabelinfrastrukturen mit Highspeed LAN-Strukturen auf Basis von Ethernet.

Können Wireless LAN-Netze, die heute in der Regel mit ca. 11 und zukünftig vielleicht mit 22 oder 54 Mbit/s Bruttoübertragungskapazitäten, Kabelinfrastrukturen ersetzen? Ist eine strategische Entscheidung für Wireless LAN als Ersatz von Kabel sinnvoll und richtig?

Diesen Fragestellungen möchten wir im Weiteren auf den Grund gehen und mit folgenden Facetten beleuchten:

- Bandbreite
- Sicherheit
- Kosten
- TK-Integration
- Verfügbarkeit



**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

## **Die Bandbreite im Wireless LAN**

Wireless LAN-Infrastrukturen nach IEEE 802.11 b/a bieten heute Bruttoübertragungskapazitäten von optimalerweise 11 oder 54 Mbit/s. Optimalerweise bedeutet hier, dass diese Bandbreite nur erreicht werden kann, wenn eine sehr hohe Packungsdichte der Access Points im jeweiligen Abschnitt erreicht wird und die Übertragungseigenschaften der Funkstrecke 100%ig passen. In der Regel dürfte die normale Bandbreite einer Wireless LAN-Übertragung bei ca. 50 % der Maximalbandbreite liegen. Demzufolge können 5 oder 25 Mbit/s als normaler Wert einer Übertragungskapazität verstanden werden.

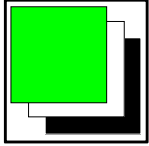
Damit erreicht man zunächst einmal die Hälfte der Bandbreite, im Vergleich zu den heute üblichen 10 bzw. 100 Mbit bei Ethernet-Infrastrukturen. Dies aber mit einem häufig nicht beachteten, aber entscheidenden Abstrich:

Die Ethernet-Infrastrukturen werden heute mit Switchingtechnologie aufgebaut und stellen die Bandbreite je Nutzer zur Verfügung. Wireless LAN-Infrastrukturen spiegeln sich jedoch im Funkäther ab und emulieren demzufolge ein Netzwerk, in welchem sich die Nutzer die zur Verfügung stehende Bandbreite teilen müssen. Wie im alten, auf Hub basierenden, Ethernet sind demzufolge die damit verbundenen Restriktionen gültig.

Blickt man zurück auf die Anfänge geschwichteter Ethernet-Infrastrukturen, so hat es aus unserer Erfahrung heraus einen deutlich höheren Mehrwert gebracht die Anschlüsse zu switchen, als deren Bandbreite zu erhöhen. Auch heute sind aus unserer Sicht noch 10 Mbit/s je Endgerät häufig ausreichend. Würde diese Bandbreite aber durch 10 bis 20 Nutzer geteilt, würde ein eklatanter Engpass entstehen. Dies konnte in der Vergangenheit in Hub Ethernet-Infrastrukturen immer wieder nachgewiesen und entsprechend durch den Einsatz von Switchingkomponenten kompensiert werden.

Diese Situation würde mit dem Einsatz von Wireless LAN, anstatt geschwichteten Ethernet-Infrastrukturen auf Basis von Kabeln, erneut entstehen.

Zusammenfassend ist die Bandbreitenentwicklung im Wireless LAN durchaus erfreulich und bietet in der Regel genügend rechnerische Bandbreite an. Unter Berücksichtigung des Shared Mediums „Funkäther“ ist jedoch ein deutlicher Abstrich in der Performance gegenüber klassischen Ethernet-Infrastrukturen mit Switchingkomponenten zu verzeichnen.



## +++RÖWAPLAN InfoWelle +++ Technologieinformation+++

### **Sicherheit im Wireless LAN**

Man hat einiges getan, um Wireless LAN-Infrastrukturen sicher zu machen. Neben den Wireless LAN-eigenen Security-Mechanismen, auf Basis der SSID, sind auch Konzepte unter Berücksichtigung von IEEE 802.1x „Authentifikationsmechanismen“ oder der Einsatz von VPN-Techniken möglich. Zu beachten ist hierbei, dass Security-Konzepte im Wireless LAN sehr aufwendig sind. Man stelle sich vor, dass sämtliche Funkübertragungstrecken über ein VPN abgesichert werden. Die entsprechenden Architekturen sowie Trust Center-Mechanismen und die damit verbundenen Konfigurationen in den Endgeräten weisen einen erheblichen Konfigurations- und Betriebsaufwand auf. Werden dagegen Abstriche an der Security-Architektur gemacht, öffnet man sein Netzwerk für unerlaubten Zugriff.

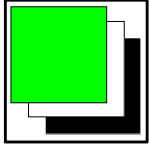
Ist es bei Kabelnetzen relativ einfach den „simplen Hacker“ abzuwehren, so sind komplexe Security-Architekturen im Funknetz nötig, um hochsensible Daten schützen zu können. Insbesondere „Men in the Middle“-Attacken sind in Wireless LAN-Infrastrukturen einfach möglich, da die Anmeldung eines Wireless LAN Clients am Access Point immer über den Äther kommuniziert und damit von außen einsehbar ist.

Ein offenes betreiben von Wireless LAN-Infrastrukturen, auf Basis der SSID, kann für professionelle Anwender nicht die Lösung sein. Dies trifft insbesondere dann zu, wenn Wireless LAN-Infrastrukturen für sämtliche Kommunikationsströme eines Unternehmens Verwendung finden sollen. Hier ist demzufolge zwingend ein umfassendes Security-Konzept, mindestens auf Basis von IEEE 802.1x und unter Berücksichtigung von MAC-Adresslisten in den Access Points erforderlich. Darüber hinaus wäre ein VPN-Konzept für die Übertragung sensibler Daten durchaus sinnvoll. Dennoch sind immer Security-Abstriche in Kauf zu nehmen, wenn Wireless LAN-Infrastrukturen zum Tragen kommen.

### **Die Kosten von Wireless LAN**

Häufig wird argumentiert, dass man doch durch den Einsatz von Wireless LAN die aufwendige und teure Kabelinfrastruktur einsparen kann. Sicher könnte dies der Fall sein, jedoch müssen die Kosten exakt gegenübergestellt werden.

Aus unserer Erfahrung heraus kostet ein Kupferkabel link durchschnittlich Euro 250,00. Eine Wireless LAN PCM CIA-Adapterkarte, die zusätzlich in Laptop's oder Endgeräte eingebaut werden muss, kostet ca. den gleichen Preis, wenn eine Übertragungskapazität von 54/22 Mbit/s nach IEEE 802.11 a/g zugrunde gelegt wird. Gespart wird demzufolge nichts. Die Ursache hierfür ist insbesondere, dass bei den meisten heute verfügbaren Endgeräten noch ein deutlicher Aufpreis für integrierte Wireless LAN-Antennen zu bezahlen ist oder separate PCM CIA-Adapterkarten oder Netzwerkadapterkarten für Desktop's beschafft werden müssen. Die Ethernet-Adapter sind in fast allen Fällen „on Board“.



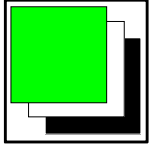
**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

Infrastrukturen bestehen natürlich nicht nur aus Kabel- bzw. Adapterkarten. Sowohl in einem geschichteten Ethernetumfeld als auch bei der Implementierung eines Wireless LAN-Netzes sind selbstverständlich Backbone-Netzwerkinfrastrukturen aufzubauen. Im Falle eines geschichteten Ethernets sind dies zum einen Verteilerschränke mit eingebauten Switchingkomponenten, im anderen Fall Access Points, die entsprechend verkabelt und angeschlossen werden müssen. Aber auch Access Points brauchen eine Connecting-Möglichkeit an eine Ethernet Backbonestruktur. Diese Verkabelung kann demzufolge nicht vollständig eliminiert werden. Für beide Netzstrukturen sind demzufolge Backbone-Infrastrukturen im Campusgelände erforderlich, die im Falle der Ethernet Desktop-Anschlussvariante in Switchingkomponenten ausgebaut wird und im Falle einer Wireless LAN-Implementierung als Access Points ausgelegt sind. Überschlagen können die Infrastrukturen für beide technologischen Ansätze, unter Kostengesichtspunkten, in etwa gleich bewertet werden.

Zusammenfassend ist festzustellen, dass durch die oben dargestellte Argumentation kein Kostenvorteil durch Wireless LAN-Infrastrukturen erzielt werden kann. Die Mehrpreise bei der Implementierung der Clients kompensieren die Einsparungen im Bereich der Kabelinfrastrukturen.

Die Kostendarstellung geht zudem davon aus, dass keine „Sondernutzer“ an die Wireless LAN-Infrastruktur angeschlossen werden müssen. Handelt es sich beispielsweise um Maschinen, die keine Wireless LAN-Implementierung ermöglichen oder beispielsweise Drucker, die keinen Anschluss einer PCM CIA-Adapterkarte für Wireless LAN-Übertragung bieten, sind Wireless LAN-Bridges einzusetzen. Die oben angesetzten Euro 250,00 für eine 802.11 a/g-Adapterkarte sind dann gegen ca. Euro 750,00 (und mehr, je nach Standard) einer Wireless LAN-Bridge auszutauschen. Das Kostenmodell wird dann sehr schnell zu Ungunsten der Wireless LAN-Infrastruktur kippen.

Unter Betriebsgesichtspunkten könnte ein gewisser Vorteil durch das Eliminieren von Patchtätigkeiten im Kabelumfeld resultieren. Andererseits ist zu beachten, dass insbesondere die Security-Architektur von Wireless LAN einen hohen Betriebsaufwand erfordert. Es ist zu empfehlen, die PCM CIA-Adapterkarten zentral auszugeben bzw. zu verwalten, um die zugrunde liegenden MAC-Adressen des eigenen Unternehmens exakt zu registrieren und an den jeweiligen Access Points zu hinterlegen. Demzufolge erfolgt eine „Patchung“ hier nicht mehr vor Ort, sondern über elektronische Verfahren und Freischaltungen im Access Point. Die zugrunde liegenden Aufwände dürften zwar etwas geringer, aber keinesfalls zu vernachlässigen sein.



**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

## **TK-Integration**

Eine sinnvolle Nutzung von Wireless LAN könnte die Eliminierung einer DECT-Lösung sein. Es besteht die Möglichkeit über Wireless LAN-Telefone und Voice over IP-Einsatz eine mobile Kommunikationslösung zu schalten. So weit so gut.

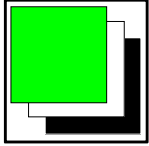
Unter der Berücksichtigung einer eingesparten Kabelinfrastruktur müssten aber auch sämtliche Desktop-Apparate durch Wireless LAN-Endgeräte ersetzt werden. Es gibt demzufolge nur noch „Handys“. Dies ist sowohl für „Chefs“ als auch für „Sekretärinnen“ kaum zumutbar. Die Leistungsmerkmale von Handgeräten entsprechen in keiner Weise dem, was die Nutzer heute von ihren Telefonen gewohnt sind. Einen Rückschritt nimmt kaum einer in Kauf. Der Anschluss von Telefonen an Wireless LAN-Infrastrukturen könnte nur unter Verwendung von Voice over IP und entsprechenden Wireless LAN Bridges erfolgen. Die Kosten wären exorbitant.

Anderenfalls müssen die TK-Endgeräte weiterhin über Kabelinfrastrukturen angeschlossen werden. Dies bedeutet, sowohl die Trassierung für die Kabelführung als auch die Verteilerräume müssten nach wie vor für den Anschluss von Telefonen und Faxgeräten aufgebaut werden.

## **Wireless LAN und Verfügbarkeit**

Das Design von Wireless LAN-Netzen ist nicht simpel. Sowohl die Ausleuchtung und Platzierung der Access Points als auch deren Überlagerung müssen exakten Designvorgaben folgen, um Störungen und Beeinflussungen zu vermeiden. Dies ist in einem leeren Gebäude durchaus in den Griff zu bekommen und flächendeckend zu realisieren. Zu beachten ist, dass eine Redundanz im Sinne einer doppelten Ausleuchtung eines Bereiches mit zwei Access Points sehr aufwendig bzw. kaum möglich ist, wenn die Designkriterien von Wireless LAN zugrunde gelegt werden.

Viel problematischer wiegt aber die Tatsache, dass das „Public Frequenzband“ von anderen Quellen benutzt und entsprechend beeinflusst werden kann. Zitiert sei hier die immer wieder genannte Mikrowelle, die im gleichen Frequenzband arbeitet. Bei unseren praktischen Tests konnten aber an vielerlei anderen Stellen Beeinflussungen festgestellt werden. So nutzen einige Anlagen und Systeme, beispielsweise in der Produktionstechnik - aber vielleicht zukünftig auch in der Haus- oder Meldetechnik, das gleiche Frequenzband. Diese Beeinflussungen sind nicht auszuschließen, würden aber den Betrieb der Wireless LAN-Infrastrukturen verkomplizieren oder verhindern und insbesondere bei der Fehlersuche deutliche Probleme aufweisen. Speziell, wenn die Frequenzen nur sporadisch und an einzelnen Punkten - vielleicht sogar mobil - in Betrieb gehen, ist für die Netzbetreiber kaum nachzuvollziehen warum entsprechende Störungen in der Datenübertragung vorliegen.



**+++RÖWAPLAN InfoWelle +++ Technologieinformation+++**

**Zusammenfassung: (Kernaussage)**

Unter heutigen Gesichtspunkten und unter Berücksichtigung der vorn dargestellten Argumentation empfehlen wir heute Kabelinfrastrukturen nicht durch Wireless LAN-Infrastrukturen zu ersetzen. Wir sehen hier weder einen Kosten- noch einen Nutzensvorteil.

Viel mehr sehen wir Wireless LAN-Infrastrukturen punktuell oder flächendeckend eingesetzt als eine sinnvolle Ergänzung der Kabelinfrastrukturen, um flexible und mobile User beispielsweise in Besprechungszimmern, für Außendienstmitarbeiter oder temporäre Mitarbeiter zur Verfügung zu stellen. Der hier notwendige administrative Aufwand kann in engen Grenzen betrieben werden, die Masse der Nutzer würde jedoch nach wie vor ihre Desktop-Anwendungen über Kabel sicherstellen.

Die oben dargestellte Argumentation und die darauf basierende Schlussfolgerung stellt eine Zusammenfassung unserer Erfahrungen aus vergangenen Projekten dar. Selbstverständlich besteht jeweils die Möglichkeit, die Argumentation auszubauen und entsprechende Aspekte detailliert zu beleuchten.

Sollte hierzu Bedarf und Interesse bestehen, können Sie sich gern an uns wenden.

erstellt im November 2003

**RÖWAPLAN**

*Ingenieurbüro - Unternehmensberatung*  
*Datennetze und Kommunikationsnetze*

Brahmsweg 4  
73453 Abtsgmünd

Tel.: 07366/96 26-0  
Fax: 07366/96 26-26  
E-Mail: [info@roewaplan.de](mailto:info@roewaplan.de)  
<http://www.roewaplan.de>