



---

# Vorlesung

## VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J.Buchmann

WS-05/06, V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: [wboehmer@cdc.informatik.tu-darmstadt.de](mailto:wboehmer@cdc.informatik.tu-darmstadt.de)





# Vorlesungsinhalte

---

- **Einsatz von Virtual Private Networks**
  - **VPN-Marktbetrachtungen**
  - **IPSec und MPLS für VPN der zweiten Generation**
    - **IPSec und Performance Aspekte**
  - **Planungsaspekte**
  - **Phasenplan zur Durchführung eines VPN-Projektes**
    - **Analyse**
    - **Konzept**
    - **Realisierung**
    - **Betrieb**





## Einsatz von Virtual Private Networks (VPN)

- Kosten-Nutzen-Verhältnis neben Flexibilität und Skalierbarkeit der VPN-Technologie stellt die herkömmliche Kommunikationstechnologie betriebswirtschaftlich in den Schatten.
- Die Zielgruppe beinhaltet nicht mehr die großen und ganz großen Unternehmen, sondern auch kleinere und mittelständische Firmen nehmen sich mehr und mehr dieser Technik an.
- Für Unternehmen stellt sich nicht mehr die Frage, ob ein VPN für die eigene Firma relevant ist oder nicht, sondern nur noch die Frage, wie und mit wem ein VPN umgesetzt werden soll.
- Die VPN-Technologie unterliegt, wie alle am Markt angebotenen Produkte einem wirtschaftlichen Lebenszyklus (*Produktionslebenszyklus*).
- Der Produktionslebenszyklus beschreibt fünf Lebensstufen in einem Produkt. (*Innovators, Early Adopters, Early Majority, Late Majority, Laggards*)





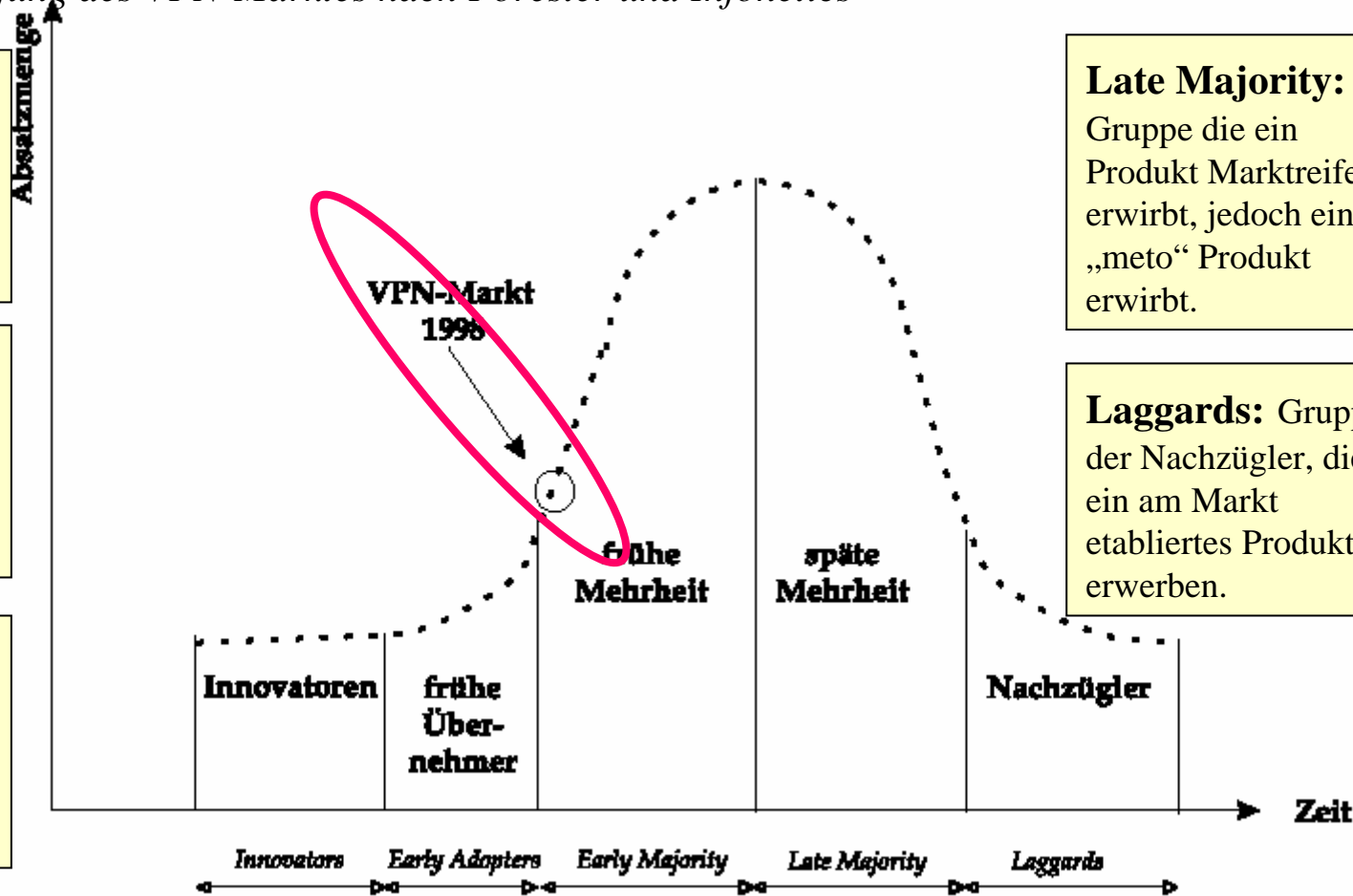
# Produktlebenszyklus bezogen auf den VPN-Markt

Einstufung des VPN-Marktes nach Forester und Infonetics

**Innovators:** Gruppe die frühzeitig bereit ist ein Produkt mit Kinderkrankheiten zu kaufen

**Early Adopters:** Gruppe die dem eigentlichen Markttrend voraus sind.

**Early Majority:** Gruppe die dem Produkt zum Durchbruch am Markt verhilft.



**Late Majority:** Gruppe die ein Produkt Marktreife erwirbt, jedoch ein „meto“ Produkt erwirbt.

**Laggards:** Gruppe der Nachzügler, die ein am Markt etabliertes Produkt erwerben.

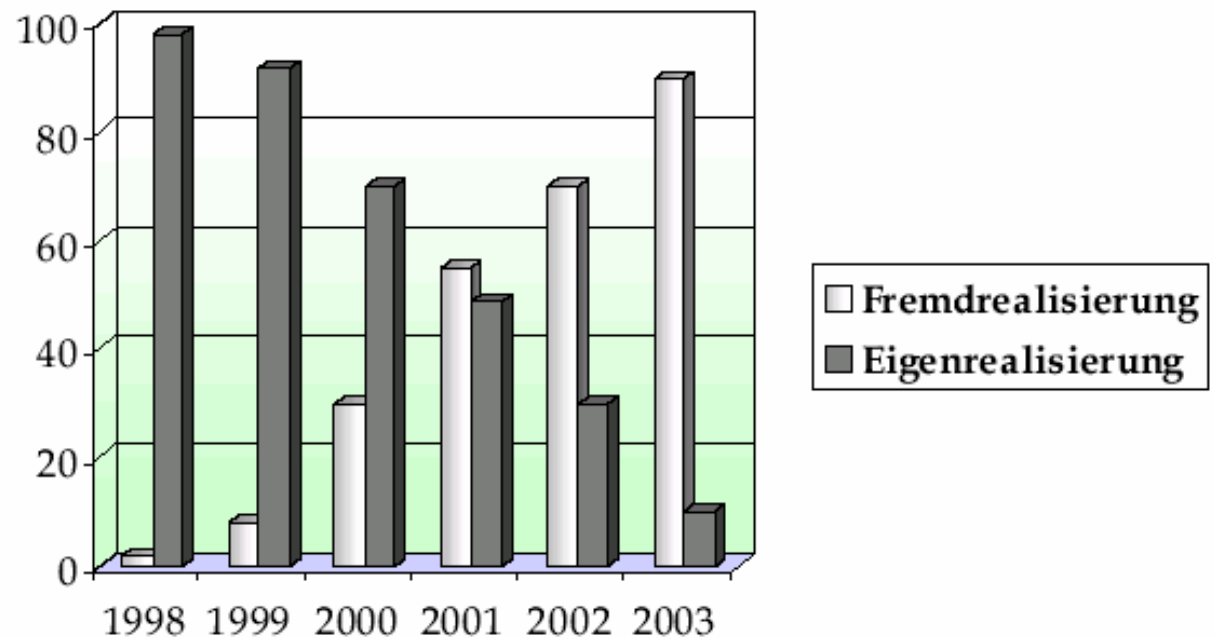




## Entwicklung des VPN-Marktes

- Umkehrung der Verhältnisse:

- Die deutlich abnehmende Eigenrealisierung geht in eine deutlich zunehmende Fremdrealisierung über.
- Break-point im Jahr 2001



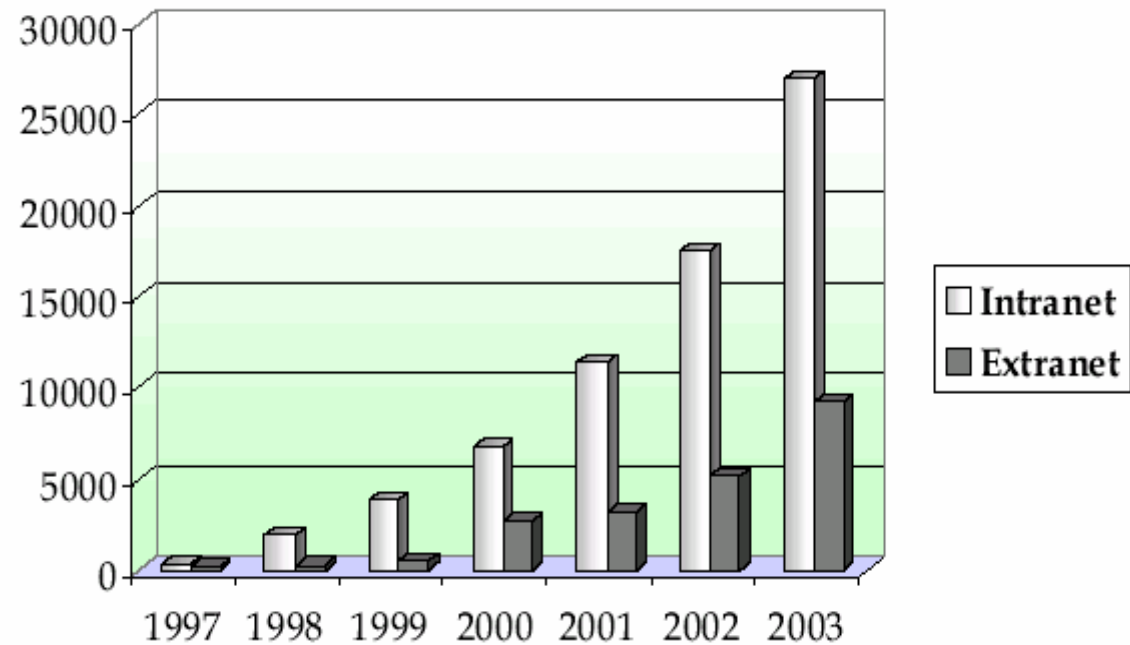
Quelle: Cahners In-Stat. Group 2001



# Intra- und Extranet-Entwicklung



Darstellung einer sich zunehmend verändernden Geschäftswelt. Folge: breitbandige Netzwerkverbindungen verlagern sich zum Netzrand und End-Nutzer-Anwendungen gehen zurück ins Innere der Unternehmensnetzwerke. Geschäftsbeziehungen werden vermehrt in einer virtuellen Welt mit vertrauenswürdigen Verbindungen zu Anbietern, Partnern, Mitarbeitern und Kunden abgewickelt.



## Veränderungen der Geschäftswelt (TeleChoice, 2001)



- Die Geschäftswelt wird zukünftig bestimmt werden durch:
  - eine Globalisierung und einen zunehmenden Wettbewerb,
  - Eine Dezentralisierung mit gleichzeitiger Zunahme von mobilen Mitarbeitern und einer Erhöhung des Telekommunikationsaufkommens,
  - einer weiteren Verbreitung des IP-Protokolls in den Netzwerken,
  - einer Zunahme der Web-basierenden internen Prozesse mit begleitender Kosteneinsparung der administrativen Bürotätigkeit,
  - die Intergration der Zulieferkette aus Kosten und Strategiegründen,
  - einer Konzentration auf das Kerngeschäft mit einer erhöhten Bereitschaft zum Outsourcing
  - Eine perfektere Infrastruktur zu geringeren Kosten
  - Einen zunehmenden Bedarf an hoch vertraulichen, flexiblen und hoch sicheren Netzwerken.





## Vorteile einer CPE-basierenden IP-VPN-Lösung für Kunden und Provider

Kunden-Vorteile	Service-Provider-Vorteile
<ul style="list-style-type: none"><li>● Kontrolle, Kontrolle, Kontrolle.</li><li>● Kontrolle über Sicherheitseinrichtungen, Credentials, Systeme und direkten Zugriff auf das Access Netzwerk.<ul style="list-style-type: none"><li>– Volle Ende-zu-Ende-Verschlüsselung (inkl. der lokalen Zugriffe).</li><li>– Dedizierter Einfluss auf das Equipment zur Aggregation und zur Verschlüsselung.</li><li>– Ende-zu-Ende-Zugriff kann entweder beim Kunden oder beim Service-Provider gewartet werden.</li></ul></li><li>● Wartung erfolgt unabhängig vom ISP bzw. Carrier.</li><li>● Kontrolle, welches Equipment eingekauft wird. Es kann das am Markt beste Equipment eingekauft werden.</li><li>● Die Lösung kann wesentlich feiner, auf die Netzbedürfnisse einer <i>Site-to-Site</i>, abgestimmt werden.</li></ul>	<ul style="list-style-type: none"><li>● Geringe Investitionen erforderlich.</li><li>● Deutlich bessere Absicherung der letzten Meile durch eine Ende-zu-Ende-Verschlüsselung</li><li>● Möglichkeit einer Einflussnahme für bestimmte Kunden, die eine übergeordnete Kontrolle einfordern. (z.T. besitzen große Firmen ein ausgeklügeltes CPE-VPN und Firewall-Überwachungssystem und ziehen eine eigene Wartung vor.</li><li>● Keine große Umstellung für die Kunden erforderlich, die ihre Frame-Relay oder ATM-Netze ebenfalls nicht selbst betreut haben.</li><li>● Eine ideale Möglichkeit andere gemanagte Dienste, wie managed Router, Ethernet oder Switches anzubieten.</li></ul>





## **Nachteile** einer CPE-basierenden IP-VPN-Lösung für Kunden und Provider

Kunden-Nachteile	Service-Provider-Nachteile
<ul style="list-style-type: none"><li>● Erfordert umfangreiche Installationszeit.</li><li>● Keine mit Carriern vergleichbare Vertraulichkeit und Verfügbarkeit.</li><li>● Als Kunde müssen alle Zeitvorgaben des Providers bei gemeinsam anfallenden Wartungsarbeiten und Problemen hingenommen werden.</li><li>● Begrenzte Skalierbarkeit: Eingeschränkte Möglichkeiten um zusätzliche Services oder Funktionalitäten nachträglich ins Equipment einzusetzen.</li><li>● Es ist üblicherweise ein Einzelanbieter für das gesamte Equipment vorgegeben.</li></ul>	<ul style="list-style-type: none"><li>● Lange Installationszeit = Umsatzeinbußen.</li><li>● Eventuell hohe Installationskosten, falls ein kompletter Austausch aller Sites innerhalb des VPN, des Fernzugriffs sowie bei schwierigen Sites, erforderlich wird.</li><li>● Hohe Management- und Wartungskosten bei einem Upgrade; bestimmte Wartungsprobleme ziehen einen kompletten Austausch der Kunden-Sites nach sich.</li><li>● Geringere Performance-Leistung gegenüber einer reinen Carrier-Leistung.</li><li>● Es muss bei nahezu allen Installations- und Wartungsproblemen der Kunde mit einbezogen werden.</li><li>● Begrenzte Skalierbarkeit: Schwierig, den Kunden erweiterte Services und Funktionalitäten zu verkaufen.</li><li>● Eingeschränkte Management-Möglichkeit, eingeschränkte Fernwartbarkeit und Überwachungsmöglichkeit, solange Plattformen unterschiedlicher Hersteller betreut werden.</li></ul>



# Kunden- und Service-Provider-Vorteile einer Netzbasierenden IP-VPN-Lösung



Kunden-Vorteile	Service Provider Vorteile
<ul style="list-style-type: none"> <li>● Geringe Gesamtkosten (weniger Personal, weniger Kapital, geringerer Ressourcen-Bedarf für das interne Netzwerk-Management).</li> <li>● Schnellere Planung, Konzeption und Implementierung.</li> <li>● Einfacheres und schnelleres Hinzufügen neuer Sites.</li> <li>● Kein technologisches und kein Investitionsrisiko bei einem zwingenden Technologie-Wechsel, bedingt durch ein Upgrade in dem Carrier-Netzwerk; anders als bei einer CPE-Lösung.</li> <li>● Flexiblere und einfachere Gestaltung von Funktionalitäten und Absicherungen.</li> <li>● Einfachere Wartung (z.B. keine langen Wartezeiten bei Hard- und Software-Upgrades).</li> <li>● Neue Dienstleistungen können ohne eine Equipmentänderung vorgenommen werden.</li> </ul>	<ul style="list-style-type: none"> <li>● Gesamtgewinn größer und schneller als bei einer CPE-Lösung.</li> <li>● Hohe skalierbare Architektur.</li> <li>● Umfangreiche Kundenanpassungen sind nun möglich.</li> <li>● Flexible und einfache Gestaltungen von Funktionalitäten und Absicherungen sind mittels zentralisierten Management möglich.</li> <li>● Datenabsicherung entspricht der bei Frame-Relay und ATM, inkl. der letzten Meile.</li> <li>● Eine logische Aggregation von tausenden von Kunden ist möglich.</li> <li>● Kostengünstige, zentralisierte und flexible Einrichtung.</li> <li>● Eröffnet neue Märkte für Service-Provider.</li> <li>● Günstige Markt- und Zeitvorteile, falls man sich in der frühen Übernehmer bzw. frühen Mehrheit befindet.</li> <li>● Beibehalten des alten Kundenstammes während neue Dienste angeboten werden können.</li> <li>● Kein kompletter Austausch von Sites.</li> <li>● Dienste können schneller eingesetzt werden mit gleichzeitiger Umsatz Generierung.</li> </ul>



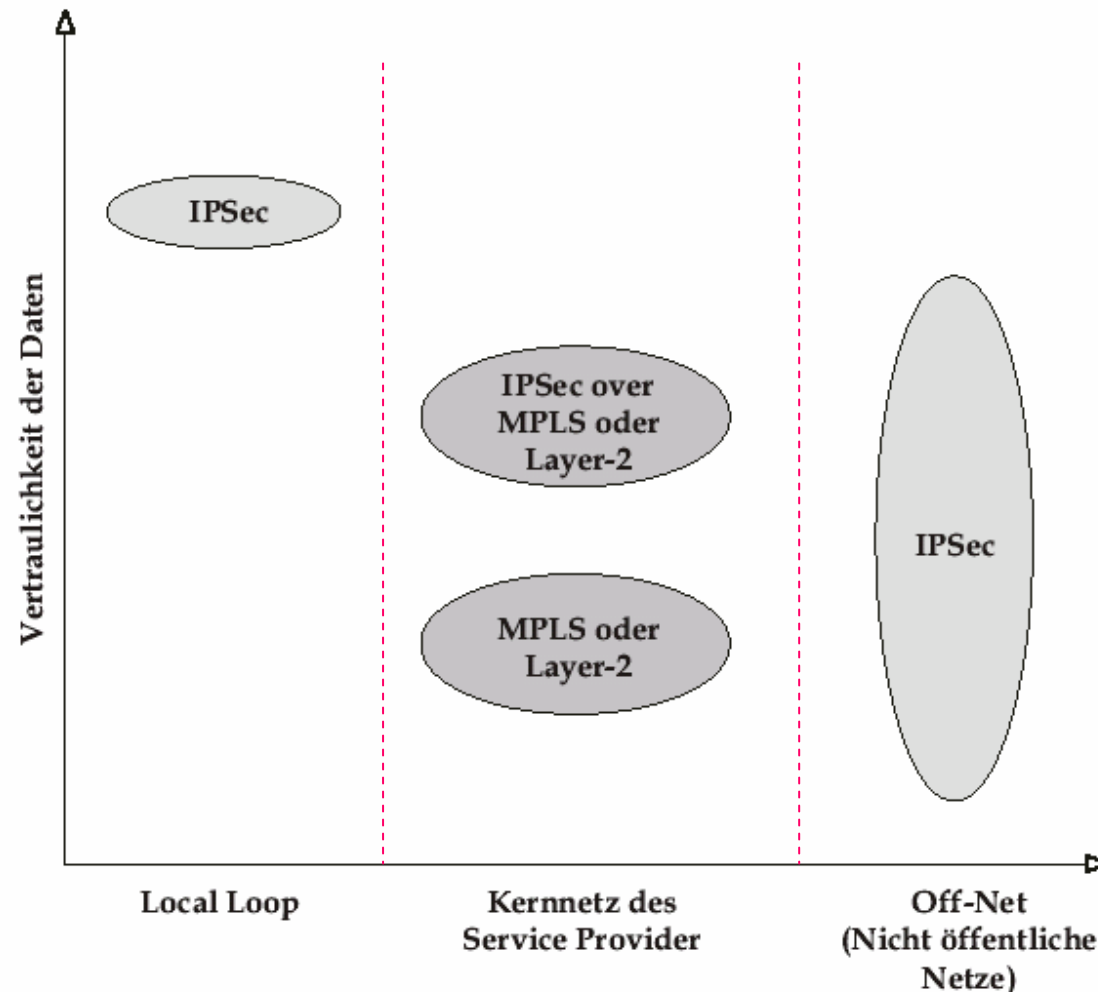
31.01.2006

Folie 10 / 24



# Datenvertraulichkeit und Netzstrukturen

- **Datenvertraulichkeit als Funktion der typischen Einsatzgebiete**
- **Im Bereich des Local Loop herrscht IPSec**
- **Im Bereich des Kernetz des Providers gibt es mehrere Varianten**
- **Im nicht öffentlichen Bereich herrscht IPSec.**





## Eigenschaften für VPN der zweiten Generation

Eigenschaften	Beschreibung
Skalierbarkeit	Ein VPN muss einfach skalierbar sein, angefangen von einer SOHO-Lösung bis hin zu großen Unternehmenslösungen, und es muss global erreichbar sein. Dabei ist die Möglichkeit, einem VPN kurzfristig Bandbreiten und Zugangspunkte hinzuzufügen, ein springender Punkt. Denn in dem heutigen dynamischen und aggressiven Markt kann schnell ein größeres Projekt gewonnen oder verloren werden. Somit muss eine adhoc-Reaktion wie Zuwachs oder Reduzierung eines VPN möglich sein.
Sicherheit	Für einen geschäftskritischen Datenverkehr muss gewährleistet sein, dass Sicherheitsmechanismen für die Vertraulichkeit, Paket-Authentifizierung, Nutzer Authentifizierung, Verkehrstrennung, Zugriffskontrolle und Tunnelverfahren, zur Verfügung stehen.
Dienstgütern (QoS)	Es muss eine Priorisierung für geschäftskritischen und übertragungskritischen Datenverkehr vorhanden sein. QoS-Funktionalitäten, wie <i>Queuing</i> , congestion avoidance, traffic shaping und Paket-Klassifizierung, müssen genauso wie ein Routing-Service durch ein optimales Routing-Protokoll gegeben sein.
Management	Es ist essentiell für ein kosteneffektives Netzmanagement, dass QoS-Parameter, Sicherheitsmaßnahmen und Billing-Informationen über ein Monitoring-System ständig erfasst werden, um z.B. neue Dienste zeitnah zu installieren oder SLAs zu kontrollieren.
Zuverlässigkeit	Es muss ein vorhersagbarer, mit extrem hoher Verfügbarkeit ausgestatteter, Service vorhanden sein, den Geschäftskunden erwarten und auch einfordern.





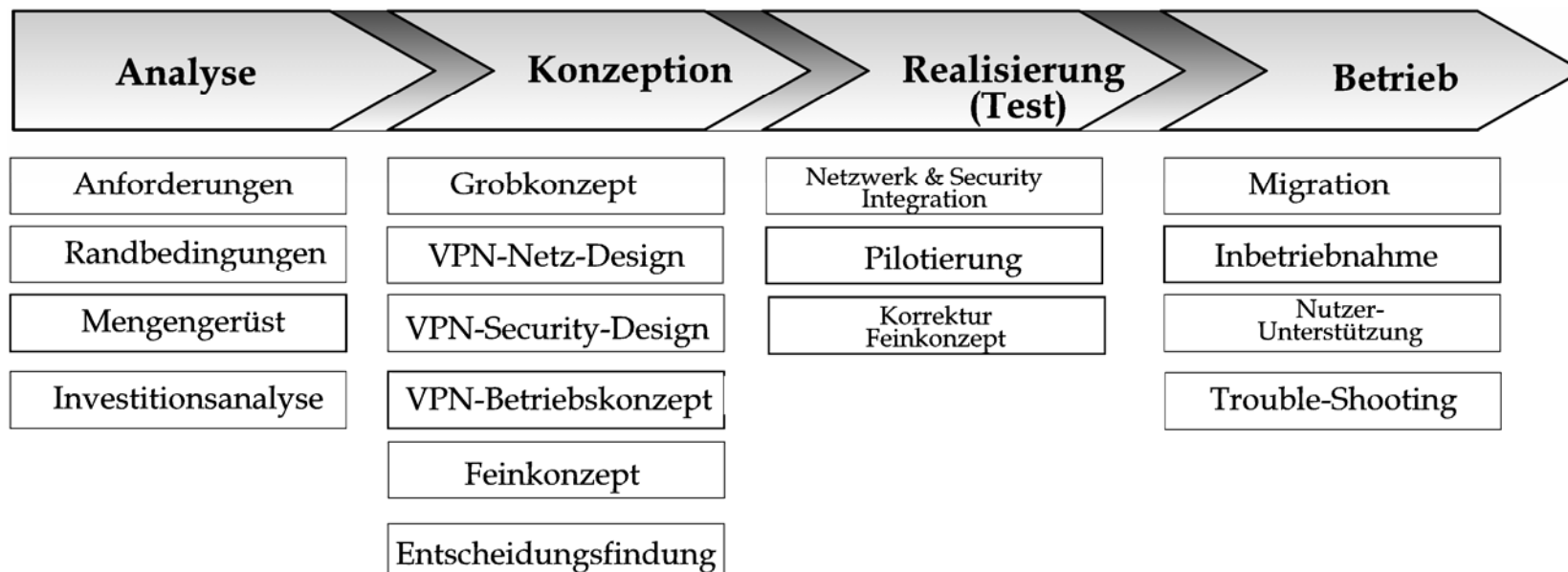
## VPN-Planungsaspekte

- Eine VPN-Planung kann im wesentlichen in zwei Punkten zusammengefasst werden.
  - Ein Nutzen muss im Sinne von verbesserten Geschäftsprozessen deutlich sichtbar werden. Dies kann z.B. dadurch erreicht werden, indem verstärkt Unternehmensprozesse im Intranet abgebildet und abgewickelt werden.
  - Nachweisliche Kosteneinsparungen im IT-Budget zu verzeichnen sind. Dies müsste schon in der Konzeptphase herausgearbeitet werden.





# Phasenplan zur Durchführung eines VPN-Projektes

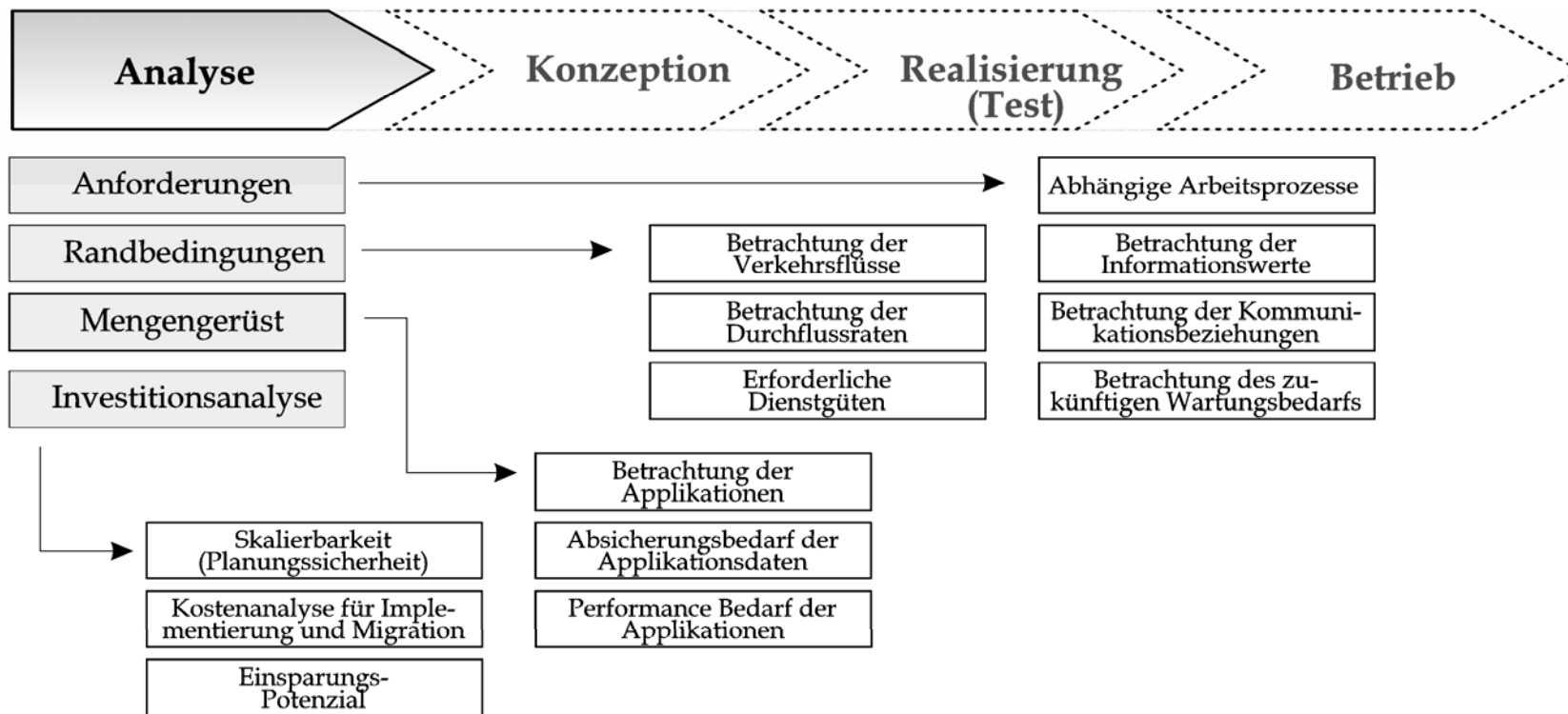


(No-Go / Go)





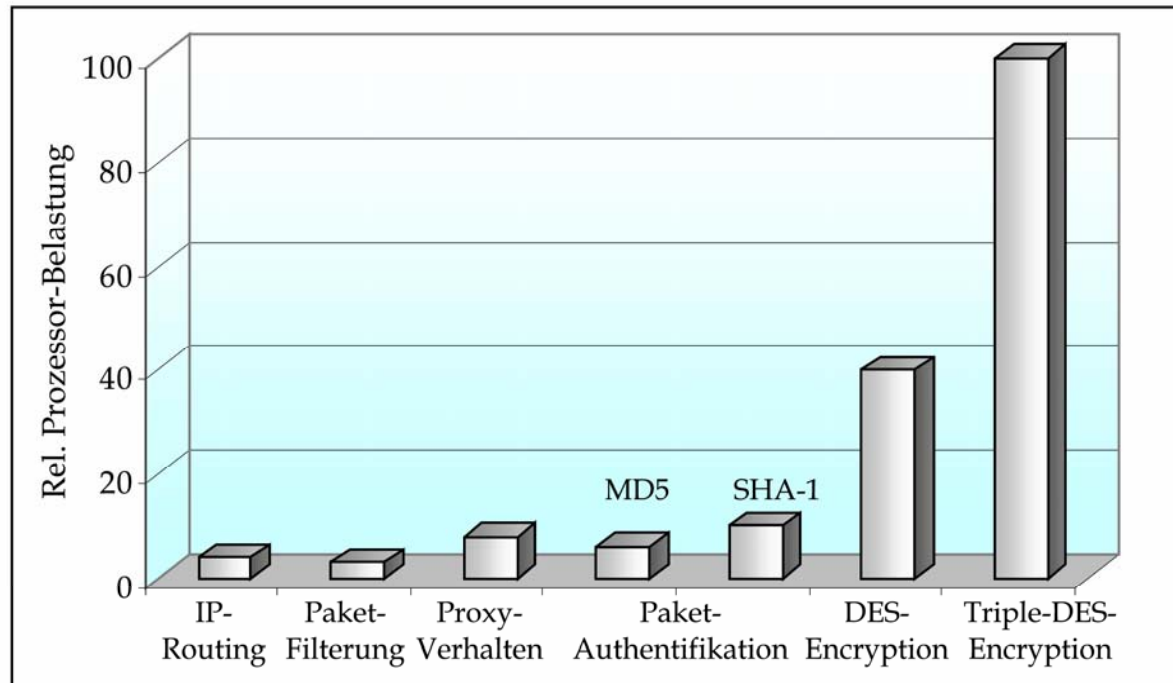
# Phasenplan / Analyse



# Analyse / Performance



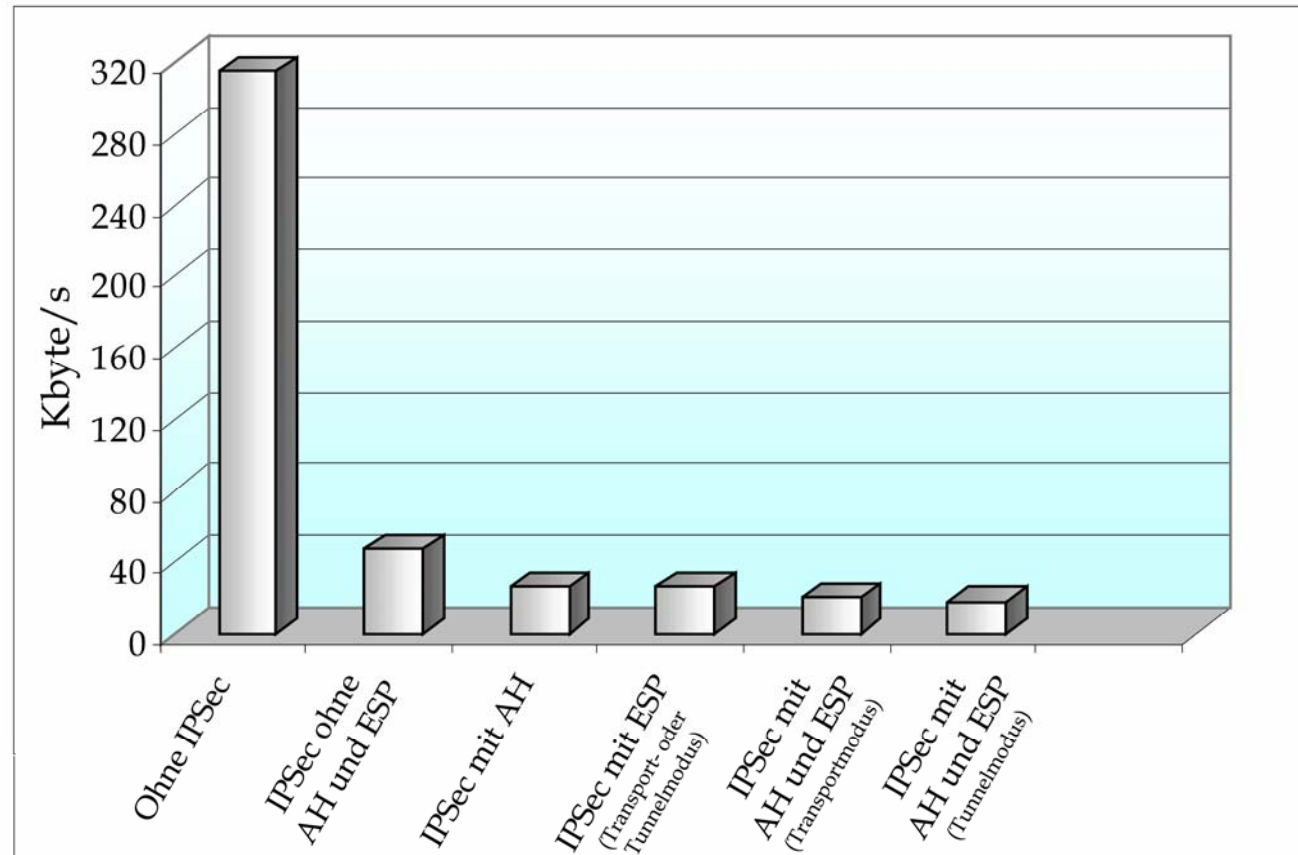
- **Geschwindigkeits-  
einbuße durch  
Verschlüsselungs-  
verfahren und  
Hashverfahren**
- **Die relative  
Prozessoraus-  
lastung steigt bei  
3DES über-  
proportional an.**



# IPSec und Performance Aspekte



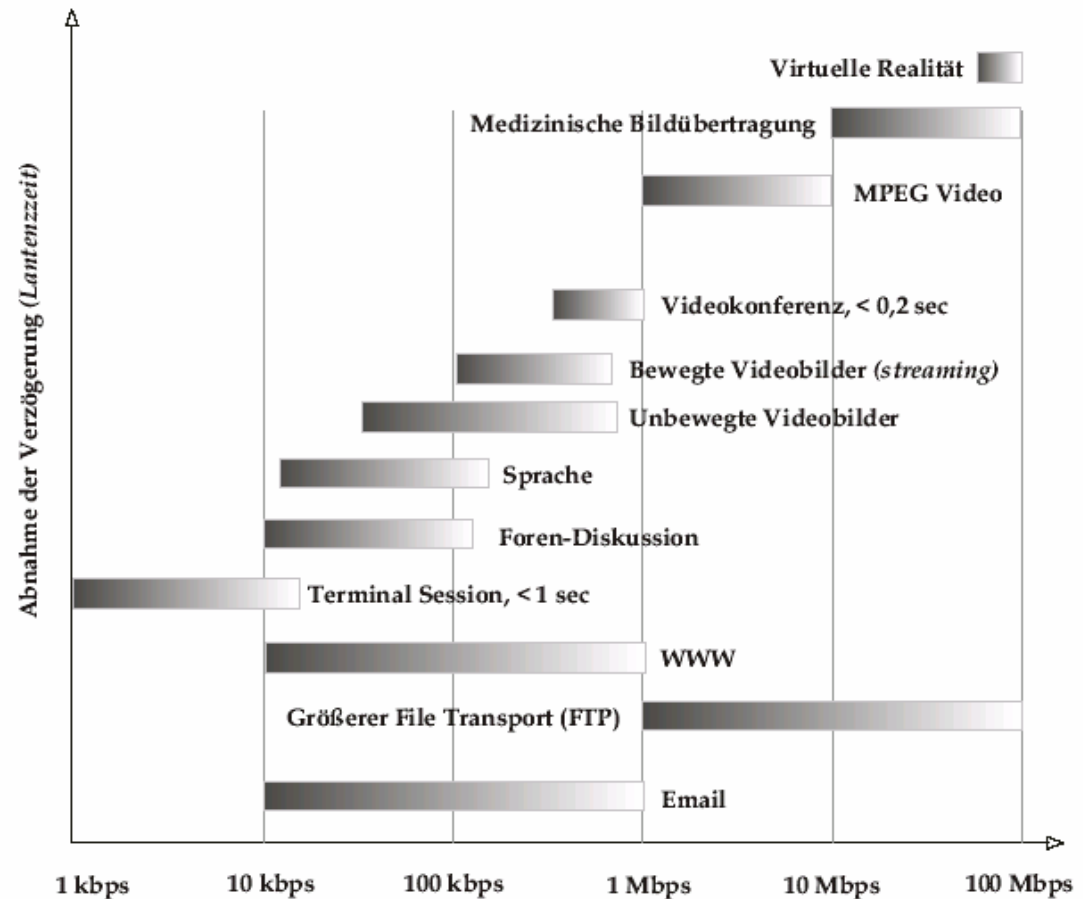
- **Ohne (IPSec) Verschlüsselung wird ein Durchsatz von ca. 290 Kbyte/s**
- **Mit Einsatz von IPSec erfolgen drastische Performance Einbußen, die sich untereinander nur geringfügig unterscheiden.**



# Überblick: Bandbreitenbedarf einiger Applikationen



- Je breitbandiger die Applikationen werden, um so geringer darf die Latenzzeit sein.
- Der Übertragungsbereich erstreckt sich heute von wenigen Kbps bis hin zu über 100 Mbps.





# Verfügbarkeit

$$V = \frac{MTBF}{MTBF + MTTR}$$

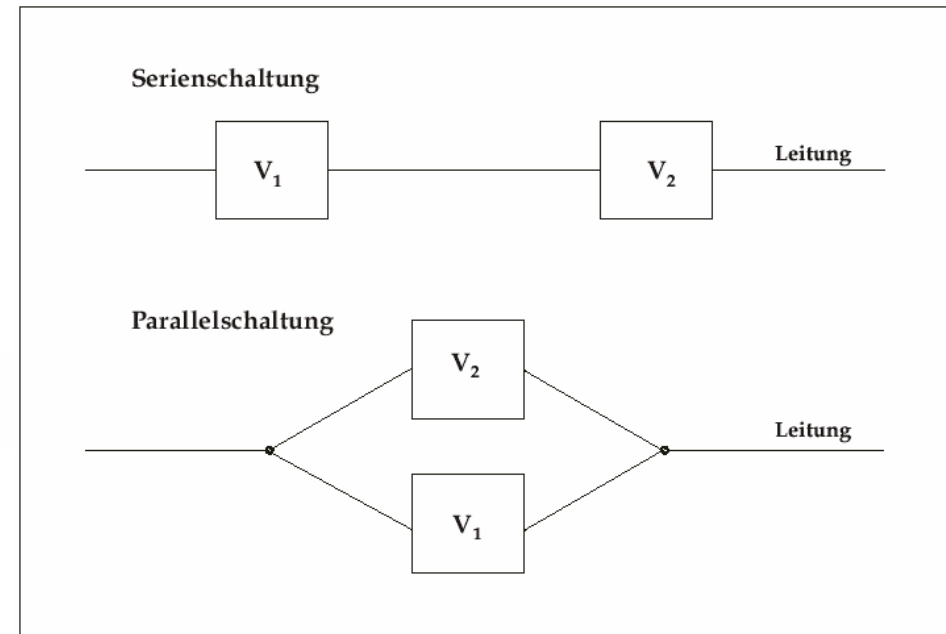
$$U = 1 - V = \frac{MTTR}{MTBF + MTTR}$$

$$V_{\text{Serie}} = V_i \cdot V_{i+1} \cdot \dots \cdot V_n,$$

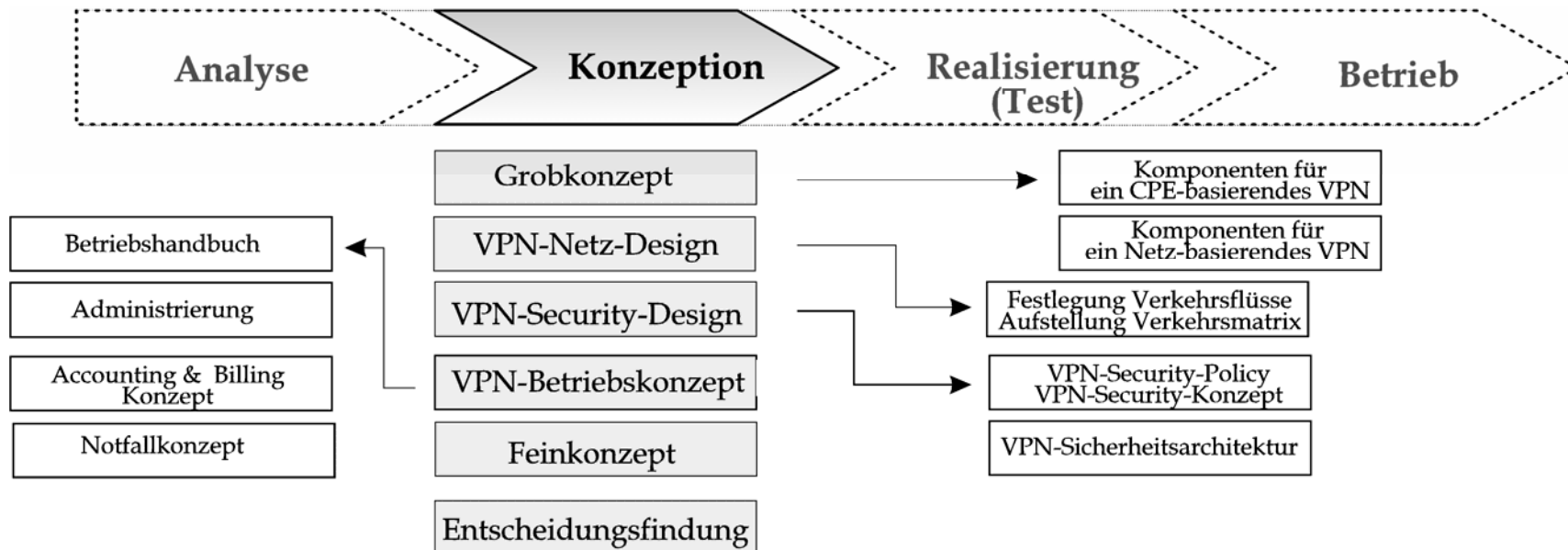
$$V_{\text{Serie}} = \frac{MTBF_i}{MTBF_i + MTTR_i} \cdot \frac{MTBF_{i+1}}{MTBF_{i+1} + MTTR_{i+1}} \cdot \dots \cdot \frac{MTBF_n}{MTBF_n + MTTR_n}$$

$$U_{\text{parallel}} = U_1 \cdot U_2 = (1 - V_1) \cdot (1 - V_2) = 1 - V_1 - V_2 + V_1 \cdot V_2,$$

$$V_{\text{parallel}} = (1 - U_{\text{parallel}}) = V_1 + V_2 - V_1 \cdot V_2.$$



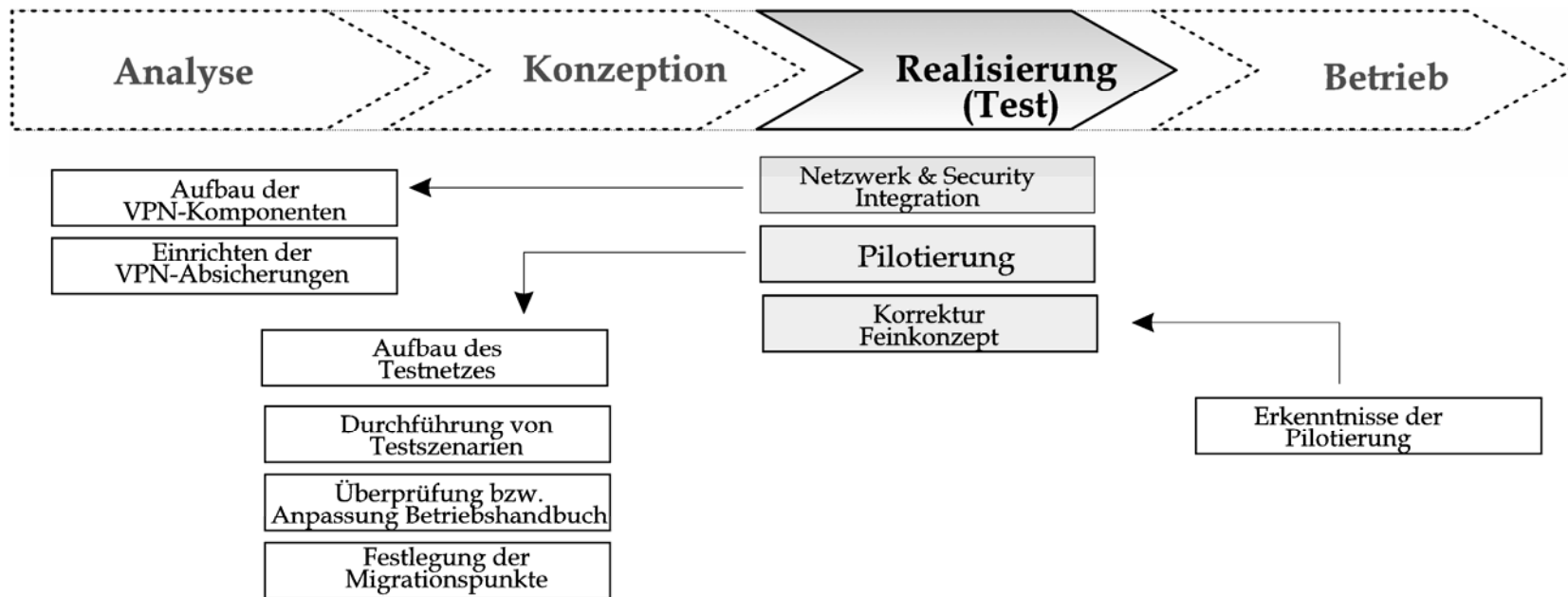
# Phasenplan / Konzeption



(No-Go / Go)

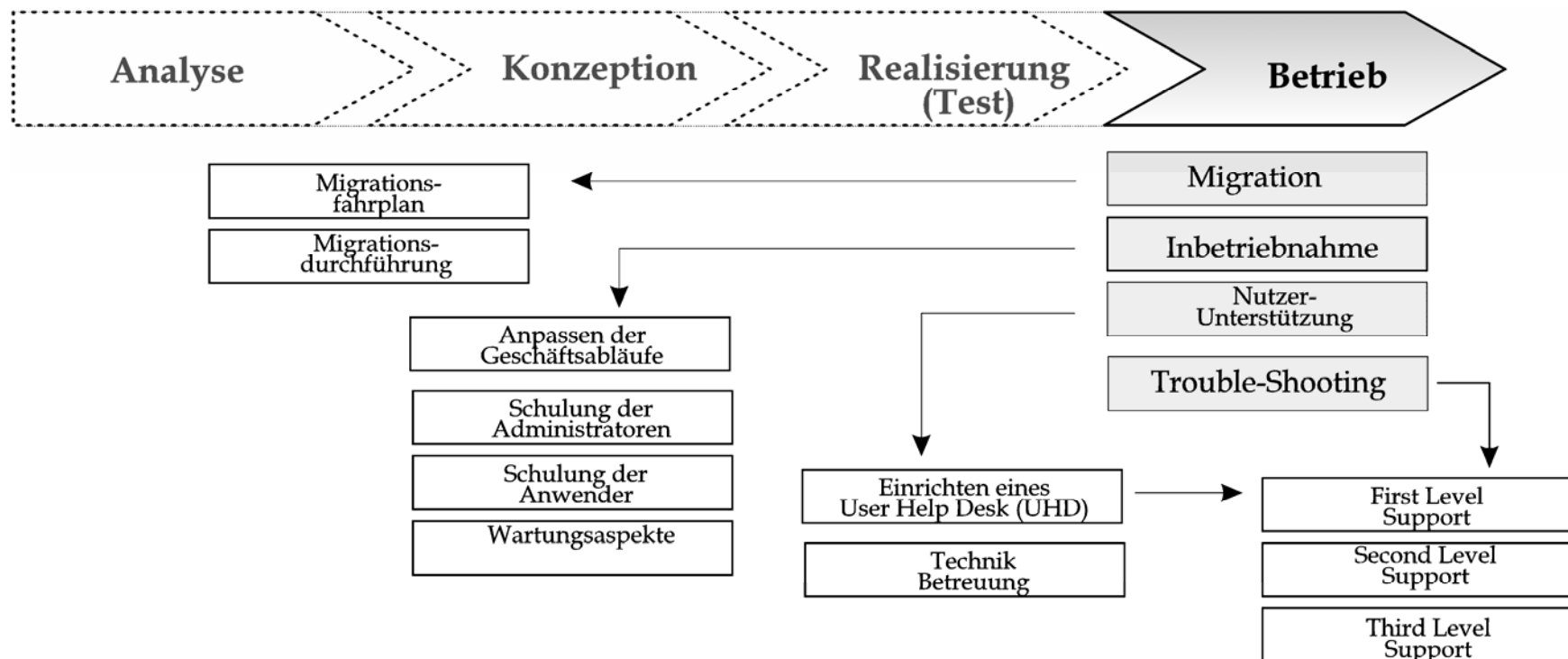


# Phasenplan / Realisierung





# Phasenplan / Betrieb



# Übungen

---



- Frage: Welche Art von VPN würden Sie aufbauen, wenn es lediglich um vertrauliche Abfragen einer Web-Applikation (Frames) über ein öffentliches Netz erfolgen soll?
- Frage: Welche Phase/Aktivität würden Sie zu Beginn eines VPN- Projektes durchführen wollen?
- Frage: Welches sind deutliche Anzeichen, das die VPN-Technologie ihren Zenit überschritten hat?
- Frage: Wie kann die Nichtverfügbarkeit einer Kommunikationsverbindung theoretisch berechnet werden?





## Literatur

---

- <http://www.tu-darmstadt.de/vv/comments/20.250.1>
- **Telechoice, 2001: Telechoice and Celox: IP-VPNs and Land Run for New Revenue, Whitepaper, prepared for celox Networks, Apr. 2001, TeleChoice, Inc. 1307S. Boulder Ave., Suite 120, Tulsa OK 74119.**
- **Cahners In-Stat Group, 2001: IP-VPN-Market oppertunities; An end-user survey study: TX0103EU, pub.date May, 2001.**
- **Performance Messungen (IPSec) Universität Helsinki (TCM) 1995.**
- **Intra- und Extranet-Entwicklung für die Jahr 1997-2003, Yankee Group, 1999.**
- **Michler E., 1984: Grundlagen der Theorie der Zuverlässigkeit, Lehrbriefe für das Hochschulstudium, TU-Dresden.**

