INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Klassifizierung und Bewertung von VPN Lösungen für die Neuausrichtung der europaweiten Extranetstrategie der BMW AG

Bearbeiter:	Martin Sailer
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Markus Garschammer Harald Rölle Dirk Provoost, BMW AG

INSTITUT FÜR INFORMATIK
DER TECHNISCHEN UNIVERSITÄT MÜNCHEN

Diplomarbeit

Klassifizierung und Bewertung von VPN Lösungen für die Neuausrichtung der europaweiten Extranetstrategie der BMW AG

Bearbeiter:	Martin Sailer
Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Markus Garschammer Harald Rölle Dirk Provoost, BMW AG
Abgabetermin:	15. Juli 2002

Hiermit versichere ich, daß ich die vorliegende Diplomarbeit selbständig verfaßt und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 15. Juli 2002

. . . .
(Unterschrift des Kandidaten)

Zusammenfassung

In dieser Arbeit werden Werkzeuge entwickelt, die in verschiedenen Phasen des Planungsprozesses eines VPNs unterstützend wirken. Zum einen wird mit einer generellen Kriteriensammlung die Grundlage für eine systematische Bestimmung der spezifischen Anforderungen eines Unternehmens geschaffen. Weiterhin wird eine Klassifizierung vorgenommen, die den Auswahlprozess hinsichtlich einer geeigneten VPN Technologie erheblich verkürzt. Abschließend werden die erstellten Werkzeuge anhand eines konkreten Szenarios, dem BMW Extranet, eingesetzt. Dabei wird unter Verfeinerung der generellen Kriterien ein spezifischer Kriterienkatalog erstellt, und eine VPN Technologie damit exemplarisch bewertet.

Inhaltsverzeichnis

Kapitel 1

Einleitung

In der Informationstechnologie sehen sich Unternehmen mit einer rasanten Entwicklung konfrontiert. Ihr Kerngeschäft stützt sich in immer höherem Maße auf eine verteilte und vernetzte IT-Struktur, um den Anforderungen des Marktes gerecht werden zu können. Internationale Märkte und die zunehmende Verflechtung der Unternehmen haben zur Folge, dass der Datenaustausch zwischen den Beteiligten stark zunimmt. Entsprechend wird es als Aufgabe der Kommunikationsdienste angesehen, derartigen Bedürfnissen nachzukommen.

Besondere Bedeutung kommt in diesem Zusammenhang den vernetzten Systemen zu: Sie sollen unabhängig von der geographischen Verteilung lokale Netzsegmente oder mobile Einzelplatzsysteme schnell, flexibel und kostengünstig verbinden und damit in das Unternehmensnetz (*Corporate Network*) integrieren. Traditionell wurde dies durch die Verwendung eigener Infrastrukturen oder durch das Anmieten von Standardfestverbindungen (Leased Line) gelöst. Allerdings wirken sich hierbei hohe Kosten und eine mangelnde Flexibilität hinsichtlich steigender Bandbreitenbedürfnisse nachteilig aus. Zur Lösung dieser angesprochenen Probleme bietet sich der Einsatz von Virtual Private Networks (VPN) an.

Der Begriff VPN wurde zum ersten Mal 1985 von US Sprint als Bezeichnung für ihren, auf geschlossenen Benutzergruppen basierenden, Kommunikationsdienst, verwendet [ML94a]. Seitdem dient er als Beschreibung für eine Vielzahl von Produkten und Lösungen verschiedenster Hersteller und Provider. Diese Uneinheitlichkeit in der Definition des Begriffs VPN, erfordert eine eigene Beschreibung im Kontext dieser Arbeit.

Definition des Begriffs VPN Die Definition des Begriffs VPN wird im Folgenden in zwei Schritten vorgenommen. Zunächst werden die in der Abkürzung VPN enthaltenen Wörter bestimmt, und danach zu einer umfassenden Definition zusammengefasst.

Der Begriff **Netzwerk**, im Sinne von Rechnernetz, wird mittlerweile weitgehend einheitlich verwendet. Vereinfacht ausgedrückt, bezeichnet man damit eine Anzahl von Geräten, die in einer bestimmten Form miteinander kommunizieren können (siehe auch [Tan96]). Als Geräte treten Computer, Router, Drucker usw. auf. Auf eine weiterführende Definition, einschließlich der auftretenden Protokolle, wird in diesem Zusammenhang verzichtet. Für eine umfassende Darstellung soll auf [Tan96] verwiesen werden.

Als **privat** wird die Kommunikation zwischen zwei oder mehreren Geräten angesehen, bei der Außenstehenden der Inhalt, sowie die Kommunikationsbeziehung selbst, verborgen bleibt. Damit besitzt private Kommunikation einen exklusiven Charakter, der es Außenstehenden nicht erlaubt, einzuwirken.
Weiterhin lässt sich die Bedeutung des Begriffs, durch sein Antonym öffentlich verdeutlichen. Eine öffentliche Netzinfrastruktur (*shared network*) wird von mehreren autonomen Organisationen genutzt und von einem (oder mehreren) Anbietern betrieben. Charakteristisch ist dabei vor allem, dass die Benutzung dieser Ressourcen nicht einer bestimmten Organisation vorbehalten ist. Ein Beispiel für eine solche Struktur stellt das öffentliche Telefonnetz oder das globale Internet dar. Im Gegensatz dazu steht die Benutzung einer privaten Netzinfrastruktur nur einer bestimmten Organisation - oftmals in der Form von dedizierten, selbstverwalteten, physikalischen Leitungen - zur Verfügung. In diesem Zusammenhang kann auch von einem exklusiven Zugriff gesprochen werden. Ein Beispiel dieser Struktur stellt ein Unternehmensnetz dar, bei dem keine externe Kommunikationsmöglichkeit vorhanden ist.

Mit **virtuell** werden Eigenschaften bezeichnet, die zwar nicht physikalisch, aber in ihrer Funktionalität vorhanden sind. Auf ein VPN übertragen, drückt dies aus, dass die Eigenschaften einer privaten Kommunikation bzw. Netzinfrastruktur vorhanden sind, aber keine physikalische Verbindungen in Form von dedizierten Leitungen bestehen. Vielmehr wird eine private Kommunikation über eine öffentliche Netzinfrastruktur realisiert. Dazu wird eine logische Partitionierung der unterliegenden Infrastruktur vorgenommen, mit dem Ziel, eine geschlossene Benutzergruppe (*Closed User Group*) zu erzeugen. Kommunikation bzw. logische Verbindungen innerhalb der Gruppe besitzen dabei die bereits angesprochenen privaten Eigenschaften.

Daraus kann nun folgende Definition abgeleitet werden:

> *Ein virtuelles privates Netz (VPN) ist ein Netz von logischen Verbindungen innerhalb einer geschlossenen Benutzergruppe mit den Eigenschaften einer privaten Kommunikation. Dazu wird eine logische Partitionierung einer öffentlichen Netzinfrastruktur vorgenommen, mit dem Ziel, geschlossene Benutzergruppen zu erzeugen.*

In ähnlicher Weise wird auch in anderen Arbeiten der Begriff VPN verwendet, allerdings in einer weniger formalen Beschreibung. Beispielsweise findet sich in[Lip01],[CS98] und [FH98] folgende Definition:

> *A VPN is a private network constructed within a public network infrastructure, such as the Internet.*

Vor allem die, im Vergleich zu privaten Netzen geringeren Kosten gelten als der Hauptgrund, weshalb sich Unternehmen für ein VPN entscheiden. Weiterhin sind eine hohe Flexibilität in der Wahl der Übertragungsbandbreiten zu nennen. Allerdings gilt es bei der Einführung und Planung eines VPNs eine Reihe von Aspekten zu beachten.

1.1 Planung eines VPNs

Die Einführung eines VPNs muss von einer sorgfältigen und zielführenden Planung begleitet werden. Dabei gilt es technische, organisatorische und betriebswirtschaftliche Aspekte zu behandeln. Betrachtet man den Lebenszyklus eines VPNs, kristallieren sich vier, in der Planung zu berücksichtigende Phasen heraus (Abbildung 1.1) :

Analyse-Phase beschäftigt sich im Wesentlichen mit den spezifischen Anforderungen bezüglich des entstehenden VPNs, sowie den zu beachtenden Randbedingungen.

Konzeptions-Phase basiert auf den in der Analyse-Phase gewonnenen Erkenntnissen. Es wird die VPN Lösung inklusive Netz- und Security-Design sowie ein Betriebskonzept festgelegt und daraus ein Feinkonzept erarbeitet. Basierend auf diesem Feinkonzept findet eine Entscheidungsfindung hinsichtlich der VPN Lösung statt. Wurde diese erfolgreich abgeschlossen, tritt die Realisierungs-Phase ein, ansonsten werden Änderungen des Feinkonzepts erforderlich.

Realisierungs-Phase beinhaltet den Betrieb des VPNs in einer Pilotumgebung. Somit werden die erarbeiteten Konzepte erprobt und unter Umständen modifiziert.

Betriebs-Phase entspricht der Einführung des VPNs bzw. dem regulären Betrieb gemäß dem Betriebskonzept. Falls erforderlich wird eine Migration der bestehenden VPN Lösung vorgenommen.

Die Verantwortlichkeiten in den verschiedenen Phasen liegen nicht zwingend beim Unternehmen. Abhängig vom Grad an Fremdrealisierung des VPNs (Outsourcings) können bestimmte Phasen in den Aufgabenbereich eines Providers fallen. In diesem Zusammenhang muss auf die Bedeutung der Analyse-Phase hingewiesen werden: Die Qualität darin gewonnener Ergebnisse beeinflußt die darauffolgenden Phasen nachhaltig, unabhängig davon, ob das VPN eigenständig oder in Zusammenarbeit mit einem Provider realisiert werden soll.

Für diese Arbeit bzw. die darin verfolgten Ziele nehmen die Analyse- und Konzeptions-Phase besondere Bedeutung ein. Genauer betrachtet, die in diesen Phasen auftretenden Probleme und Schwierigkeiten:

- Das Ermitteln der spezifischen Anforderungen stellt einen schwierigen Prozess dar. Neben den bestehenden Anforderungen gilt es, zukünftige Entwicklungen abzuschätzen und richtig zu interpretieren. Erschwerend kommt noch hinzu, dass die mit der Analyse betraute Abteilung oftmals nicht zugleich für die Entwicklung von Anwendungen zuständig ist. Letzteres verdeutlicht, dass eine Basis von möglichen bzw. generellen Anforderungen vorhanden sein sollte, um darauf basierend Spezifische ableiten zu können.

- Die Auswahl einer geeigneten VPN Lösung innerhalb der Konzeptions-Phase bringt einen erheblichen Zeitaufwand mit sich. Voraussetzung ist eine umfassende Kenntnis aller verfügbaren VPN Technologien respektive den inhärenten Eigenschaften. Unterstützend sollte hier eine Klassifizierung von VPN Lösungen wirken. Ausgehend von Anforderungen niedriger Granularität können somit Technologien ausgeschlossen bzw. in die Auswahl einbezogen werden.

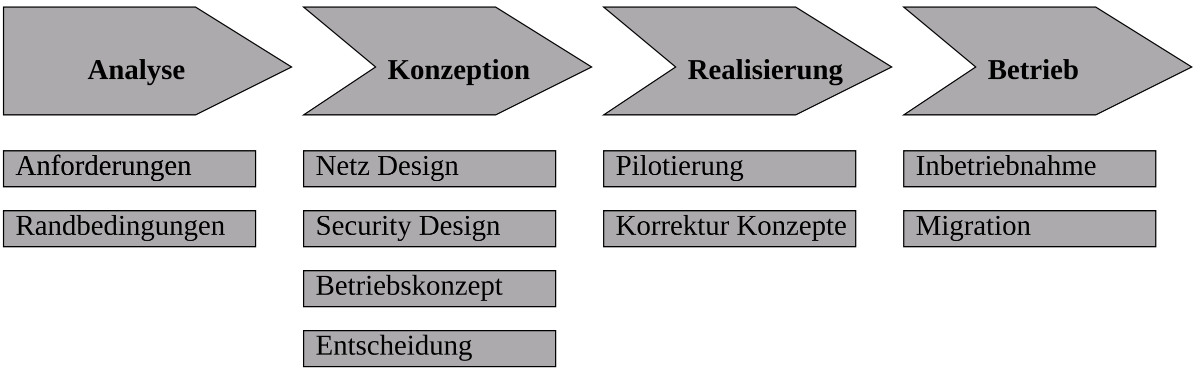

Abbildung 1.1: Phasenplan zur Einrichtung eines VPN (Quelle [Böh02])

1.2 Aufgabenstellung

Die BMW AG betreibt seit 1997 für mehrere tausend BMW-Händler in Europa ein sogenanntes Extranet (siehe Abschnitt 1.4). Diese VPN Lösung ermöglicht es BMW Händlern, zentral bereitgestellte Anwendungsdienste zu nutzen. Neue technologische Möglichkeiten zur Realisierung des Extranets ermöglichen eine Überarbeitung bzw. Neuausrichtung der Extranet Strategie.

Dafür sollen innerhalb des BMW internen Projekts *dealer network strategy* die notwendigen Arbeitsschritte ausgeführt und letztendlich eine Strategie festgelegt werden. Eine Umsetzung der Strategie ist für die nächsten zwei Jahre geplant. In den Aufgabenbereich des Projekts fallen die im Phasenplan (Abbildung 1.1) dargestellte Analyse- und Konzeptions-Phase. Besondere Bedeutung kommt dabei der Auswahl einer geeigneten VPN Lösung zu.

Das Ziel vorliegender Arbeit besteht darin, diesen Auswahlprozess zu unterstützen. Zum einen soll dafür eine generelle Kriteriensammlung für VPN Lösungen erarbeitet werden. Damit wird das Ziel verfolgt, eine Anforderungsbasis für die Analyse-Phase bereitzustellen, anhand derer spezifische Anforderungen von BMW ermittelt werden können. Basierend auf diesen spezifischen Anforderungen soll ein Kriterienkatalog zur Bewertung von VPN Lösungen erstellt werden. Weiterhin wird eine Klassifizierung von VPN Lösungen vorgenommen, um den in der Konzeptions-Phase auftretenden Auswahlprozess von Technologien zu vereinfachen. Es erfolgt eine Auswahl der für BMW geeigneten Lösungsklassen und deren Bewertung mit Hilfe des erstellten Kriterienkatalogs.

1.3 Vorgehensweise in dieser Arbeit

Wie bereits erwähnt wurde, kann ein Kriterienkatalog allein den Entscheidungsprozess in einem Unternehmen nicht hinreichend unterstützen. Die Anzahl der möglichen Lösungen in Bezug auf Technologien und Organisationsverhältnisse ist zu umfangreich, um alle möglichen Permutationen zu bewerten. Um überhaupt den Kriterienkatalog anwenden zu können, ist es also notwendig, vorab die spezifischen Klassen von VPN Lösungen für ein Unternehmen zu bestimmen.

Weiterhin liegt der Anspruch dieser Arbeit darin, eine generelle Sichtweise auf VPN Lösungen zu vermitteln. Aus diesem Grund werden Anforderungen zunächst generell formuliert und für den szenario spezifischen Kriterienkatalog angepasst.

Die in Abbildung 1.3 dargestellte Vorgehensweise spiegelt die beiden genannten Ansprüche wieder. Aktionen drücken die, mit Kapiteln korrespondierenden Arbeitsschritte aus. Das in einer Aktion erarbeitete Ergebnis ist in der Graphik rechts auf gleicher Höhe dargestellt. Oftmals fließen Ergebnisse in eine Aktion mit ein oder werden von einer Aktion explizit vorausgesetzt. Entsprechende Verbindungspfeile signalisieren derartige Beziehungen.

Im ersten Teil wird auf generelle und damit szenariounabhängige Gesichtspunkte eingegangen. Dazu erfolgt zunächst die Betrachtung der verschiedenen Varianten von VPN Lösungen in Bezug auf Anwendungsgebiete, technische Verfahren und organisatorische Verteilung. Daran schließt sich die Vorstellung eines Referenzmodells an, in das die besprochenen Varianten eingeordnet werden.

Der nächste Schritt umfasst die Bestimmung von grundlegenden Anforderungen an VPNs im Hinblick auf die Erstellung eines Kriterienkatalogs. Um auch hier eine geeignete Abstraktion vorzunehmen, wird ein *Top-Down* Vorgehen zugrunde gelegt. Dabei geht es nicht um die Beachtung technischer Details, sondern vielmehr um die Ermittlung genereller Anforderungen aus verschiedenen Sichtweisen wie z.B. der VPN befindlichen Applikationen. Ergebnis dieser Aktion ist eine generelle Kriteriensammlung zur Bewertung von VPN Lösungen.

Um Entscheidungen bezüglich der eingesetzten Technologien treffen zu können, ist es erforderlich die spezifischen Vor- und Nachteile derselben zu kennen. Dazu werden im nächsten Kapitel, in einem *Bottom-up* Vorgehen, Technologien im Kontext der gefundenen Anforderungen betrachtet. Die in Kapitel 2 vorgestellten technischen Grundlagen ermöglichen eine Einordnung in Technologieklassen und dienen somit zur Abgrenzung klassenspezifischer Anforderungen. Als Resultat entsteht eine Gegenüberstellung von VPN Technologien und den in Kapitel 3 ermittelten Anforderungen.

Am Anfang dieses Abschnitts wurde angemerkt, dass eine Bewertung aller möglichen VPN Lösungen zu zeitintensiv und damit für den Auswahlprozess eines Unternehmens ungeeignet ist. Aus diesem Grund wird in der nächsten Aktion eine Definition von VPN Lösungsklassen vorgestellt, basierend auf der in Kapitel 4 erarbeiteten Gegenüberstellung. Klassen werden dann aus Kombinationen von Anforderungen in niedriger Granularität und der entsprechenden Umsetzung durch Technologien gebildet. Eine Gegenüberstellung von unternehmensspezifischen Anforderungen mit den Eigenschaften einer Klasse führt zu individuellen Lösungsklassen.

Im nächsten Teil der Abhandlung kommen die erarbeiteten Werkzeuge in einem konkreten Anwendungsfall zum Einsatz. Das BMW Extranet, das von BMW Händlern europaweit genutzt wird, dient dabei als Szenario.
Zunächst werden BMW-spezifische Anforderungen ermittelt, und die generische Kriteriensammlung unter Einbeziehung dieser Anforderungen angepasst und verfeinert. Dabei entsteht ein BMW-spezifischer Kriterienkatalog.

Zuletzt wird, basierend auf der erarbeiteten Klassifizierung, eine Lösungsklasse für das BMW Extranet abgeleitet, und anschließend exemplarisch mit dem spezifischen Kriterienkatalog bewertet. Dabei wird ein Vergleich mit der bestehenden Lösung erarbeitet.

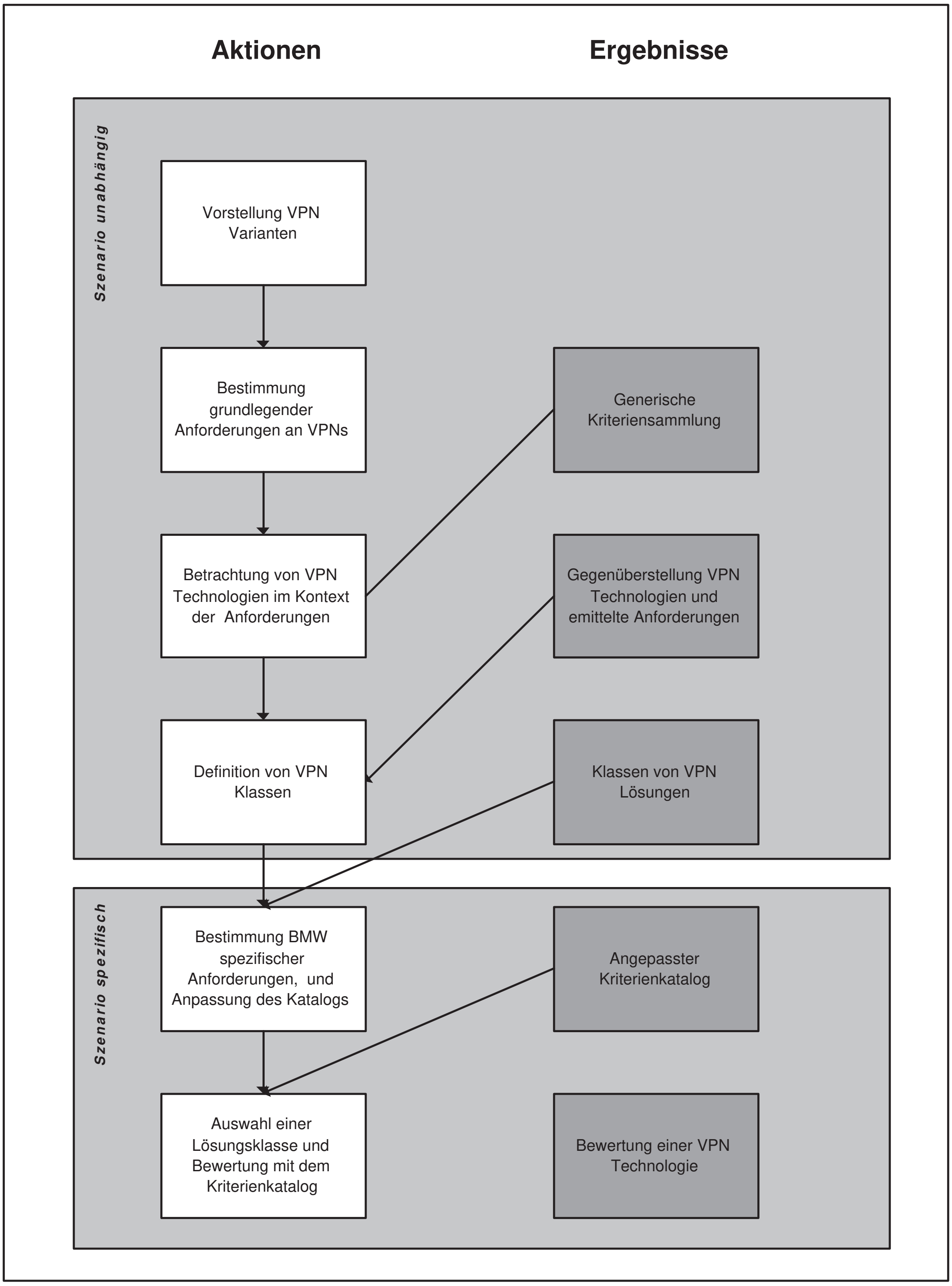

Abbildung 1.2: Vorgehensweise in dieser Arbeit

1.4 Das Extranet der BMW AG

Die BMW AG betreibt für ihre Händler eine - als Extranet bezeichnete - VPN Lösung in zehn europäischen Ländern. Der Begriff Extranet drückt hierbei die organisatorischen Beziehungen aus: Die Händler stellen eigenverantwortliche Organisationen dar, die mit BMW in einem vertraglich zugesicherten Verhältnis stehen. Damit beschränkt sich der Zugriff für Händler auf ausgewählte Anwendungen, die getrennt vom Unternehmensnetz zur Verfügung gestellt werden.

In Abbildung 1.4 erfolgt die Darstellung der Struktur des Extranets in Bezug auf Anwendungen, Diensten und Benutzern. Security Komponenten wie Firewalls finden in dieser Darstellung keine Beachtung. Dabei lassen sich folgende grundlegende Bestandteile identifizieren:

BMW Access LAN Darin werden Applikationen zur Verfügung gestellt, die von allen, an das Extranet angeschlossenen Händlern benutzt werden (internationale Applikationen). Darunter fallen etwa Anwendungen zur Bestellung von Fahrzeugen (*Online Ordering*) oder Ersatzteilen (*Parts Ordering*).

Service Area (zweifach vorhanden) In den Betrieb des Extranets sind zwei Hauptprovider involviert. Beide stellen in einer eigenen Service Area den Teilnehmern des Extranets zusätzliche Dienste zur Verfügung. Namentlich sind dies ein DNS und Email Dienst sowie ein Internetzugang.

Concentration Point (einer pro Land) In jedem an das Extranet angeschlossenen Land wird auf die Kommunikationsdienste eines nationalen Providers zurückgegriffen (*nationales Extranet*). Der Concentration Point stellt dabei den Übergang von den Hauptprovidern zu dem, für das Land zuständigen, nationalen Provider her. Die Verbindung von den Service Areas zu den Concentration Points wird von den Hauptprovidern mit Hilfe eines Frame Relay Dienstes hergestellt (*internationales Extranet*).

BMW Niederlassung (eine pro Land) Eine BMW Niederlassung ist in jedem, an das Extranet angeschlossene Land vorhanden, und mit dem Concentration Point direkt verbunden. In den Niederlassungen werden sogenannte nationale Anwendungen den Händlern des entsprechenden Landes zur Verfügung gestellt. Als Beispiele sind die Verteilung von Produkt Broschüren oder der Zugriff auf einen Gebrauchtwagenmarkt zu nennen.

Händler, Teleworker und IT-Partner (insgesamt 2323) Händler und Teleworker stellen die unmittelbaren Benutzer des Extranets dar. Als Teleworker bezeichnet man mobile Benutzer, die typischerweise mit Hilfe einer ISDN oder Modemeinwahllösung Zugang zum nationalen Extranet aufnehmen. Dahingegen verfügen Händler über ein eigenes lokales Netzwerk und sind an das nationale Extranet über eine Standardfestverbindung angebunden. Zusätzlich treten IT Partner auf, die für die Administration der Händler-Netze verantwortlich sind. Ihr Zugriff ist allerdings auf die entsprechenden Händler beschränkt. Die nationalen Provider sind für den Datentransport zwischen Concentration Point und Händlern bzw. Teleworkern zuständig.

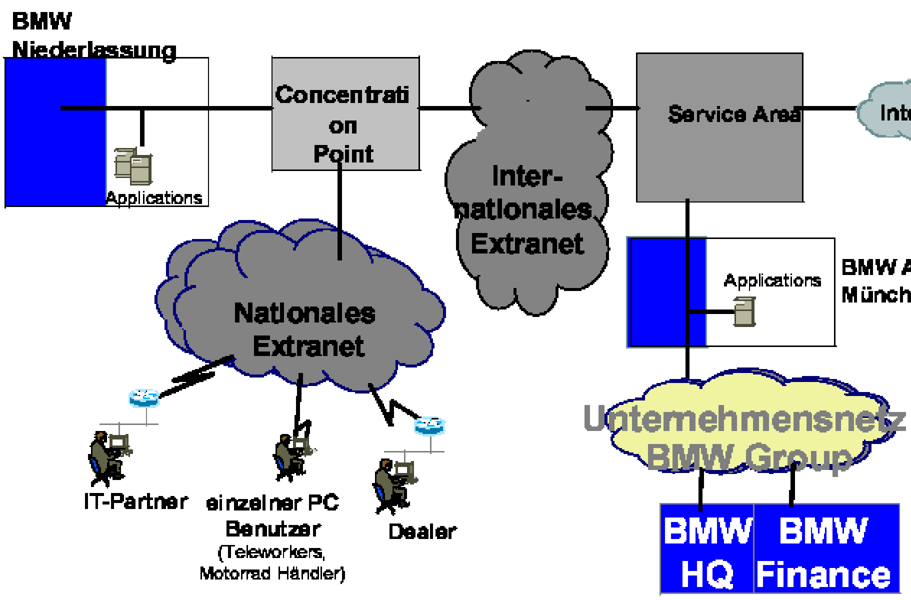

Abbildung 1.3: Die Stuktur des BMW Extranets - Anwendungen, Dienste und Teilnehmer

Zwischen der BMW AG und den involvierten Providern wurden weiterhin vertragliche Vereinbarungen bezüglich der Güte der Kommunikationsdienste getroffen (Service Level Agreement). Beispielsweise wird in diesem Zusammenhang eine Zielverfügbarkeit von 99,8 % pro Jahr für den Frame Relay Dienst von der Service Area zu einem Land garantiert.

Wie anhand des BMW Extranets deutlich wird, ist ein VPN nicht auf eine bestimmte Technologie oder Einsatzfeld im Sinne von Teilnehmern festgelegt. Vielmehr existieren eine Reihe von Typen, die im folgenden Kapitel dargestellt werden.

Kapitel 2

VPN Typen

In diesem Kapitel werden grundlegende VPN Typen anhand mehrerer Gesichtspunkte vorgestellt. Zunächst liegt das Augenmerk auf den möglichen Einsatzfeldern eines VPNs. Weiterhin wird kurz auf die technischen Verfahren zur Realisierung eines VPNs eingegangen. Im darauffolgenden Abschnitt werden dann Varianten, die sich aus der organisatorischen Verteilung bei der Einrichtung eines VPNs ergeben, diskutiert. Anschließend wird eine Verzahnung von organisatorischen und technischen Varianten anhand des von der *ppvpn* Workgroup [Cal02] des IETF ausgearbeiteten Referenzmodells aufgezeigt.

2.1 Einsatzfelder von VPNs

Die Einsatzfelder eines VPNs stehen in direktem Zusammenhang mit den Eigenschaften der darin auftretenden Teilnehmer. Anders ausgedrückt, die Art der Teilnehmer charakterisiert das Einsatzfeld des VPNs. Dabei treten folgende Ausprägungen auf (siehe auch [Lip01]), die auch im Hinblick auf Vorteile gegenüber privaten Netzen, vorgestellt werden:

Remote-Access Einzelne, oft auch mobile Teilnehmer, stellen VPN Verbindungen über Einwahllösungen her. Typisches Beispiel hierfür ist ein Benutzer, der sich von seinem Laptop aus, über ein Modem in das Unternehmensnetz einwählt. Während dafür in der Vergangenheit vor allem Zugangstechniken wie Modems (und damit verbundene Protokolle wie V.90, V.34, V.34+), ISDN (V.120) und GSM (V.110) verwendet wurden, kommen nun auch DSL und Kabelmodems vermehrt zum Einsatz. Im Falle von Modems und ISDN stellt sich die Frage nach dem Übergang vom öffentlichen Telefonnetz in das Unternehmensnetz. Dafür sind sogenannte Remote Access Concetratoren (RACs) notwendig, die in der Lage sind, eine breite Palette von

Protokollen aus diesem Bereich zu unterstützen. Der Betrieb eines RACs ist aber für ein Unternehmen mit einer Reihe von Nachteilen verbunden:

- Beschaffung der RACs bedeutet hohe Investitionskosten
- eine ständige Anpassung an neue technische Gegebenheiten ist notwendig
- die Grundgebühr für Anschlüsse auf Unternehmensseite sowie die Verbindungsgebühren (vor allem für Auslandsgespräche) sind mit hohen Kosten verbunden
- RACs sind nicht in der Lage DSL oder Kabelmodem Verbindungen zu terminieren

Unter Berücksichtigung der genannten Faktoren erweist es sich deshalb oftmals günstiger für ein Unternehmen, einen Service Provider zu beauftragen und bestimmte Teile der Remote Access Lösung an ihn outzusourcen. Typischerweise stellt der Provider Einwahlknoten, sogenannte Point of Presence (POP) zur Verfügung, in denen die Einwahlverbindungen terminieren. Der weitere Datentransport findet über die Backbone Struktur des Providers oder über das Internet statt.

Die Vorteile für das Unternehmen liegen vor allem in der Ersparnis variabler und fixer Kosten: Einerseits fallen die Verbindungsgebühren des Benutzers nur für den Zugang zum nächstgelegenen POP an, andererseits trägt der Provider die Investitionskosten für RACs und ähnliche Komponenten. Letzteres resultiert aus einer breiteren Unterstützung von Zugangstechnologien - DSL und Kabelmodems werden bereits in vielen Ländern angeboten.

Der erste Ansatz (selbstständiger Betrieb der Einwahllösung) erfordert technische Lösungen vor allem im Bereich der RACs und wird deshalb im Rahmen dieser Arbeit vernachlässigt. Im Hinblick auf VPN Technologien erweist sich der zweite Ansatz als relevant, bei dem die Einwahlverbindungen in den POPs des Providers terminieren und nicht beim Unternehmen selbst. Daraus erwächst die Notwendigkeit, eine logische Verbindung vom Benutzer der Einwahllösung zum Unternehmen durch entsprechende VPN Technologien abzubilden. Wie bereits erwähnt, können die Daten vom POP zum Unternehmen über das Provider Backbone oder das Internet transportiert werden. Etwaige Sicherheitsanforderungen, die sich daraus ergeben, müssen außerdem mit Hilfe der Technologien abgedeckt werden.

Site-to-Site Verteilte Standorte eines Unternehmens, respektive die in den Standorten vorhandenen lokalen Netzsegmente, werden über ein VPN miteinander verbunden. Aufgrund des hohen Datenaufkommens finden oftmals

Standardfestverbindungen Verwendung. Eine charakteristische Eigenschaft dieses Typs besteht darin, dass die Standorte in das Corporate Network integriert werden, es entsteht gewissermaßen ein Wide Area Network (WAN). Für die Wegewahl (Routing) sind somit eine Integration in das unternehmensweite Routingschema sowie die Vergabe unternehmensweit eindeutiger IP Adressen erforderlich.
Analog zum Remote Access erweist es sich für das Unternehmen oftmals als kostengünstiger einen Service Provider zu beauftragen (Outsourcing). Durch Service Level Agreements (SLAs) sichert der Provider vertraglich bestimmte Dienstgüteparameter zu. In diesen Bereich fallen die Größen Round Trip Delay oder Maximum Downtime. Erfüllt der Provider diese Zusagen nicht, werden die Kosten für den Kunden in der Höhe der ausgehandelten Penalties gemindert.
Die in diesem Bereich angesiedelten Technologien sind für den WAN Bereich ausgelegt und müssen es dem Provider erlauben, mehrere Kunden VPNs gemäß der ausgehandelten SLAs zu betreiben. Konkreter ausgedrückt, müssen die Technologien hohe Übertragungsgeschwindigkeiten, QoS, und das Bilden von geschlossenen Benutzergruppen zulassen. Außerdem soll die Technologie mehrere Übertragungsprotokolle unterstützen, um den Kundenwünschen gerecht zu werden.

Vielerorts wird zusätzlich zwischen *Intranet-* und *Extranet-VPNs* unterschieden ([Böh02], [Kos98]). Dabei drückt Intranet aus, dass alle Teilnehmer des VPNs demselben Unternehmen angehören. Im Gegensatz dazu wird ein Extranet (siehe auch 1.4) zur Anbindung von unternehmensexternen Teilnehmern verwendet.

Es ist zu beobachten, dass in der Praxis selten einer der vorgestellten Typen exklusiv auftritt. Vielmehr finden sich Kombinationen aus Remote Access und Site-to-Site VPNs. Dies lässt sich leicht nachvollziehen, wie folgendes Beispiel illustriert: Betreibt ein Provider eine Remote Access Lösung für den Kunden, ist die Verbindung von dem POP zum Zugangsknoten des betreffenden Unternehmens gewissermaßen ein Site-to-Site VPN.

2.2 Technische Verfahren zur Realisierung eines VPNs

Die Varianz von VPN Typen drückt sich auch in den technischen Verfahren, die zu ihrer Realisierung verwendet werden, aus. Die in diesem Zusammenhang auftretenden Typen werden im Folgenden vorgestellt. Eine genauere Betrachtung technischer Verfahren und den darauf basierenden Technologien findet sich in Kapitel 4.

Das Bilden von geschlossenen Benutzergruppen (CUG) wird in Abschnitt 1 als Grundeigenschaft von VPNs vorgestellt. Entsprechend kommt den technischen Verfahren, die diese Eigenschaft umsetzen, große Bedeutung zu. Stellt man Konzepte und Protokolle von VPN Technologien in diesem Zusammenhang gegenüber, kristallisieren sich zwei grundlegende Verfahren und damit VPN Typen heraus: Tunnel-basierte und Netz-basierte. Daneben bieten zur Realisierung von client-server VPNs verwendete Verfahren eine Alternative zu VPN Technologien im herkömmlichen Sinn.

Tunnel-basiertes VPN Mit diesem Begriff werden VPNs bezeichnet, die zur Datenübetragung zwischen VPN Teilnehmern auf das *Tunneling* Verfahren zurückgreifen. Grundlage dieses Verfahrens ist das Kapseln von Paketen eines Netzwerkprotokolls in ein neues Netzwerkprotokoll. Abbildung 2.2 zeigt einen solchen Vorgang. Das ursprüngliche Paket (mit einem Schicht 3 Header) wird mit einem neuen Schicht 3 Header versehen (Encapsulation) und zusätzlich ein Tunnel-Header eingefügt. Letzterer signalisiert dem Empfänger, dass es sich um ein Paket des betreffenden Tunneling Protokolls handelt. Er wertet den Header aus, entpackt das originale Paket (Decapsulation) und transportiert es weiter. Zwischen Sender und Empfänger, den sogenannten Tunnelendpunkten, deren Netzwerkadressen durch den neuen Schicht 3 Header festgelegt werden, entsteht eine Tunnel [Lip01]. Als konkrete Anwendung des gezeigten Beispiel ist ein Transport von IPX Paketen über ein IP Netz zu nennen. Wie daraus ersichtlich wird, besteht ein Vorteil dieses Verfahrens in der Möglichkeit, einen Datentransport trotz unterschiedlicher Protokolle derselben Schicht (im Beispiel Schicht 3) vorzunehmen. Dies gewinnt im Kontext von VPNs an Bedeutung, falls das Unternehmen Übertragungsprotokolle verwendet, die sich von denen des Providers unterscheiden.

Ein weiterer Vorteil dieses Verfahrens wird beim Einsatz in VPNs ersichtlich, speziell im Umfeld von IP-Netzen; denn der eingefügte Header verwendet dasselbe Protokoll wie der des ursprünglichen Paketes. Wird beispielsweise “IP in IP” getunnelt, können dadurch private, nicht registrierte IP Adressen verborgen werden und die entsprechenden Pakete über das Internet transportiert werden.

Mit Hilfe von Tunneling werden normalerweise Punkt zu Punkt Verbindungen zwischen zwei Teilnehmern erzeugt. Es gibt allerdings auch Technologien die 1 zu n Kommunikationsbeziehungen unterstützen. Implementiert werden Tunneling Verfahren entweder als Hardware (z.B. in einem Router) oder als Softwarekomponenten (z.B. als Teil des Betriebssystems).
Als Nachteil des Tunneling Verfahrens ist der entstehende Overhead anzuführen. Damit wird die Vergrößerung des Paketes, hervorgerufen durch die zusätzlichen Header, bezeichnet. Der tatsächliche Umfang dieses Mehraufwands ist implementierungsabhängig und somit ein Kriterium um Tunnel-basierte Technologien zu vergleichen.

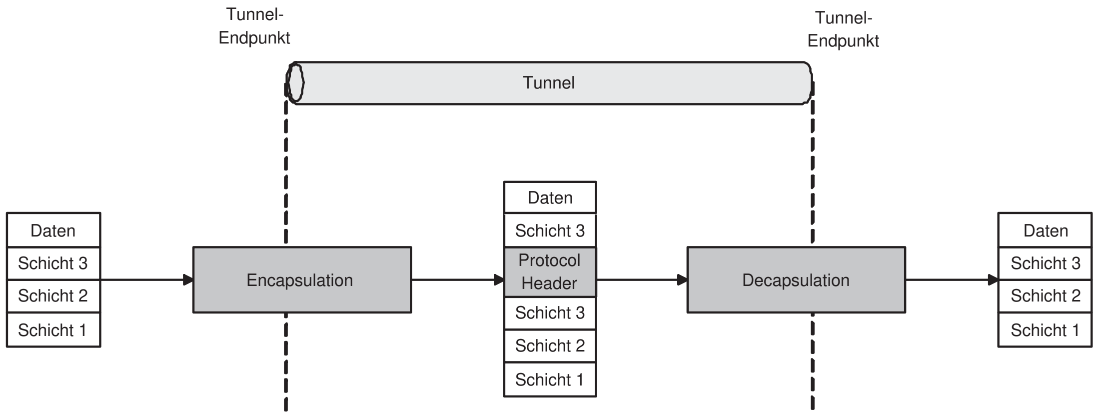

Abbildung 2.1: Übersicht Tunneling Verfahren

Netz-basiertes VPN Netz-basierte VPN werden durch den Einsatz von datenpaketvermittelten Technologien realisiert. Technologien, die in diesen Bereich fallen, weisen die Gemeinsamkeit auf, dass sie nicht primär für den Einsatz in VPNs konzipiert wurden. Vielmehr handelt es sich um WAN Technologien, deren Eigenschaften für die Anwendung im VPN Umfeld genutzt werden. Sie sind damit für ein Unternehmen nur unmittelbar einsetzbar, falls entsprechende Ressourcen in Form von Übertragungsleitungen vorhanden sind. Im Allgemeinen implementieren Service Provider netz-basierte Technologien in ihrer Backbone Struktur und bieten Unternehmen VPN Dienstleistungen darauf basierend an. Unterschiede zu Tunnel-basierten Technologien bestehen vor allem in der Weise, wie der Datenverkehr auf dem Weg durch die *shared networks* geschützt wird. Dafür sind keine Mechanismen wie Datenverschlüsselung vorgesehen, eine Separation der Datenströme wird durch das eingesetzte Switching bzw. Routing Verfahren gelöst.

Deswegen ist es nicht verwunderlich, dass Anforderungen wie Datenverschlüsselung keine unmittelbare Berücksichtigung in der Spezifikation entsprechender Technologien finden. Um dennoch den gewünschten Effekt zu erzielen, bietet sich beispielsweise eine Kombination mit Tunnel-basierten Technologien an, die entsprechende Verschlüsselungsverfahren implementieren.

Client-server VPN Als Alternativen zu VPN Technologien im herkömmlichen Sinn finden in der Praxis Verfahren Anwendung, mit deren Hilfe als client-server VPNs bezeichnete Lösungen implementiert werden [Kos01]. Anders als die bisher beschriebenen Verfahren sind sie in höheren Schichten (über der Transportschicht) des OSI Modells angesiedelt und nicht darauf ausgelegt, verschiedene Netze miteinander zu verbinden. Vielmehr zielen sie darauf ab, Security Mechanismen für einen bestimmten Kreis von client-server Anwendungen zur Verfügung zu stellen. In diesem Zusammenhang werden gegenseitige Authentisierung von client und server sowie eine Verschlüsselung der ausgetauschten Daten unterstützt. Das populärsteAnwendungsgebiet sind in dieser Weise geschützte Verbindungen zwischen Browser und Webserver.

2.3 Organisatorische Verteilung bei der Einrichtung eines VPNs

In diesem Abschnitt werden Varianten in Bezug auf die organisatorische Verteilung zwischen Unternehmen und Provider in der Planung und dem Betrieb eines VPNs vorgestellt. Die Varianten unterscheiden sich dabei in dem Grad der Eigenrealisierung durch das Unternehmen.

In [Lip01] werden in diesem Zusammenhang drei Kategorien erwähnt: eine Eigenrealisierung (*In-house*), Mischrealisierung (*Hybrid*) sowie Fremdrealisierung (*Outsourcing*). Allerdings ist diese Einteilung zu grob, um die möglichen Ausprägungen zu erfassen. Je nach vertraglicher Vereinbarung können feine Stufen von mischrealisierten VPNs auftreten.

In ähnlicher Weise schätzt dies [Böh02] ein. Er schlägt einen kontinuierlichen Übergang vor, in dem sich sechs Stufen erkennen lassen (Abbildung 2.3). Der Übergang beginnt in der Abbildung links mit einer Eigenrealisierung, die eine hohe Eigenverantwortung des VPN betreibenden Unternehmens nach sich zieht, bis hin zu einer nahezu völligen Fremdrealisierung durch einen Provider. Beispielsweise wird in einem eigenrealisierten VPN nur ein Internetzugang mit einer entsprechenden Bandbreite vom Provider zur Verfügung gestellt.

In diesem Zusammenhang muss erwähnt werden, dass mit dem Grad der Fremdrealisierung eine Aussage über das Vetrauensverhältnis zwischen Provider und Unternehmen verknüpft ist. Betreibt ein Unternehmen ein VPN mit hoher Fremdrealiserung, vertraut es dem Provider implizit, die geforderten Security Anforderungen zu erfüllen.

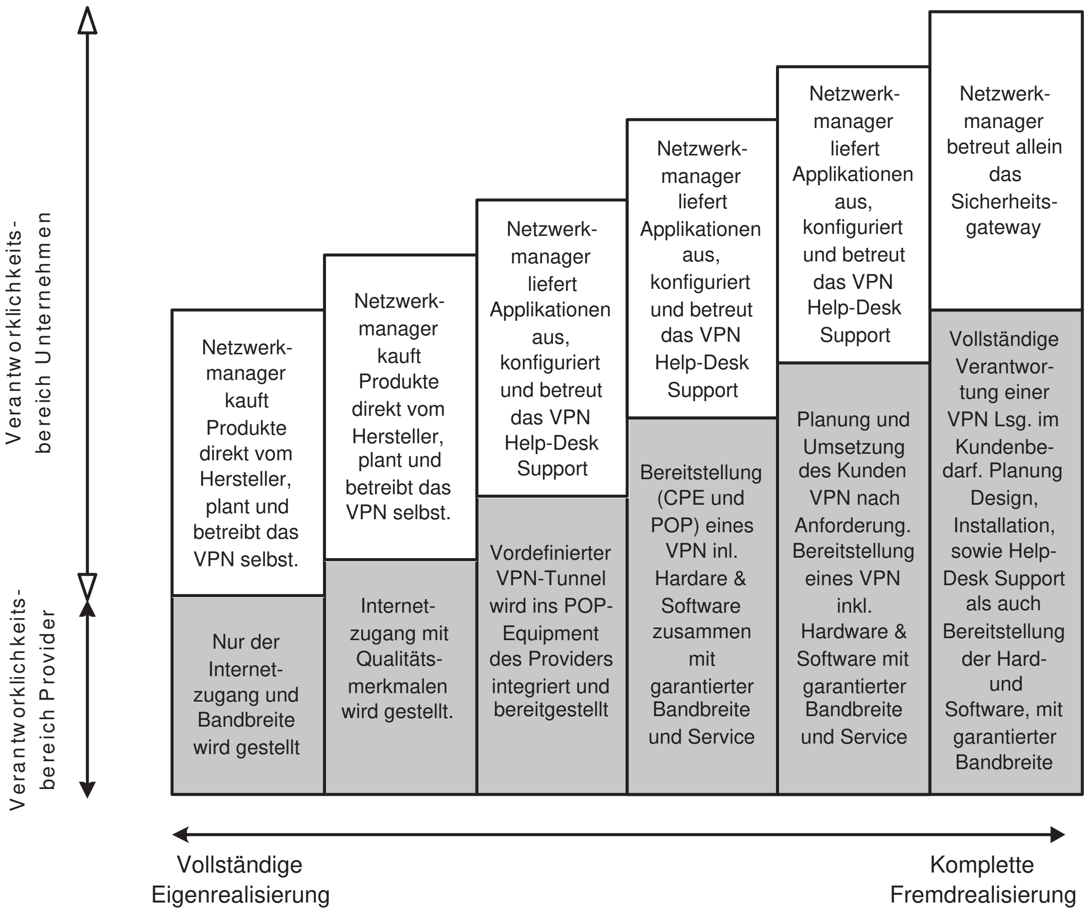

Abbildung 2.2: Organistorische Verteilung in Planung und Betrieb eines VPNs

2.4 Das ppvpn Referenzmodell

In der *provider-provisioned Virtual Private Network Working Group* des IETF wurde ein Referenzmodell für VPNs ausgearbeitet [GLH+00]. Anhand dieses Modells wird die Verzahnung von organisatorischen und technischen Varianten deutlich. Entscheidend für den Typ des VPNs ist dabei, ob Provider oder Unternehmen den Router auf Kundenseite administrieren.

In Abbildung 2.4 wird das Referenzmodell dargestellt. Dabei werden folgende Abkürzungen verwendet:

- **CE (Customer Edge)**
  Mit CE werden die Netzkomponenten bezeichnet, die vom Unternehmen eingesetzt werden, um Verbindung zum Provider Netz aufzunehmen. Es kann sich dabei um einen Router oder Switch handlen, je nach Typ des Access Networks.

- **PE (Provider Edge)**
  Dabei handelt es sich um Netzkomponenten, die vom Provider verwendet werden, um mit CEs zu kommunizieren. Wiederum kann es sich dabei um einen Switch oder Router handeln, je nach Typ des Provider Networks.

- **P (Provider)**
  P haben keinen direkte Verbindung mit CE Netzkomponenten. Vielmerh handelt es sich um Switches oder Router die im *core* Bereich eines Providers eingesetzt werden, und PEs miteinander verbinden.

Anhand der Funktionalitäten die diese Geräte übernehmen sowie der Art der Verbindung zwischen CE und PE lassen sich vier Ausprägungen identifizieren. Die Unterscheidung basiert im Wesentlichen darauf, wo die VPN Verbindungen terminieren, bzw. zwischen welchen Geräten sie aufgebaut sind.

CE-based VPNs Die wichtigste Eigenschaft dieses Typs besteht darin, dass der Service Provider kein Wissen über das Unternehmensnetz besitzt, dies also nur der CE kennt. Management Systeme werden in dieser Betrachtung außer Acht gelassen. Üblicherweise wird das VPN durch Tunnel zwischen CEs aufgebaut, mit den in Abschnitt 4.2 vorgestellten Technologien GRE, IPSec oder L2TP. Aus Routing Sichtweise des Unternhemensnetzes stellen sich die Tunnel wie Punkt zu Punkt Verbindungen dar.

- **Provider provisioned CE-based VPN**
  Oftmals zeigt sich der Provider für das Management und den Betrieb der CEs verantwortlich. In diesem Fall handelt es sich um provider provisioned CE-based VPN, bei dem der Provider die Tunnel und das Routing zwischen den CEs verwaltet. Als Konsequenz ist das Routing im privaten Netzwerk des Unternehmens sowohl unter der Kontrolle des Providers als auch des Unternehmens.

- **Customer provisioned CE-based VPN**
  Im Gegensatz zum provider provisioned CE-based VPN übernimmt das Unternehmen das Management der CEs und damit auch der Tunnel. Weiterhin konfiguriert das Unternehmen das Routing zwischen den CEs.

PE-based VPNs Bei PE basierenden VPNs wird das VPN von den Provider Edge Routern zur Verfügung gestellt. Als Resultat wird die Existenz des VPNs vor den CEs verborgen, die sich wie gewöhnliche Router im Unternehmensnetz verhalten. Das Unternehmensnetz wird hierbei durch Tunnel zwischen PEs verbunden. Durch Encapsulation werden die Tunnel technisch realisiert (GRE, IPSec oder IP in IP Tunnel, siehe Abschnitt 4.2). Bei PE basierenden VPNs erfolgt eine

Unterscheidung dahingehend, ob der Dienst auf OSI Schicht 2 oder 3 erbracht wird.

- **Layer 3 PE-based VPN**
  Hierbei muss dem Provider der IP Namensraum des Unternehmens bekannt sein, gewöhnlich sind dafür die PEs zuständig. Der Provider unterstützt IP Forwarding auf Basis des IP Namensraumes des Unternehmens. Daraus ergibt sich, dass der Provider für das Provisioning und Management des VPNs verantwortlich ist.

- **Layer 2 PE-based VPN**
  Der Provider realisiert das VPN auf Basis von Schicht 2 Forwarding und Signalisierung. Er stellt also Schicht 2 Verbindungen zwischen den CEs zur Verfügung.

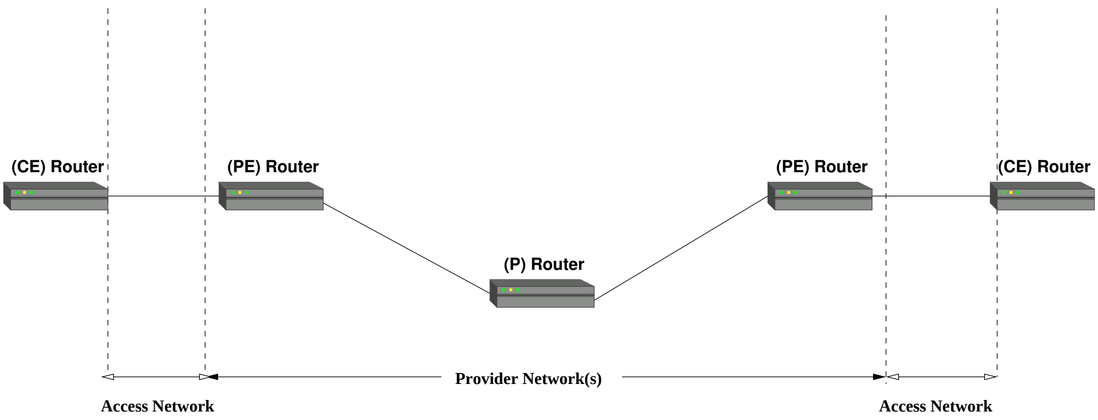

Abbildung 2.3: Das ppvpn Referenzmodell

2.5 Zusammenfassung der VPN Typen

Wie in diesem Kapitel verdeutlicht wurde, existieren eine Reihe von VPN Typen im Bezug auf die Bereiche Einsatzfeld, technisches Verfahren und organisatorischer Verteilung. Ein VPN Lösung stellt eine Kombination von Typen in den unterschiedlichen Bereichen dar. Wie aus dem BMW Extranet ersichtlich wird, können dabei auch mehrere Typen aus einem Bereich, wie etwa gleichzeitig Remote-Acess und Site-to-Site, auftreten.

Ähnlich vielseitig wie die Typen einer VPN Lösung sind auch die an sie gestellten Anforderungen. Im nächsten Kapitel wird auf generelle Anforderungen aus mehreren Gesichtspunkten eingegangen.

Kapitel 3

Analyse zur Gewinnung von generischen Anforderungen an VPNs

In diesem Kapitel werden generische Anforderungen an VPNs in Form einer Kriteriensammlung erarbeitet. Damit wird das Ziel verfolgt, eine Anforderungsbasis zu ermitteln, anhand derer spezifische Anforderungen abgeleitet werden können. In Bezug auf den Phasenplan (Abschnitt 1.1) ausgedrückt, wird somit die Anforderungsbestimmung aus der Analyse-Phase unterstützt.

Im Zuge der Analyse soll eine möglichst generelle Sichtweise eingenommen werden, um eine Applikabilität für ein breites Feld von VPN Konzepten sicherzustellen. Der hierfür notwendige Abstraktionsgrad wird durch eine Modellierung der betrachtungsrelevanten Teile des Szenarios (BMW Extranet) erreicht. Dabei wurden drei grundlegende Anforderungsdimensionen identifiziert.

Im Abschnitt 1.4 rfolgte die Erläuterung der Grundstruktur der bestehenden Extranet Lösung. Daraus geht hervor, dass Applikationen die zentrale Rolle einnehmen und somit im Mittelpunkt der Betrachtung stehen. Der einfachste Fall der Modellbildung enthält also Anwendungen und die von ihnen verwendeten Kommunikationsdienste.
Aus der Sicht der Anwendungen stellen die Kommunikationsdienste eine End-to-End Verbindung zur Verfügung, über die, für die Anwendungen relevante Daten übertragen werden. Im Zusammenhang mit VPN Lösungen treten Problemstellungen auf, deren Lösung Funktionen erfordert, die über den Umfang reiner Transportdienste hinausgehen. Beispielsweise erlangen securityspezifische Belange Relevanz, falls die zu übertragenden Daten in irgendeiner Form geschützt werden sollen. Entsprechend muss eine umfassende Modellbildung diese zusätzlichen Eigenschaften berücksichtigen, um eine spätere Unterscheidung der Lösun-

gen zuzulassen. Die erste Anforderungsdimension beschäftigt sich also mit den funktionalen Anforderungen aus Sicht der Anwendungen.

Will man VPN Lösungen umfassend betrachten, ist es notwendig, Anforderungen, die zusammen mit einer Fremdrealisierung auftreten, zu berücksichtigen. Darunter fallen vor allem die Aufgabenverteilungen im Rahmen des Betriebs einer VPN Lösung, als auch die Anzahl und Funktionen der involvierten Akteure. Letzteres trägt der geographischen Ausdehnung großer VPN Lösungen Rechnung. In dieser Arbeit untersuchte Lösungen sollen letztendlich eine europaweite Kommunikation über ein VPN ermöglichen.
Ein anwendungslastiges Modell eignet sich nur bedingt dazu, diese Größen auszudrücken. Aus diesem Grund werden in einem zweiten Modell die Akteure und ihre Interaktionen betrachtet. Dabei wird der Standpunkt eines Unternehmens vertreten. Anforderungen, die sich an einen im Zuge der Fremdrealisierung eines VPNs auftretenden Dienstleister richten und die Beschaffenheit der Interaktionen ausdrücken, werden dann ausgehend von diesem Modell aufgezeigt. Damit sind die an einen Dienstleister gestellten Anforderungen Inhalt dieser Dimension.

Innerhalb der letzten Anforderungsdimension erfolgt die Behandlung betriebswirtschaftlicher Aspekte. In gewisser Weise wird somit der Standpunkt der Unternehmensführung eingenommen.

3.1 Funktionale Anforderungen aus Sicht der Anwendungen

Unternehmen verfolgen mit dem Betrieb von VPNs in erster Linie das Ziel, eine gemeinsame Nutzung von Ressourcen in Form von Anwendungen zu unterstützen. Damit wird offensichtlich, dass die an eine VPN Lösung gestellten Anforderungen stark von den Eigenschaften der eingesetzten Applikationen beinflusst werden. Dieser Abschnitt beschäftigt sich mit in diesem Zusammenhang auftretenden Anforderungen.

Die Anforderungen von Anwendungsseite richten sich primär an die im VPN zur Verfügung gestellten Kommunikationsdienste. Besondere Bedeutung kommt dabei der Dienstgüte (QoS) und Security zu. [1] zu.

Das in Abbildung 1 dargestellte Modell verdeutlicht die, diesem Teil der Analyse zugrundeliegende Sichtweise. Aus dem Blickwinkel von im VPN befindlichen Anwendungen (1), stellt sich das zur Datenübertragung genutzte VPN als Kommunikationsdienst (3) mit gewissen Eigenschaften dar. Bestimmte Anwendungen

[1] In dieser Arbeit wird die ursprüngliche Bezeichnung Security weiterverwendet, da der deutsche Begriff Sicherheit eine andere Bedeutung trägt.

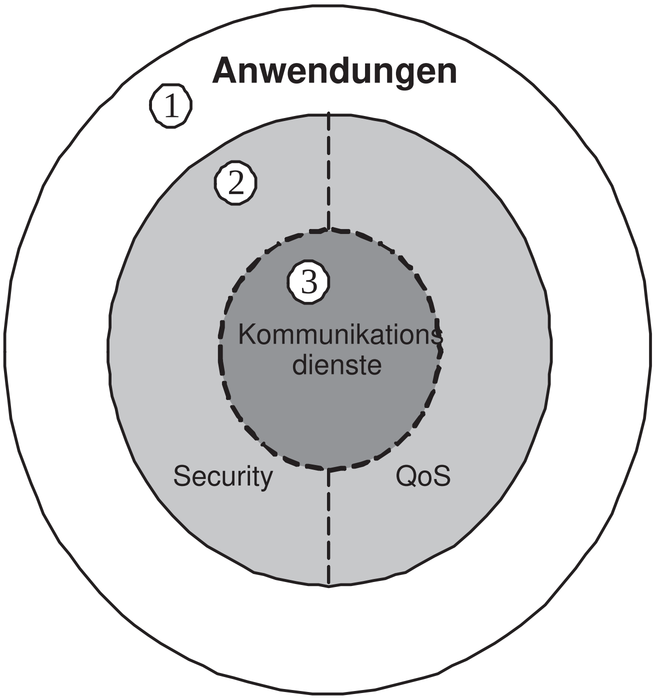

Abbildung 3.1: VPN Modell - Anwendungen

erfordern Funktionen in Form von Zusatzdiensten bzw. über reine Transportdienste hinausgehende Eigenschaften, was in dem mit (2) beschrifteten Ring ausgedrückt wird.

3.1.1 Adressierung

Die Adressierung von Netzknoten in Form von IP-Adressen nimmt neben der Verwendung im Internet auch in vielen LANs die dominante Rolle ein. Obwohl die Vergabe von IP-Adressen innerhalb eines Standortes meist kontrolliert erfolgt, haben es viele Unternehmen versäumt, ein einheitliches, unternehmensweites Adressierungskonzept zu erstellen. Als Folge entstanden - unter Verwendung von privaten IP-Adressbereichen [RMK+96] - Insellösungen, deren IP-Adressbereich sich unternehmensweit gesehen überlappt. Eine Reorganisation ist aber meist mit hohen Kosten verbunden, weswegen als Lösung dieser Problematik vermehrt das Network Adress Translation (NAT) Protokoll zum Einsatz kommt, das eine Umsetzung von privaten auf öffentliche Adressen erlaubt. Die hier besprochenen Kommunikationsdienste sollen beide Alternativen zulassen, also überlappende private Adressbereiche unterstützen und die Verwendung von NAT nicht restriktieren.

3.1.2 Kommunikationsbeziehungen

Kommunikationsdienste sollen in der Lage sein, die vom Unternehmen gewünschten Kommunikationsbeziehungen zwischen VPN Teilnehmern bzw. den korrespondierenden Anwendungen zu realisieren. Die Palette reicht dabei von einer uneingeschränkten, bidirektionalen Kommunikation zwischen allen VPN Teilnehmern (*any-to-any*) zu komplexeren Kommunikationsbeziehungen. Anwendungen, die eine zentrale Vergabe von Daten vorsehen, erfordern 1-n Kommunikationsbeziehungen, was mit dem technischen Begriff *Multicast* umschrieben ist. Außerdem wird häufig in Extranets durch Unternehmens-*Policy* vorgeschrieben, die Kommunikation aller Teilnehmer untereinander einzuschränken, und somit das vorliegende VPN in weitere Benutzergruppen zu partitionieren.

Damit stellen komplexe Kommunikationsanforderungen, wie sie an vorausgegangenen Beispielen verdeutlicht wurden, zusätzlich Herausforderungen an die Skalierbarkeit der Kommunikationsbeziehungen. Skalierbarkeit drückt in diesem Zusammenhang die Möglichkeit aus, viele VPN Partitionierungen zu bilden und ist dementsprechend quantifizierbar durch die Anzahl derselben. Weiterhin lässt die Anzahl der möglichen Teilnehmer oder Sites in einem VPN Rückschlüsse auf die Skalierbarkeit der Kommunikationsbeziehungen zu. Technischer ausgedrückt, entspricht dies etwa der Anzahl von Tunnel oder Routen, die in einem VPN möglich sind (siehe 4.2).

Im *Lifecycle* eines VPNs werden Änderungen der Kommunikationsbeziehungen, beispielsweise aufgrund des Wegfalls oder Hinzufügens einer Site, immer wieder erforderlich. Eine wichtige Anforderung richtet sich in diesem Zusammenhang an die Flexibilität oder Einfachheit, mit der Unternehmen entsprechende Änderungen durchführen können. Ein automatisches Erkennen von Teilnehmern (*auto discovery*) hilft dabei, den Aufwand zu reduzieren. Weiterhin liegt das Augenmerk auf den mit Änderungen verbundenen Auswirkungen auf die Komplexität bzw. Anzahl der konfigurierten Verbindungen. Im Besonderen ist hierbei das Hinzufügen von neuen Sites und das damit verbundene Wachstum der Komplexität (linear oder quadratisch) zu nennen. Entscheidenden Einfluss auf die Komplexität übt dabei die verwendete Topologie aus, deren zwei Ausprägungen in Abbildung 3.1.2 dargestellt sind. Während in einer vollvermaschten Topologie Teilnehmer direkt miteinander kommunizieren können, erfolgt die Kommunikation in einer Hub-and-spoke Topologie indirekt über einen dedizierten Knoten, der als Hub bezeichnet wird. Direkte Verbindungen bestehen in letzterer Topologie nur zwischen Teilnehmern (spokes) und dem Hub. Es gilt n-1 Verbindungen zu konfigurieren, wobei n der Teilnehmeranzahl entspricht (lineares Wachstum). Im Gegensatz dazu erfordert die Vollvermaschung eine Konfiguration von $\frac{n(n-1)}{2}$ Verbindungen (exponentielles Wachstum). Es ist zu beachten, dass Topologien keine Festlegung hinsichtlich der Kommunikationsbeziehungen beinhalten. Beispielsweise ist bei einer Hub-and-spoke Topologie eine *any-to-any* Kommunikation ohne Einschrän-

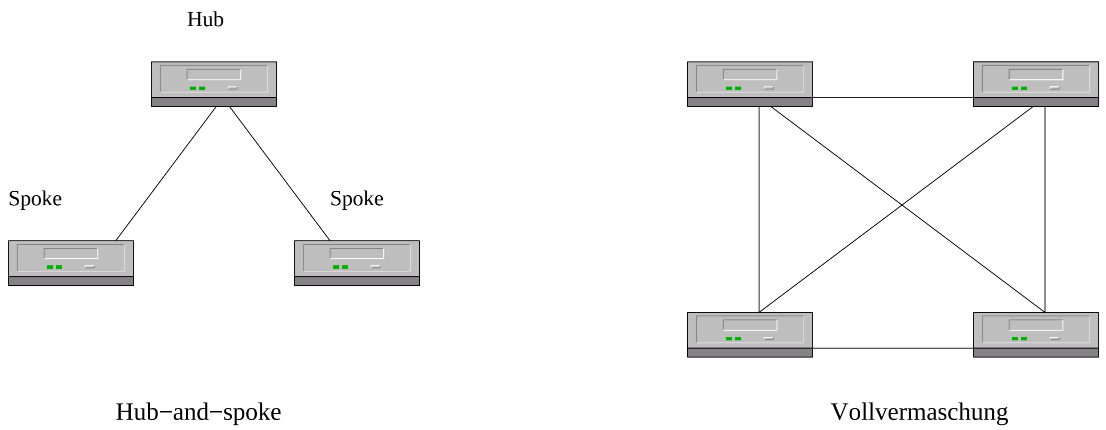

Abbildung 3.2: Die Topologien Hub-and-Spoke und Vollvermaschung

kungen möglich. In jedem Fall liegt es an den Kommunikationsdiensten, genannte Ausprägungen sowohl in Rein- als auch als Mischform (partielle Vermaschung), zu unterstützen.

3.1.3 Transparenz für Applikationen

Im Zuge des Auswahlprozesses ist es für Unternehmen vor allem von Bedeutung, welche Auswirkungen potenzielle Lösungen auf die eingesetzten Anwendungen haben. Anders ausgedrückt stellt sich die Frage, ob Anwendungen für den Einsatz im VPN modifiziert werden müssen. Notwendig werden kann dies beispielsweise durch den Einsatz von VPN Technolgien, die nur IP als Vermittlungsschicht-Protokoll akzeptieren.

Anpassungen von Anwendungen sind mit Kosten verbunden und damit für Unternehmen in den seltensten Fällen erstrebenswert. Als Anforderung formuliert, sollen sich die darunterliegenden Kommunikationsdienste für Anwendungen transparent darstellen. Das beinhaltet eine freie Auswahl von Vermittlungsschicht- Protokollen, um Kompatibilität zu sogenannten *legacy* Anwendungen zu gewährleisten. Gleichermaßen impliziert eine Transparenz für Anwendungen, dass erforderliche Security Maßnahmen in hohem Maße durch die Transportdienste oder konkreter ausgedrückt der VPN Technologie abgedeckt werden. Der Umkehrschluss würde wiederum eine Anpassung der Anwendungen nach sich ziehen und zusätzlich erhöhte Rechenkapazitäten - hervorgerufen durch Verschlüsselungsverfahren - erfordern. Mit in diesem Zusammenhang auftretenden Security-Anforderungen beschäftigt sich Abschnitt 3.1.5.1.

3.1.4 Anpassungsfähigkeit

Die Forderung nach Anpassungsfähigkeit zieht sich durch viele Bereiche dieser Analyse. An dieser Stelle stehen Anforderungen in Bezug auf die Skalierbarkeit der Anpassungsfähigkeit der Kommunikationsdienste im Mittelpunkt. In diesem Sinne bezeichnet Anpassungsfähigkeit die Flexibilität für Unternehmen in der Auswahl der eingesetzten Bandbreiten (siehe auch Abschnitt 3.1.6) und Zugangstechniken.

In Abschnitt 2.1wurden die verschiedenen Einsatzgebiete von VPNs vorgestellt. Mögliche Zugangstechniken in den Einsatzfeldern fanden dabei Erwähnung. Dadurch wurde verdeutlicht, dass vor allem im Bereich Remote Access VPNs eine Vielzahl von potenziellen Zugangstechniken zur Auswahl stehen. Die Anforderung an die Anpassungsfähigkeit der Kommunikationsdienste besteht nun darin, eine breite Masse dieser Zugangstechniken in allen Einsatzbereichen zu unterstützen. Gleichermaßen sollen neuere Technolgien, wie xDSL bei Remote Access VPNs, möglichst schnell für das Unternehmen nutzbar werden.

Wie sich in den letzten Jahren beobachten ließ, nimmt der durchschnittliche Bandbreitenbedarf von Anwendungen ständig zu. Sollen Kommunikationsdienste anpassbar sein, müssen sie diesen Bandbreitenbedarf abdecken können und bedarfsgerechte, feine Abstufungen von Bandbreitengrößen anbieten.

Aber der Bandbreitenbedarf von Applikationen und Zugangstechniken ist nicht als statisch anzusehen. Im Lebenszyklus eines VPNs verändern sich beide Anforderungen, und eine Anpassung wird nötig. Anpassungsfähigkeit heißt in diesem Fall, dass Änderungen schnell und unkompliziert durchgeführt werden können. Darin eingeschlossen sind kurzfristige Bandbreitenreservierungen für spezielle Applikationen.

3.1.5 Security Dienste

Dieser Begriff umfasst im Zusammenhang mit VPNs eine weitreichende Problematik. Ein umfassendes Sicherheitskonzept darf sich nicht auf Teilbereiche beschränken, wie sie durch die Modellbildung implizit gegeben sind. Es würde aber den Rahmen dieser Arbeit sprengen, Security relevante Aspekte in vollem Umfang zu behandeln.

Von der Betrachtung ausgeschlossen sind ebenfalls Problematiken im Bereich der Sicherung und Administration von Endsystemen. Am Beispiel des BMW Extranets bedeutet dies: Fragen, bezüglich der Absicherung der Händler LANs oder der *BMW Service Area* kommen nicht zum Tragen. Die damit verbundene Firewall Problematik wird lokal gelöst und ist nicht Bestandteil der VPN Lösungen, die in dieser Arbeit untersucht werden.

Die in diesem Zusammenhang an eine VPN Lösung gestellten Anforderungen lassen sich aufgrund von drei Dimensionen ableiten, wie im Folgenden ausgeführt wird.

Mehrdimensionale Betrachtung des Begriffs Security Eine differenzierte Betrachtung von VPN Lösungen hinsichtlich der verwendeten Security Konzepte setzt eine Gegenüberstellung in diesem Sachverhalt relevanter Merkmale voraus. Zum Auffinden und sinnvollen Gruppieren der Merkmale bietet sich eine Unterteilung in Dimensionen an, wie sie unter anderem in [Rei97] zu finden ist. In dieser Weise und unter Berücksichtigung des zugrundeliegenden Modells (siehe 1) lassen sich drei Dimensionen unterscheiden:

- Verfolgte Ziele der Security Dienste
- Bedrohungen für die Security Dienste

Die Ziele und Bedrohungen beschreiben, welcher Schutzbedarf den Applikationen zugrunde liegt bzw. vor welchen Angriffen sie überhaupt geschützt werden müssen.

3.1.5.1 Verfolgte Ziele der Security Dienste

Um ein Verständnis der Security-Problematik im Kontext von VPN Lösungen zu erlangen, wird zunächst eine allgemeine Definition der in diesem Zusammenhang relevanten Begriffe dargestellt. Letztere repräsentieren zugleich die Anforderungen, die an die Entität Applikationen – und die zwischen ihnen unter Benutzung der Transportdienste übertragenen Daten – gestellt werden.

Weiterhin sollen aus dem Bereich BMW Extranet gewählte Beispiele den Bezug zwischen allgemeinen Anforderungen und einer konkreten Problemstellung, wie sie im Bereich einer VPN Lösung existiert, herstellen. Eine Definition der Anforderungen, in Anlehnung an [ISO89], wird im Folgenden gegeben:

Vertraulichkeit bezeichnet den Zustand, in dem Informationen nur dem vorgesehenen Kreis von Berechtigten zugänglich bzw. bekannt sind.
Bsp: Sicherheitskritische Daten, z.B. Kundendaten bei der Bestellung eines Fahrzeugs können nur von dem jeweiligen Händler und berechtigten Personen der BMW AG eingesehen werden.

Integrität bezeichnet den Zustand der Korrektheit und Unverfälschtheit von Daten. In diesem Zustand sind nur erlaubte und beabsichtigte Veränderungen zugelassen und möglich.
Bsp: Die Anzahl von Ersatzteilen, die ein Händler nachbestellt, kann während der Datenübertragung nicht verändert werden.

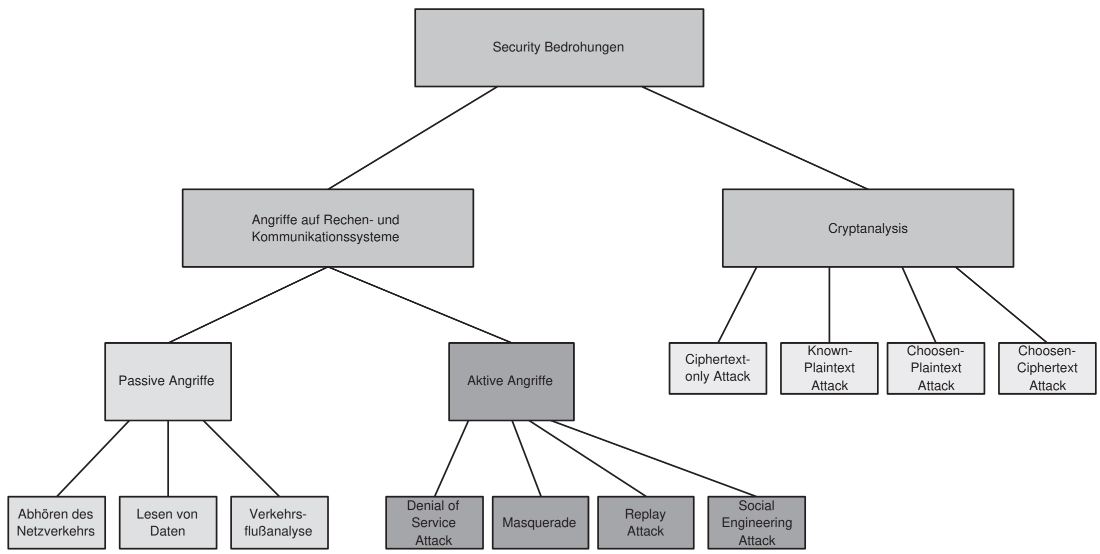

Abbildung 3.3: Die Security Bedrohungen in der Übersicht

Authentizität bezeichnet den Zustand, in dem die Identität eines Kommunikationspartners bzw. die Urheberschaft an einem Objekt sichergestellt ist.
Bsp: Die BMW AG kann sicherstellen, dass es sich bei dem Kommunikationspartner, z.B. in einer Online-Bestellung um den angegeben Händler handelt.

Zugriffskontrolle bezeichnet den Zustand, in dem die Benutzung einer Ressource nur berechtigten Benutzern vorbehalten ist. Weiterhin werden die Zugriffsrechte für einen Benutzer durch Berechtigungen gesteuert.
Bsp: Die BMW AG schränkt die Kommunikation zwischen Händlern ein, so dass nur eine bestimmte Gruppe von Händlern miteinander kommunizieren kann.

Oft wird im Zusammenhang mit sicherer Kommunikation auch der Begriff *Verbindlichkeit* genannt. Damit werden Funktionalitäten bezeichnet, die denen einer Unterschrift auf einem Dokument ähneln. Die damit verbundenen Anforderungen werden im Rahmen dieser Arbeit unter dem Anforderungspunkt *Authentizität* behandelt.

3.1.5.2 Bedrohungen für Security Dienste

Die Analyse potentieller Bedrohungen (Bedrohungsanalyse) stellt ein probates Mittel dar, um den konkreten Schutzbedarf von Applikationen und Kommunikationssystemen zu ermitteln. Im Zusammenhang mit VPN Lösungen entstehen

Bedrohungen vor allem durch Angriffe (Attacks) auf die im Modell vorhandenen Entitäten Applikationen und Transportdienste. Richten sich Angriffe gegen Maßnahmen, die zum Schutz der Entitäten ergriffen wurden (vor allem Verschlüsselungstechniken), spricht man von Cryptanalysis. Abbildung 3.1.5.2 zeigt eine Klassifizierung der Sicherheitsbedrohungen.

Grundsätzlich können Angriffe von Benutzern mit Zugriffsrechten für das System (von "innen") oder von Personen außerhalb des Systems (von "außen"), erfolgen. Erstere stellen dabei eine große Herausforderung an Sicherheitskonzepte dar, da ein Kompromiss zwischen dem Komfort für den Benutzer eines Systems und den eingesetzten Schutzmaßnahmen gefunden werden muss.

Angriffe auf Applikationen Die Bedrohungen für Applikationen werden maßgeblich von deren Struktur bestimmt, eine generelle Sichtweise ist also nur bedingt möglich. Mögliche Kriterien für die Bedrohungsanalyse sind:

- Architektur (z.B. Client/Server)
- Schnittstellen (z.B. Webanwendung)
- Protokolle (z.B. http)

Angriffe auf Kommunikationsdienste In diese Rubrik fallen Angriffe sowohl auf Netzkomponenten als auch auf die Kommunikationsströme zwischen Applikationen. In diesem Zusammenhang lässt sich eine Unterscheidung dahingehend vornehmen, ob es sich um aktive oder passive Angriffe handelt (siehe Tabelle 3.1.5.2).

passive Angriffe	Abhören des Netzverkehrs (Wiretapping)
	Lesen von Daten (z.B. von Backupdaten)
	Verkehrsflussanalyse (Traffic Analysis)
aktive Angriffe	Verfügbarkeit von Diensten wird verschlechtert oder verhindert (Denial-of-Service Attack)
	Vortäuschen einer anderen Identität (Masquerade, Man in the Middle Attack)
	Nochmaliges Senden einer vorher abgehörten Nachricht (Replay Attack)
	Täuschung von berechtigten Nutzern (Social Engineering Attack)

Tabelle 3.1: Angriffe auf Kommunikationsdienste

Cryptanalysis Technische Maßnahmen zur Umsetzung der Security-Anforderungen basieren oftmals auf Verschlüsselungsverfahren und kryptographischen Protokollen. Mit Cryptanalysis bzw. Protocol Attack werden Angriffe auf diese Verfahren und Protokolle bezeichnet. Während Protocol Attacks analog zu den Angriffen auf Kommunikationssysteme eingeteilt werden , muss die Cryptanalysis gesondert betrachtet werden.

Angriffe gegen Verschlüsselungsverfahren zielen darauf ab, den Schlüssel abzuleiten und somit eine unberechtigte Entschlüsselung vorzunehmen. Üblicherweise ist der Verschlüsselungsalgorithmus dem Angreifer bekannt, eine Entschlüsselung ist also prinzipiell möglich. Entscheidendes Kriterium ist der dabei anfallende Rechen- und Zeitaufwand. Beispielsweise können Verfahren, deren Entschlüsselung mehrere Jahre dauert, als relativ sicher angesehen werden. Die verschiedenen Arten der Angriffe werden im Folgenden nach zunehmender Mächtigkeit des Verfahrens angeordnet (siehe auch[Rei97]):

Ciphertext-only Attack: Der Angreifer versucht, ausgehend von chiffrierten Texten den Schlüssel abzuleiten.

Known-Plaintext Attack: Der Angreifer ist zusätzlich zu den chiffrierten Texten im Besitz der dazugehörigen Klartexte, um den Schlüssel abzuleiten.

Chosen-Plaintext Attack: Der Angreifer ist in der Lage beliebige eigene Klartexte selbst mit dem zu findenden Schlüssel zu chiffrieren.

Chosen-Ciphertext Attack: Der Angreifer kann verschiedene verschlüsselte Texte mit dem zu brechenden Schlüssel dechiffrieren lassen.

Das konkrete Vorgehen des Angreifers wird durch die Angriffsart nicht festgelegt. Eine einfache Methode stellt ein Brute Force Attack dar, bei dem systematisch alle möglichen Schlüssel durchprobiert werden.

3.1.6 Quality of Service/Class of Service

In jüngster Zeit lässt sich ein vermehrter Einsatz von *zeitkritischen* Anwendungen in Unternehmensnetzen beobachten. Neben Anwendungen wie VoIP zur Integration von Sprachdiensten in Corporate Networks, entsteht vor allem durch Anwendungen mit besonderer wirtschaftlicher Bedeutung für Unternehmen (*mission critical*) ein gesteigerter Bedarf nach Kommunikationsdiensten mit vordefinierter Dienstgüte. Reine Bandbreitenzuweisungen sind in diesem Zusammenhang nicht ausreichend, um den Bedürfnissen derartiger Anwendungen gerecht zu werden. Vor allem reine IP Netze stellen entsprechende Anforderungen vor eine große Herausforderung - das IP Protokoll kennt keinerlei Priorisierung, die Übertragung findet *best-effort* statt.

In diesem Abschnitt werden typische Anforderungen in diesem Bereich vorgestellt und in Relation zu Dienstgüteparametern gesetzt. Dabei treten eine Reihe von Schwierigkeiten auf: Genaue Aussagen hinsichtlich der benötigten Dienstgüteparameter sind natürlich nur in Verbindung mit einer Anforderungsanalyse entsprechender Anwendungen zu treffen. Weiterhin besteht eine starke Abhängigkeit zwischen den verfügbaren Dienstgüten und der verwendeten Netztechnologie. Erschwerend für eine Auswahl von generellen Dienstgüteparametern wirkt sich auch das Fehlen einer allgemein gültigen Definition aus. Das hat auch zur Folge, dass Quality-of-Service in der Praxis meist durch proprietäre Lösungen realisiert wird.

Zunächst wird der Unterschied zwischen Class of Service und Quality of Service anhand der in [Böh02] vorgestellten Definition aufgezeigt:

Quality of Service (QoS) Hierunter versteht man Dienstgüte, die für eine einzelne Sitzung (Session) eingerichtet ist.

Class of Service (CoS) Hierbei werden gleichartige Datenströme in einer Klasse zusammengefasst, der vom Netz eine oder mehrere Dienstgüten zugeordnet werden. Einzelne Sessions erhalten damit keine individuellen Dienstgüten (QoS).

Eine Dienstklasse setzt sich aus Untergruppen möglicher Dienstgüteparameter zusammen. Dabei stehen die Eigenschaften dieser Klassen in direktem Verhältnis zu den Anwendungen. Das bedeutet, Daten einer bestimmten Anwendung werden mit den Eigenschaften der zugeordneten CoS Klasse transportiert. Dabei kommt dem Signalisierungsverfahren Bedeutung zu. Beispielsweise können Anwendungen durch Setzen von Status Flags in IP Paketen, dem Kommunikationsdienst die geforderte CoS mitteilen.

Um Anforderungen von Anwendungen umfassend zu berücksichtigen, ist eine Abbildung von anwendungsorientierten QoS (z.B. Sprachqualität) auf netzabhängige QoS (z.B. Jitter) notwendig. Das hierbei auftretende Abbildungsproblem, das vor allem auf fehlende allgemeine Definitionen für QoS-Hierarchien zurückzuführen ist, wird in [HA93] beschrieben. Aus diesem Grund orientieren sich Kriterien im Kriterienkatalog an netzabhängigen Dienstgüteparametern, die Abbildung bleibt einer szenario spezifischen Anwendungsanalyse vorbehalten. Im Folgenden werden vier typische netzabhängige Dienstgütemerkmale vorgestellt:

Bandbreite (bandwidth) bezeichnet die Anzahl von Bits, die pro Zeiteinheit übertragen werden, z.B. kbit/s oder Mbit/s.

Verzögerungszeit (delay) beschreibt die Zeit, die von der Datenanforderung bis zum Eintreffen der Daten verstreicht.

Variation der Verzögerungszeit (jitter) legt Schwankungen in der Verzögerungszeit fest. Eine hohe Variation bedeutet, dass die Vezögerungszeit sich laufend ändert und damit nicht vorherbestimmbar ist.

Zuverlässigkeit wird in Bit- und Paketfehlerraten ausgedrückt. Diese berechnen sich aus dem Verhältnis von korrekt übertragenen zu verlorenen oder korrupierten Bits bzw. Paketen.

Verfügbarkeit wird immer relativ zu einem Bezugssystem in Form eines prozentualen Wertes angegeben. Wie etwa eine Verfügbarkeit für ein Provider Backbone von 99,999% pro Jahr.

Neben diesen Dienstgütemerkmalen sind außerdem Aussagen bezüglich des QoS Diensttyps relevant. Damit wird festgelegt, inwieweit eine Einhaltung der Dienstgüteparameter garantiert wird (siehe auch [Ste98]).

Deterministisch Eine Einhaltung der Anforderungen und damit der benötigten QoS Parameter wird garantiert. Für eine QoS-Parameterspezifikation kommen folgende Varianten in Frage:

- Einzelner Wert: $\mathrm{QoS}_{\mathrm{val}}$ (z.B. Mittelwert, Schwellwert)
- Werteintervall: $[\mathrm{QoS}_{\mathrm{min}}, \mathrm{Qos}_{\mathrm{ave}}]$ (z.B. Minimum und Mittelwert)
  Ausgehend davon können Regionen akzeptabler und inakzeptabler Qualität festgelegt werden
- Wertetripel: $(\mathrm{QoS}_{\mathrm{min}}, \mathrm{QoS}_{\mathrm{ave}}, \mathrm{Qos}_{\mathrm{max}})$
- Statistische Angaben: $\mathrm{P}(\mathrm{QoS}(\mathrm{t}) < \mathrm{QoS}_{\mathrm{max}}) = \mathrm{p}$

Statistisch Qualitätsanforderungen werden mit einer gewissen Wahrscheinlichkeit garantiert. Die QoS Parameter basieren auf historischen Werten, Grundlage ist also Analyse des statistischen Systemverhaltens. Beispielsweise wird $\mathrm{QoS} < \mathrm{QoS}_{\mathrm{ave}}$ vorausgesagt, mit $\mathrm{QoS}_{\mathrm{ave}}$ als QoS Mittelwert über einen bestimmten Zeitraum.

Ohne Garantien (Best Effort) es werden keine oder nur partielle Garantien gegeben.

Ferner stellt sich im Zusammenhang mit QoS Parametern und Diensttypen immer die Frage, für welchen Bereich diese gültig sind. Beispielsweise sind im Referenzszenario (siehe Abbildung 2.4) folgende Gültigkeitsbereiche möglich:

- Provider Backbone (PE zu PE)

- Access Network (CE zu PE)

- Ende zu Ende (CE zu CE)

Wie schon erwähnt wurde, sind die angebotenen OoS Parameter und Diensttypen von der verwendeten Netztechnologie oder dem verwendeten Verfahren (z.B. Diffserv oder RSVP in IP-Netzen) abhängig. Dem wird eine Verfeinerung der aufgeführten Kriterien im Zuge der 4.2 gerecht.

3.2 Anforderungen an den Dienstleister in einem fremdrealisierten VPN

In Abschnitt 2.3 wurde auf die verschiedenen Kooperationsgrade zwischen Unternehmen und Provider in Bezug auf Betrieb und Verwaltung eines VPNs eingegangen. Entscheidet sich ein Unternehmen für das Outsourcing in einem der beschriebenen Kooperationsgrade, gilt es einen geeigneten Provider für dieses Vorhaben auszuwählen. Ziel ist es, gemeinsam einen VPN Dienst gemäß den im ersten Teil der Analyse beschriebenen Anforderungen zu erbringen. Dieser Abschnitt stellt die in diesem Zusammenhang auftretenden Anforderungen an Provider und deren Dienstleistung aus Sicht des Unternehmens dar.

Zunächst ist es erforderlich, die im Zuge eines VPN Outsourcings auftretenden Akteure zu identifizeren. Die Betrachtung der Interaktionen zwischen den Akteuren dient dann im weiteren Verlauf als Quelle zur Anforderungsfindung. Eine entsprechende Aufteilung wird in Abbildung 3.2 dargestellt, die gerichteten Pfeile drücken dabei die gemeinsame Motivation aller Akteure aus, den VPN Service zu erbringen. Im Folgenden werden die in der Abbildung gezeigten Akteure näher beschrieben:

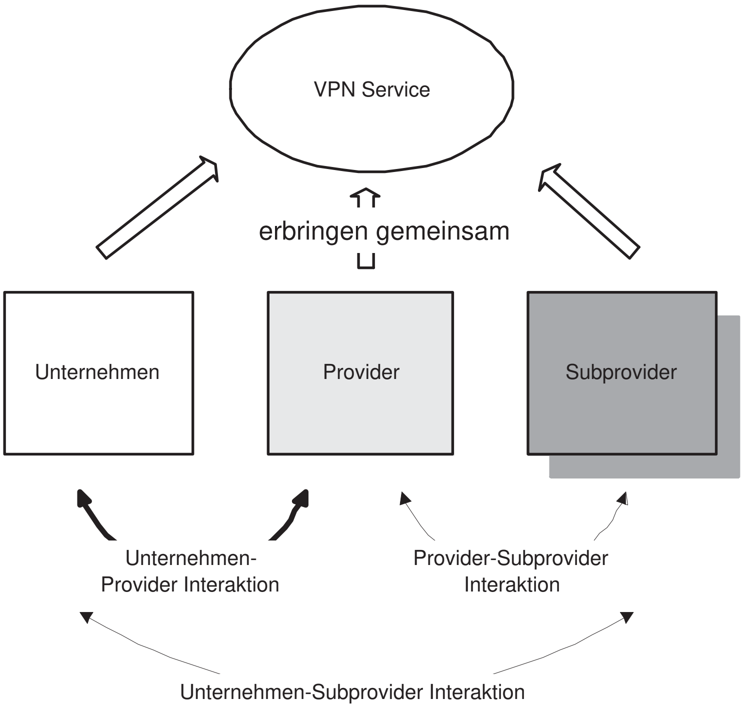

Abbildung 3.4: Die Akteure und Interaktionen im Kontext eines VPN Service

Unternehmen Das Unternehmen ist der Dienstnutzer des VPN Service. Abhängig von dem festgelegten Kooperationsgrad zwischen ihm und dem Provider wirkt das Unternehmen an der Erbringung des VPN Service mit.

Provider Der Provider erbringt die an ihn vergebenen Teile des VPN Service. Er stellt dazu Ressourcen wie Hardwareequipment, Netzinfrastruktur und Personal zur Verfügung.

Subprovider (Carrier) Provider sind oft nicht in der Lage eine eigene Netzinfrastruktur in allen, von dem Unternehmen gewünschten, Regionen zur Verfügung zu stellen. In diesem Fall wird es notwendig, auf Subprovider in den entsprechenden Regionen zurückzugreifen.

Interaktionen treten in diesem Modell zwischen allen Akteuren auf, sind aber für die vorliegende Analyse unterschiedlich relevant. Vorwegnehmend lässt sich feststellen, dass Unternehmen vor allem an einer unkomplizierten Abwicklung der Dienstleistung interessiert sind. Damit verbunden wird die Bindung an einen, dedizierten Vertragspartner favorisiert. Auf das Modell angewendet, hat dies folgende Auswirkungen: Unternehmen-Subprovider-Interaktionen sind auf ein geringes Maß zu beschränken und damit dem Provider bzw. der Provider-Subprovider-Interaktion überlassen. Diese Anforderung wird im Punkt one-stop-shopping

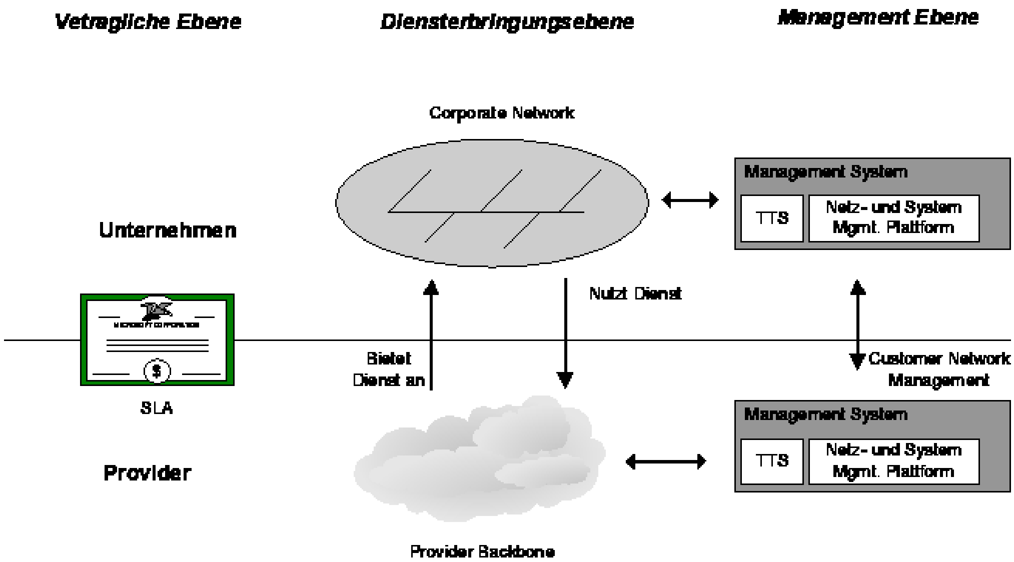

Figure 3.5: Die Interaktionsebenen von Provider und Unternehmen

weiter ausgeführt. Als Konsequenz beschränkt sich die vorliegende Analyse auf Unternehmen-Provider-Interaktionen, was im Modell durch die Hervorhebung des entsprechenden Pfeils verdeutlicht ist.

3.2.1 Anforderungen an die Provider-Unternehmen-Interaktionen

Die Interaktionen zwischen Unternehmen und Provider finden auf mehreren Ebenen statt [LLN]. Im Kontext dieser Analyse sind folgende Ebenen von Interesse , die graphisch in Abbildung 3.2.1 dargestellt sind:

Vetragliche Ebene Das Unternehmen als Dienstnutzer verhandelt mit dem Provider über die Beschaffenheit der von ihm erbrachten Dienstleistung. Die daraus resultierenden gegenseitigen Rechte, Pflichten und Ansprüche werden in einem vertraglichen Rahmen zusammen mit einem sogenannten Service Level Agreement (SLA) festgelegt.

Diensterbringungsebene Das Unternehmen tritt als Betreiber seines Corporate Networks auf und nutzt Kommunikationsdienste, die der Provider mit Hilfe seines Backbones anbietet.

Management Ebene Unternehmen und Provider setzen Management-Systeme für ihr Corporate Network bzw. Backbone ein. Die Integration beider Systeme wird als Anforderung im Abschnitt Customer Network Management behandelt.

Nachfolgend werden die Anforderungen vom Standpunkt des Unternehmens aus in den jeweiligen Ebenen dargestellt und damit auch Anforderungen bestimmt, die eine Auswahl des geeigneten Providers unterstützen. Um den chronologischen Ablauf dieses Auswahlprozesses zu berücksichtigen, werden Anforderungen auf der Diensterbringungsebene vorrangig behandelt. Dem liegt eine Vorgehensweise zugrunde, in der das Unternehmen eine Vorauswahl über in dieser Ebene behandelten Anforderungen trifft.

3.2.1.1 Anforderungen an die Diensterbringungsebene

Wie in 3.2 dargestellt, erbringen Unternehmen und Provider zusammen den VPN Service. Das Kernstück dieses Service, die Kommunikationsdienste, wurden ausführlich inAbschnitt 3.1 behandelt. Die darin vorgestellten Anforderungen gelten natürlich auch im Zusammenspiel mit einem Provider, d.h. sein Backbone muss in diesem Fall Entsprechendes leisten. Zusätzlich fallen in diesem Zusammenhang weitere Anforderungen an den Provider an, die im Folgenden ausgeführt werden.

Ein wichtiges Unterscheidungsmerkmal für Provider stellt die Präsenz dar. Damit wird ausgedrückt, in welchen geographischen Regionen der Provider seinen Dienst anbieten kann. Weiterhin fällt darunter die Anzahl der in einer Region verwendeten POPs. Vor allem für die Unternehmen, die über mehrere Länder oder sogar Kontinente erstreckende VPNs planen, kommt der Präsenz entscheidende Bedeutung zu.

Darüberhinaus sollte ein Provider die Vorgaben des Unternehmens bezüglich der eingesetzten VPN Technologie erfüllen können. Voraussetzung dafür ist ein vielfältiges Angebot unterschiedlicher VPN Lösungen, die zusätzlich auf Wunsch des Unternehmens angepasst werden können.

Zudem besteht für Unternehmen oftmals Interesse daran, zusätzliche Dienste über den Provider zu beziehen. Vor allem Internet-Konnektivität hat sich zu einem unverzichtbaren Bestandteil für Unternehmen entwickelt und tritt deshalb - gewissermaßen als Basisdienst- als eigenständige Anforderung in diesem Bereich auf. Ferner fallen darunter zusätzliche Dienste wie etwa Domain Name Service (DNS) oder zentrale Emailserver, die Teilnehmern des Unternehmens VPN zur Verfügung gestellt werden. Ein Provider soll entprechende Dienstleistungen anbieten und in das Unternehmens-VPN integrieren können. Besondere Internet- Konnektivität stellt eine große Herausforderung an die Integration dar: Es muss sichergestellt werden, dass der Datenverkehr von VPN und Internet strikt getrennt bleiben. Ansonsten besteht Gefahr, dass durch Datenaustausch (*split tunneling*) die Security-Maßnahmen im VPN kompromittiert werden.

3.2.1.2 Anforderungen an die Vertragliche Ebene

Nachdem das Unternehmen einen geeigneten Provider ermittelt hat, werden Eigenschaften der Dienstleistung mit diesem verhandelt und vertraglich fixiert. Dabei sollte der Provider im Rahmen eines Service Level Agreement (SLA) bestimmte Qualitätsparameter der Dienstleistung garantieren. Als Kandidaten für diese Parameter kommen primär alle in Abschnitt 3.1 beschriebenen Anforderungen in Frage sowie mittlere Fehlerbehebungszeit und Dauer der Wartungsfenster. Idealerweise werden alle Anforderungen des Unternehmens in dem SLA zugesichert, was aber in der Praxis eher selten vorkommt. Hier ist es Aufgabe des Unternehmens zu entscheiden, welche Garantien unbedingt erforderlich sind.
Ebenfalls sollten Eskalationsverfahren und damit die Konsequenzen von Nichteinhaltungen des SLA festgelegt werden (*Penalties*). Denkbar sind in diesem Fall eine Minderung des monatlichen Zahlungsaufwandes oder Ersatzzahlungen. In diesem Zusammenhang gilt es zu prüfen, ob die ausgehandelten SLAs technisch überhaupt erfüllbar sind oder ob der Provider bewusst Penalties in Kauf nimmt.

Weiterhin sollte sich für ein Unternehmen der durch das Outsourcing hervorgerufene administrative Aufwand auf ein geringes Maß reduzieren. Diese Anforderung wird mit dem Begriff one-stop-shopping [ML94b] umschrieben, d.h ein Provider deckt sämtliche Belange des Unternehmens ab. Dazu sollte er gegebenfalls Vereinbarungen mit Subprovidern treffen, um von seiner Infrastruktur nicht bewältigbare Anforderungen zu erüllen. Vor allem in geographisch weit verteilten VPNs verfügen Provider selten in allen Regionen über eine eigene Infrastruktur und müssen demzufolge auf lokale Anbieter in diesen Regionen zurückgreifen. Für das Unternehmen sollten sich diese Vorgänge transparent darstellen, der Provider tritt als zentraler Ansprechpartner auf. Dies verpflichtet den Provider gleichermaßen, Störungen und Probleme in Zusammenhang mit dem Subprovider eigenständig zu lösen, um die Dienstleistung für das Unternehmen in vereinbarter Qualität zu erbringen.

3.2.1.3 Anforderungen an die Managementebene

Das Netz- und Systemmanagement stellt einen elementaren Bestandteil im Betrieb einer Netzinfrastruktur dar und wird in dieser Weise von Unternehmen in Corporate Networks eingesetzt. Gleichermaßen liegt es im Aufgabenbereich eines Providers sein eigenes Netz zu managen. Entschließt sich ein Unternehmen, Teile des VPNs an einen Provider outzusourcen, resultierten daraus zwei verschiedene Management Domänen: Das Unternehmen managt den in seinem Corporate

Network befindlichen Teil des VPNs und der Provider den in seinem Netz liegenden (vergleiche Abbildung 3.2.1). Ein großer Nachteil für das Unternehmen besteht darin, dass keine Mangementinformationen zwischen ihm und dem Provider ausgetauscht werden. Damit ist das Unternehmen nicht in der Lage, die ausgehandelten QoS-Parameter zu überwachen oder zu kontrollieren. Genausowenig lässt dieser Umstand Freiraum für ein integriertes Fehlermanagement oder ein automatisiertes Konfigurationsmanagement. Aus diesen Gründen besteht für das Unternehmen die Anforderung nach einem Customer Network Management, das im Folgenden beschrieben wird:

Customer Network Management Service

Mit Customer Network Management Service werden Maßnahmen bezeichnet, die es dem Unternehmen ermöglichen, das VPN als Teil ihrer eigenen Netzinfrastruktur zu sehen [HA93]. Damit stellt Customer Service Management in gewisser Weise die Brücke zwischen dem Netzmanagement des Unternehmens und des Providers her [LLN]. Natürlich beschränkt sich dabei die Weitergabe der Informationen auf das betreffende VPN des Unternehmens. Im Folgenden werden relevante Funktionsbereiche des Customer Service Managements und die damit verbundenen Anforderungen im Zusammenhang mit VPNs vorgestellt, die aus einer Kombination von [HA93] und[LLN] hervorgehen:

Konfigurationsmanagement Darin enthalten sind Möglichkeiten auf die Konfiguration des vom Provider gebotenen Transportdienstes zuzugreifen und die Konfiguration (insbesondere der verbundenen QoS Parameter) zu ändern. Weiterhin soll es dem Unternehmen die Möglichkeit bieten, vom Provider angebotene Zusatzdienste zu abonnieren bzw. das Abonnement aufzulösen.

Fehler- und Leistungsmanagement Unternehmen sollen in die Lage versetzt werden, QoS-Parameter und Verstöße gegen die ausgehandelten SLAs zu überwachen (SLA Monitoring) und zu kontrollieren. Insbesondere sollen Unternehmen bei auftretenden Störungen automatisch benachrichtigt werden, aber gleichzeitig die Möglichkeit erhalten, ihrerseits festgestellte Störungen an den Provider zu melden.
Weiterhin soll der Provider Messdaten, die z.B in Form von History Logs vorliegen, auswerten und aufbereiten. Als Resultat stehen dem Unternehmen in einem vordefinierten Intervall (z.B. einmal pro Monat) Leistungsberichte zur Verfügung.

Abrechnungsmanagement, Benutzerverwaltung Die Benutzerverwaltung schließt eine Namens- und Adressverwaltung der im VPN vorhandenen Teilnehmer mit den zugehörigen Verzeichnisdiensten ein. Weiterhin sind Autorisierungsdaten, also Betriebsmittelberechtigungen für Teilnehmer,

Bestandteil der Benutzerverwaltung. Das Unternehmen soll Zugriff auf den für ihn relevanten Teil der Benutzerverwaltung erhalten, insbesondere Änderungen der Benutzer- und Autorisierungsdaten durchführen können.
Im Zuge des Abrechnungsmanagement soll es dem Unternehmen ermöglicht werden, Auskunft über die von ihm genutzten Dienste, z.B. genutzte Ressourcen, in Verbindung mit den dadurch entstandenen Kosten zu erhalten. Zusätzlich sollen dem Kunden Informationen in Bezug auf das gültige Abrechnungssystem sowie die Rechnung in elektronischer Form zur Verfügung stehen.

Customer Network Management bezeichnet in erster Linie die kontrollierte Weitergabe von Informationen von einem Provider an ein Unternehmen bezüglich des entsprechenden VPNs. Für die Beschaffenheit der Informationen gilt: Sie sollen aussagekräftig sein und den aktuellen Stand wiedergeben. Dies bedeutet, dass ausgehandelte SLAs und QoS in einer sinnvollen Relation zueinander wiedergegeben werden sollen.

Ferner erlangen erwähnte Informationen Bedeutung, wenn Störungen den Quality of Service beeinträchtigen. In diesem Fall soll das Customer Service Mangement dazu beitragen, die Quelle der Störungen ausfindig zu machen, ohne dabei von Zuständigkeitsbereichen und organisatorischen Grenzen abhängig zu sein. Vor allem wenn mehrere Subprovider in den Betrieb des VPNs involviert sind, ist für Unternehmen entscheidend, Fehler übergreifend ausfindig zu machen.

Weiterhin sollen die Informationen in einer geeigneten Form dargestellt werden. Dazu trägt eine, den Bedürfnissen des Unternehmens angepasste, Visualisierung der Informationen bei.
Viele der genannten Funktionen zielen darauf ab, Arbeitsabläufe des Unternehmens zu automatisieren. Daher ist es als essentiell anzusehen, dass eine Möglichkeit geschaffen wird, die vom Provider weitergegebenen Informationen in die Management-Plattform des Unternehmens zu integrieren. Zu diesem Zweck soll der Provider entsprechende Schnittstellen zur Verfügung stellen.

3.3 Betriebswirtschaftliche Anforderungen

Entscheidungen hinsichtlich einer approbiaten VPN Lösung können und werden in Unternehmen nicht allein von den in den Abschnitten 3.1 und 3.2 beschriebenen Anforderungen abhängig gemacht. Vielmehr tragen betriebswirtschaftliche Kriterien in hohem Maße zur Entscheidungsfindung bei und repräsentieren damit in gewisser Weise Anforderungen aus Sicht der Unternehmensleitung. Da entsprechende Fragestellungen nicht zentraler Gegenstand dieser Analyse sein sollen, beschränken sich folgende Ausführungen auf einen kleinen Rahmen.

3.3.1 Kosten der VPN Lösung

Einen entscheidenden Punkt aus Sicht der Unternehmensführung stellen die durch das VPN entstehenden Kosten dar. Letztere sind definiert als "Aufwand von Gütern und Dienstleistungen zur Erstellung betrieblicher Leistungen". In diesem Zusammenhang ist folgende Unterscheidung angebracht:

- **Investitionskosten**
  Kosten für die Neuanschaffung von Komponenten für das VPN. Darin enthalten sind auch Kosten für die Installation und Konfiguration der Komponenten sowie die Schulung der Mitarbeiter. Ist ein Provider in den Aufbau des VPN involviert, fließen auch die von ihm dafür berechneten einmaligen Kosten ein.

- **Laufende Kosten**
  Diese bilden die Kosten für den Betrieb und die Wartung des VPN. Im Falle des Outsourcings müssen neben den vom Provider fix veranschlagten auch nutzungsabhängige Kosten mitberücksichtigt werden.

- **Migrationskosten**
  Nicht zu vernachlässigen sind Kosten, die durch eine Migration der bestehenden VPN Lösung anfallen.

3.3.2 Zukunftssicherheit der VPN Lösung

Die Betriebsphase einer VPN Lösung (siehe auch Abschnitt 1.1) erstreckt sich in der Regel über mehrere Jahre. Aus diesem Grund besteht die Anforderung hinsichtlich einer Zukunftssicherheit der eingesetzten Lösung und damit einem Schutz der von dem Unternehmen getätigten Investitionen.

Obwohl sich Voraussagen in diesem Zusammenhang schwer vornehmen lassen, gibt es dennoch gewisse Anhaltspunkte für die Zukunftssicherheit der eingesetzten Technologie: Eine abgeschlossene Standardisierung durch anerkannte Organisationen wie die IETF begünstigen eine herstellerübergreifende Verbreitung der Technologie. Weiterhin deutet ein hoher Reifegrad einer Technologie auf eine weniger starke Veränderung derselben hin, was letztlich eine zukünftige Interoperabilität erleichtert. Auch von Unternehmensberatungen veröffentlichte *strategy* papers zu dieser Thematik können sich als hilfreich erweisen.

Letztendlich wird die Zukunftssicherheit in hohem Maße durch die Genauigkeit der in der Analyse vorgenommen Voraussagen beeinflusst. Wurde die Entwicklung von Anwendungen richtig prognostiziert und in der Auswahl der Lösung berücksichtigt, kann von einer hohen Zukunftssicherheit ausgegangen werden.

3.4 Ergebnis der Analyse

In diesem Kapitel wurden eine Reihe von Anforderungen aus verschiedenen Sichtweisen dargestellt und somit eine generelle Kriteriensammlung erarbeitet. Damit wird Unternehmen eine strukturierte Vorgehensweise in der Analyse-Phase ermöglicht. Wie bereits in Abschnitt 1.1 dargestellt wurde, werden in dieser Arbeit die in der Betriebs-Phase eines VPNs auftretenden Aspekte vernachlässigt. Dementsprechend finden Kriterien, wie die Interoperabilität der eingesetzten Hard- und Softwarekomponenten oder die Integration in bestehende Netzstrukturen keinen Einzug in die Kriteriensammlung.

Die in Abschnitt 3.1 beschriebene Anforderungen aus Sicht der Anwendungen sind vor allem an die Kommunikationsdienste einer VPN Lösung und damit auch an die eingesetzte Technologie gerichtet. Das nächste Kapitel gibt Aufschluß darüber, inwieweit VPN Technologien diesen Anforderungen gerecht werden.

Kapitel 4

Betrachtung von VPN Technologien

In der vorgenommenen Analyse (Kapitel 3) wurden prinzipielle Anforderungen an eine VPN Lösung, ausgehend von verschiedenen Gesichtspunkten, ermittelt. Funktionale Anforderungen, im applikationsspezifischen Modell (Abbildung 1) beschrieben, sind vor allem an die technische Realisierung der VPN Lösung gerichtet. Im Hinblick auf eine Auswahl geeigneter VPN Lösungsklassen ist es von entscheidender Bedeutung, die Merkmale und damit auch Vor- und Nachteile bestehender Technologien zu kennen. Deswegen werden in diesem Kapitel Technologien, die zur Realisierung einer VPN Lösung eingesetzt werden, im Kontext der ermittelten Anforderungen betrachtet.

Das Spektrum möglicher Technologien ist weitreichend, insbesondere wenn proprietäre, also herstellerspezifische Lösungen berücksichtigt werden. Die jeweiligen Beschreibungen in Form von RFCs oder Herstellerangaben folgen zudem keinem einheitlichen Schema in Bezug auf grundlegende technische oder funktionelle Eigenschaften. Daraus erwächst die Notwendigkeit, eine Grundlage in Form von relevanten Merkmalen zu erarbeiten, die eine strukturierte Betrachtung von Technologien unterstützt.

4.1 Relevante Merkmale für den Vergleich von VPN Technologien

Die relevanten Merkmale für einen Vergleich von VPN Technologien sind in hohem Maße abhängig von den in Abschnitt 2.2 erläuterten technischen Verfahren. Dementsprechend werden die jeweiligen Merkmale nach dem verwendeten Verfahren gegliedert.

Im Hinblick auf eine Klassifizierung von VPN Lösungen (Kapitel 5) sind vor allem die mit den Merkmalen verknüpften Eigenschaften von Bedeutung. Aus diesem

Grund werden Vor- und Nachteile bestimmter Merkmale dargestellt, die es in der Klassifizierung zu berücksichtigen gilt.

4.1.1 Merkmale von Tunnel-basierten Technologien

Im Folgenden werden Merkmale vorgestellt, die dazu geeignet sind Tunnel-basierte Technologien gegeneinander abzugrenzen und somit zu vergleichen.

OSI Schicht 2 oder3 Diese Unterscheidung fundiert auf dem Typ der ursprünglichen Pakete, die mit Hilfe der Tunnel-basierten Technologie eingekapselt und transportiert werden. Tragen diese Pakete einen Sicherungsschicht-Header, fällt die Technologie in die Klasse Schicht 2-Tunneling. Analog wird ein Tunneling Protokoll, das Pakete mit einem Schicht 3 Header einkapselt, der Klasse Schicht 3-Tunneling zugeordnet. Gemäß dieser Einordnung handelt es sich bei dem in Abbildung 2.2 gezeigten Beispiel um Schicht 3-Tunneling.
Es ist zu beachten, dass mit dieser Klassifizierung keine Aussage über den Header des entstehenden Paketes getroffen wird. Mit Hilfe von Schicht 2-Tunneling können beispielsweise Pakete mit Sicherungsschicht-Header in Pakete mit Schicht 2- oder Schicht 3-Header eingekapselt werden.
Generell hat Schicht 2-Tunneling den Vorteil, dass eine breitere Anzahl von Vermittlungsschicht-Protokollen unterstützt wird. Dies ist vor allem in Verbindung mit dem Point-to-Point Protokoll (PPP) möglich: In PPP-Rahmen können verschiedene Schicht 3-Protokolle enthalten sein. Mit der Kapselung von Paketen mit PPP-Headern wird diese Eigenschaft ausgenutzt. Allerdings verursacht Schicht 2-Tunneling in der Regel einen größeren Overhead.

Tunneling Modell Diese Unterscheidungsmerkmale stehen in engem Zusammenhang mit den in Abschnitt 2.3 behandelten Organisationsbeziehungen. Ausschlaggebend ist dabei, in welcher Form oder ob überhaupt Service Provider und Unternehmen kooperieren. Technisch ausgedrückt, wird betrachtet, zwischen welchen Geräten der Tunnel verläuft, also wo die Tunnelendpunkte liegen. Die dabei möglichen existierenden Ausprägungen sind in Abbildung 4.1.1 illustriert:

- **Innerhalb Provider**
  Der Tunnel wird allein vom Provider zur Verfügung gestellt und verläuft deswegen auch nur innerhalb der Provider- Netzstruktur. Damit werden auch die technischen Mittel ausschließlich vom Provider erbracht, das Unternehmen muss keine entsprechende Hard- und Software betreiben.

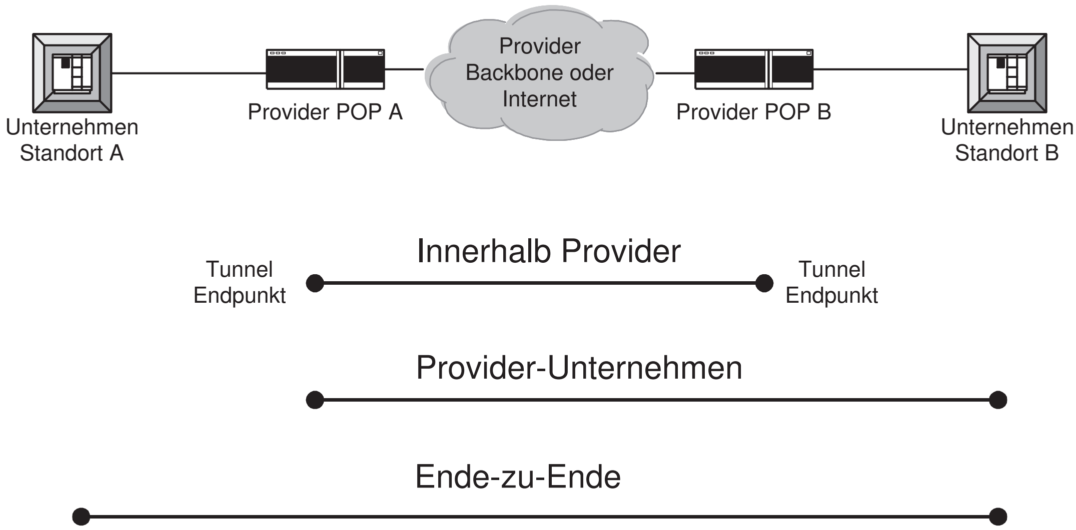

Abbildung 4.1: Die verschiedenen Tunneling Modelle

- **Provider-Unternehmen**
  Unternehmen und Provider kooperieren, d.h. der Tunnel wird vom Provider initiiert und endet auf Unternehmensseite. Das bedeutet auch gemeinsame Pflege der technischen Betriebsmittel und Benutzerdaten. Letztere muss das Unternehmen über vom Provider zur Verfügung gestellte Schnittstellen einpflegen.
- **Ende-zu-Ende**
  Das Unternehmen stellt den Tunnel selbst zur Verfügung, der Tunnel beginnt und endet auf Unternehmensseite. Damit liegt der Betrieb in Unternehmenshand, was sowohl Hard- und Software als auch geschultes Personal angeht.

Vor allem das bestehende Vertrauensverhältnis zwischen Provider und Unternehmen hat entscheidenden Einfluss auf die Wahl des Tunnel-Modells: Vertraut das Unternehmen dem Provider nicht hinsichtlich Security kritischer Fragen, will es sicherlich auf einen Ende-zu-Ende-Tunnel zurückgreifen und somit diesen Bereich in Eigenverantwortung abdecken. In der Praxis stehen aber oftmals nicht alle der genannten Alternativen zur Verfügung, was nicht zuletzt auf die eingesetzte Tunnel-basierte Technolgie zurückzuführen ist. Der Frage, welche Tunnel-Technologien sich für welches Modell eignen, wird in der Beschreibung der Technologien nachgegangen.

Security Dienste In der Top-Down-Analyse wurde in Abschnitt 3.1.5.1 auf Security-Anforderungen von VPN Lösungen eingegangen. Dabei wurden

Kriterien genannt, deren Umsetzung wiederum ein wichtiges Kriterium für die Beurteilung von VPN Technologien darstellt. Im Kontext von Tunnel-basierten VPN Technologien muss erwähnt werden, dass das Tunneling-Verfahren keine Security-Mechanismen enthält, vielmehr liegt es an den Protokollen bzw. Technologien entsprechende Funktionalitäten zu implementieren. Dabei wird für **Authentisierung** beispielsweise auf gängige Protokolle wie PAP, CHAP oder RADIUS zurückgegriffen. Um aber das Kriterium Vertraulichkeit zu erfüllen, müssen **Verschlüsselungsverfahren** in die Tunnel-basierte Technologie integriert werden. Inwieweit diese genannten Punkte in den bestehenden Technologien erfüllt sind, wird in der Vorstellung 4.2 behandelt und konkretisiert.

Voluntary oder compulsory Dieses Merkmal drückt aus, welchen Einfluss der Benutzer auf die Konfiguration der Tunnel-basierten Technologien ausübt. Genauer ausgedrückt, ob der Tunnel für den Benutzer transparent initiiert wird (*compulsory*) oder dieser Vorgang benutzergesteuert (*voluntary*) ist. Dabei diktiert die Implementierungsweise oftmals den Einfluss des Benutzers: Hardwarebasierte Tunneling-Lösungen sind in der Regel compulsory, während softwarebasierte Lösungen Benutzerinteraktionen erfordern. Letztere können beispielsweise in Form eines Softwareclients, den der Benutzer startet (**client initiated**), ablaufen. Benutzerfehler sind allerdings nicht auszuschließen und Softwarelösungen bieten weniger Schutz vor potentiellen Angreifern. Deswegen sind aus Security Sicht Hardwarelösungen zusammen mit compulsory Tunneling vorzuziehen. Weiterhin spricht für compulsory-Tunneling eine höhere Benutzerfreundlichkeit, im Idealfall bleibt die Existenz des Tunnels vor dem Benutzer verborgen. Dem gegenüber steht eine höhere Flexibilität, wie sie durch voluntary-Tunneling geboten wird. Ein Benutzer ist in der Lage, verschiedene Tunnel zu konfigurieren und den Approbiaten bei Bedarf zu initiieren.

4.1.2 Merkmale von netz-basierten Technologien

Ähnlich den Tunnel-basierten Technologien existiert eine Reihe von Merkmalen, die es erlaubt, Netz-basierte Technologien gegeneinander abzugrenzen und zu vergleichen.

Hinsichtlich eines Vergleichs Netz-basierter Technologien ist es vor allem von Interesse, in welcher Weise das Bilden von geschlossenen Benutzergruppen ermöglicht wird, was im weiteren Sinne auch die Ressourcenverteilung zwischen diesen Benutzergruppen einschließt. Entscheidend ist dabei die entstehende Komplexität innnerhalb des Konfigurationsmanagements, da sich Letztere direkt auf die Flexibilität hinsichtlich Konfigurationsänderungen und Anzahl der unterstützten Gruppen (VPNs) auswirkt.

Weiterhin spielen die in Abschnitt 3.1.6 genannten **QoS** Anforderungen eine wichtige Rolle. Entscheidend ist dabei nicht nur, ob eine Technologie QoS unterstützt, sondern in welcher Weise das Unternehmen Einfluss darauf nehmen kann. Beispielsweise kann durch das Markieren von Paketen eine Priosierung des Datenverkehrs vorgenommen werden.

Die grundlegenden Unterschiede zwischen Netz-basierten VPN Technologien werden anhand des zugrundeliegenden Routing-Modells erkennbar. Zur Veranschaulichung trägt das Beispielszenario in Abbildung 4.1.2 bei. Es zeigt vier Standorte eines Unternehmens, die mit einem Provider-Backbone durch sogenannte *edge devices* (siehe auch [FH98]) verbunden sind. Innerhalb des Backbones, dem *core,* operieren *core devices*. In diesem Beispiel wurde bewusst auf eine eindeutige Bestimmung der devices verzichtet, da deren Typ ein charakteristisches Merkmal der im Folgenden vorgestellten Ausprägungen von Netz-basierten Technologien darstellt:

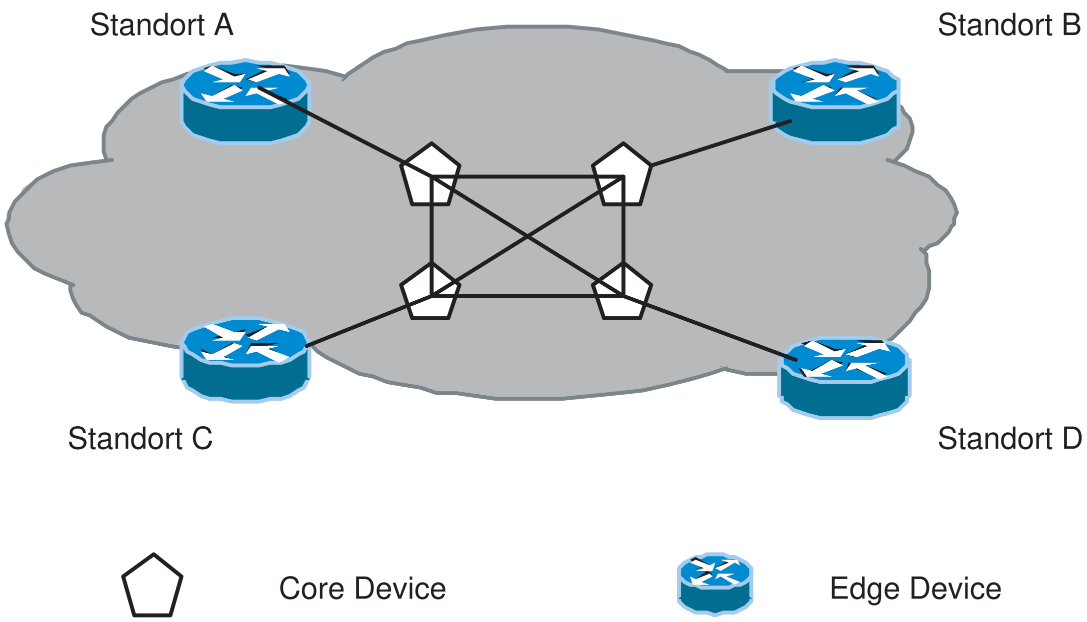

Abbildung 4.2: Beispielszenario für Netz-basierte Technologien

Peer-to-Peer Das Verhältnis der Netzknoten zueinander im Hinblick auf die Wegewahl ist entscheidendes Merkmal für dieser Klasse zugehöriger Technologien. Die Wegewahl (Routing) zählt zu den Hauptaufgaben der Vermittlungsschicht und wird in Netzen durch Router realisiert. Sind die Router dem Pfad, den Daten zu ihrem Bestimmungsort zurücklegen, benachbart (peers), spricht man von einem Peer-to-Peer-Modell. Im Kontext von Wegewahl bedeutet dies, dass die Router Erreichbarkeitsinformationen untereinander austauschen und darauf basierend Weiterleitungsentscheidungen

treffen (hop-by-hop). Die genannten Eigenschaften sind vor allem im Bereich von gerouteten IP-Netzen zu finden, ein Ansatz, der immer höhere Verbreitung in Provider core Netzen findet. Dabei werden ausschließlich IP-Router im Backbone eingesetzt, als Schicht 2-Protokoll dient PPP. Auf Switching-Komponenten wird in diesem Ansatz verzichtet. Der Hauptvorteil liegt in der hohen resilience gegenüber Ausfällen von Komponenten: Gemäß der Designziele des IP-Protokolls und des genannten hop-by-hop-Routings werden Alternativrouten dynamisch gewählt. Daraus resultiert eine hohe Verfügbarkeit des core-Netzes.
Um ein geroutetes Netz im Sinne von geschlossenen Benutzergruppen zu partitionieren, existieren folgende Methoden:

- **Controlled Route Leaking**
  Der Austausch von Wegewahlinformationen zwischen Routern wird beschränkt und gleichzeitig sichergestellt, dass nur VPN Teilnehmer derselben Benutzergruppe untereinander erreichbar sind. Dies kann zum Beispiel durch **Access-Listen** auf den Provider Edge Routern bewerkstelligt werden. Unter der Annahme, dass Standort A und B zu einem VPN gehören, werden am Beispiel des Szenarios in Abbildung 4.1.2 an Standort A nur Wegeinformationen bezüglich Standort B verfügbar gemacht und vice versa. Alle anderen Standorte erhalten ebenfalls keine Routen zu Standort A oder B, verfügen also über keine Kenntnis bezüglich der Existenz dieser Standorte.
- **Virtuelle Router**
  Das virtuelle Router-Konzept sieht die Möglichkeit vor, auf einem physischen Router mehrere logische Router zu emulieren. Um dies zu erreichen, verfügt ein virtueller Router über mehrere unabhängige *Routing* und *Forwarding* Tabellen. Die Anwendung im Bereich von VPNs besteht darin, genannte Tabellen für jede Benutzergruppe separat zu führen. Ein PE, der mit mehreren Standorten verschiedener VPNs verbunden ist, wird so in die Lage versetzt, Weiterleitungsentscheidungen basierend auf der Benutzergruppe zu treffen. Dabei ist zu beachten, dass an dem PE ankommende Pakete in irgendeiner Form "markiert" sein müssen, um eine Zuordnung zu der korrekten VPN Routing-Tabelle zu ermöglichen. In welcher Weise dies realisiert wird, ist Abschnitt 4.2 zu entnehmen.

Im Szenario: Die *edge* und *core devices* sind benachbarte Router, die Wegewahl-Informationen miteinander austauschen. Werden beispielsweise Daten von Standort A nach B übertragen, setzt sich der Weg - aus Sicht der Vermittlungsschicht - aus allen core Routern zusammen, die passiert werden. Benutzergruppen werden auf dem PEs mit Hilfe von *Controlled Route Leaking* oder *Virtuellen Routern* gebildet.

Overlay Im Gegensatz zum Peer-to-Peer-Modell wird der Pfad durch das core Netz und somit die Wegewahl nicht anhand des Vermittlungsschicht-Protokolls bestimmt. Vielmehr stellen in diesem Bereich angesiedelte Technologien eigene Protokolle zur Verfügung, die funktionell Schicht 3-Aufgaben erfüllen [Tan96]. Zu diesem Zweck erlauben sie, verbindungsorientierte Punkt zu Punkt Verbindungen zwischen Netzknoten zu etablieren. Die Möglichkeit, über eine Konkatenation mehrerer Punkt zu Punkt-Verbindungen virtuelle Pfade zu kreieren, macht entsprechende Technologien für den Einsatz in VPNs interessant. Von dem Standpunkt aus, mit Hilfe dieser Technologien Schicht 3-Protokolle wie IP transportieren zu wollen, operieren Overlay-Technologien auf der Sicherungsschicht. Für das Vermittlungsschicht-Protokoll stellt sich dabei der Endpunkt des Pfades als direkt erreichbar dar, die Netzknoten dazwischen sind nicht sichtbar. Diese Eigenschaft, als cut-through bezeichnet, ist die Grundlage des Overlay-Modells.

Als Konsequenz aus dem Overlay-Modell entsteht ein geswitchtes Netz, dessen Netzknoten aus Switches aufgebaut ist. In diesem Zusammenhang muss erwähnt werden, dass im Overlay-Modell Skalierungsprobleme auftreten können, die in einem direkten Zusammenhang mit dem Grad der Vermaschung stehen: Sollen alle Teilnehmer einer Gruppe über Punkt zu Punkt Verbindungen untereinander erreichbar sein (Vollvermaschung), gilt es $\frac{n(n-1)}{2}$ Verbindungen zu konfigurieren, wobei n die Anzahl der Netzknoten repräsentiert. Bei einer hohen Anzahl von Teilnehmern entstehen somit ernstzunehmende Schwierigkeiten für das Konfigurationsmanagement.

Die genannten Eigenschaften dienen zur Beschreibung von Netz-basierten Technologien, die im Overlay-Modell operieren. Zu diesem Modell zählen aber auch in gewisser Weise Tunnel-basierte Technologien, bei denen durch Einkapselung erreicht wird, dass Anfangs- und Endpunkte des Tunnels aus der Sicht des getunnelten Protokolls direkt erreichbar sind.

Im Szenario: Bei den core devices handelt es sich um Switches, während die edge devices Routern entsprechen. Werden IP-Pakete zwischen den edge devices übertragen, sind sie voneinander einen *hop* entfernt. Das dazwischenliegende core Netz fungiert als cut through.

Geswitchtes oder geroutetes Netz Wie bereits im Zusammenhang mit dem Overlay- und Peer-to-Peer-Modell angesprochen, bestimmt das verwendete Modell die verwendete Netzstuktur und umgekehrt. Mit Hilfe von Peer-to-Peer Technologien entsteht aus Unternehmenssicht ein virtuelles geroutetes Weitverkehrsnetz [Cle02], wobei die Routing-Domänen von Provider und Unternehmen verschieden sind. Dagegen weisen die durch den Einsatz von Overlay-Technologien entstehenden Direktverbindungen zwischen Endknoten die Eigenschaften von Standleitungen auf, und werden folglich als Virtual Leased Line (virtuelle Standleitung) bezeichnet[And02].

4.1.3 Merkmale von Technologien zum Aufbau von client-server VPNs

Charakteristisch für alle in diesen Bereich fallenden Technologien ist eine Ausrichtung auf ein bestimmtes Anwendungsgebiet im Sinne von Applikationen. Für einen Vergleich sind damit folgende Fragen relevant: Welche Art von Anwendungen können mit dieser Technologie realisiert werden und welche Modifikationen sind dazu notwendig.

Ein weiteres Merkmal stellen die mit der Technologie zur Verfügung gestellten Security-Dienste dar. Dabei dienen die in Abschnitt 3.1.5.1 vorgestellten Anforderungen bzw. deren Erfüllung als Vergleichsmerkmale.

4.2 Vorstellung der Technologien

Dieser Abschnitt befasst sich mit der Vorstellung von VPN Technologien im Kontext der in den vorausgegangen Abschnitten beschriebenen Unterscheidungsmerkmale. Ziel ist es, zum einen die spezifischen Protokolle zur Implementierung der technischen Verfahren vorzustellen und zum anderen neue Erkenntnisse im Hinblick auf eine Klassifizierung von VPN Lösungen zu erlangen. Dabei wird auf die einzelnen Technologien nur soweit eingegangen, wie es aus der Sicht der relevanten Merkmale notwendig erscheint.

4.2.1 Tunnel-basierte VPN Technolgien

Die Beschreibung aller in diesem Bereich auftretenden Technologien würde den Rahmen dieser Arbeit klar sprengen. Deswegen ist eine sinnvolle Einschränkung angebracht. Dafür sind neben dem Verbreitungsgrad auch Faktoren, wie eine bestehende Standardisierungsarbeit durch die IETF, die einen herstellerübergreifenden Einsatz fördert, ausschlaggebend. Vor diesem Hintergrund wurden GRE, PPTP, L2TP und IPSec ausgewählt. GRE stellt einen standardisierten, generellen Vorschlag für die Umsetzung des Tunneling-Verfahrens dar, der auch als Grundlage für andere Tunneling-Protokolle dient. Für PPTP und L2TP sprechen der große Verbreitungsgrad und im Falle von L2TP eine abgeschlossene Standardisierung. Unter Berücksichtigung des Trends, der sich in Offerten von Providern abzeichnet, nimmt IPSec die Rolle des wichtigsten Vertreters Tunnel-basierter Technolgien ein und wird deshalb am ausführlichsten beschrieben.

4.2.1.1 Generic Routing Encapsulation (GRE)

Das in [FLH+00] standardisierte Protokoll beschreibt ein generelles Verfahren um ein Protokoll in ein anderes einzukapseln. Im Gegensatz zu vorausgegangenen

Arbeiten auf diesem Gebiet, wurde damit ein Verfahren vorgestellt, das nicht an ein spezielles Szenario, wie beispielsweise Tunneling von IPX über IP, gebunden ist. Vielmehr sieht GRE die Möglichkeit vor, beliebige Protokolle - sowohl für das zu Tunnelende als auch das dabei entstehende Paket - zu verwenden.

Gemäß der in RFC2784 verwendeten Terminologie wird das ursprüngliche Paket als *Payload Packet* bezeichnet, das zunächst in ein GRE Paket gekapselt wird. Bei diesem Vorgang wird das Paket mit dem *GRE Header* versehen, der den Typ des Payload Packets im Feld *Payload Protocol* trägt. Abschließend wird das GRE Paket in ein weiteres Paket gekapselt und danach weitergeleitet. Der Header des entstehenden Paketes trägt dabei die Bezeichnung *Delivery Header*. In Abbildung 4.2.1.1 ist das entstehende Paket dargestellt.

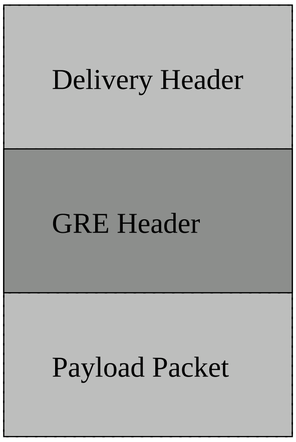

Abbildung 4.3: Aufbau eines mit GRE eingekapselten Pakets

Obwohl die Spezifikation von GRE keine Vorgaben bezüglich des einzukapselnden Protokolls stellt, ist in der Praxis eine vermehrte Anwendung im Bereich von IP zu beobachten (**Schicht 3-Tunneling**). Dies ist vor allem darauf zurückzuführen, dass die meisten Hersteller von Netzkomponenten das GRE Verfahren im Hinblick auf diese Anwendung implementiert und in ihre Komponenten integriert haben.

Vor allem das Fehlen von Security-Funktionen trägt dazu bei, dass GRE keinen hohen Verbreitungsgrad besitzt. Weiterhin werden entsprechende Software Clients in Unternehmen nur in geringem Maße verwendet, das primäre Einsatzfeld liegt in dem Innerhalb-Provider-Modell in compulsory Mode.

4.2.1.2 Point-to-Point-Tunneling-Protocol (PPTP)

Das in [HPV+99] informell beschriebene Protokoll stellt eine Erweiterung des Point-to-Point-Protokolls [SE94] dar und ist als Technologie relativ etabliert. Dies ist vor allem auf die Integration von Clientsoftware in Microsoft-Betriebssystemen zurückzuführen. Damit stellt das Ende-zu-Ende-Modell das primäre Einsatzfeld dar, bei dem einzelne Benutzer die Tunnel *voluntary* initieren. Zur Koppelung von lokalen Netzwerksegmenten erscheint PPTP nicht geeignet.

Technisch gesehen, handelt es sich um ein Schicht 2-Tunneling bei dem ein Point-to-Point-Protokoll-(PPP) Rahmen in einem GRE-Header gekapselt wird. Dadurch entsteht die Möglichkeit eine Reihe von Vermittlungsschicht-Protokollen zu tunneln.

Als Authentifizierungsmechanismen stehen die in [LS92] beschriebenen Protokolle *Password Authentication Protocol (PAP)* und *Challenge Handshake Authentication Protocol (CHAP)* zur Verfügung. Um die Vertraulichkeit der übertragenen Daten zu gewährleisten, hat Microsoft eine mit Point-to-Point Encryption (MPPE) [PZ01] bezeichnete Verschlüsselung entwickelt. Allerdings gilt das darin verwendete RSA RC4[JB02] Verfahren mit 40-Bit Schlüssellänge als unzulänglich, mittlere bis hohe Vertraulichkeitsanforderungen zu erfüllen.

4.2.1.3 Layer 2 Tunneling Protocol (L2TP)

L2TP stellt einen weiteren Vertreter von Schicht 2-Tunneling-Protokollen dar und wurde in [TVR+99] standardisiert. Diese Entwicklung verfolgte das Ziel, die Vorteile von PPTP und dem von Cisco entwickelten Layer 2 Forwarding (L2F)[VLK98] zu vereinen. Die primären Einsatzfelder stellen das Innerhalb-Provider- und Provider-Unternehmen-Modell dar. Entsprechend kann von einem compulsory Tunneling gesprochen werden, wobei der Tunnel für den Benutzer transparent initiiert wird.

L2TP sieht analog zu PPTP eine Einkapselung von PPP-Rahmen vor. Allerdings wird hierbei nicht auf GRE zurückgegriffen, sondern ein spezieller L2TP-Header hinzugefügt. Der Vorteil, verschiedene Vermittlungsschicht-Protokolle tunneln zu können, gilt aber gleichermaßen.

In [TVR+99] werden zwei funktionale Komponenten für den Aufbau eines L2TP-Tunnels beschrieben: Ein *L2TP Access Concentrator (LAC)* ist für den Aufbau des Tunnels zuständig, die Terminierung des Tunnels wird durch den *L2TP Network Server (LNS)* vorgenommen. Zwischen diesen beiden Komponenten können mehrere Tunnel und darin wiederum mehrere logische PPP-Verbindungen aufgebaut werden.
Der Einsatz von Konzentratoren, wie sie LACs und LNSs darstellen, ermöglicht eine höhere Leistungsfähigkeit - im Sinne von möglichen Tunneln - als es z.B. bei PPTP der Fall ist. Darüberhinaus existieren eine Vielzahl von performanten Hardware-Implementierungen der genannten Komponenten, was die Verwendung von L2TP in VPNs mit einer hohen Anzahl von Benutzern begünstigt.

Als Authentifizierungsverfahren stehen die von PPP unterstützten Protokolle PAP und CHAP zur Vefügung. Außerdem kann auf die Dienste eines *Remote Authentication Dial-In User Service (RADIUS)* [RRSW97]zurückgegriffen werden und somit eine flexible, Client-Server-basierte Authentifizierung vorgenommen werden. Allerdings sind in der Spezifikation von L2TP keine Mechanismen zur Sicherstellung der Vertraulichkeit von übertragenen Daten vorgesehen. Vielmehr wird vorgeschlagen, durch eine Kombination mit IPSec (Abschnitt 4.2.1.4), die gewünschte Vertraulichkeit herzustellen [PAD+01].

4.2.1.4 IP Security Protocol (IPSec)

[KA98a][Orm98]Die Entstehung von IPSec geht auf die im Jahre 1995 von der *IETF* ins Leben gerufene *IP Security Working Group* zurück. Dabei wurde das Ziel verfolgt, Erweiterungen für die fehlenden Security-Funktionalitäten des IP-Protokolls zu entwickeln. Obwohl diese Aktivitäten noch andauern, wurden inzwischen eine Reihe von Standards verabschiedet und somit ein herstellerübergreifender Einsatz ermöglicht.

IPSec stellt einen Verteter der Schicht 3-Tunneling-Protokolle dar. Wie aus den bei der Entwicklung verfolgten Zielen deutlich wird, schränkt sich IPSec auf den Einsatz von IP als Vermittlungsprotokoll ein. Das primäre Einsatzfeld stellt das Ende-zu-Ende-Modell dar, wobei die Tunnel zwischen sogenannten *Security Gateways* transparent für den Benutzer initiiert werden (*compulsory*).

Wie aus [KA98a] hervorgeht, stellt IPSec eher eine Architektur dar als ein Protokoll. In diesem Zusammenhang wurden drei Hauptbestandteile festgelegt, die einen modularen Charakter aufweisen bzw. nahezu beliebig zusammen eingesetzt werden können.

Authentication Header (AH) Bei dem AH-Header [KA98b] handelt es sich um einen speziellen Protokollkopf, der für die Authentifizierung und Integritätssicherung von IP-Paketen zuständig ist. Er wird zwischen dem ursprünglichen IP-Header und anderen Vermittlungsschicht-Elementen, wie z.B. TCP, eingebettet. Die Nutzdaten bleiben jedoch unberührt, sie werden in ihrem ursprünglichen Zustand belassen. Um die genannten Security-Anforderungen zu erfüllen, wird eine kryptographische Prüfsumme über den IP-Header und den Headern nach dem AH berechnet. Da der IP-Header in die Berechung einfließt, lassen sich anhand des AH Änderungen in der Adressinformation oder Versuche zur Umgehung des AH erkennen. Für die Berechnung der kryptographischen Prüfsumme sind die Hash-Algorithmen HMAC-MD5-96 [MG98a] und HMAC-SHA-1 [MG98b] zwingend vorgesehen. Abbildung 4.4 stellt ein mit AH-Header versehenes IP-Paket dar.

Abbildung 4.4: IPSec AH-Header

Encapsulating Security Payload (ESP) Der ESP-Header garantiert die Vertraulichkeit der zu übertragenden Daten. Im Gegensatz zum AH-Header ist ein ESP-Header in der Lage, sowohl eine Verschlüsselung als auch eine Authentifizierung zu leisten. Die eigentlichen Nutzdaten werden zwischen dem ESP-Header und ESP-Trailer eingebettet (siehe Abbildung 4.2.1.4). Als Verschlüsselungsverfahren sind zwingend DES-CBC [MD98] und NULL [GK98] vorgesehen.

Abbildung 4.5: IPSec ESP-Header

Schlüsselmanagement IPSec setzt symmetrische kryptographische Schlüssel ein um einen IP-Paket-Transport abzusichern. Allerdings besitzt IPSec keinerlei Mechanismen, um diese notwendigen Schlüssel für die Kommunikationspartner zu erzeugen oder zu verteilen. Eine Möglichkeit besteht in der Verwendung von manuellen Schlüsselaustauschverfahren, was aber aus Security-Gesichtspunkten bedenklich ist: Um ein hohes Sicherheitsniveau zu gewährleisten, ist es nämlich unabdingbar, die für die Datenübertragung eingesetzten Schlüssel in bestimmten Intervallen zu ändern. Automatische Schlüsselaustauschverfahren werden dieser Aufgabe gerecht und greifen dabei meistens auf eine *Certification Authority (CA)* zurück. Authentifizierung wird nun entweder direkt oder indirekt durch die CA vorgenommen. Beim häufiger verwendeten Verfahren der indirekten Authentisierung, signiert die CA die Public Keys der Ipsec Kommunikationspartner. Eine gegenseitige Überprüfung der Partner kann nun durch Verifizierung der CA-Signatur erreicht werden. Die direkte Authentifizierung erfolgt im Gegensatz dazu, indem die Kommunikationspartner die CA befragen, um ihr Gegenüber zu verifizieren. Der Nachteil des letzteren Verfahrens liegt darin, dass die CA einen Single Point of Failure darstellt und somit für Angriffe verwundbar ist. Den im Zusammenhang mit IPSec am häufigsten eingesetzten Vertreter von automatischen Schlüsselaustauschverfahren stellt das *Internet Key Exchange (IKE)* [HC98] dar.

Schutz vor Angriffen In Abschnitt 3.1.5.2 wurden Angriffe auf Transportdienste vorgestellt. IPSec bietet starke Security Maßnahmen, die gegen eine Reihe von Angriffen wirksam sind. Allerdings sind auch ihm Grenzen gesetzt. Daraus wird offensichlich, dass IPSec allein nicht alle Security Anforderungen abdecken kann. Vielmehr wird es notwendig, zusätzliche Mechanismen etwa in Anwendungen zu implementieren. Im Folgenden werden diese Aussagen anhand von Beispielen verdeutlicht, indem häufig verübten Angriffen IPSec Schutzmechanismen gegenübergestellt werden. Zunächst wird auf Angriffe eingegangen, für die IPSec entsprechende Security Mechanismen bereitstellt:

- **Wiretapping**
  Die ESP-Verschlüsselung von IPSec schützt den gesamten Netzverkehr einschließlich wiederverwendbarer, geheimer Passwörter und macht somit z.B. das Abhören von Passwörtern (password sniffing) unmöglich.
- **Denial-of-Service-Attacken**
  IPSec vermag SYN-Flooding-Angriffe abzuwehren, da die SYN-Nachrichten einen gültigen AH mit korrekter kryptographischer Prüfsumme besitzen müssen. Werden korrekte Anfragen mitgeschnitten und dann für einen SYN-Flooding-Angriff verwendet, so kann man dem durch einen Schlüsselaustausch entgegen wirken.
- **Session-Hijacking**
  Verbindungen, die durch Authentication Headers (AHs) geschützt sind, können nicht übernommen werden, da der Angreifer nicht in der Lage, ist gültige AHs zu erzeugen. Für die Generierung gültiger AHs benötigt er den geheimen Schlüssel.

Dem gegenübergestellt, werden folgende Angriffe durch IPSec nicht abgedeckt:

- IPSec bietet keinen Schutz, falls jemand Zugang zum geheimen Schlüssel bekommen hat. Die Sicherheit, die IPSec bietet hängt immer von dem Schlüssel ab. Liegt der Schlüssel z.B. auf einem Rechner der von einem Hacker geknackt worden ist, so kann IPSec keinen Schutz mehr bieten. Nicht außer Acht gelassen werden sollte, dass auch verschlüsselte Netzwerk-Pakete aufgezeichnet werden können. Dies hat zur Folge, daß die Schlüssel bis hin zu ihrer Vernichtung mit besonderer Sorgfalt verwaltet werden sollten. Falls der Schlüssel auch erst Wochen oder Monate später in falsche Hände gelangt, könnten die aufgezeichneten Netzwerk-Pakete entschlüsselt werden. Was Aufzeichnungen betrifft, kann man auch davon ausgehen, dass evtl. die Gefahr besteht, eine heute noch gutverschlüsselte Nachricht in der Zukunft entschlüsseln zu können. Wichtig in diesem Zusammenhang ist die Schlüssellänge, die je nach Risikoeinschätzung ausreichend lang sein sollte.

- IPSec bietet z.T. keinen umfassenden Schutz vor Paketschnüfflern (*Sniffer*). Bei der Nutzung von IPSec zur Sicherung einer Kommunikation sind für Außenstehende mehr Komponenten des Netzverkehrs sichtbar als z.B. bei der verbindungsorientierten Verschlüsselung. Je nachdem, wie IPSec konfiguriert wurde, können Außenstehende feststellen, welche Rechner an Ihren Standorten miteinander kommunizieren. Zumindest kann man den Netzverkehr zwischen den Standorten ablesen. Ungeschützt sind Informationen über Paketgröße, Anzahl der Verbindungen und Daten in Protokollfeldern, die zu Netzwerkverkehrsanalysen ausgewertet werden.

- Cut-and-Paste und Rewrite Angriffe: IPSec kann je nach Konfiguration nicht vor Cut-and-Paste Angriffen schützen. Wird IPSec eingesetzt um ein VPN einzurichten ohne den AH-Header zu verwenden, so kann der Netzverkehr aufgezeichnet werden und an eine dritte Person (Insider) innerhalb des vertrauenswürdigen Standortes gesendet werden. Diese dritte Person kann somit diese Nachrichten in Klartext empfangen, da die Nachricht vorher durch den IPSec-Proxy entschlüsselt wurde. Wird die Zieladresse durch den ESP-Tunnelmodus verborgen, so können immer noch Rewrite-Angriffe gestartet werden. Wenn ein Angreifer ein im ESP-Tunnelmodus verschlüsseltes Paket zwischen Person X und Person Y abfängt, so kann er das abgefangene Paket an ein von Person X an den Insider gesendetes Paket anhängen, um ein neues Paket zu erzeugen. Dieses Verfahren enthüllt dabei einige Daten, selbst wenn es bei DES CBC angewendet wird. Schutz bietet hier jeweils die Verwendung des Authentication Header (AH).

4.2.2 Netz-basierte VPN Technologien

In dem Bereich von Netz-basierten VPN Technologien werden die Technologien *Frame Relay*, *Asynchronous Transfer Mode (ATM)* und *Multi-Protocol Label Switching (MPLS)* vorgestellt. Während ATM und Frame Relay etablierte Technologien darstellen, beschreibt MPLS die jüngste Entwicklung im WAN Bereich und bietet gleichermaßen interessante Eigenschaften für den Einsatz in VPNs.

4.2.2.1 Frame Relay (FR)

Bei Frame-Relay-Netzen handelt es sich um vermaschte Netze, in denen Pakete über sogenannte Frame Handler (FH) vermittelt werden. In den Backbone-Netzen erfolgt der Datentransport über sogenannte FH-Knoten. Als Zugangskomponenten dienen Adapterkomponenten (Frame Relay Access Devices, FRAD), die die LAN oder andere Protokolle auf die Netzzugangsschnittstelle abbilden [HA93]. Frame Relay stellt den Nachfolger von X.25 dar, kommt aber mit erheblich weniger Steuerdaten aus, was sich in einem hohen Netto-Durchsatz niederschlägt.

Frame Relay stellt einen verbindungsorientierten Datenübertragungsdienst zur Verfügung. Es besteht die Möglichkeit, geschaltete (*Switched Virtual Connections, SVCs*) sowie permanente virtuelle Verbindungen (*Permanent Virtual Connections, PVCs*) einzurichten und damit geschlossene Benutzergruppen zu erzeugen. Die einzelnen virtuellen Verbindungen werden dabei mit Hilfe eines *Data Link Connection Identifiers* (*DLCI*) identifiziert. In Bezug auf die in Abschnitt 4.1.2 vorgestellten Merkmale trägt das entstehende VPN damit Overlay Eigenschaften.

Die Übertragungsraten reichen von 64kbps bis 2.048 kbps und werden durch mehrere Parameter bestimmt. Zum einen ist dies die *Committed Information Rate (CIR)*, die die Übertragungsgeschwindigkeit unter normalen Bedingungen garantiert, zum anderen ist es die Datenmenge, die in einem Zeitintervall (TC) mindestens transportiert wird. Diese Größe, die mit *Commited Burst Rate* bezeichnet wird, stellt die vereinbarte Datenmenge dar, die verlustfrei über das Netz transportiert werden muss. Darüberhinaus ist Frame Relay für Stoßverkehr (*Bursty Traffic*) ausgelegt, die *Excess Burst Size* legt dabei fest, welche Datenmenge zusätzlich übertragen werden kann.

Mit Hilfe der beschriebenen Parameter sind gewisse QoS Parameter garantierbar, allerdings können aufgrund der variablen Paketlängen keine verbindlichen Aussagen bezüglich der Übertragungszeit und des Jitters (siehe Abschnitt 3.1.6) getroffen werden.

4.2.2.2 Asynchronous Transfer Mode (ATM)

ATM stellt ein paketorientiertes Verfahren dar, das die Schicht 1 und Teile der Schicht 2 im OSI-Schichtenmodell umfasst. In einem ATM Switch werden Zellen mit einer festen Länge von 53 Byte verbindungsorientiert über den jeweils gleichen Weg zwischen Quelle und Ziel vermittelt (geswitchtes Netz) [HA93]. Dabei werden abhängig vom physikalischen Medium Übertragungsraten von bis zu 622 Mbit/s erreicht.

Eine virtuelle Verbindung ist bei ATM über Pfade und Kanäle definiert. Dabei bildet die kleinste logische Einheit der Virtuelle Kanal (*Virtuell Channel, VC*). Die nächste Abstraktionsstufe stellt der Virtuelle Pfad (*Virtuell Path, VP*) dar, der aus einem Bündel von virtuellen Kanälen bestehen kann. Ausgehend davon, können *Virtual Channel Connections* und *Virtual Path Connections* eingerichtet und somit geschlossene Benutzergruppen gebildet werden. Das entstehende VPN trägt dabei Overlay Eigenschaften.

In einem ATM-Netz besteht die Möglichkeit, beim Verbindungsaufbau QoS-Parameter auszuhandeln, die für die Verbindung garantiert werden. Aufgrund der zellenorientierten Übertragung - und damit fester Paketlänge - sind Garantien hinsichtlich Verzögerung und Jitter möglich. In diesem Zusammenhang wurden verschiedene Dienstklassen definiert:

- **Constant Bit Rate (CBR)**
  Diese Dienstklasse wurde definiert für Anwendungen, die während der gesamten Verbindungsdauer eine gleichbleibende Bandbreite und Geschwindigkeit benötigen, also kritisch gegenüber Verzögerungen sind. Dienste dieser Art sind z.B. Echtzeitanwendungen, Sprach- und Videoübertragungen.
- **Real-Time Variable Bit Rate (rt-VBR)**
  Dienste dieser Klasse erzeugen keinen konstanten Zellstrom, stellen aber trotzdem hohe Anforderungen an die Übertragungsverzögerung von Zellen. Ein Beispiel bildet die komprimierte Videoübertragung.
- **Non-Real-Time Variable Bit Rate (nrt-VBR)**
  Diese Dienstklasse eignet sich für Anwendungen, die Daten nicht in Echtzeit übertragen wollen, bei denen also Verzögerungen nicht so wichtig sind. Diese Anwendungen erzeugen auch keinen konstanten Zellstrom.
- **Unspecified Bit Rate (UBR)**
  Für Dienste dieser Klasse wird keine Bandbreite ausgehandelt, sondern die Bandbreite verwendet, die zum Übertragungszeitpunkt zur Verfügung steht. In dieser Klasse findet auch keine Flusssteuerung statt, so dass sich die höheren Schichten darum kümmern müssen. Typische Anwendungen sind FTP oder email.
- **Available Bit Rate (ABR)**
  Auch in dieser Dienstklasse wird keine Bandbreite ausgehandelt. Allerdings gibt es hier eine Flusssteuerung und eine garantierte geringe Zellverlustwahrscheinlichkeit. Geeignet ist diese Klasse für remote login und Datenaustausch.

4.2.2.3 Multi-Protocol Label Switching (MPLS)

MPLS [RVC01] beschreibt die jüngste Entwicklung im Bereich von WAN Technologien. Im Kern wird eine Verknüpfung des Label-Swapping Paradigmas mit der traditionellen Routing Technologie vorgenommen [Böh02]. Im Gegensatz zu dem zeitaufwendigen Hop-by-Hop-Routing, das in IP-Netzen Anwendung findet, wird ein labelbasierter Weiterleitungsmechanismus verwendet. Router im Backbone-Bereich kontrollieren anhand einer Label-Switching-Tabelle nur noch das Label und nicht mehr das Gesamtpaket. Das MPLS Label wird dazu als *shim header* in das IP-Paket zwischen Schicht 2- und Schicht 3-Header eingefügt. Abbildung 4.6 verdeutlicht den Weiterleitungsmechanismus, der auf folgenden Komponenten basiert:

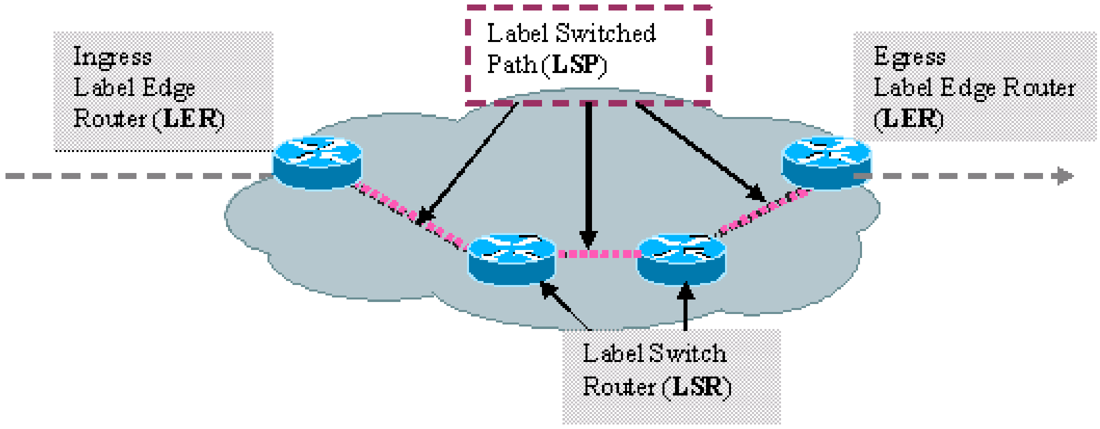

Abbildung 4.6: Weiterleitung in einem MPLS Netz

Label Edge Router versieht entweder einkommende Pakete mit einem Label (Ingress Router) oder entfernt das Label (Egress Router). Das Abbilden von IP-Adressen auf Labels und umgekehrt wird mit Hilfe einer entsprechenden Tabelle vorgenommen. Dabei werden Datenströme mit vergleichbaren Übertragungsanforderungen in sogenannte *Forwarding Equivalence Classes* zusammengefasst und mit einem gemeinsamen Label versehen.

Label Switch Router leitet das Paket entsprechend dem Label bzw. dem damit verknüpften Eintrag in der Label-Switching Tabelle weiter. Dabei tritt eine Ersetzung des Labels (label swapping) auf. Die Verteilung der Label-Switching Tabellen kann dabei durch das *Label Distribution Protocol* (LDP) [ADF+01] vorgenommen werden.

Label Switched Path stellen vorgezeichnete Wege zwischen LERs dar. Die Festlegung der LSPs kann dabei im Gegensatz zu ATM und Frame Relay automatisch erfolgen. Weiterhin können Informationen in das Routing einfließen, die nicht durch den IP Header explizit gegeben sind. Beispielsweise können Pakete, die am LER an einem bestimmten Port eintreffen, einem vordefinierten LSP zugeordnet werden.

Label Switched Paths ermöglichen die Realisierung von geschlossenen Benutzergruppen und somit VPNs. In [RR99] wird ein Verfahren beschrieben, das es erlaubt die Konfiguration von LSPs und damit VPNs automatisch vorzunehmen. In dieser Weise gebildete VPNs, verfügen über Peer-to-Peer-Eigenschaften. Damit wird das in Abschnitt 4.1.2 beschriebene n^2 vermieden.

Streng genommen liefert MPLS allein noch keine QoS-Eigenschaften. Erst in Verbindung mit IP-Switch-Geräten der nächsten Generation und Verfahren wie Constraint-Based LDP[ALAS+02] oder RSVP-TE [ABG+01] lassen sich entsprechende Garantien abgeben.

4.2.3 Alternative Technologien (client-server VPN)

Als Vetreter für Alternative Technologien wird das Secure Socket Layer Protocol (SSL) vorgestellt. Es hat sich im World Wide Web vor allem zur Absicherung der zwischen Browser und Server bestehenden HTTP Verbindung etabliert.

4.2.3.1 Secure Socket Layer (SSL)

SSL ist kein anwendungsspezifisches Protokoll, wie etwa Verschlüsselungsverfahren für Email (z.B. PGP). Es liegt vielmehr unterhalb der Anwendungsschicht und kann eine sichere Datenübertragung für verschiedenste Anwendungen bieten.(siehe Abbildung 4.7)

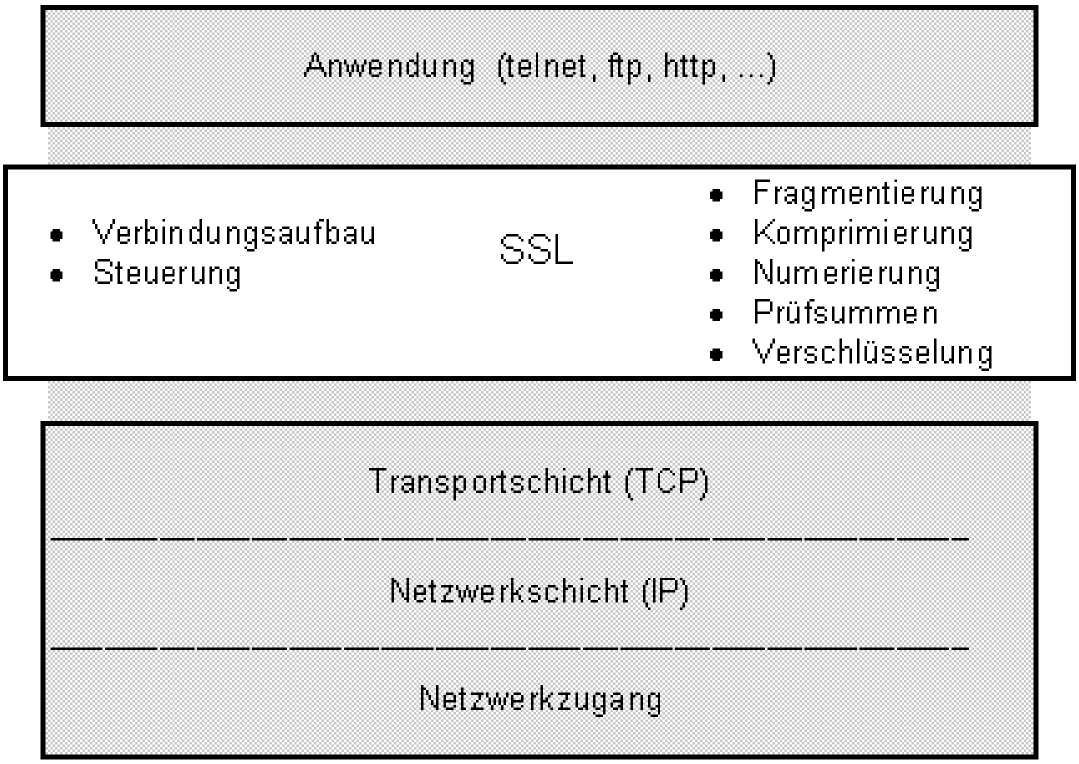

Abbildung 4.7: Das Secure Socket Layer Protocol in der Übersicht

Dabei ist SSL aus Sicht der Transportschicht eine Anwendung und aus Sicht der Anwendung die Transportschicht (Socket). Dadurch ist SSL transparent für und kann mit verschiedenen Anwendungen und Transportprotokollen benutzt werden. Allerdings erfordert SSL eine Modifikation der Anwendungen bzw. des entsprechenden Quellcodes. Es besteht aus 2 Schichten, die in Abbildung 4.8 dargestellt werden.

Abbildung 4.8: Schichten von SSL

Das Steuerprotokoll ist verantwortlich für die Verbindungsaushandlung und ist austauschbar. Zur Zeit gibt es nur einen Vorschlag für ein solches Protokoll - das Handshake Protokoll. Letzeres erfüllt folgende Funktionalitäten:

- Aushandeln der Verbindungsmodalitäten
- Austausch von Zertifikaten und Schlüsseln
- Überprüfung der Verbindung

Die zweite Schicht stellt der Record Layer dar, er liefert für eine SSL Verbindung wichtigen Eigenschaften:

Vertraulichkeit Durch das Handshake Protokoll wird ein gemeinsamer Sitzungsschlüssel ausgehandelt. Er wird vom Record Layer zur Verschlüsselung der Nutzlast eingesetzt.

Integrität Es erfolgt eine Hash-Wert-Bildung und die Nachricht wird mit *Message Authentication Code* (*MAC*) versehen.

SSL untestützt eine Reihe von Verschlüsselungsverfahren unterschiedlicher Stärke und kann dadurch mittleren bis hohen Vetraulichkeitsanforderungen gerecht werdeb.

4.2.4 Ergebnis der Vorstellung von Technologien

Stellt man die in diesem Abschnitt vorgestellten Technologien gegenüber, wird erkennbar, daß sich vor allem in drei Punkten grundlegend unterscheiden. Zum einen sind das die Security Dienste, die von einer Technologie zur Verfügung gestellt. Weiterhin bestehen Unterschiede bezüglich der Möglichkeit Dienstgütegarantien zu vereinbaren (QoS) und der Skalierbarkeit. Letztere drückt sich in der Anzahl von möglichen Verbindungen bzw. Tunneln aus.

Entsprechende Erkenntnisse hinsichtlich dieser Unterscheidungsmerkmale werden im nächsten Kapitel aufgegriffen. Darin wird ein Klassifizierung bezüglich dieser Merkmale vorgenommen, und dabei VPN Technologien mit Lösungsklassen verknüpft.

Kapitel 5

Klassifizierung von VPN Lösungen

Im Abschnitt 3.1 erfolgte die Darlegung funktionaler Anforderungen an VPN Lösungen aus Sicht der verwendeten Anwendungen. Weiterhin wurden in Abschnitt 4.2 VPN Technologien betrachtet und deren Eigenschaften vorgestellt. Das Ziel dieses Kapitels besteht nun darin, Relationen zwischen funktionalen Anforderungen und passenden Technologien herzustellen und somit eine Klassifizierung von VPN Lösungen zu gewinnen. Klassen repräsentieren also eine Menge von funktionalen Anforderungen, kombiniert mit einer Auswahl von Technologien, die in der Lage sind, diese Anforderungen zu erfüllen. Wie bereits in 1 erwähnt, dient dieses Vorgehen der Vorauswahl von VPN Technologien und unterstützt damit den in Abbildung 1.1 dargestellten Phasenplan eines Unternehmens.

Beachtet man die Vielzahl von funktionalen Anforderungen, wird schnell klar, dass nicht alle in die Klassifizierung mitaufgenommen werden können. Vielmehr gilt es eine angemessene Auswahl zu treffen, um die Anzahl entstehender Klassen in einem überschaubaren Rahmen zu halten und somit eine Übersichtlichkeit zu gewährleisten. Angemessen drückt in diesem Fall die Bereitschaft aus, eine möglichst objektive und allgemeingültige Auswahl vorzunehmen und somit funktionale Unterscheidungsmerkmale in den verknüpften Technologien gebührend zu berücksichtigen. Eine in diesem Sinne vorgenomme Auswahl wird im folgenden Abschnitt vorgestellt.

5.1 Auswahl von funktionalen Anforderung für die Klassifizierung

Im Hinblick auf eine Klassenbildung muss primär der Fragestellung nachgegangen werden, welche Anforderungen direkten Einfluss auf die Auswahl einer geeigneten Technologie ausüben. Dabei zeigt sich, dass die Betrachtung des Anwendungsgebiets alleine keine unmittelbaren Rückschlüsse zulässt. Vielmehr erweist es sich als

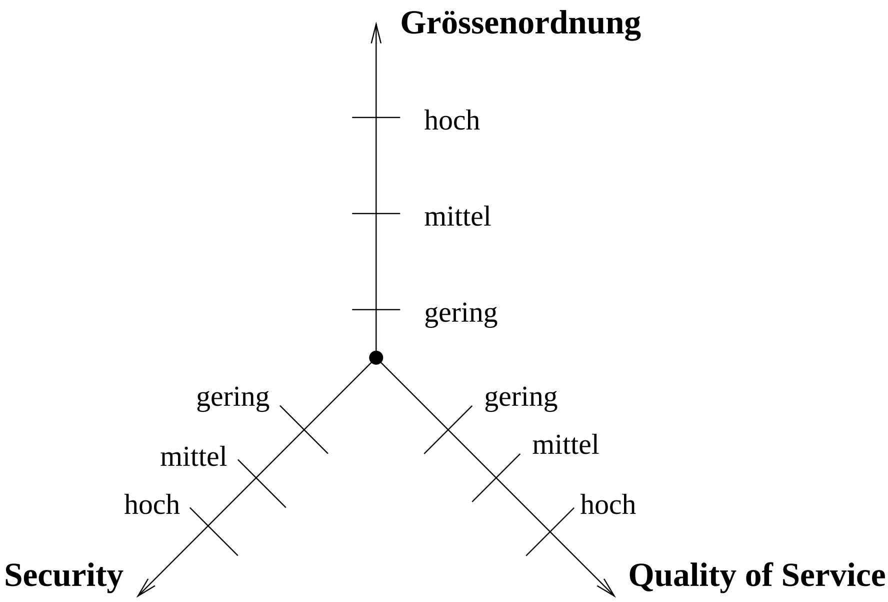

Abbildung 5.1: In der Klassifizierung betrachtete Dimensionen und Stufen

notwendig, mehrere Anforderungen zu berücksichtigen, um letztlich eine Aussage darüber treffen zu können, ob eine Technologie für die vorliegende Aufgabenstellung geeignet ist. Dementsprechend erscheint ein zweistufiges Vorgehen sinnvoll: Zunächst werden adäquate Anforderungsdimensionen festgelegt und zusätzlich in jedem Bereich verschiedene Stufen definiert. Letztere repräsentieren den Umfang bzw. die relative Stärke der in diesem Bereich angesiedelten Anforderungen. Aus den bereits angesprochenen Gründen der Übersichtlichkeit wird eine Unterteilung in drei Anforderungsdimensionen und jeweils drei Stufen vorgenommen, was eine Gesamtanzahl von 27 Klassen nach sich zieht.

Die ersten beiden Anforderungsdimensionen entstehen unter Berücksichtigung der am Anfang von Abschnitt 3.1 vorgestellten Erkenntnisse: Darin wurden **Security** und **QoS** Anforderungen eine tragende Rolle eingeräumt, da sie entscheidenden Einfluss auf die Abwicklung geschäftlicher Vorgänge in einem VPN nehmen. Die dritte Dimension spiegelt Anforderungen bezüglich der **Größenordung** des VPN wieder. Sie setzt sich aus der Anzahl von Sites und Telearbeitern[1] in einem VPN zusammen.

Zusätzlich werden die Dimensionen nach dem Umfang der vorliegenden Anforderungen in die Stufen **gering**, **mittel** und **hoch** unterteilt. Abbildung 2 stellt die nach diesem Muster vorgenomme Einteilung dar.

[1]Mit Telearbeitern werden Teilnehmer in einer Remote Access Lösung bezeichnet.

5.1.1 Die Anforderungsdimension Security

Für diese Dimension relevante Anforderungen wurden ausführlich in Abschnitt3.1.5.1 behandelt. Eine Einordnung in die erwähnten Stufen erfolgt primär aufgrund dieser Security Anforderungen. Zusätzlich werden für die Einhaltung der Anforderungen nötigen Security-Maßnahmen unter Berücksichtigung der verwendeten Kommunikationsplattform (Internet oder private Netzinfrastuktur[2]) erwähnt.

Geringe Security Anforderungen Im VPN übertragene Daten bedürfen keiner Absicherung hinsichtlich Authentizität, Vertraulichkeit und Integrität. Lediglich eine Zugriffskontrolle für das VPN mit Hilfe einer einfachen Benutzerauthentifizierung wird verlangt. Diese Stufe enthält keine Einschränkungen hinsichtlich der verwendeten Kommunikationsplattform.

Mittlere Security Anforderungen Es sollen unternehmensinterne Daten über das VPN ausgetauscht werden, die aber keine höchstvertraulichen Informationen enthalten (mittlere Vertraulichkeit). Für Tunnel-basierte Technologien wird - falls das Internet als Kommunikationsplattform dient - der Einsatz von Verschlüsselungsverfahren geringer bis mittlerer Schlüssellänge sowie eine Hashwert-Bildung zur Sicherstellung der Datenintegrität notwendig. In einer privaten Infrastruktur hingegen wird ein vergleichbarer Grad von Vertraulichkeit bereits durch entsprechende netz-basierte Technologien hergestellt, es sind deshalb keine weiteren Security Maßnahmen notwendig. Weiterhin ist eine einfache Benutzerauthentifizierung Bestandteil dieser Stufe.

Hohe Security Anforderungen Ein Austausch von höchstvertraulichen Daten soll vorgenommen werden. Zusätzlich wird eine Authentizität und Integrität der übertragenen Daten gefordert. Dazu werden Verschlüsselungsverfahren mit hoher Schlüssellänge, eine Hash-Wertbildung zur Bestimmung der Datenintegrität und eine Public Key Infrastruktur vorausgesetzt. Letztere erlaubt eine starke Benutzerauthentifizierung und eine darauf basierende Zugriffskontrolle. Das Internet ist für diese Stufe als Kommunikationsplattform nicht geeignet.

5.1.2 Die Anforderungsdimension QoS

Die in Abschnitt 3.1.6 vorgestellten QoS Anforderungen bestimmen die Ausprägungen der verschiedenen Stufen dieser Dimension. Analog zu der Dimension Security werden Auswirkungen der in einer Stufe enthaltenen Anforderungen auf die Auswahl der Kommunikationsplattform behandelt.

[2] Die Netzinfrastuktur eines Providers, wird auch als privat betrachtet

Geringe QoS Anforderungen Die Nutzung von zeitkritischen Anwendungen im VPN ist nicht vorgesehen. Auch eine Priosierung von Datenströmen bestimmter Anwendungen ist nicht notwendig. Damit ist ein Best-Effort-Dienst für diese Stufe ausreichend, bei dem einzig die Bandbreite und Zuverlässigkeit für den Zugangsbereich (siehe Referenzmodell) statistisch festgelegt sind. Damit eignen sich als Kommunikationsplattform Internet und private Infrastruktur gleichermaßen.

Mittlere QoS Anforderungen Das Unternehmen möchte das VPN für geschäftskritische Anwendungen nutzen. Dafür sind eine Ende-zu-Ende festgelegte Verfügbarkeit, Bandbreite und Zuverlässigkeit notwendig. Darüberhinaus sollen diese Parameter deterministisch vorherbestimmbar sein. Bei einer Kommunikation über das Internet sind entsprechende Garantien (noch) nicht möglich. Deshalb sind für diese Stufe netz-basierte Technologien und damit die Kommunikation über Provider- Backbone zwingend erforderlich.

Hohe QoS Anforderungen Die Verwendung von geschäfts- und zeitkritischen Anwendungen im VPN ist geplant. Entsprechend wird Wert auf eine Festlegung von Bandbreite, Verzögerung, Variation der Verzögerung, Verfügbarkeit und Zuverlässigkeit gelegt. Zudem sollen diese Parameter eine Ende-zu-Ende Gültigkeit besitzen und deterministisch vorherbestimmbar sein. Außerdem soll eine Priosierung von Datenströmen bestimmter Anwendungen in mehrere Classes-of-Service möglich sein.

5.1.3 Die Anforderungsdimension Größenordnung

Mit dieser Dimension werden Einflüsse der Anzahl von Teilnehmern - in Form von Remote-Benutzern und Sites - eines VPNs auf die Auswahl applikabler Technologien berücksichtigt. Dabei muss erwähnt werden, dass letztere nicht aufgrund ihrer Spezifikation auf eine bestimmte Anzahl von Teilnehmern beschränkt sind. Vielmehr zeigt sich, dass durch entstehende Komplexität, Grenzen bezüglich der Managebarkeit bestimmter Technologien gesetzt sind. Hervorgerufen wird dies vor allem durch das in Abschnitt 4.1.2 beschriebene n^2-Problem. Die Einteilung in Stufen erfolgt anhand von typischen Werten, wie sie sich in Angeboten von Herstellern beobachten lassen.

Geringe Anforderungen Größenordnung Das VPN soll bis zu 10 Sites und 50 Telearbeiter unterstützen.

Mittlere Anforderungen Größenordnung Es sollen bis zu 1000 Sites und 5000 Telearbeiter möglich sein.

Hohe Anforderungen Größenordnung In dem VPN sollen deutlich mehr als 1000 Sites und 5000 Telearbeiter möglich sein.

Es ist zu beachten, dass die angegebenen Werte einen aktuellen Stand der Technologie wiederspiegeln. Dementsprechend können neuere Entwicklungen zu unterschiedlichen Werten führen.

5.2 Beschreibung der entstehenden Klassen

Die Klassen von VPN Lösungen gehen aus den möglichen Kombinationen der in den Dimensionen vorgestellten Stufen hervor. Es soll somit ermöglicht werden, ausgehend von einer individuellen Kombination, die dafür passenden Technologien zu ermitteln. Wiederholungen in der Beschreibung sind deshalb nicht vermeidbar. Die Bezeichnung der Stufen wird aus Übersichtlichkeitsgründen abgekürzt. Abschließend werden die entsprechenden Klassen in tabellarischer Form 5.2 dargestellt.

Klasse 1 (geringe Security, geringe QoS, geringe Größenordnung) Alle Tunnel-basiertenTechnologien bieten eine Benutzerauthentifizierung und erfüllen damit die gestellten Security Anforderungen. Gleichermaßen wird in allen netz-basierten Technolgien die gewünschte Funktionalität vom CPE Equipment bereitgestellt. Unter Berücksichtigung der geringen QoS und Größenordnungsanforderungen erscheint der Einsatz von netz-basierten Technologien dennoch nicht sinnvoll. PPTP stellt in Verbindung mit dem Internet als Kommunikationsplattform die geeignetste und kostengünstigste Technologie für diese Klasse dar. Die Integration in das Standard-Betriebssystem ermöglicht einen Tunnelaufbau in voluntary Modus. Damit wird keine Anschaffung von neuer Hardware nötig, und die Anforderung hinsichtlich der Größenordnung wird dennoch erfüllt. Ein Internet Service Provider liefert üblicherweise die gewünschten Aussagen über die Bandbreite und Zuverlässigkeit im Zugangsbereich.

Klasse 2 (geringe Security, geringe QoS, mittlere Größenordnung) Aufgrund der mittleren Größenordnung des VPNs werden bei Verwendung von Tunnel-basierten Technologien, entsprechende leistungsfähige Komponenten zur Terminierung der Tunnel notwendig. Für L2TP steht in diesem Bereich eine große Auswahl von Hardwarekomponenten zur Verfügung, was vor allem auf die Standardisierung dieser Technologie zurückzuführen ist. Damit stellt L2TP mit compulsory Tunneling die geeigneteste Technologie in dieser Klasse dar. Für die Auswahl der Kommunikationsplattform bestehen keine Einschränkungen.

Klasse 3 (gering Security, geringe QoS, hohe Größenordnung) Die hohe Größenordnung führt in Verbindung mit der auftretenden n^2-Problematik zu einer großen Herausforderung für das Konfigurationsmanagement. Alle Technologien, die Overlay Eigenschaften besitzen, sind von dieser Problematik betroffen. MPLS verspricht dagegen in der Peer-to-peer Betriebsart eine Lösung für diese Problematik und wird deshalb als geeignetste Technologie für diese Klasse angesehen.

Klasse 4 (geringe Security, mittlere QoS, geringe Größenordnung) Durch die mittleren QoS Anforderungen bedingt, wird der Einsatz von netzbasierten Technologien und die Kommunikation über eine private Infrastruktur notwendig. Alle erläuterten netz-basierten Technologien erfüllen die gestellten QoS und Größenordnungsanforderungen. Frame Relay gilt in diesem Bereich als die kostengünstigste und ist damit für diese Klasse geeignetste Technologie. Die Commited Information Rate (CIR) zusammen mit Verfügbarkeits- und Zuverlässigkeitswerten eines Provider Backbones liefern dabei die gewünschten QoS Funktionalitäten.

Klasse 5 (geringe Security, mittlere QoS, mittlere Größenordnung) Hier besteht kein Unterschied zu Klasse 4. Alle netz-basierten Technologien erfüllen die im Vergleich dazu gestiegenen Größenordnungsanforderungen. Damit stellt analog zu Klasse 4 Frame Relay die geeignetste Technologie dar.

Klasse 6 (geringe Security, mittlere QoS, hohe Größenordnung) Wie bereits in der Beschreibung von Klasse 4 ausgeführt, erfordert eine mittlere QoS Anforderungsstufe die Verwendung von netz-basierten Technologien. Bedingt durch die hohen Größenanforderungen kommt bei Verwendung von ATM oder Frame Relay die n^2-Problematik zum Tragen: Sollen n VPN Teilnehmer vollvermascht verbunden werden, gilt es $\frac{n(n-1)}{2}$ VCs bzw. PVCs zu konfigurieren. Dies stellt eine große Herausforderung hinsichtlich des Konfigurationsmanagements dar und demzufolge eine geringe Eignung für hohe Größenordnungen von VPNs. MPLS wird in der mit Peer-to-peer bezeichneten Ausprägung [RR99] von diesem Problem nicht betroffen, und gilt deshalb als geeignetste Technolgie für diese Klasse.

Klasse 7 (geringe Security, hohe QoS, geringe Größenordnung) Bedingt durch die hohen QoS Anforderungen wird der Einsatz von netz-basierten Technologien erforderlich. Frame Relay erlaubt keine Festlegung derart umfangreicher Anforderungen, speziell kein CoS und scheidet damit als Kandidat aus.

ATM bietet gegenüber MPLS aufgrund der zellenbasierten Übertragung die höheren Zusicherungsmöglichkeiten für zeitkritische Anwendungen und entspricht damit der geeignetsten Technologie für diese Klasse.

Klasse 8 (geringe Security, hohe QoS, mittlere Größenordnung) Es besteht kein Unterschied zu Klasse 7. ATM erfüllt auch die mittleren Größenanforderungen und gilt deswegen auch hier als geeignetste Technologie.

Klasse 9 (geringe Security, hohe QoS, hohe Größenordnung) Derart hohen QoS Anforderungen kann nur in Verbindung mit ATM oder MPLS entsprochen werden. Wegen der bei ATM auftretenden n^2-Problematik und den damit entstehenden Schwierigkeiten im Konfigurationsmanagement des VPN, gilt MPLS in der Peer-to-peer Betriebsart[RR99] als geeignetste Technologie dieser Klasse.

Klasse 10 (mittlere Security, geringe QoS, geringe Größenordnung) Aufgrund der mittleren Security Anforderungen wird für Tunnel-basierte Technologien - falls das Internet als Kommunikationsplattform dient - der Einsatz von Verschlüsselungsverfahren geringer bis mittlerer Schlüssellänge sowie eine Hashwert-Bildung erforderlich. IPSec wird als einzige Tunnel-basierte Technologie diesen Anforderungen gerecht. Alternativ erfüllen netz-basierte Technologien, die geschlossene Benutzergruppen in einer privaten Netzinfrastruktur ermöglichen, eine vergleichbare Funktionalität. IPSec, im Transportmodus mit AH/ESP Header zur Absicherung einer Kommunikation über das Internet, stellt die kostengünstigste und damit geeignetste Variante dar.

Klasse 11 (mittlere Security, geringe QoS, mittlere Größenordnung) Es besteht kein Unterschied zu Klasse 10 hinsichtlich der Auswahl einer geeigneten Technologie. Die Verwendung von Hardwarekomponenten ermöglicht eine performante Ver- und Entschlüsselung der Daten. Somit stellt IPSec im Transportmodus mit AH/ESP Header und dem Internet als Kommunikationsplattform wiederum die kostengünstigste und geeignetste Technologie dar.

Klasse 12 (mittlere Security, geringe QoS, hohe Größenordnung) Bedingt durch die hohe Größenordnung des VPNs, treten bei Technologien mit Overlay Eigenschaften, und der damit entstehenden n^2-Problematik, Schwierigkeiten hinsichtlich des Konfigurationsmanagements auf. Die für diese Security Stufe notwendige Datenver- und -entschlüsselung für die Kombination Tunnel-basierte Technologie/Internet erfordert einen zusätzlichen Rechenaufwand in den entsprechenden Komponenten. Deshalb eignen sich netz-basierte Technologien und im besonderen MPLS in der Peer-to-peer Betriebsart [RR99] für diese Klasse.

Klasse 13 (mittlere Security, mittlere QoS, geringe Größenordnung) Durch die mittleren QoS Anforderungen bedingt, wird der Einsatz von netzbasierten Technologien und somit die Kommunikation über eine private Infrastruktur notwendig. Die gestellten Security Anforderungen werden dabei von allen netz-basierten Technologien erfüllt. Frame Relay gilt in diesem Bereich als kostengünstigste und wird deshalb als geeignetste Technologie betrachtet.

Klasse 14 (mittlere Security, mittlere QoS, mittlere Größenordnung) Es besteht kein Unterschied zu Klasse 14. Frame Relay erfüllt die mittleren Größenanforderungen und gilt deswegen auch hier als geeignetste Technologie.

Klasse 15 (mittlere Security, mittlere QoS, hohe Größenordnung) Wie bereits in der Beschreibung von Klasse 13 erwähnt, sind nur netz-basierte Technologien in der Lage, die mittleren QoS Anforderungen zu erfüllen. Dabei führt die hohe Größenordnung des VPNs bei Technologien, die Overlay Eigenschaften besitzen, zu nicht zu unterschätzenden Herausforderungen für das Konfigurationsmanagement. Dafür verantwortlich ist die auftretende n^2- Problematik. MPLS ist in der mit Peer-to-peer bezeichneten Ausprägung [RR99] von dieser Problematik nicht betroffen und gilt deshalb als geeignetste Technologie für diese Klasse.

Klasse 16 (mittlere Security, hohe QoS, geringe Größenordnung) Die hohen QoS Anforderungen können nur mit MPLS oder ATM realisiert werden. Beide erfordern die Verwendung einer privaten Infrastruktur und erfüllen damit verbunden die mittleren Security Anforderungen. ATM bietet gegenüber MPLS aufgrund der zellenbasierten Übertragung die höheren Zusicherungsmöglichkeiten für zeitkritische Anwendungen und entspricht damit der geeignetsten Technologie für diese Klasse.

Klasse 17 (mittlere Security, hohe QoS, mittlere Größenordnung) Es besteht kein Unterschied zu Klasse 16. ATM erfüllt die mittleren Größenanforderungen und gilt deswegen auch hier als geeignetste Technologie.

Klasse 18 (mittlere Security, hohe QoS, hohe Größenordnung) Derart hohen QoS Anforderungen kann nur in Verbindung mit ATM oder MPLS entsprochen werden. Wegen der bei ATM auftretenden n^2-Problematik und den damit entstehenden Schwierigkeiten im Konfigurationsmanagement des VPN, gilt

MPLS in der Peer-to-peer Betriebsart[RR99] als geeignetste Technologie dieser Klasse.

Klasse 19 (hohe Security, geringe QoS, geringe Größenordnung) Die hohen Security Anforderungen können nur in Verbindung von IPSec mit einer netz-basierten Technologie bzw. einer privaten Infrastruktur erfüllt werden. Konkreter ausgedrückt, wird IPSec im Tunnelmodus mit AH/ESP Header und einem starken Verschlüsselungsverfahren wie Triple DES erforderlich. Zudem wird für den Schlüsselaustausch eine Public Key Infrastruktur notwendig. Dabei ist zu beachten, dass die bei der Ver- und Entschlüsselung erforderliche Rechenleistung eine große Herausforderung für Security Komponenten darstellen. In Verbindung mit den geringen QoS- und Größenanforderungen stellt dies aber kein unüberwindbares Hindernis dar. Für die netz-basierte Technologie bietet sich Frame Relay als kostengünstigste Variante an.

Klasse 20 (hohe Security, geringe QoS, mittlere Größenordnung) Hier besteht kein Unterschied zu Klasse 19. Durch den Einsatz von entsprechend leistungsfähigen Security Komponenten, kann IPSec mit den vorgestellten Parametern eingesetzt werden.

Klasse 21 (hohe Security, geringe QoS, hohe Größenordnung) Für diese Klasse sind keine konkreten Aussagen möglich. Es gilt herauszufinden, ob Security Komponenten verfügbar sind, die derartig hohe Größenordnungen in Zusammenhang mit IPSec und den in Klasse 19 beschriebenen Parametern bewältigen.

Klasse 22 (hohe Security, mittlere QoS, geringe Größenordnung) Analog zu Klasse 19 werden IPSec mit höchster Sicherheitsfunktionalität und der Einsatz netz-basierter Technologien notwendig. Letztere sind alle in der Lage gewünschte QoS Anforderungen zu erfüllen. Frame Relay wird als kostengünstigste Technologie in diesem Bereich betrachtet und erhält damit den Vorzug gegenüber MPLS und ATM.

Klasse 23 (hohe Security, mittlere QoS, mittlere Größenordnung) Es besteht kein Unterschied zu Klasse 22 hinsichtlich der applikablen Technologien. Frame Relay ist gleichermaßen in der Lage die Anforderungen hinsichtlich der Größenordnung zu erfüllen und gilt deshalb in Kombination mit IPSec als geeignetste Variante.

Klasse 24 (hohe Security, mittlere QoS, hohe Größenordnung) Wie auch in Klasse 21 beschrieben, sind hier keine konkreten Aussagen möglich. Zwar werden die vorliegenden QoS Anforderungen von allen netz-basierten Technologien erfüllt, aber es muss geprüft werden, ob Komponenten verfügbar sind, die IPSec mit höchster Sicherheitsfunktionalität in dieser Grössenordnung des VPNs unterstützen. Wegen der bei ATM und Frame Relay auftretenden n^2-Problematik und den damit entstehenden Schwierigkeiten im Konfigurationsmanagement des VPN, gilt MPLS in der Peer-to-peer Betriebsart[RR99] als geignetste Kombination zu IPSec für diese Klasse.

Klasse 25 (hohe Security, hohe QoS, geringe Größenordnung) Diese Klasse ist in der Praxis sehr schwer zu realisieren. Der durch die hohen Schlüssellängen bedingte Rechenaufwand, zusammen mit dem durch ESP und AH Header entstehenden Overhead, erschwert die Durchsetzung hoher QoS Anforderungen sehr stark. Besonders die von zeitkritischen Anwendungen geforderte minimale Verzögerungszeit ist davon betroffen. Allerdings finden sich zumindest für diese geringe Größenordnung Produkte von Herstellern, die die geforderten QoS Parameter teilweise ermöglichen.

Klasse 26 (hohe Security, hohe QoS, mittlere Größenordnung) Aufgrund der hohen Security Anforderungen und dem damit nötig werdenden Einsatz von IPSEC mit höchster Sicherheitsfunktionalität, sind die hohen QoS Anforderungen aus den in Klasse 25 bereits genannten Gründen nicht erfüllbar. Das Ver- und Entschlüsseln der Daten bedeutet einen zu großen Rechen- und damit Zeitaufwand, um damit Anwendungen wie etwa Voice-over-IP in einem VPN mittlerer Größe zur Verfügung zu stellen.

Klasse 27 (hohe Security, hohe QoS, hohe Größenordnung) Diese Klasse kann in der Praxis in dieser Form nicht realisiert werden. Das Hindernis stellt hier weniger die netz-basierte Technologie dar - mit ATM könnten gewünschte QoS Anforderungen durchaus erfüllt werden- sondern die Leistungsfähigkeit der Security Komponenten wie IPSec Konzentratoren. Es sind momentan keine Komponenten verfügbar, die den, durch die Verschlüsselung entstehenden, Rechenaufwand in einer für zeitkritische Anwendungen akzeptalen Zeit bewältigen.

5.3 Bewertung der vorgenommenen Klassifizierung

Mit der vorgenommenen Klassifizierung wurden typische Anforderungen eines Unternehmens VPN Technologien gegenübergestellt. Dabei zeigt sich, dass her-

Kl.	S	Q	G	empfohlene Technologie
1	gering	gering	gering	PPTP
2	gering	gering	mittel	L2TP mit compulsory Tunneling
3	gering	gering	hoch	MPLS
4	gering	mittel	gering	Frame Relay
5	gering	mittel	mittel	Frame Relay
6	gering	mittel	hoch	MPLS mit Peer-to-peer
7	gering	hoch	gering	ATM
8	gering	hoch	mittel	ATM
9	gering	hoch	hoch	MPLS mit Peer-to-peer
10	mittel	gering	gering	IPSec
11	mittel	gering	mittel	IPSec
12	mittel	gering	hoch	MPLS
13	mittel	mittel	gering	Frame Relay
14	mittel	mittel	mittel	Frame Relay
15	mittel	mittel	hoch	MPLS
16	mittel	hoch	gering	ATM
17	mittel	hoch	mittel	ATM
18	mittel	hoch	hoch	MPLS
19	hoch	gering	gering	IPSec in Verbindung mit Frame Relay
20	hoch	gering	mittel	IPSec in Verbindung mit Frame Relay
21	hoch	gering	hoch	nicht bestimmt
22	hoch	mittel	gering	IPSec in Verbindung mit Frame Relay
23	hoch	mittel	mittel	IPSec in Verbindung mit Frame Relay
24	hoch	mittel	hoch	nicht bestimmt
25	hoch	hoch	gering	nicht bestimmt
26	hoch	hoch	mittel	nicht bestimmt
27	hoch	hoch	hoch	nicht bestimmt

Tabelle 5.1: Die Lösungsklassen im Überblick

vorgerufen durch die niedrige Granulärität der Betrachtung die Nichtberücksichtigung von speziellen Anforderungen nicht vermeidbar ist. Besteht beispielsweise nur der Wunsch webbasierte Anwendungen über das VPN zur Verfügung zu stellen, muss die Verwendung von SSL in Betracht gezogen werden. Weiterhin könnte das Unternehmen gewillt sein, andere Vermittlungsschichtprotokolle als IP einzusetzen. In diesem Fall ist eine alleinige Verwendung von IPSec nicht ausreichend und die Kombination mit einer anderen Tunnel-basierten Technologie wird erforderlich (etwa IPSec over L2TP).

Die für eine Klasse geltenden Anforderungen entstanden aus Kombinationen der Dimensionen und darin auftretender Stufen. In der Praxis kommen bestimmte Kombinationen aber eher selten vor. Bestehen beispielsweise hohe Security Anforderungen, ist der Fall, dass die QoS Anforderungen gleichzeitig niedrig sind eher unwahrscheinlich. Klassen mit einer derart "asymmetrischen Verteilung" sind also für die Praxis weniger relevant.

Mit der Klassifizierung wurde ein weiteres Werkzeug zur Unterstützung vorgestellt. Im weiteren Teil dieser Arbeit werden nun die entwickelten Werkzeuge in einem konkreten Szenario, dem BMW Extranet angewendet. Dazu wird im nächsten Kapitel zuerst ein spezifischer Kriterienkatalog erstellt.

Kapitel 6

Erstellung des spezifischen Kriterienkatalogs

In den vorausgegangenen Kapiteln wurden Hilfsmittel entwickelt, um den Auswahlprozess hinsichtlich einer geeigneten VPN Lösung zu unterstützen. Der nachfolgende Teil dieser Arbeit widmet sich nun der Anwendung dieser Hilfsmittel in einem konkreten Szenario, dem Extranet der BMW AG (siehe 1.4) .

Für das verfolgte Ziel, die Neuausrichtung der Extranet-Strategie sind für BMW vor allem funktionale Merkmale von Interesse (Abschnitt 3.1). Dabei liegt das Hauptaugenmerk auf den Unterschieden zu der bestehenden Lösung. Die Anwendung des Kriterienkatalogs soll also Erkenntnisse liefern, in welchem Maß sich eine potentielle neue Lösung von dem bestehenden Extranet in Bezug auf funktionale Merkmale unterscheidet.

Zunächst gilt es, die spezifischen Anforderungen der BMW AG zu bestimmen. Dafür werden die, in Abschnitt 3.1 erarbeiteten, generellen Kriterien angepasst. BMW-relevante Kriterien werden dabei im Hinblick auf das Szenario konkretisiert (Verfeinerung) und nicht zutreffende Kriterien ausgeschlossen (Reduzierung). Im Zuge der Verfeinerung werden außerdem zusätzliche, in der Analyse nicht behandelte Kriterien mitaufgenommen. Um eine Bewertung von Lösungen vorzunehmen, ergibt sich weiterhin die Notwendigkeit, einen Bewertungsmaßstab und eine Gewichtung der Kriterien untereinander festzulegen. Ein Berechnungsverfahren beschreibt in diesem Zusammenhang, in welcher Form Gesamt- und Teilergebnisse berechnet werden können. Als Ergebnis dieser Arbeitsschritte liegt ein spezifischer Kriterienkatalog zur Bewertung von VPN Lösungen vor.

Der nächste Schritt beinhaltet eine Auswahl geeigneter Lösungsklassen für das BMW Extranet (Kapitel 7). Ausgehend von der in Kapitel 5 beschriebenen Klassifizierung, werden geeignete Stufen der Anforderungsdimensionen ausgewählt. Die Bewertung der daraus resultierenden Klassen mit dem Kriterienkatalog, erlaubt es objektive Vergleiche durchzuführen und trägt somit letztendlich zur Entscheidungsfindung bei (7).

6.1 Ermitteln der spezifischen Anforderungen der BMW AG

In dem BMW-internen Projekt *dealer network strategy* bestand ein wichtiger Aufgabenblock darin, spezifische Anforderungen bezüglich der VPN Lösung zu ermitteln. Im Folgenden werden die in diesem Zusammenhang ausgeführten Arbeitsschritte bzw. verwendeten Hilfsmittel kurz vorgestellt. Weiterhin wird auf Randbedingungen eingegangen. Die daraus gewonnenen Anforderungen werden an dieser Stelle nicht ausgeführt, sie fließen in den Kriterienkatalog mit ein und werden dementsprechend in Abschnitt 6.3behandelt.

Im Zuge der Anforderungsermittlung wurde ein Fragebogen (Questionnaire) formuliert und an die internen Auftragsgeber (Vetriebsgesellschaften) sowie Endbenutzer, repräsentiert durch Niederlassungen in den jeweiligen Ländern, verteilt. Dabei wurden folgende Bereiche berücksichtigt und in entsprechenden Fragen ausgedrückt:

- **Zufriedenheit**
  Es sollten die positivsten und negativsten Aspekte der bestehenden Lösung genannt werden. Damit wurde das Ziel verfolgt, Schwachstellen ausfindig zu machen und diese in der neuen Strategie zu berücksichtigen.

- **Zukünftige und bestehende funktionale Anforderungen**
  Dieser Teil basierte größtenteils auf den in Abschnitt 3.1 vorgestellten funktionalen Anforderungen. Dabei wurden Fragen bezüglich des Ist-Zustandes sowie der zukünftigen Entwicklung dieser Anforderungen gestellt. Beispielsweise sollte dazu der aktuelle und erwartete Anstieg des Bandbreitenbedarfs angegeben werden. Weiterhin wurde auf die in der bestehenden Lösung angebotenen Dienste wie DNS eingegangen. Es sollte damit herausgefunden werden, ob auf zusätzliche Dienste eventuell verzichtet werden kann und welche Auswirkungen dies auf den Betrieb des VPNs hat. Mit diesem Teil des Fragebogens wurde das Ziel verfolgt, den aktuellen Zustand des Extranets zu ermitteln und die zukünftige Entwicklung von Anwendungen und Diensten abzuschätzen.

- **Strategische Fragen**
  In diesem Teil des Fragebogens sollten Einschätzungen hinsichtlich einer möglichen Lösung gegeben werden. Dabei wurde beispielsweise nach der

Auswirkung einer Internet-basierten Lösung auf die eingesetzten Anwendungen gefragt. Die Intention dieses Abschnitts bestand darin, Argumente für oder gegen eine mögliche Internet Lösung zu sammeln.

Neben dem Fragebogen, diente eine Schutzbedarfsanalyse der Anwendungen als Quelle zur Anforderungsbestimmung. Diese wurde von einer externen Firma zusammen mit einer abstrakten Sicherheitsarchitektur entwickelt. Die aus dieser Analyse gewonnenen Ergebnisse fließen in den Kriterienkatalog mit ein und werden an dieser Stelle nicht weiter behandelt.

Randbedingungen Durch die Liberalisierung der Gruppenfreistellungsverordnung (GVO) wird es Autohändlern ermöglicht, mehrere Autotypen gleichzeitig anzubieten. Damit fallen die engen vertraglichen Beziehungen zwischen Händlern und Automobilkonzernen. In diesem Zusammenhang stellt sich für BMW die Frage, inwieweit Belange des Händlers in seinen Verantwortlichkeitsbereich fallen. Auf das Extranet bezogen bedeutet dies: Es gilt zu klären, ob bisher zur Verfügung gestellte Dienste wie Internetzugang oder email in Zukunft zwingend erforderlich sind. Diese Fragestellung konnte noch nicht verbindlich beantwortet werden.

6.2 Vorstellung des Kriterienkatalogs

Der Kriterienkatalog stellt kein standardisiertes und festgelegtes Verfahren dar. Er wurde in verschiedenen Arbeiten ([Sch99] , [Gie00], [Bre02]) angewandt und dabei leicht unterschiedlich definiert. Die Methodik eines Kriterienkatalogs beschreibt für ihn geltende Regeln in Form von erlaubten Eigenschaften, Bewertungs- und Gewichtungsmaßstäben sowie das zur Berechnung von Teil- und Gesamtergebnissen benutzte Verfahren (Berechnungsverfahren).

Die Entwicklung einer neuen Methodik für den Kriterienkatalog stellt kein mit dieser Arbeit verfolgtes Ziel dar. Vielmehr wird auf die in [Bre02]) vorgestellte Methodik zurückgegriffen. Sie stellt eine Verbesserung gegenüber den in vorausgegangenen Arbeiten entwickelten Verfahren dar und eignet sich in dieser Form auch für die vorliegende Aufgabenstellung. In den nächsten Abschnitten werden die wichtigsten Elemente dieser Methodik vorgestellt.

Zunächst gilt es jedoch, die grundlegenden Eigenschaften des Werkzeugs Kriterienkatalog vorzustellen und dabei in diesem Zusammenhang verwendete Begriffe zu bestimmen.

6.2.1 Einführung und Begriffsbestimmung

Mit Kriterienkatalog wird ein Werkzeug bezeichnet, das ausgehend von einer Kriteriensammlung, die Bewertung verschiedener Szenarien ermöglicht. Darin sind folgende grundlegende Bestandteile enthalten (siehe auch [Sch99], [Bre02] und [Gie00]):

- eine Sammlung bzw. Menge von Kriterien zusammen mit den korrespondierenden Beschreibungen
- den Kriterien zugeordnete Eigenschaften (auch Attribute genannt, z.B. Bewertungen)
- Aussagen über die Beziehungen der Kriterien untereinander (z.B. „B ist Teilkriterium von A“)
- ein Berechnungsverfahren, das festlegt, wie anhand der Ausprägungen von Attributen ein numerisches Gesamtergebnis ermittelt wird

Weiterhin wird prinzipiell zwischen drei Arten von Kriterien unterschieden. Unterschiede treten dabei vor allem in der Bewertung der Kriterien auf:

Basiskriterien umfassen keine weiteren Teilkriterien und sind deshalb als atomar anzusehen. Ihre Bewertung erfolgt direkt anhand eines innerhalb der Kriterienbeschreibung festgelegten Maßstabes (Bewertungsmaßstab). Basiskriterien stehen nur in Beziehung zu Hauptkriterien und sollten deshalb hinsichtlich der Bewertung möglichst unbeeinflusst von anderen Basiskriterien sein.

Hauptkriterien sind komplexe Kriterien, die sich aus anderen (Haupt- und Basis-) Kriterien zusammensetzen. Für ihre Bewertung werden die Beziehungen zu den betreffenden Teilkriterien berücksichtigt und in einer Funktion ausgedrückt. Die Gewichtungen, als Attribute der Beziehungen, legen dabei fest, in welchem Maß die Bewertungen der Teilkriterien in das Ergebnis miteinfließen.

Wurzel stellt ein spezielles Hauptkriterium dar und ist in jedem Katalog nur einmal vorhanden. Die Bewertung der Wurzel entspricht der des Gesamtszenarios, welches in dieser Arbeit durch eine Lösungsklasse repräsentiert wird. Dazu werden nach einer festgelegten Funktion (siehe Berechnungsverfahren) alle im Katalog dokumentierten Beziehungen und Attribute errechnet.

Darüberhinaus gelten folgende Regeln für die Beziehungen der Kriterien untereinander (nach [Bre02]):

erreichter Erfüllungsgrad	Gewichtung g
Kriterium ist äußerst wichtig für die Erfüllung des Hauptkriteriums	4
Kriterium ist sehr wichtig für die Erfüllung des Hauptkriteriums	3
Kriterium ist wichtig für die Erfüllung des Hauptkriteriums	2
Kriterium ist weniger wichtig für die Erfüllung des Hauptkriteriums	1

Abbildung 6.1: Abstufungen für die Gewichtung von Teilkriterien

- Die Zuordnung eines Teilkriteriums zu einem Hauptkriterium und umgekehrt, ist die einzig erlaubte Beziehung.
- Es existiert genau ein Wurzelkriterium, das nicht Teilkriterium eines anderen Kriteriums ist. Daraus folgt, dass alle Kriterien, außer der Wurzel, Teilkriterien eines anderen sind.
- Kriterien dürfen nicht Teilkriterien ihrer selbst sein.
- ein Kriterium darf nicht einziges Teilkriterium eines anderen sein.

6.2.2 Gewichtung der Kriterien

Um die Bedeutung eines Basiskriteriums für die Erfüllung des Hauptkriteriums auszudrücken, wird eine Gewichtung eingeführt. Die Vergabe der Gewichte beginnt mit der Wurzel und wird von dort aus in einem der Breitensuche ähnelndem Verfahren, dem Kriterienbaum nach unten laufend, ausgeführt. Die Gewichtung wurde nach den Bedürfnissen der BMW AG durchgeführt und wird in der Beschreibung jedes Hauptkriteriums in Abschnitt 6.3 verzeichnet.

Die Gewichtung (g) geht von vier Abstufungen aus, die den Erfüllungsgrad des Kriteriums wiederspiegeln. Der dazu verwendete Schlüssel wird in Abbildung 6.1 dargestellt. Im Gegensatz zu [Sch99] und [Gie00] wurde auf die Angabe von K.O. - Kriterien verzichtet. Das bezweckte Ergebnis - der Ausschluss eines Szenarios bei Nichterfüllung eines K.O.-Kriteriums, wird in dieser Arbeit bereits durch die Auswahl der Lösungsklassen erreicht und findet deshalb im Kriterienkatalog keine Verwendung.

Gewichte werden im Gegensatz zu [Sch99] und [Gie00] nicht als Attribute von Basiskriterien aufgefasst. Vielmehr wird der in [Bre02] entwickelte Ansatz zu Grunde gelegt: Gewichte gelten als Eigenschaften von Beziehungen zwischen Kriterien. Damit wird deren Bedeutung für die Berechnung von Hauptkriterien hervorgehoben, während der erstere Ansatz die globale Wichtigkeit eines Kriteriums ausdrückt. Abbildung 6.2.2 stellt einen in dieser Weise angefertigten Beispielkatalog dar, bei dem alle relativen Gewichte feststehen, bevor mit der Bewertung begonnen wird.

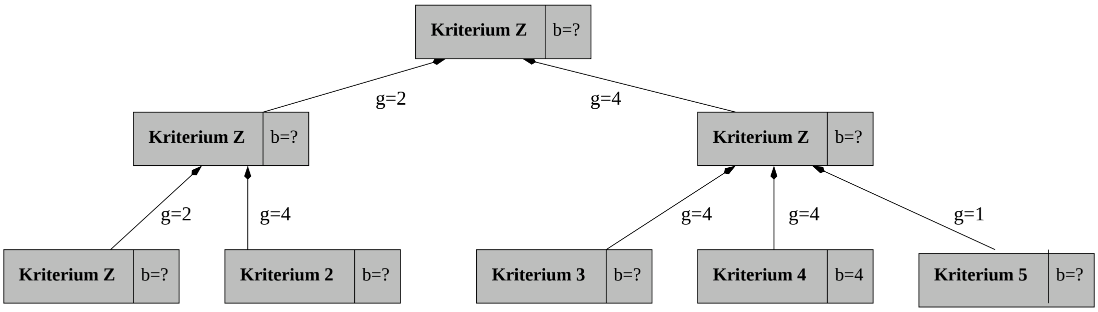

Abbildung 6.2: Gewichteter Beispielkatalog

6.2.3 Wertung der Kriterien

Der Vergleich von Lösungsklassen wird erst durch die Einführung einer Bewertung der Kriterien ermöglicht. Die Bewertung zeigt an, ob und wenn ja, zu welchem Grad ein Kriterium erfüllt wird. In dieser Arbeit wird der Erfüllungsgrad durch fünf Stufen ausgedrückt, die durch ein Symbol sowie eine Bewertungszahl (b) attribuiert sind. Letztere wird nach den im Berechnungsverfahren (Abschnitt6.2.4) festgelegten Regeln verarbeitet und fließt somit in den numerischen Vergleich von Lösungsklassen mit ein. Abbildung 6.3 stellt den in dieser Arbeit verwendeten Bewertungsschlüssel dar.

Im Gegensatz zu der in [Sch99] und [Gie00] vorgestellten Bewertung wird eine Übererfüllung von Kriterien nicht gesondert gewertet, sondern wie eine volle Erfüllung behandelt. Entstehen Nachteile aus der Übererfüllung, so werden diese in einem eigenen Kriterium berücksichtigt. Dieser Fall tritt beispielweise ein, wenn durch eine Übererfüllung höhere Kosten entstehen.

erreichter Erfüllungsgrad	Symbol	vergebene Bewertungszahl b
Kriterium wird voll erfüllt	++	4
Kriterium wird zum größten Teil erfüllt	+	3
Kriterium wird in mittlerem Umfang erfüllt	o	2
Kriterium wird kaum erfüllt	-	1
Kriterium wird nicht erfüllt	–	0

Abbildung 6.3: Abstufungen für Erfüllungsgrad einzelner Kriterien

6.2.4 Berechnungsverfahren

Die Anwendung des Kriterienkatalogs soll letztendlich eine numerische Bewertung einer Lösungsklasse produzieren. Das Berechnungsverfahren legt dabei Regeln fest, nach denen die Geamtpunktzahl aus den für Basiskriterien vergebenen Werten berechnet wird.

Die Bewertung eines Hauptkriteriums H mit n Teilkriterien (1..n) wird nach folgender Formel vorgenommen, wobei g der Gewichtung eines Teilkriteriums und b der vergebenen Bewertungszahl entspricht:

$$b_H = \frac{\sum_{i=1}^{n} b_i g}{\sum_{i=1}^{n} g} \tag{6.1}$$

Die Berechnung wird beginnend mit dem Wurzelkriterium rekursiv vorgenommen. Eine Anwendung auf den in Abbildung 6.2.2 dargestellten Beispielkatalog liefert dabei folgendes Ergebnis (Abbildung 6.4):

Kriterium	Gewicht g	Bewertung b
Kriterium Z		**3,19**
Kriterium A	2	1,33
Kriterium 1	1	2
Kriterium 2	2	1
Kriterium B	4	4,11
Kriterium 3	4	4
Kriterium 4	4	4
Kriterium 5	1	5

Abbildung 6.4: Bewertung des Beispielkatalogs

6.3 Struktur des Kriterienkatalogs

Der Kriterienkatalog wurde in Anlehung an die in Kapitel 3 durchgeführte Analyse erstellt. Seine Struktur orientiert sich an der in der Analyse vorgenommen Gliederung, die im Folgenden vorgestellt wird.

Wie bereits am Anfang dieses Kapitels erwähnt wurde, ist es für BMW von besonderem Interesse, die Unterschiede zur bestehenden Lösung im Bezug auf funktionale Merkmale zu ermittlen. Dementsprechend werden im Kriterienkatalog ausschließlich die in Abschnitt 3.1 vorgestellten funktionalen Anforderungen aus Sicht der Anwendungen betrachtet. Die Wurzel des Katalogs stellen damit die funktionalen Merkmale einer VPN Lösung dar. Letztere wird in dieser Arbeit durch die ausgewählte Lösungsklasse bestimmt (Abschnitt 7.1) und steht somit erst zum Zeitpunkt der Bewertung fest.

Die nächste Ebene des Kriterienkatalogs stellen Hauptkriterien dar. Sie entprechen den in Abschnitt 3.1 vorgestellten Bereichen innerhalb der funktionalen Anforderungen aus Sicht der Anwendungen. Für BMW nicht relevante Bereiche werden dabei von der Betrachtung ausgeschlossen. Die in diesem Zuge vorgenommenen Änderungen werden in der Vorstellung des Kriterienkatalogs (6.3) weiter ausgeführt.

Auf der untersten Ebene befinden sich die Basiskriterien. Sie gehen aus einer Anpassung der in 3.1 genannten Kriterien bzw. Anforderungen hervor. Dabei werden, ausschließlich für BMW relevante, Kriterien hinsichtlich des Szenarios konkretisiert. Um innerhalb der Bewertung (Abschnitt 7.2) einer Lösung Aussagen bezüglich der Unterschiede zum bestehenden Extranet zu ermöglichen, werden die Erscheinungsformen von Kriterien unter Einbeziehung der bestehenden Lösung formuliert.

Wurzelkriterium - Funktionale Merkmale der VPN Lösung

Kriterium	Gewicht
Funktionale Merkmale der VPN Lösung	
Adressierung	1
Kommunikationsbeziehungen	4
Anpassbarkeit	3
Security	3
Quality of Service	3

Die Abbildung von Kommunikationsbeziehungen stellt einen verbesserungswürdigen Punkt des bestehenden Extranets dar und erhält deshalb die höchste Gewichtung. Desweiteren soll den spezifischen Bedürfnissen von Händlern möglichst gut entsprochen werden können, was sich in einer Einstufung der Anpassbarkeit als *sehr wichtig* niederschlägt. Ebenso werden Security und QoS Kriterien von BMW als *sehr wichtig* für die Erfüllung des Hauptkriteriums angesehen. Weiterhin werden Kriterien im Bereich Adressierung als *weniger wichtig* eingestuft, da im Zuge der bestehenden Extranet Lösung bereits eine kontrollierte Vergabe von IP-Adressen stattgefunden hat. Die in der Analyse vorgestellte Anforderung Tranparenz für Anwendungen hat für BMW keine Bedeutung. Einerseits wird bereits zur Kommunikation zwischen Anwendungen die Internet-Protokollfamilie verwendet, andererseits beschäftigen sich interne Projekte mit einer Weiterentwicklung entprechender Anwendungen. Dabei wird unter anderem auch eine Integration von Security Maßnahmen in die Applikationen vorgesehen.

Kriterium I
Adressierung

Kriterium	Gewicht
Adressierung	
Verwendung von privaten IP-Adressen	4
Weiterverwendung des bestehenden Adressschemas	3
Interoperabilität mit Network Address Translation	2

Zur Kommunikation im Extranet werden ausschließlich private IP-Adressen verwendet, das entprechende Kriterium erhält damit die Gewichtung *äußerst wichtig*. Desweiteren wird eine Weiterverwendung des bestehenden Adressschemas als *sehr wichtig* für die Erfüllung des Hauptkriteriums angesehen. Eine Interoperabilität mit NAT wird als *wichtig* eingestuft.

Kriterium I.I
Verwendung von privaten Adressen

- Anforderung:

  Die Händler sollten nicht mit im Internet direkt erreichbaren (öffentlichen) IP-Adressen auftreten. Daraus folgt für die VPN Lösung, dass eine Verwendung von privaten IP-Adressen [RMK+96] zur Kommunikation zwischen BMW und den Händlern unterstützt werden sollte, wie sie es bereits in der bestehenden Lösung der Fall ist.

- Verwendete Erscheinungsformen:

  A Private IP Adressen sind ohne Einschränkungen möglich.

  B Es müssen bestimmte, vom Provider zugewiesene Bereiche von privaten IP Adressen verwendet werden.

  C Die Verwendung von privaten IP-Adressen ist nicht möglich.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	$\circ$	2
C	sehr schlecht	$--$	0

Kriterium I.II
Weiterverwendung des bestehenden Adressschemas

- Anforderung:

  In dem bestehenden Extranet der BMW AG wurden den Händlern private IP-Adressen nach einem festgelegten Adressierungsschema zugeordnet. Damit wird es BMW unter anderem möglich, Datenübertragungen zum Händler zu initieren. Die Einführung einer neuen Lösung sollte keine Änderungen dieses Schemas erfordern.

- Verwendete Erscheinungsformen:

  A Es sind keine Änderungen des verwendeten Adressierungsschemas erforderlich.

B Änderungen des Schemas sind notwendig.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	sehr schlecht	−−	0

Kriterium I.III
Interoperabilität mit Network Adress Translation

- Anforderung:

  Network Adress Translation (NAT) wird bereits in der bestehenden Extranet Lösung verwendet. Die neue Lösung sollte dies nicht einschränken und eine Interoperabilität mit NAT gewährleisten.

- Verwendete Erscheinungsformen:

A NAT wird ohne Einschränkungen unterstützt.

B Neben NAT und der verwendeten VPN Technologie ist die Einführung eines zusätzlichen Verfahrens (etwa ein zusätzlicher Tunnel) notwendig.

C NAT wird nicht unterstützt.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2
C	sehr schlecht	−−	0

Kriterium II
Kommunikationsbeziehungen

Kriterium	Gewicht
Kommunikationsbeziehungen	
Einbindung von IT Partnern	3
Möglicher Anstieg in der Anzahl von Teilnehmern	4
Unterstützte Topologien	3
1-n Kommunikationsbeziehungen	2

Als *äußerst wichtig* für die Erfüllung des Hauptkriteriums wird die Skalierbarkeit der Kommunikationsbeziehungen, und damit der mögliche Anstieg in der Anzahl von Teilnehmern eingestuft. Die Einbindung von IT-Partnern ist in der bestehenden Lösung umständlich realisiert und wird damit als *sehr wichtig* angesehen. Ebenso gilt das Kriterium unterstützte Topologien als *sehr wichtig.* Zukünftige Anwendungen im BMW Extranet sehen eine zentrale Distribution von Daten und damit 1-n Kommunikationsbeziehungen vor. Das entsprechende Kriterium wird aus diesem Grund als *wichtig* betrachtet.

Kriterium II.I
Einbindung von IT Partnern

- Anforderung:

  Wie bereits in Abschnitt 1.4 erwähnt, treten die IT-Partner von Händlern als Teilnehmer im Extranet auf. In diesem Zusammenhang wird zwischen globalen IT-Partnern, die mehrere Händler betreuen, und dedizierten, nur einem Händler zugeordneten, IT-Partnern unterschieden. Der Zugriff von IT-Partnern beschränkt sich dabei ausschließlich auf die von ihnen betreuten Händlern. In gewisser Weise ist somit eine Partitionierung des VPNs notwendig. In der bestehenden Lösung sind dazu allerdings Sonderlösungen, wie zusätzliche Firewalls notwendig. Eine neue Lösung sollte dabei ohne Sonderlösungen auskommen, und alle auftretenden Kommunikationswünsche erfüllen.

- Verwendete Erscheinungsformen:

  A IT-Partner können ohne Einschränkungen eingebunden werden.

  B Es ist eine Sonderlösung , wie etwa die Verwendung von zusätzlichen Firewalls, zur Einbindung von IT-Partnern erforderlich.

  C IT Partner können nicht eingebunden werden.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2
C	sehr schlecht	−−	0

Kriterium II.II
Möglicher Anstieg in der Anzahl von Teilnehmern

- Anforderung:

  Im Zuge der Deregulierung des Automobilhändlermarktes ist ein Anstieg der Anzahl von Händlern und damit VPN Teilnehmern gegenüber der bestehenden Lösung zu erwarten. Die VPN Lösung sollte in dieser Hinsicht keine Einschränkungen aufweisen.

- Verwendete Erscheinungsformen:

  A Die Teilnehmeranzahl kann um bis zu 50 Prozent ansteigen.

  B Die Teilnehmeranzahl kann um bis zu 25 Prozent ansteigen.

  C Die Teilnehmeranzahl kann um bis zu 10 Prozent ansteigen.

  D Keine zusätzlichen Teilnehmer können hinzugefügt werden

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2
C	schlecht	-	1
D	sehr schlecht	−−	0

Kriterium II.III
Unterstützte Topologien

- Anforderung:

  Die Bedürfnisse zukünftiger Anwendungen sind in diesem Bereich schwer abzuschätzen. Deswegen sollten sowohl Hub-and-Spoke, partiell vermaschte als auch vollvermaschte Topologien möglich sein. Im Gegensatz dazu, wird in der bestehenden Lösung wird nur eine Hub-and-spoke Topologie unterstützt.

- Verwendete Erscheinungsformen:

  A Hub-and-Spoke, partielle Vermaschung und Vollvermaschung sind möglich.

  B Es sind entweder nur Hub-and-Spoke oder vollvermaschte Topologien möglich.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2

Kriterium II.IV
1-n Kommunikationsbeziehungen

- Anforderung:

  Im Extranet werden Anwendungen eingesetzt, die das Versenden des selben Datenstroms an alle angeschlossenen Händler vorsehen. Allerdings bietet die bestehende Lösung in dieser Hinsicht nur die Möglichkeit, das Versenden durch mehrere 1-1 Kommunikationsbeziehungen zu realisieren. Die neue VPN Lösung sollte derartige 1-n Kommunikationsbeziehungen technisch unterstützen (Multicast) .

- Verwendete Erscheinungsformen:

  A Es sind technisch 1-n Kommunikationsbeziehungen möglich.

  B Es werden technisch nur 1-1 Kommunikationsbeziehungen unterstützt.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	sehr schlecht	–	0

Kriterium III
Anpassbarkeit

Kriterium	Gewicht
Anpassbarkeit	
Unterstützte Zugangstechnologien	4
Erhöhung der Bandbreite	4

BMW betrachtet das Kriterium unterstützte Zugangstechnologien als *äußerst wichtig* für die Erfüllung des Hauptkriteriums. Ebenso gilt die Erhöhung der Bandbreiten als *äußerst wichtig*. Weiterhin wird die Möglichkeit eine flexible Änderung von Zugangstechnologien und Bandbreiten vozunehmen, als *sehr wichtig* eingestuft.

Kriterium III.I
Unterstützte Zugangstechnologien

- Anforderung:

  In der bestehenden Lösung werden hauptsächlich ISDN und Standardfestverbindungen als Zugangstechnologien eingesetzt. In der der neuen Lösung sollten darüberhinaus DSL und UMTS verfügbar sein.

- Verwendete Erscheinungsformen:

  A Es sind ISDN, DSL, UMTS und Standardfestverbindungen möglich.

  B Es sind ISDN,DSL und Standardfestverbindungen möglich.

  C Es sind entweder nur ISDN oder nur Standardfestverbindungen möglich.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	gut	+	2
C	mittel	∘	1
D	sehr schlecht	−−	0

Kriterium III.II
Erhöhung der Bandbreite

- Anforderung:

  Es ist eine Steigerung des aufkommenden Datenvolumens um etwa den Faktor vier pro Jahr zu erwarten. Die neue Lösung sollte diese Steigerung nicht einschränken und dementsprechend eine Erhöhung der Übertragungsbandbreiten zulassen.

- Verwendete Erscheinungsformen:

  A Eine Steigerung des Datenvolumens bis zu einem Vierfachen kann bewältigt werden.

  B Es kann nur das aktuelle Datenvolumen bewältigt werden, eine Steigerung ist nicht möglich.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	sehr schlecht	−−	0

Kriterium IV
Security

Kriterium	Gewicht
Security	
Vertraulichkeit der ausgetauschten Daten	4
Zugriffskontrolle und Authentisierung	4
Integrität der ausgetauschten Daten	3

Im Einklang mit der durchgeführten Bedrohungsanalyse für Anwendungen wird die Vetraulichkeit der ausgetauschten Daten als *äußerst wichtig* angesehen. Ebenso gilt die Zugriffskontrolle als *äußerst wichtig* für die Erfüllung des Hauptkriteriums. Die Datenintegrität wird in diesem Zusammenhang als *sehr wichtig* eingestuft.

Kriterium IV.I
Vertraulichkeit der ausgetauschten Daten

- Anforderung:

  In der bestehenden Extranetlösung wird die Vertraulichkeit der übertragenen Daten auf zwei Arten gewährleistet:

  - Im Bereich des internationalen Extranets durch Frame-Relay in der Netzinfrastruktur des Hauptproviders.
  - In den nationalen Extranets durch Einsatz von Tunnel-basierten Technologien wie L2TP und L2F.

  Es soll in der neuen Lösung ein vergleichbares Maß an Vertraulichkeit der übertragenen Daten gewährleistet werden.

- Verwendete Erscheinungsformen:

  A Die Vertraulichkeit der übertragenen Daten ist höher zu bewerten, als in der bestehenden Lösung.

  B Die Vertraulichkeit der übertragenen Daten entspricht der in der bestehenden Lösung.

  C Die Vertraulichkeit der übertragenen Daten ist niedriger zu bewerten als in der bestehenden Lösung.

  D Die Vertraulichkeit der übertragenen Daten ist nicht gegeben.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	gut	+	3
C	schlecht	-	1
D	sehr schlecht	−−	0

Kriterium IV.II
Zugriffskontrolle und Authentisierung

- Anforderung:

  In der bestehenden Extranet Lösung werden Zugriffskontrollen basierend auf folgenden Authentisierungsverfahren vorgenommen:

  – In den nationalen Extranets durch CHAP bei Einwahllösungen bzw. Konfiguration der Router in Standardfestverbindungen.
  – Einem RADIUS Server in der Service Area der Hauptprovider für das internationale Extranet.

  Es sollen vergleichbare starke Authentisierungsverfahren für die Zugriffskontrolle in der neuen Lösung möglich sein.

- Verwendete Erscheinungsformen:

  A Die Authentisierungsverfahren für die Zugriffskontrolle sind stärker als in der bestehenden Lösung.

  B DieAuthentisierungsverfahren für die Zugriffskontrolle entsprechen in ihrer Stärke denen der bestehenden Lösung.

  C Die Authentisierungsverfahren für die Zugriffskontrolle sind weniger stark als in der bestehenden Lösung.

  D Es sind keine Authentisierungsverfahren für die Zugriffskontrolle vorhanden.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	gut	+	3
C	schlecht	−−	1
D	sehr schlecht	−	0

Kriterium IV.III
Integrität der ausgetauschten Daten

- Anforderung:

  In der bestehenden Extranet Lösung von BMW sind keine Mechanismen zur Sicherstellung der Integrität von ausgetauschten Daten vorhanden. Eine neue Lösung sollte jedoch entsprechende Funktionen enthalten.

- Verwendete Erscheinungsformen:

  A Verfahren zur Sicherstellung der Integrität sind vorhanden.

  B Es sind keine Verfahren zur Sicherstellung der Integrität von übertragenen Daten vorhanden.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	sehr schlecht	–	0

Kriterium V
Quality of Service

Kriterium	Gewicht
Quality of Service	
Bandbreite	4
Verfügbarkeit	4
Zuverlässigkeit	3

BMW betrachtet die Dienstgüteparamter Bandbreite und Verfügbarkeit als *äußerst wichtig* für die Erfüllung des Hauptkriteriums. Weiterhin wird die Zuverlässigkeit mit *sehr wichtig* gewichtet.

Kriterium V.I
Bandbreite

- Anforderung:

  In der bestehenden Lösung sind (technische) Bandbreitengarantien im Bereich des internationalen Extranets durch Commited Information Rates des Frame Relay Dienstes deterministisch festgelegt. Weiterhin erscheint einer dieser Dienstgüteparameter als ausreichend und soll deshalb in der neuen Lösung in vergleichbarer Form vorhanden sein.

- Verwendete Erscheinungsformen:

  A Eine deterministische Bandbreitengarantie kann gegeben werden.

  B Es kann nur eine statistische Bandbreitengarantie gegeben werden.

  C Es können keine Bandbreitengarantien gegeben werden.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2
C	sehr schlecht	−−	0

Kriterium V.II
Verfügbarkeit

- Anforderung:

  Verfügbarkeitsgarantien sind in der bestehenden Lösung sowohl für die Bereiche internationales als auch nationales Extranet deterministisch gegeben. Die neue Lösung sollte eine ähnliche Verfügbarkeit aufweisen.

- Verwendete Erscheinungsformen:

  A Die Verfügbarkeit ist höher als in der bestehenden Lösung.

  B Die Verfügbarkeit ist ähnlich wie in der bestehenden Lösung.

  C Die Verfügbarkeit ist geringer als in der bestehenden Lösung.

  D Es sind keine Verfügbarkeitsgarantien möglich.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	○	2
C	schlecht	-	1
D	sehr schlecht	–	0

Kriterium V.III
Zuverlässigkeit

- Anforderung:

  In der bestehenden Lösung sind Paketfehlerraten deterministisch festgelegt. In der neuen Lösung sollten ähnliche Paketfehlerraten auftreten, und garantiert werden können.

- Verwendete Erscheinungsformen:

  A Die Paketfehlerrate ist geringer als in der bestehenden Lösung.

  B Die Paketfehlerrate ist ungefähr gleich wie in der bestehenden Lösung.

  C Die Paketfehlerrate ist höher als in der bestehenden Lösung.

- Maßstab:

Ausprägung	Wertung	Erfüllung	Punkte
A	sehr gut	++	4
B	mittel	$\circ$	2
C	sehr schlecht	$--$	0

6.4 Ergebnis des Kriterienkatalogs

Der entstandene Kriterienkatlog repräsentiert die spezifischen Anforderungen von BMW. Die Erscheinungsformen wurden in Relation zu den funktionalen Merkmalen der bestehenden Lösung formuliert. Damit wird bei der Anwendung des Katalogs ein Vergleich mit der bestehenden Lösung ermöglicht. Die Auswahl einer Lösungsklasse und anschließende Bewertung wird im nächsten Kapitel ausgeführt.

Kapitel 7

Anwendung des Kriterienkatalogs

In diesem Kapitel wird der in Abschnitt 6.3 vorgestellte, spezielle Kriterienkatalog angewandt. In Einbeziehung der in Kapitel 5 dargestellten Klassifizierung erfolgt zunächst eine Auswahl der den Anforderungen von BMW entsprechenden Lösungsklasse.

Den nächsten Schritt stellt eine exemplarische Bewertung der Lösungsklasse dar. Dazu wird unter den einer Lösungsklasse zugeordneten Technologien, eine ausgewählt und mit dem Kriterienkatalog bewertet. Die Wahl richtet sich dabei nach den Präferenzen von BMW. Anschließend werden die Ergebnisse der Bewertung kurz zusammengefasst.

7.1 Auswahl der Lösungsklasse für das BMW Extranet

Die Auswahl der Lösungsklasse stellt eine Anwendung der in Abschnitt 5 vorgestellten Klassifizierung dar. Darin wurden drei grundlegende Anforderungsdimensionen bestimmt und jeweils in drei Stufen eingeteilt. Für die Auswahl einer Lösungsklasse für das BMW Extranet reicht es aus, die geeigneten Stufen in jeder Anforderungsdimension zu bestimmen. Die approbiate Lösungsklasse lässt sich dann direkt ablesen (siehe Tabelle 5.2).

Für die in der Klassifizierung festgelegten Anforderungsdimensionen Security und QoS können die Stufen einfach bestimmt werden: Der Vergleich von möglichen Stufen mit den BMW spezifischen Anforderungen (siehe Abschnitt 6.1), liefert die Erkenntnis, dass die mittleren Security und QoS Stufen fast deckungsgleich mit den Anforderungen von BMW in diesen Bereichen sind. Weiterhin erscheint, unter Berücksichtigung der Anzahl von Teilnehmern im BMW Extranet, ebenfalls die mittlere Größenordnungsstufe als geeignet. Damit fällt die Auswahl auf die in der Klassifizierung beschriebene Lösungsklasse 14, die noch einmal in Tabelle 7.1 dargestellt wird.

Security	QoS	Grössenordnung	Geeignete Technologien
mittel	mittel	mittel	**Frame Relay**, ATM, MPLS

Tabelle 7.1: Die Lösungsklasse für das BMW Extranet

Wie bereits in der Beschreibung der Lösungsklasse (Abschnitt 5.2) erwähnt wurde, gilt Frame Relay in Verbindung mit der Netzinfrastruktur eines Providers als kostengünstigste und damit geeigneteste Technologie in dieser Klasse.

Allerdings erscheint für BMW eine andere Technologie geeignet, die auch mit dem Kriterienkatalog bewertet werden soll: Das in Abschnitt 4.2 beschriebene *Secure Socket Layer*-Protokoll in Verbindung mit Internet als Kommunikationsplattform. Dafür sprechen vor allem strategische Gründe, die in Verbindung mit der als Randbedingung vorgestellten Deregulierung des Automobilhändlermarktes (Abschnitt 6.1) stehen. Die von BMW übernommenen Verantwortungen gegenüber den Händlern sollen drastisch reduziert werden. Die Verwendung des Internets als Kommunikationsplattform trägt hierzu bei: Die Händler sollen selbstständig einen Internetzugang beantragen und BMW stellt nur - über das Internet erreichbare - Anwendungen bereit. Die Kosten im Betrieb des Extranets können so erheblich gesenkt werden.

Mit dem Kriterienkatalog soll nun untersucht werden, inwieweit den funktionalen Anforderungen von BMW mit einer auf SSL basierenden VPN Lösung entsprochen wird.

7.2 Bewertung einer auf SSL basierenden VPN Lösung

Der in 6.3 vorgestellte, spezielle Kriterienkatalog wird nun zur Bewertung einer auf SSL basierenden VPN Lösung, mit dem Internet als Kommunikationsplattform, eingesetzt. Dabei wird in folgender Weise vorgegangen.

Vor jeder Hauptkriterienbewertung werden erst die hierfür erforderlichen Bewertungen der Teilkriterien nach den Vorgaben der Kriterienbeschreibung bestimmt. Im Anschluss daran wird die Bewertung des Wurzelkriteriums (Gesamtergebnis) berechnet. Letzteres stellt die funktionalen Merkmale einer SSL basierenden VPN Lösung dar.

Die Bewertungen der Hauptkriterien werden nach dem in 6.2.4 beschriebenen Verfahren berechnet. Die dargestellten Ergebnisse sind auf eine Nachkommastelle gerundet, Zwischenergebnisse gehen aber in der vollen Genauigkeit (15 Dezimalstellen) in die Berechnung ein.

I.I - Verwendung von privaten Adressen

Eine Adressierung im Internet anhand von privaten IP-Adressen ist nicht möglich.

C	sehr schlecht	−−	0

I.II - Weiterverwendung des bestehenden Adressschemas

Bei der Kommunikation über das Internet kann das bestehende Adressschema nicht weiterverwendet werden, da Adressierung mit privaten IP-Adressen nicht möglich ist.

B	sehr schlecht	−−	0

I.III - Interoperabilität mit Network Adress Translation

SSL operiert über der Schicht 4 des OSI-Schichtenmodells und beeinflusst deshalb NAT in keinster Weise. Ein Einsatz ist also problemlos möglich.

A	sehr gut	++	4

I - Adressierung

Kriterium	Gewicht	Bewertung
Adressierung		0,89
Verwendung von privaten IP-Adressen	4	0
Weiterverwendung des bestehenden Adressschemas	3	0
Interoperabilität mit Network Address Translation	2	4

Wie Einzelbewertungen der Basiskriterien zeigen, stellt nur die Interoperabilität mit NAT einen sehr gut erfüllten Punkt dar. Beim Einsatz von NAT werden Anpassungen der bestehenden Adressierung in hohem Maße notwendig.

II.I - Einbindung von IT Partnern Eine Partitionierung des mit SSL aufgebauten client-server VPNs ist nicht möglich. Allerdings können Händler und IT-Partner über das Internet kommunizieren, die Einbindung ist also möglich.

A	sehr gut	++	4

II.II - Möglicher Anstieg in der Anzahl von Teilnehmern

Der Anstieg der Teilnehmeranzahl wird durch Leistungsfähigkeit der Web-Server bestimmt. Für Internetzugänge besteht allerdings keine Beschränkung.

A	sehr gut	++	4

II.III - Unterstützte Topologien

SSL wird in der Regel zusammen mit Client-Server-Anwendungen eingesetzt. Die dabei verwendete Topologie kann gewissermaßen als Hub-and-Spoke verstanden werden. Andere Vermaschungsgrade sind nicht möglich.

B	mittel	∘	2

II.IV - 1-n Kommunikationsbeziehungen

Mit SSL geschützte Client-Server-Anmwendungen unterstützen nur 1-1 Kommunikationsbeziehungen.

B	sehr schlecht	−−	0

II - Kommunikationsbeziehungen

Kriterium	Gewicht	Bewertung
Kommunikationsbeziehungen		2,83
Einbindung von IT Partnern	3	4
Möglicher Anstieg in der Anzahl von Teilnehmern	4	4
Unterstützte Topologien	3	2
1-n Kommunikationsbeziehungen	2	0

Die Bewertungen der Teilkriterien zu diesem Hauptkriterium fallen überwiegend gut aus. Allerdings werden sogenannte *SSL Accelerator* erforderlich, will man einen Anstieg von Teilnehmern ermöglichen.

III.I - Unterstützte Zugangstechnologien

Da jeder Händler den Internetzugang frei wählen, sind die unterstützten Zugangstechnolgien nicht beschränkt.

A	sehr gut	++	4

III.II - Erhöhung der Bandbreite

Jeder Händler kann die Bandbreite im Zugangsbereich nach seinen Bedürfnissen erhöhen.

A	sehr gut	++	4

III - Anpassbarkeit

Kriterium	Gewicht	Bewertung
Anpassbarkeit		4
Unterstützte Zugangstechnologien	4	4
Erhöhung der Bandbreite	4	4

Bei der Verwendung des Internets als Kommunikationsplattform besteht ein hohes Maß an Anpassbarkeit, wie aus der Bewertung offensichlich wird.

IV.I - Vertraulichkeit der ausgetauschten Daten

SSL bietet Security Dienste, die in der bestehenden Lösung nicht vorhanden sind. Allerdings ist das Internet als potentiell unsicherer als ein Provider Backbone einzuschätzen

B	gut	+	3

IV.II - Zugriffskontrolle und Authentisierung

Durch die Verwendung der beidseitigen Authentisierung, zusammen mit einer Certification Authority kann ein vergleichbare Stärke an Authentifisierung und damit Zugriffskontrolle gewährleistet werden wie in der bestehenden Lösung.

B	gut	+	3

IV.III - Integrität der ausgetauschten Daten

Mit Hilfe des SSL-Handshake-Protokolls kann die Datenintegrität gewährleistet werden.

A	sehr gut	++	4

IV - Security

Kriterium	Gewicht	Bewertung
Security		3,27
Vertraulichkeit der ausgetauschten Daten	4	3
Zugriffskontrolle und Authentisierung	4	3
Datenintegrität	3	4

Von SSL zur Verfügung gestellte Security Dienste erweisen sich als ausreichend für die von BMW gestellten Anforderungen in diesem Bereich. Eine hohe Bewertung dieses Hauptkriteriums verdeutlicht dies.

V.I - Bandbreite

Bei der Kommunikation über das Internet können keine Bandbreitengarantien gegeben werden.

C	sehr schlecht	−−	0

V.II - Verfügbarkeit

Es können keine Verfügbarkeitsgarantien für eine inernetgestützte Kommunikation gegeben werden.

D	sehr schlecht	−−	0

V.III - Zuverlässigkeit

Garantien hinsichtlich der Garantie des internets sind nicht möglich. Zudem ist in der Regel die Paketfehlerrate höher als in einer Provider Netzinfrastruktur

C	sehr schlecht	−−	0

V - Quality of Service

Kriterium	Gewicht	Bewertung
Quality of Service		0
Bandbreite	4	0
Verfügbarkeit	4	0
Zuverlässigkeit	3	0

Zu Zeit sind keine Qualitätsgarantien für den Datentransport über das Internet möglich. Dementsprechend können derartige Bedürfnisse in keinster Weise erfüllt werden.

Wurzelkriterium - Funktionale Merkmale der VPN Lösung

Kriterium	Gewicht	Bewertung
Funktionale Merkmale der VPN Lösung		2,43
Adressierung	1	0,89
Kommunikationsbeziehungen	4	2,83
Anpassbarkeit	3	4
Security	3	3,27
Quality of Service	3	0

Das Gesamtergebnis fällt gut aus, was vor allem auf die sehr gute Anpassbarkeit des Internets zurückzuführen ist. Weiterhin erfüllen die von SSL gebotenen Security-Dienste BMW spezifische Anforderungen in diesem Bereich überdurchschnittlich. Allerdings werden durch den Einsatz von SSL weitreichende Veränderungen notwendig. Vor allem müssen alle bestehenden und zukünfitgen Anwendungen für den Einsatz von SSL angepasst werden.

7.3 Zusammenfassung der Bewertung

In diesem Kapitel wurde eine Anwendung des speziellen Kriterienkatalogs vorgenommen. Zunächst wurde, auf die Klassifizierung basierend, eine geeignete Lösungsklasse für BMW ausgewählt. Gemäß den Präferenzen von BMW wurde dann allerdings die als VPN alternative geltende Technologie SSL bewertet. Dabei zeigte sich, daß in dem Bereichen Security die BMW Anforderungen erfüllt wurden. Weiterhin besteht durch die Verwendung des Internets als Kommunikationsplattform eine hohes Maß an Anpassbarkeit. Allerdings können QoS Anforderungen in keinster Weise erfüllt werden. Darüberhinaus imacht SSL eine Modifikation aller Anwendungen erforderlich. Hier muss abgewogen werden, ob stragische Gründe ein höheres Gewicht als die funktionalen Anforderungen einnehmen.

Im nächsten Kapitel werden nochmal die Ergebnisse dieser Arbeit zusammengefasst.

Kapitel 8

Zusammenfassung und Ausblick

In der vorliegenden Diplomarbeit wurden Werkzeuge entwickelt, die in verschiedenen Phasen des Planungsprozesses eines VPNs unterstützend wirken.

Am Anfang dieses Prozesses steht die Analyse-Phase, in der das Ziel verfolgt wird, die spezifischen Anforderungen des Unternehmens zu bestimmen. Die mit der Analyse betraute Fachabteilung sieht sich dabei vor das Problem gestellt, dass die an eine VPN Lösung gestellten Anforderungen mit dem eingenommenen Standpunkt variieren. Beispielsweise sind für die Entwicklung von Anwendungen zuständige Abteilungen in der Regel eher an funktionalen Eigenschaften interessiert, während Entscheidungsträger eine betriebswirtschaftliche Sichtweise einnehmen. Eine weitere Fragestellung liefert der Grad der Eigenrealisierung eines VPNs und in diesem Zusammenhang die Auswahl eines geeigneten Dienstleisters.

An dieser Stelle ist ein strukturiertes Vorgehen angebracht, wobei die verschiedenen Interessenvetreter miteinbezogen werden müssen. Die in dieser Arbeit entwickelte, generelle Kriteriensammlung liefert hier entscheidende Ansatzpunkte und berücksichtigt gleichermaßen verschiedene Standpunkte bzw. Sichtweisen auf eine VPN Lösung. Die generellen Kriterien stellen dabei das Grundgerüst für eine systematische Bestimmung von spezifischen Anforderungen eines Unternehmens zur Verfügung. Dabei bleibt die generelle Kriteriensammlung nicht auf die Anwendung für VPNs beschränkt. Vor allem die für die Auswahl eines Diensleisters vorgestellten Kriterien können leicht auf andere Outsourcing-Szenarien übertragen werden.

Die Schnittstelle zu anderen Interessengemeinschaften kann durch Formulierung geeigneter Fragebögen geschaffen werden. Hier besteht ein Spielraum für zukünftige Arbeiten. Beispielsweise erfordert die Einbeziehung von Endbenutzern in den Analyse-Prozess eine Darstellung der technischen Eigenschaften in einer für sie geeigneten Form.

Den nächsten Abschnitt des Planungsprozesses stellt die Konzeptions-Phase dar. Hier gilt es unter anderem abzuwägen, welche VPN Lösung die individuellen Bedürfnisse des Unternehmens am Besten erfüllt. Voraussetzung dafür ist eine umfassende Kenntnis aller verfügbaren VPN Technologien respektive der inhärenten Eigenschaften. Allerdings ist die Auswahl in Frage kommender Technologien groß und die Betrachtung aller Kandidaten bringt einen erheblichen Zeitaufwand mit sich. An dieser Stelle setzt die in dieser Arbeit vorgenommene Klassifizierung an. Ausgehend von Anforderungen niedriger Granularität können Technologien ausgeschlossen bzw. in die Auswahl einbezogen werden und somit zu erheblicher Zeitersparnis führen.

Die Betrachtung von VPN Technologien nimmt eine wichtige Rolle in der Planung eines VPNs ein. Erschwerend wirkt sich in diesem Zusammenhang aus, dass die jeweiligen Beschreibungen in Form von RFCs oder Herstellerangaben keinem einheitlichen Schema in Bezug auf für den Einsatz in VPNs ausschlaggebende Eigenschaften folgen. Aus diesem Grunde wurde in dieser Arbeit eine Grundlage in Form von relevanten Merkmalen geschaffen, die eine strukturierte Betrachtung von Technologien unterstützen.

Im Zuge der Planung eines VPNs stellt die Entscheidungsfindung hinsichtlich der eingesetzten Lösung einen kritischen Punkt dar. Dieser Prozess soll möglichst durchsichtig und damit lesbar nachvollziehbar werden. Unterstützend wirkt hierbei der in dieser Arbeit entwickelte Kriterienkatalog. Durch Festlegung eines Berechnungsverfahrens wurde ein numerischer Vergleich von VPN Lösungen ermöglicht.

Eine konkrete Anwendung der entwickelten Werkzeuge wurde in dieser Arbeit anhand des BMW Extranets durchgeführt. Eine Anpassung der generellen Kriteriensammlung führte dabei zu einem speziellen Kriterienkatalog. Weiterhin wurden Vorschläge in Bezug auf in diesem Szenario geeignete Technologien anhand eines Vergleichs der BMW-spezifischen Anforderungen mit den in der Klassifizierung erarbeiteten Klassen erbracht. Eine Bewertung der von BMW favorisierten Technolgie wurden anschließend mit Hilfe des speziellen Kriterienkatalogs vorgenommen. Hierbei verdeutlichte sich der breite Anwendungsbereich der erarbeiteten Kriteriensammlung. Obwohl eine als VPN Alternative geltende Technologie für die Bewertung herangezogen wurde, konnten dennoch sinnvolle Ergebnisse erzielt werden.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[ABG+01] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan und G. Swallow. RFC 3209: RSVP-TE: Extensions to RSVP for LSP Tunnels. RFC, IETF, Dezember 2001.

[ADF+01] L. Andersson, P. Doolan, N. Feldman, A. Fredette und B. Thomas. RFC 3036: LDP Specification. RFC, IETF, Januar 2001.

[ALAS+02] J. Ash, Y. Lee, P. Ashwood-Smith, B. Jamoussi, D. Fedyk, D. Skalecki und L. Li. RFC 3214: LSP Modification Using CR-LDP. RFC, IETF, Januar 2002.

[And02] Loa Andersson. PPVPN L2 Framework. Internet Draft, IETF, Juni 2002.

[Böh02] Wolfgang Böhmer. *VPN Virtual Private Networks*. Hanser Verlag München Wien, 2002.

[Bre02] M. Brenner. Entwicklung eines Kriterienkatalogs zur Evaluierung des Anwender Supports in der BMW AG. Diplomarbeit, Ludwig-Maximilians-Universität München, Januar 2002.

[Cal02] Ross Callon. A Framework for Layer 3 Provider Provisioned Virtual Private Networks. Internet Draft, IETF, April 2002.

[Cle02] Jeremy De Clercq. Applicability Statement for Provider Provisioned CE-based Virtual Private Networks. Internet Draft, IETF, Juli 2002.

[CS98] Mike Erwin Charlie Scott, Paul Wolfe. *Virtual Private Networks*. O'Reilly & Associates, second. Auflage, 1998. ISBN 1565925297.

[FH98] Paul Ferguson und Geoff Huston. What is a VPN?, April 1998.

[FLH+00] D. Farinacci, T. Li, S. Hanks, D. Meyer und P. Traina. RFC 2784: Generic Routing Encapsulation (GRE). RFC, IETF, Marz 2000.

[Gie00] F. Giemsa. Evaluation von Outsourcing-Beziehungen für die IT-Hotline der BMW AG. Diplomarbeit, Ludwig-Maximilians-Universität München, November 2000.

[GK98] R. Glenn und S. Kent. RFC 2410: The NULL Encryption Algorithm and Its Use With IPsec. RFC, IETF, November 1998.

[GLH+00] B. Gleeson, A. Lin, J. Heinanen, G. Armitage und A. Malis. RFC 2764: A Framework for IP Based Virtual Private Networks. RFC, IETF, Februar 2000.

[HA93] H.-G. Hegering und S. Abeck. *Integriertes Netz– und Systemmanagement.* Addison–Wesley, 1993.

[HC98] D. Harkins und D. Carrel. RFC 2409: The Internet Key Exchange (IKE). RFC, IETF, November 1998.

[HPV+99] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little und G. Zorn. RFC 2637: Point-to-Point Tunneling Protocol. RFC, IETF, Juli 1999.

[ISO89] Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. IS 7498-2, International Organization for Standardization and International Electrotechnical Committee, 1989.

[JB02] Michael Swift John Brezak. The Microsoft Windows 2000 RC4-HMAC Kerberos encryption type. Internet Draft, IETF, Mai 2002.

[KA98a] S. Kent und R. Atkinson. RFC 2401: Security Architecture for the Internet Protocol. RFC, IETF, November 1998.

[KA98b] S. Kent und R. Atkinson. RFC 2402: IP Authentication Header. RFC, IETF, November 1998.

[Kos98] David Kosiur. *Building* $\frac{3}{4}$ *Managing Virtual Private Networks.* John Wiley & Sons, first. Auflage, 1998. ISBN 0471295264.

[Kos01] Dave Kosiur. VPNs: Types and Issues, October 2001.

[Lip01] Manfred Lipp. *VPN - Virtuelle Private Netzwerke.* Addison-Wesley, 2001.

[LLN] M. Langer, S. Loidl und M. Nerb. Customer Service Management: A more Transparent View to Your Subscribed Services.

[LS92] B. Lloyd und W. Simpson. RFC 1334: PPP Authentication Protocols. RFC, IETF, Oktober 1992.

[MD98] C. Madson und N. Doraswamy. RFC 2405: The ESP DES-CBC Cipher Algorithm With Explicit IV. RFC, IETF, November 1998.

[MG98a] C. Madson und R. Glenn. RFC 2403: The Use of HMAC-MD5-96 within ESP and AH. RFC, IETF, November 1998.

[MG98b] C. Madson und R. Glenn. RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH. RFC, IETF, November 1998.

[ML94a] Marben Michel Louis. Virtual Private Networks Vol.I, IBC VPN Services. Technical report, 1994.

[ML94b] Marben Michel Louis. Virtual Private Networks Vol.I, State of the Art. Technical report, 1994.

[Orm98] H. Orman. RFC 2412: The OAKLEY Key Determination Protocol. RFC, IETF, November 1998.

[PAD+01] B. Patel, B. Aboba, W. Dixon, G. Zorn und S. Booth. RFC 3193: Securing L2TP using IPsec. RFC, IETF, November 2001.

[PZ01] G. Pall und G. Zorn. RFC 3078: Microsoft Point-To-Point Encryption (MPPE) Protocol. RFC, IETF, Marz 2001.

[Rei97] Helmut Reiser. Sichere TCP/IP-basierte Kommunikation bei der BMW AG. Diplomarbeit, Fachbereich Informatik, Universität München, 1997.

[RMK+96] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot und E. Lear. RFC 1918: Address Allocation for Private Internets. RFC, IETF, Februar 1996.

[RR99] E. Rosen und Y. Rekhter. RFC 2547: BGP/MPLS VPNs. RFC, IETF, Marz 1999.

[RRSW97] C. Rigney, A. Rubens, W. Simpson und S. Willens. RFC 2138: Remote Authentication Dial In User Service (RADIUS). RFC, IETF, April 1997.

[RVC01] E. Rosen, A. Viswanathan und R. Callon. RFC 3031: Multiprotocol Label Switching Architecture. RFC, IETF, Januar 2001.

[Sch99] C. Scheiter. Erstellung eines Kriterienkatalogs zum Vergleich verschiedener Netzkonzepte für BMW und Rover. Diplomarbeit, Technische Universität München, August 1999.

[SE94] W. Simpson und Ed. RFC 1661: The Point-to-Point Protocol (PPP). RFC, IETF, Juli 1994.

[Ste98] R. Steinmetz. *Multimedia Technolgie*. Springer Verlag, 1998.

[Tan96] Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall International Editions, third. Auflage, 1996.

[TVR+99] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn und B. Palter. RFC 2661: Layer Two Tunneling Protocol L2TP. RFC, IETF, August 1999.

[VLK98] A. Valencia, M. Littlewood und T. Kolar. RFC 2341: Cisco Layer Two Forwarding (Protocol) LL2F“. RFC, IETF, Mai 1998.