Hauptseminar Wintersemester 2003/2004

Neue Ansätze im IT-Service-Management – Prozessorientierung (ITIL/eTOM)

Einführung – Referenzszenario

Auszug aus:

Sailer, M., Klassifizierung und Bewertung von VPN–Lösungen für die Neuausrichtung der europaweiten Extranetstrategie der BMW AG, Diplomarbeit, Technische Universität München, August, 2002.

Lehr- und Forschungseinheit für
Kommunikationssysteme und Systemprogrammierung

Ludwig-Maximilians-Universität München

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.

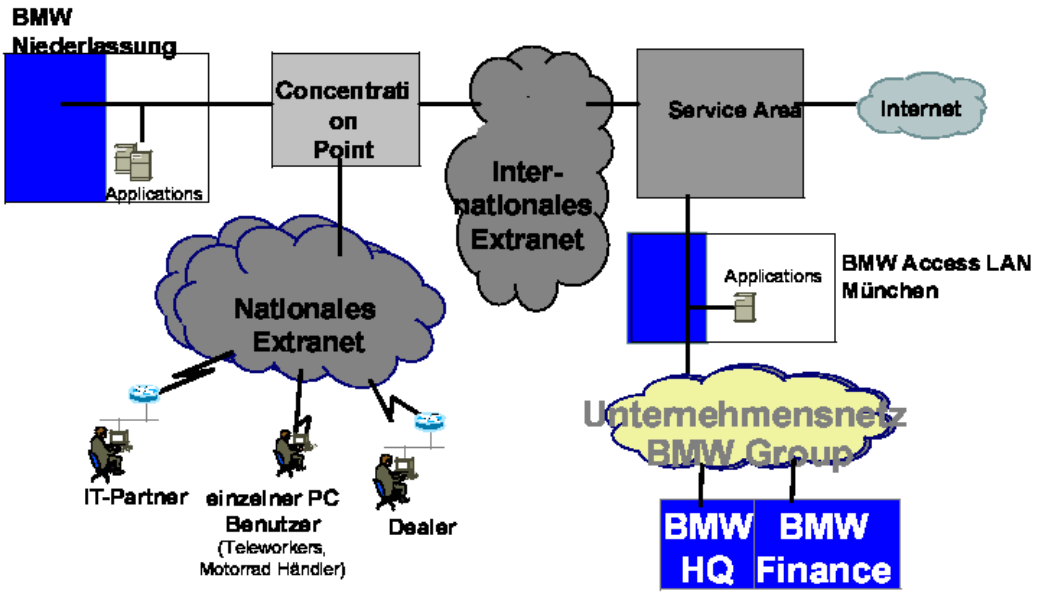

Abbildung 1.3: Die Stuktur des BMW Extranets - Anwendungen, Dienste und Teilnehmer

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.

Hauptseminar Wintersemester 2003/2004

Neue Ansätze im IT-Service-Management – Prozessorientierung (ITIL/eTOM)

Einführung – Referenzszenario

Auszug aus:

Reiser, H., Sicherheitsarchitektur für ein Managementsystem auf der Basis Mobiler Agenten, Dissertation, Ludwig–Maximilians–Universität München, Dezember, 2001.

Lehr- und Forschungseinheit für
Kommunikationssysteme und Systemprogrammierung

Ludwig-Maximilians-Universität München

kommunikation der nächsten Generation (UMTS) hat die Idee der kontextsensitiven Systeme zentrale Bedeutung.

Aber auch im produzierenden Gewerbe, z.B. zur Steuerung und Optimierung von Produktionsprozessen [SuBu 01] oder zur Ferndiagnose und Fernüberwachung von Automatisierungssystemen [PlWe 01] finden Mobile Agenten Verwendung.

Daneben werden sie auch in Zulieferer– oder Händlerketten eingesetzt, um Supply–Chain–Management zu betreiben. Wertschöpfungsnetzwerke oder –ketten (**Supply Chains**) werden aus Entitäten gebildet, die für die Beschaffung von Rohstoffen, deren Transformation in Halbfertig– und Fertigprodukte sowie die Verteilung dieser Produkte zuständig sind. Das Supply Chain Management umfasst den kompletten Wertschöpfungsprozess [GSWA 01], der sich durch Mobile Agenten abbilden und unterstützen lässt.

2.2 Szenarios für das Management mit Hilfe von Mobilen Agenten

Der Fokus dieser Arbeit soll auf Mobilen Agenten liegen, die im IT–Management eingesetzt werden. Dieser Abschnitt beschreibt einige Szenarios aus der Praxis, die einerseits die Anwendung von Mobilen Agenten im IT–Management aufzeigen, andererseits aber auch Sicherheitsprobleme, die sich durch ihren Einsatz ergeben, verdeutlichen.

2.2.1 Dienst– und QoS–Management in Customer–Provider Hierarchien

Durch die zunehmende Komplexität von Diensten und IT–Infrastrukturen sowie aufgrund deren räumlicher Verteilung ist es für ein Unternehmen unerlässlich, Netzinfrastrukturen oder Dienste von einem Provider zu kaufen oder zu mieten. Dies gilt auch für Unternehmen, die selbst wieder als IT–Dienstleister auftreten und **Mehrwertdienste (value added services)** an ihre Kunden weiterverkaufen. Dadurch entstehen Kunden–Dienstleister Hierarchien (Customer–Provider Hierarchies) bzw. **Multiprovider Hierarchien**. In einer solchen Hierarchie tritt ein Unternehmen in verschiedenen Rollen auf. Einerseits in der Rolle des Kunden, der Dienste von einem Provider einkauft, andererseits aber auch in der Rolle des Providers, der Mehrwertdienste an eigene Kunden weiterverkauft.

Ein Dienstleister geht dabei mit seinem Kunden **Dienstgütevereinbarungen** (**Service Level Agreements (SLA)**)[Schm 01] ein, deren Erfüllung bzw. Einhaltung er vertraglich zusichert. In diesen SLAs werden für jeden Dienst Qualitätseigenschaften festgelegt, die in ihrer Gesamtheit die Dienstgüte, auch

Problem: Überwachung des QoS in Multiprovider Hierarchien

als **Quality of Service (QoS)** bezeichnet, ausmachen.Dazu ist es notwendig Kennzahlen für die QoS–Parameter und unter Umständen auch Messverfahren zu deren Bestimmung in den SLAs festzulegen. Werden SLAs verletzt, weil die vereinbarten QoS–Parameter nicht eingehalten werden, so sind vom Dienstleister i.d.R. Strafen zu bezahlen oder Nachlässe zu gewähren. Es ist klar, dass die Erfüllung der Dienstgütevereinbarung für einen Provider auch unmittelbar von der Dienstgüte der, von eigenen Zulieferern, eingekauften Dienste abhängt.

Neben der vertraglichen Gestaltung und den rechtlichen Problemen beim Abschluss von SLAs besteht auch das Problem der Überwachung der QoS–Parameter und der Beweis– bzw. Nachweispflicht bei der Verletzung der SLA. Um diese Problematik zu verdeutlichen soll im Folgenden ein exemplarisches Szenario vorgestellt werden, das im Rahmen diverser Forschungskooperationen mit IT–Dienstleistern und großen Netzbetreibern (*DeTeSystem, Siemens, Bayerische Motorenwerke AG*) untersucht wurde [HaRe 99, Hojn 99, Knoe 99].

Szenario: Extranet – Anbindung von Partnerunternehmen

Die BMW AG betreibt **Intranets**, d.h. firmeneigene, „interne“, abgeschlossene Netze, die auf den Internetprotokollen basieren. Damit werden Systeme in verschiedenen Standorten oder innerhalb von Standorten und Abteilungen miteinander verbunden und abteilungs– und standortübergreifende Dienste zur Verfügung gestellt (vgl. z.B. [Albe 98]). Um die Vorteile und Marktchancen von E–Commerce nutzen zu können, sollten im Bereich **Business to Business Commerce (B2B)**, d.h. im Bereich der Geschäftsbeziehungen zwischen eigenständigen Unternehmen [Merz 99], Kompetenzen aufgebaut und Lösungen realisiert werden. Inspiriert von der *Automotive Network eXchange (ANX)* Initiative amerikanischer Kfz–Hersteller (genauer der *Automotive Industrie Action Group [AIAG]*) sollten bestimmte Dienste und Netzinfrastrukturen aus den BMW Intranets auch für Händler, Zulieferer und IT–Partner zur Verfügung gestellt werden, um die Geschäftsprozesse mit diesen Partnerunternehmen zu vereinfachen und zu beschleunigen. So sollte bspw. Händlern die Möglichkeit gegeben werden, Autos online zu bestellen und zu konfigurieren. Die Partnerunternehmen bilden ein so genanntes **Extranet**, d.h. ein „externes“ Netzwerk, für eine abgeschlossene Benutzergruppe außerhalb von BMW. Die verschiedenen Intra– und Extranets zusammen bilden das weltweite BMW Unternehmensnetz, das auch als **Corporate Network (CN)** bezeichnet wird.

Abbildung 2.1 zeigt die Realisierung des Händler–Extranets. Die Netzinfrastruktur für die Verbindung der mehr als 1000 Händler wurde (in Deutschland) von der DeTeSystem realisiert. Die Händler werden entweder über Standleitungen oder ISDN–Wählleitungen mit einem *Point–of–Presence (POP)* verbunden. Sie bilden auf der Infrastruktur der DeTeSystem, bzw. der Telekom die auch von anderen Kunden der DeTeSystem und der Telekom genutzt wird, ein **virtuelles privates Netz (VPN)**. Daneben werden auch Dienste wie z.B. DNS, Mail, Authentisierung oder ein Konfigurationsdienst für die Händler von der DeTeSystem realisiert. Dazu wurde eine Service Area eingerichtet, in der diese Dienste erbracht werden können. In dieser Service

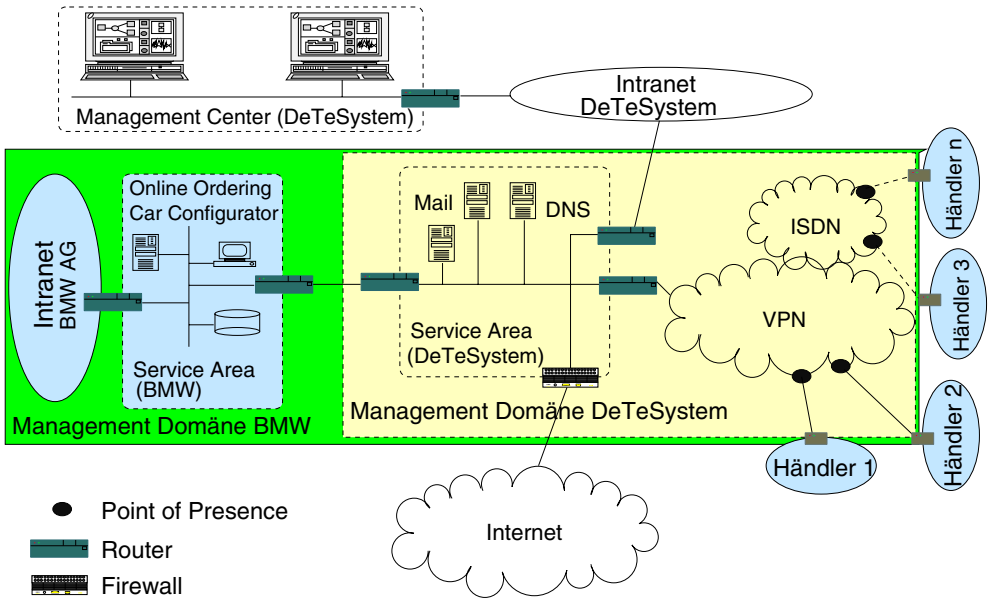

Abbildung 2.1: Extranet Szenario

Area wird dem Händler auch ein wohldefinierter und gesicherter Zugangspunkt zum Internet bereit gestellt. Die beschriebenen Infrastrukturen mit den Diensten müssen von der DeTeSystem, als Extranet–Provider, implementiert werden. Daneben muss sie auch das Management für alle von ihr realisierten Dienste und Komponenten — über die Domänengrenzen hinweg — erbringen.

Die Dienste, die den Händlern von BMW zur Verfügung gestellt werden, werden durch Server in einer eigenen Service Area bei BMW erbracht. Das Management der BMW–Dienste und der BMW Service Area obliegt BMW.

Ein Händler, der die *Online Ordering* Applikation nutzen will, wählt sich bei seinem PoP ein und wird über das VPN und die Service Area der DeTeSystem zu dem Server in der Service Area von BMW geroutet.

Die Händler kaufen alle ihre Dienste bei BMW ein, das bedeutet, dass BMW gegenüber dem einzelnen Händler als Provider, auch für die von der DeTeSystem erbrachten Dienste, auftritt. Die Dienstgüte wird also zwischen dem jeweiligen Händler und BMW vertraglich vereinbart. Können die vereinbarten QoS–Parameter (z.B. Erreichbarkeit, Antwortzeit, Durchsatz u.a.) nicht eingehalten werden, so erhält der Händler von BMW Rabatte auf seine abonnierten Dienste. BMW selbst hat wiederum eine Dienstgütevereinbarung mit der DeTeSystem abgeschlossen, die Konventionalstrafen bei einer Verletzung der SLAs vorsieht. Abbildung 2.2 zeigt einen Ausschnitt aus dieser Multiprovider Hierarchie unter vertraglichen und organisatorischen Gesichtspunkten. Neben der rein vertraglichen Beziehung, d.h. wer schließt mit wem eine Dienstgütevereinbarung, zeigt die Abbildung auch, von wem die Dienste erbracht bzw. administriert werden. Dabei zeigt sich, dass viele Dienste erst durch das Zusammenwirken mehrer Organisationseinheiten erbracht und ver-

SLAs zwischen zwei Vertragspartnern; Diensterbringung über Providergrenzen hinweg

waltet werden können. Der DNS–Dienst wird z.B. technisch von der DeTeSystem erbracht. BMW muss aber die Informationen, die zur Konfiguration des Dienstes benötigt werden (z.B. Adressschemata), zur Verfügung stellen und laufend aktualisieren. Es wird deutlich, dass ein Kunde, der ein SLA mit seinem Provider schließt, nicht erkennen kann, wer die vereinbarten Dienste tatsächlich erbringt. Je komplexer der Dienst ist, umso mehr „Zuliefer–Dienste“ sind darin enthalten, d.h. ein komplexer Dienst kann oft nur verteilt und über Providergrenzen hinweg, erbracht werden.

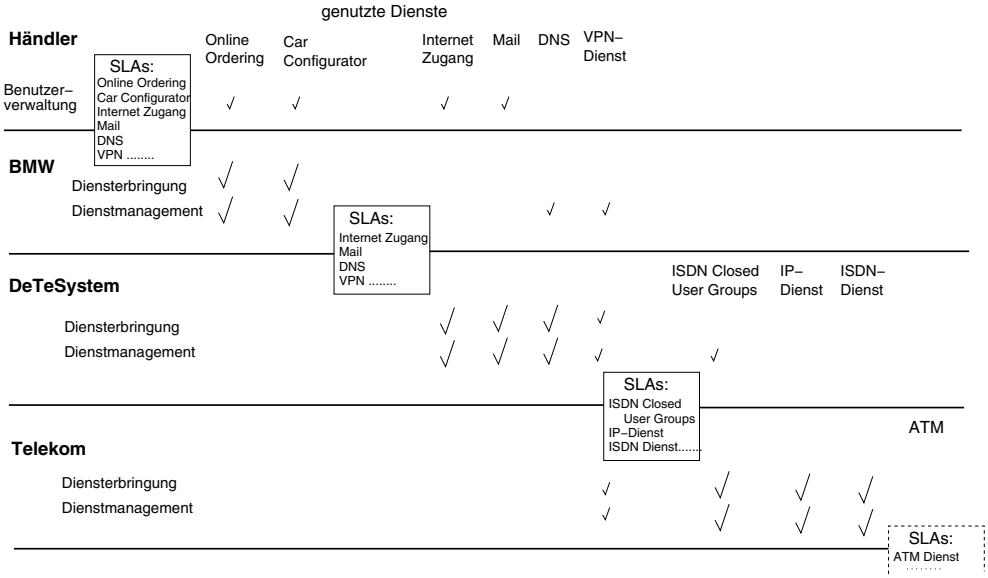

Abbildung 2.2: Multiprovider Hierarchie – Dienstgütevereinbarung und Diensterbringung

Dienstgüte definiert aus Sicht des Kunden

Bei der Überwachung der QoS Parameter in solchen Multiprovider Hierarchien treten sowohl technische als auch organisatorische Probleme auf. Falls eine SLA–Verletzung bzw. die Nichteinhaltung eines QoS–Parameters vorliegt, ist es nicht trivial, den Verantwortlichen dafür zu bestimmen. Im Folgenden sei angenommen, dass mit einem Händler eine SLA vereinbart wurde, in der ihm eine Erreichbarkeit der Online Ordering Applikation von 100 % zwischen 8^{00} und 18^{00} Uhr zugesichert wurde. Falls er den Dienst nutzen will, aber nicht erreichen kann, erhält er bestimmte Rabatte, d.h. der Regressfall tritt nur ein, falls der Händler auch versucht, den Dienst zu nutzen. Falls er den Dienst nicht erreicht, so kann dies viele Ursachen haben. Falls die Server oder Vermittlungsrechner in der Service Area von BMW nicht funktionieren, liegt die Verantwortung bei BMW. Es könnte aber auch sein, dass Komponenten oder Dienste der DeTeSystem ausgefallen sind oder der PoP nicht funktioniert und deshalb nur die Händler, die über diesen PoP angeschlossen sind, den Dienst nicht nutzen können. Das Problem kann aber auch vom Händler selbst zu verantworten sein, wenn es z.B. durch einen Fehler in seinem lokalen Netz verursacht wird.

Der Händler wird bei einer Verletzung der ihm zugesicherten Dienstgüte immer eine Erstattung und unter Umständen sogar Konventionalstrafen von

BMW verlangen. Falls die Ursache der SLA–Verletzung jedoch bei der DeTeSystem liegt wird BMW die DeTeSystem und diese ggf. wiederum die Telekom, in Regress nehmen. Für das Dienst– und QoS–Management bedeutet dies, dass Mechanismen notwendig sind, um die Einhaltung der QoS–Parameter zu überwachen und eine Zuweisung der Verantwortlichkeit bei deren Verletzung zu ermöglichen.

Die Dienstgüte wird im Beispielfall aus Kundensicht definiert, d.h. nur wenn der Kunde versucht einen Dienst zu nutzen, kann eine Verletzung der SLAs auftreten. Fällt ein Dienst aus und versucht keiner der Händler diesen zu nutzen, wird auch kein Regressanspruch entstehen. Viele QoS–Parameter lassen sich also nur „aus der Sicht“ des Händlers bestimmen. Aus diesen Gründen muss der QoS von jedem einzelnen Händler aus überwacht werden. Dies bedeutet, dass Funktionalität des BMW– bzw. des DeTeSystem–Managementsystems auf die Kundenseite delegierbar sein muss, um dort zur Ausführung gebracht zu werden. Für den Fall, dass eine Verletzung von QoS–Parametern vorliegt, ist es denkbar, geeignete Diagnosefunktionen nachzuladen, um den Verursacher zu ermitteln (vgl. auch [HaRe 00]).

QoS nur aus Händlersicht zu bestimmen

In dem angegebenen Szenario kommt erschwerend hinzu, dass individuelle Vereinbarungen mit jedem Händler (selbstständiges Unternehmen) möglich sein müssen. Die zu überwachenden QoS–Parameter unterliegen auch häufigen Änderungen, es genügt also nicht, beim Anschluss eines neuen Händlers, einen Management Agenten (im traditionellen Sinn) auf dem Rechner des Händlers zu installieren, da bei einer Änderung der SLAs dann bei jedem betroffenen Händler ein neuer Agent installiert werden müsste.

Eine Lösung dieser Probleme stellen Mobile Agenten dar. Im angegebenen Szenario muss dazu einmalig eine Ausführungsplattform für Mobile Agenten auf Seiten des Händlers installiert werden. Die Funktionen zur Überwachung der QoS–Parameter können dann individuell für jeden Händler in Form eines Mobilen Agenten implementiert und von BMW und/oder der DeTeSystem auf das System des Händlers migriert werden. Bei einer Veränderung der SLA kann der Mobile Agent entweder sehr einfach durch einen neuen mit geänderter Funktionalität ersetzt werden oder der Mobile Agent kann dynamisch neue Funktionen nachladen, um den geänderten Anforderungen gerecht werden zu können. Der Mobile Agent misst aus der Sicht des jeweiligen Händlers dessen tatsächliche QoS–Parameter. Sollten Verletzungen der SLAs erkannt werden, kann der Agent Diagnosefunktionen ausführen, um den Verursacher für die Verletzung und damit den Regresspflichtigen zu ermitteln.

Mobile Agenten überschreiten Organisationsgrenzen

Da es in Fällen von Verletzungen von SLAs um hohe Schadenssummen geht, ist sowohl die Überwachung der QoS–Parameter als auch die Beweislast von erheblicher wirtschaftlicher Relevanz für alle Beteiligten. Dies bedeutet, dass neben BMW auch die DeTeSystem ein Interesse daran hat, die QoS von Händlerseite aus zu überwachen.

erhebliche wirtschaftliche Relevanz wegen hoher Schadenssummen

Für den Händler bedeutet dies, dass auf seinem System Software von mehreren „fremden“ Firmen, in Form von Mobilen Agenten, ausgeführt wird. Damit der Händler überhaupt bereit ist dies zuzulassen, müssen höchste Sicherheits-

Sicherheitsanforderungen des Händlers

standards eingehalten werden. Der Händler muss beispielsweise kontrollieren können auf welche Informationen und Ressourcen der Mobile Agent zugreifen darf (Zugriffskontrolle). Diese Zugriffe und Aktionen des Mobilen Agenten möchte er aus Gründen der Beweissicherung auch verbindlich protokollieren (Auditing) und später auch justitiabel belegen können (Verbindlichkeit). Er will vermeiden, dass mit Hilfe eines Mobilen Agenten vertrauliche Informationen aus seinem internen Netz ausgespäht werden (Vertraulichkeit) oder die Verfügbarkeit seiner Systeme durch den Mobilen Agenten eingeschränkt wird. Er muss sicherstellen können, dass der Mobile Agent von einer vertrauenswürdigen Quelle auf sein System migriert wurde (Authentisierung der Quelle).

Sicherheitsanforderungen der Provider

Auf der anderen Seite hat auch derjenige, der einen Mobilen Agenten migriert, Anforderungen an die Sicherheit. Im Folgenden seien nur einige dieser Anforderungen exemplarisch angegeben. Grundsätzlich muss sich derjenige, der einen Mobilen Agenten migriert, auf die Daten, die der Mobile Agent zurückliefert, verlassen können. Er muss sicherstellen können, dass der Mobile Agent korrekt ausgeführt wird und dass der Mobile Agent bzw. die Daten, die er liefert, nicht manipuliert wurden (Integrität, Verbindlichkeit).

Im Beispielszenario zahlt es sich potentiell für jeden Beteiligten aus, eine geschickte Manipulation der Daten in seinem Sinne durchzuführen. Der Händler könnte durch geeignete Veränderung des Mobilen Agenten erreichen, dass er unberechtigterweise Rabatte erhält oder Einnahmen durch Konventionalstrafen erzielt. Ein Provider aus der Multiprovider Hierarchie könnte durch geschickte Manipulationen von seiner Verantwortung für eine von ihm verursachte Verletzung der Dienstgütevereinbarung ablenken. Unter Umständen könnte die Manipulation auch dazu führen, dass ein anderer Provider in der Hierarchie als Schuldiger erscheint und sich daher mit Regressforderungen konfrontiert sieht. Alle beteiligten Organisationen wollen und müssen die Nutzung ihrer Hard– und Software–Komponenten kontrollieren und ggf. auch beschränken können (Ressourcen Beschränkung).

Aus diesem Szenario lassen sich im Vorgriff auf Abschnitt 2.6, folgende konkrete Sicherheitsanforderungen an ein Managementsystem ableiten:

- Zugriffskontrolle
- Auditing
- Verfügbarkeit
- Integrität
- Verbindlichkeit
- Vertraulichkeit
- Authentisierung
- Ressourcen Beschränkung

2.2.2 Management und Betrieb von Mobilfunknetzen

Mit der dritten Generation der Mobilfunktechnik — in Europa realisiert durch das **Universal Mobile Telecommunications System (UMTS)** — sollen eine Vielzahl verschiedenster Dienste angeboten und verschiedenste Netztechnologien unterstützt werden. Das Hauptziel von UMTS ist es, einem nomadischen Benutzer einen unbeschränkten Zugang zu einer großen Zahl unterschiedlicher und auch personalisierter Dienste zu gewähren. Dabei sollen so-

Hauptseminar Wintersemester 2003/2004

Neue Ansätze im IT-Service-Management – Prozessorientierung (ITIL/eTOM)

Einführung – Referenzszenario

Auszug aus:

Schmidt, H., Entwurf von Service Level Agreements auf der Basis von Dienstprozessen, Dissertation, Ludwig–Maximilians–Universität München, Juli, 2001.

Lehr- und Forschungseinheit für
Kommunikationssysteme und Systemprogrammierung

Ludwig-Maximilians-Universität München

2.3 Dienstszenario

Zur Erläuterung und als durchgängiges Beispiel für die ganze Arbeit wird in diesem Abschnitt ein *Szenario* eingeführt. Es basiert auf einem realen Dienst, der von der BMW AG bei der Firma DeTeSystem, inzwischen in T-Systems aufgegangen, bezieht. Dabei handelt es sich um ein Extranet, das von BMW für seine Händler und Zulieferer geschaffen wurde, um die Geschäftsprozesse mit diesen zu optimieren. Dieser Dienst wurde in folgenden Arbeiten analysiert: [HaRe 99], [Hojn 99], [Knoe 99], [Sche99b], [Schm 97]. Das hier vorgestellte generische Szenario ist von diesem Dienst abgeleitet und so erweitert, daß sich alle Aspekte des in dieser Arbeit präsentierten Ansatzes damit erklären lassen.

Das Bild 2.10 zeigt die beteiligten Organisationen in der hierarchischen Schichtung, die sich durch vertraglichen Bindungen ergibt. Der *Händler* schließt eine Dienstvereinbarung mit der Firma über die Anbindung an die Firma. Die *Firma* stützt sich bei der Erbringung des Dienstes auf den Extranet-Dienst ab, über den sie eine Dienstvereinbarung mit dem Dienstanbieter abschließt. Der *Dienstanbieter* erbringt einen Teil der Dienstleistung als Eigenleistung, schließt aber für die Konnektivität in Form eines IP-VPNs wiederum eine Dienstvereinbarung mit einem *Konnektivitätsanbieter* ab.

Der Fokus liegt in allen nicht auf die Dienstleisterhierarchie bezogenen Beispielen in dieser Arbeit auf dem Extranet-Dienst, der u.a. in [Miku 00] analysiert wurde. Damit ist die Rollenverteilung, wenn nicht anders angegeben, folgendermaßen: Der Händler ist der Nutzer des Dienstes, die Firma ist der Kunde, der Dienstanbieter nimmt die Rolle Dienstleister ein und der Konnektivitätsanbieter tritt in der Rolle Lieferant auf.

Der *Extranet-Dienst* ist vereinfacht in Bild 2.11 mit Hilfe des Dienstmodells modelliert. Dabei werden die Elemente und der Zusammenhang der einzelnen Elemente des Dienstes deutlich. Die informelle Spezifikation der Funktionalität und der Realisierung ist in Bild 2.12 dargestellt. Die Händler werden über einen Point of Presence (PoP) des Lieferanten an das IP-VPN des Lieferanten angebunden. Der Händler muß dazu mindestens einen Computer besitzen, der in der Lage ist, die von der Firma und dem Dienstanbieter bereitgestellten Dienste zu nutzen, und der in der Lage ist, die Schnittstelle des PoPs zu bedienen.

Die Firma ist ebenfalls über einen PoP an das IP-VPN des Lieferanten angebunden. Sie betreibt eine Server-Farm, die den Produkt-Server für die Händler bereitstellt, um Online Bestellungen für Produkte aufzugeben und diese Produkte zu konfektionieren. Zusätzlich ist in der Server-Farm ein Managementsystem enthalten, das für das Management der Eigenleistung und die Überwachung des Dienstanbieters benötigt wird.

Der Dienstanbieter ist auch über einen PoP an das IP-VPN angebunden. In seiner Server-Farm sind die Mail-Server, DNS-Server, Web-Proxy und ein WWW-Server, der zum Management des Dienstes benötigt wird, vorhanden. Zusätzlich gibt es eine interne Firewall, die für die Sicherheit der unterschiedlichen Organisationen alle Kommunikation innerhalb des IP-VPNs filtert. D.h. alle IP-Pakete, egal ob sie von einem Händler oder von der Firma stammen, werden von der Firewall geprüft und ggf. verworfen. Insbesondere wird damit die direkte Kommunikation der Händler untereinander unterbunden, um gegenseitige Störungen zu verhindern. Eine wei-

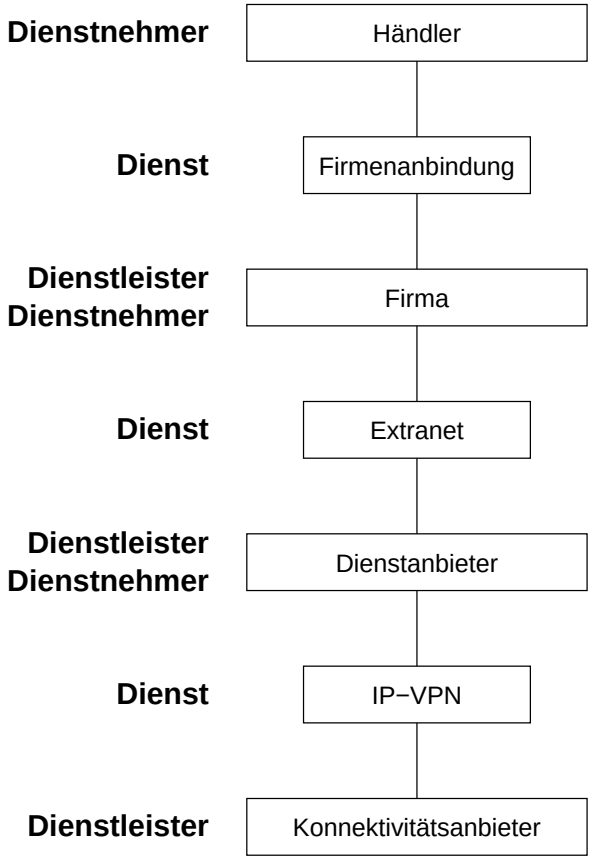

Bild 2.10: Dienstleisterhierarchie im Szenario

tere Firewall sorgt für eine sichere Anbindung an das Internet. Diese Internet-Anbindung wird ausschließlich von den Händlern genutzt. Auch in der Server-Farm des Dienstanbieters ist ein Managementsystem enthalten, das die Eigenleistung überwacht und steuert sowie das IP-VPN des Konnektivitätsanbieters überwacht.

Der Konnektivitätsanbieter ist für das IP-VPN zuständig, das er mit Hilfe eines Managementsystems überwacht und steuert.

Die in Bild 2.12 grau dargestellten Elemente des Dienstes tauchen nicht in der Dienstvereinbarung auf, sind aber für die Realisierung des Dienstes notwendig. Eine beispielhafte Dienstvereinbarung für den Dienst ist in Anhang A.1 zu finden.

Die komplexen Zusammenhänge aus Eigenleistung sowie zugekauften Leistungen erfordern ein Dienstmanagement, das in der Lage ist, über den Zustand des Dienstes ebenso Auskunft zu geben wie im Fall einer Störung bei der Identifikation des Fehlers zu helfen und die Zuordnung zu einer Organisation sicherzustellen. Die Folge daraus ist, daß insbesondere in einer Dienstleisterhierarchie Managementfunktionalität für einen zugekauften Dienst unabdingbare Voraussetzung ist, um den Dienst mit einer Eigenleistung integrieren und als Mehrwertdienst verkaufen zu können.

In diesem Szenario wird auch deutlich, daß sich Dienstausfälle fatal auswirken können. Wenn der

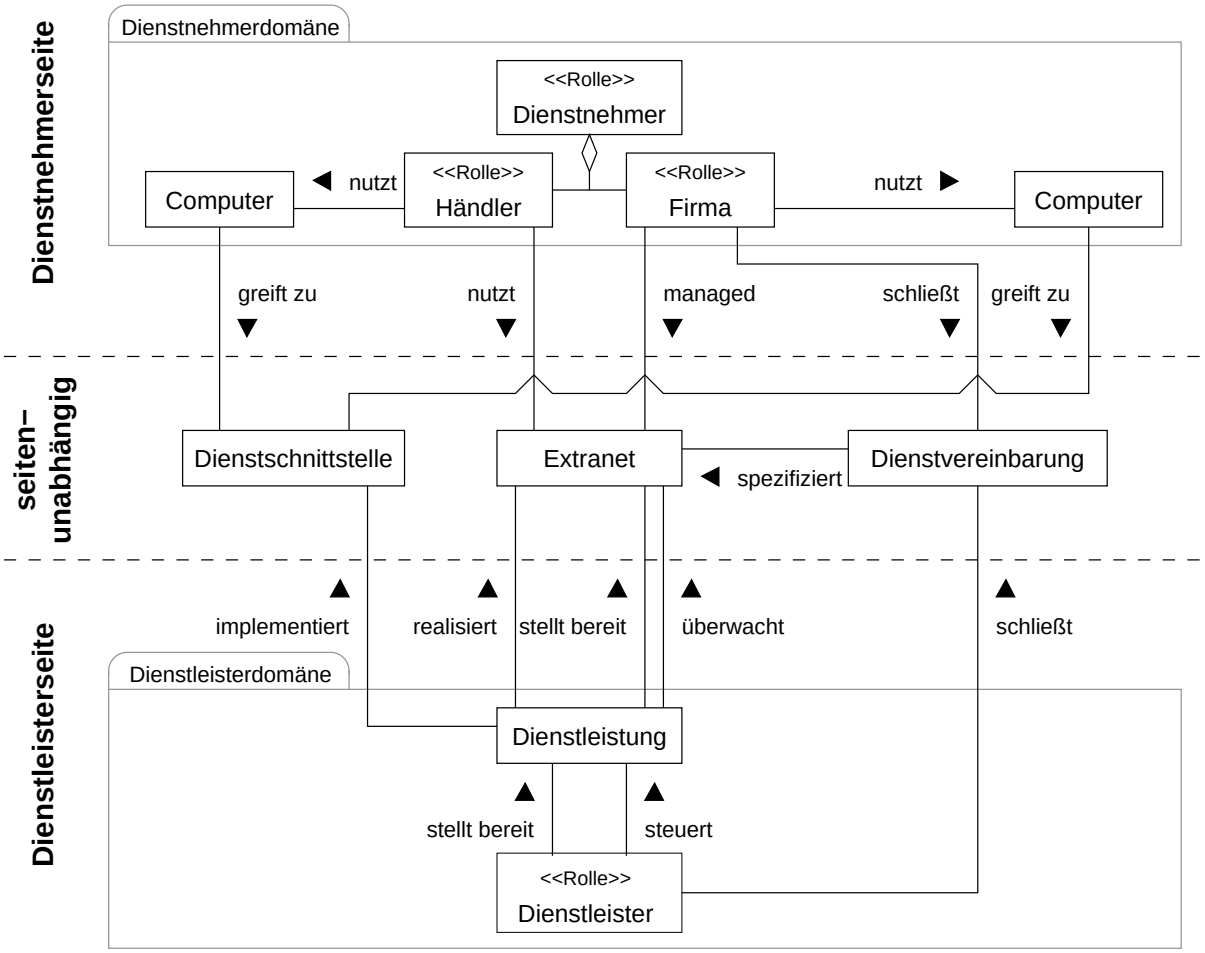

Bild 2.11: Szenariomodell

Extranet-Dienst nicht funktioniert sind die Händler nicht in der Lage die Produkte der Firma zu verkaufen, was zu erheblichen Verlusten führt, die die Kosten des Dienstes u.U. erheblich übersteigen. Deshalb kann bei solchen Diensten nicht auf Garantien verzichtet werden, die sich dann in der Realisierung des Dienstes durch entsprechende Maßnahmen zum Schutz vor Ausfällen, wie z.B. Redundanz, Reservesysteme und umfangreicherer Personalausstattung niederschlagen müssen.

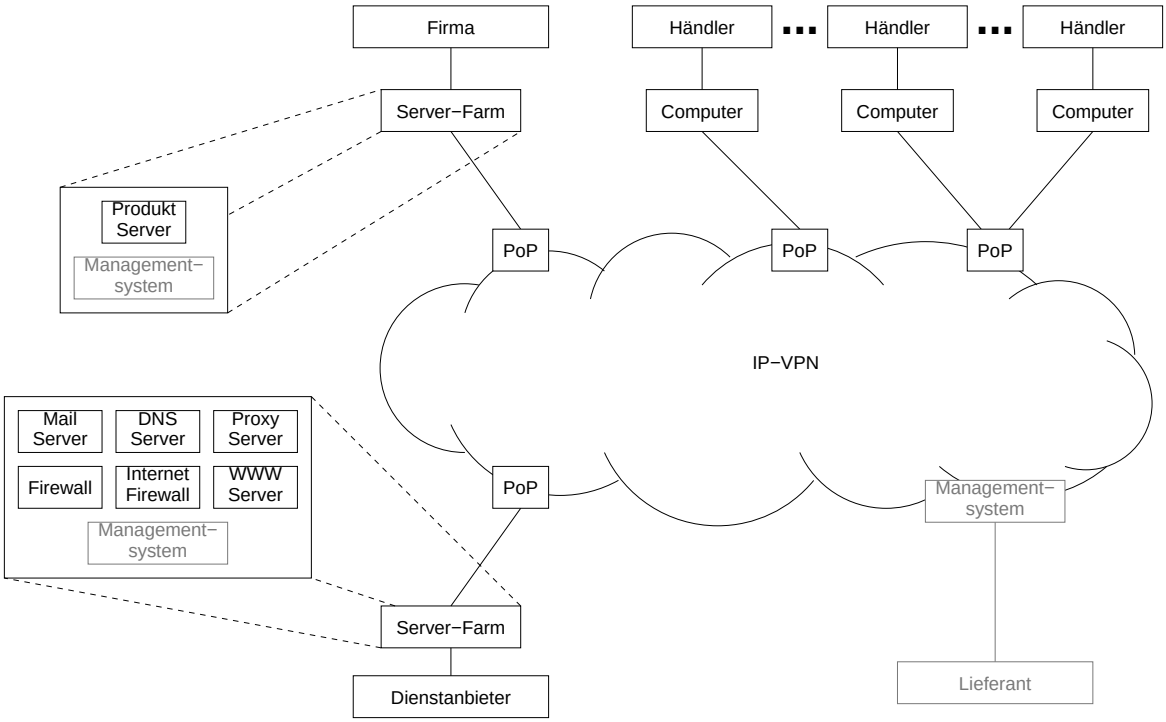

Bild 2.12: Extranet-Dienst

Hauptseminar Wintersemester 2003/2004

Neue Ansätze im IT-Service-Management – Prozessorientierung (ITIL/eTOM)

Einführung – Referenzszenario

Auszug aus:

Hojnacki, M., Einsatz des Java Dynamic Management Kit (JDMK) zur Antwortzeitüberwachung bei der DeTeSystem , Diplomarbeit, Technische Universität München, Mai, 1999.

Lehr- und Forschungseinheit für
Kommunikationssysteme und Systemprogrammierung

Ludwig-Maximilians-Universität München

zentral wichtige Dienste zur Bewältigung von Managementaufgaben bereitgestellt. Dazu gehören z.B. das Service Level Management (SLM), das Trouble Ticket System (TTS) und die Alarmintegration (PMA-ALI).
Die Management Applikationen laufen auf eigenen Servern im SRZ. Sie werden auch als Element Management System (EMS) bezeichnet.
Das Netzmanagement an sich wird jedoch in den einzelnen SMCs betrieben, wo über Konsolen der Zugriff auf die jeweiligen Management Applikationen ermöglicht wird.
Aufbauend auf dieser Infrastruktur ergibt sich nun das Anwendungsszenario dieser Diplomarbeit.

2.1.2 Anwendungsszenario

Obwohl die Realisierungen der Kundenlösungen sich von Fall zu Fall unterscheiden, können doch Parallelen festgestellt werden. Die für diese Arbeit entscheidenden Gemeinsamkeiten werden im folgenden am Beispiel eines Fahrzeugherstellers dargestellt.
Kern des Anwendungsszenarios stellt ein Fahrzeughersteller dar, der ein eigenes Rechenzentrum betreibt, um Händlern die Möglichkeit des Online–Ordering anzubieten. Diese Händler treten dem Fahrzeughersteller gegenüber wiederum als Kunden auf, da sie dieses Online–Ordering gegen Gebühr nutzen.
Die DeTeSystem realisiert und betreibt im Auftrag des Fahrzeugherstellers das dazu notwendige Computernetzwerk.
Die in Abbildung 2.2 modellhaft dargestellte Netzwerktopologie besteht aus folgenden Komponenten:

- **Virtual Private Network**
  Im Auftrag des Kunden betreibt die DTS das Extranet des Fahrzeugherstellers. Dieses Netz dient der Kommunikation im Weitverkehrsbereich und kann zum Beispiel auf der Grundlage der T-InterConnect Plattform der Deutschen Telekom AG basieren. Die Datenströme des Virtuellen Privaten Netzes (VPN) des Fahrzeugherstellers werden logisch von den Datenströmen der anderen Benutzer dieses Netzes getrennt. Diese Trennung wird durch den Einsatz der Tunneling Technik auf IP-Ebene in den aktiven Netzelementen (Routern) der Plattform erreicht.
  Der Zugang zu diesem Netz ist entweder über Standleitungen oder via ISDN möglich. Durch Zugangspunkte, sogenannte Points of Presence (PoP), wird eine Einwahlmöglichkeit angeboten. Die Authentifizierung der Benutzer erfolgt über die ISDN-Rufnummer und einen Kennwort, das mittels Challenge Handshake Protocol (CHAP) übertragen und geprüft wird.

- **Händler**
  Die Händler habe die Möglichkeit, über das Weitverkehrsnetz auf die vom Fahrzeughersteller angebotenen Dienste (z.B. Online Ordering, Internetzugang, ...) zuzugreifen. Hierzu können sie sich mittels Standleitung oder Wählverbindung in dessen Netz anmelden. Realisiert wid dieser Zugang zum VPN mit einem Router.

- **Rechenzentrum des Fahrzeugherstellers**
  In diesem Rechenzentrum werden durch den Fahrzeughersteller sämtliche relevanten Daten und Dienste für dessen Partner angeboten. Insbesondere steht in diesem RZ der für das Online Ordering benötigte Server.

- **Internet Service Area**
  Die Internet Service Area wird durch die DeTeSystem betrieben. Hier wird neben DNS– und Mail–Diensten auch der Zugang in das Internet angeboten.

- **SRZ und SMC der DeTeSystem**
  Das Management dieser Komplettlösungen wird durch die DeTeSystem im SRZ und SMC betrieben.

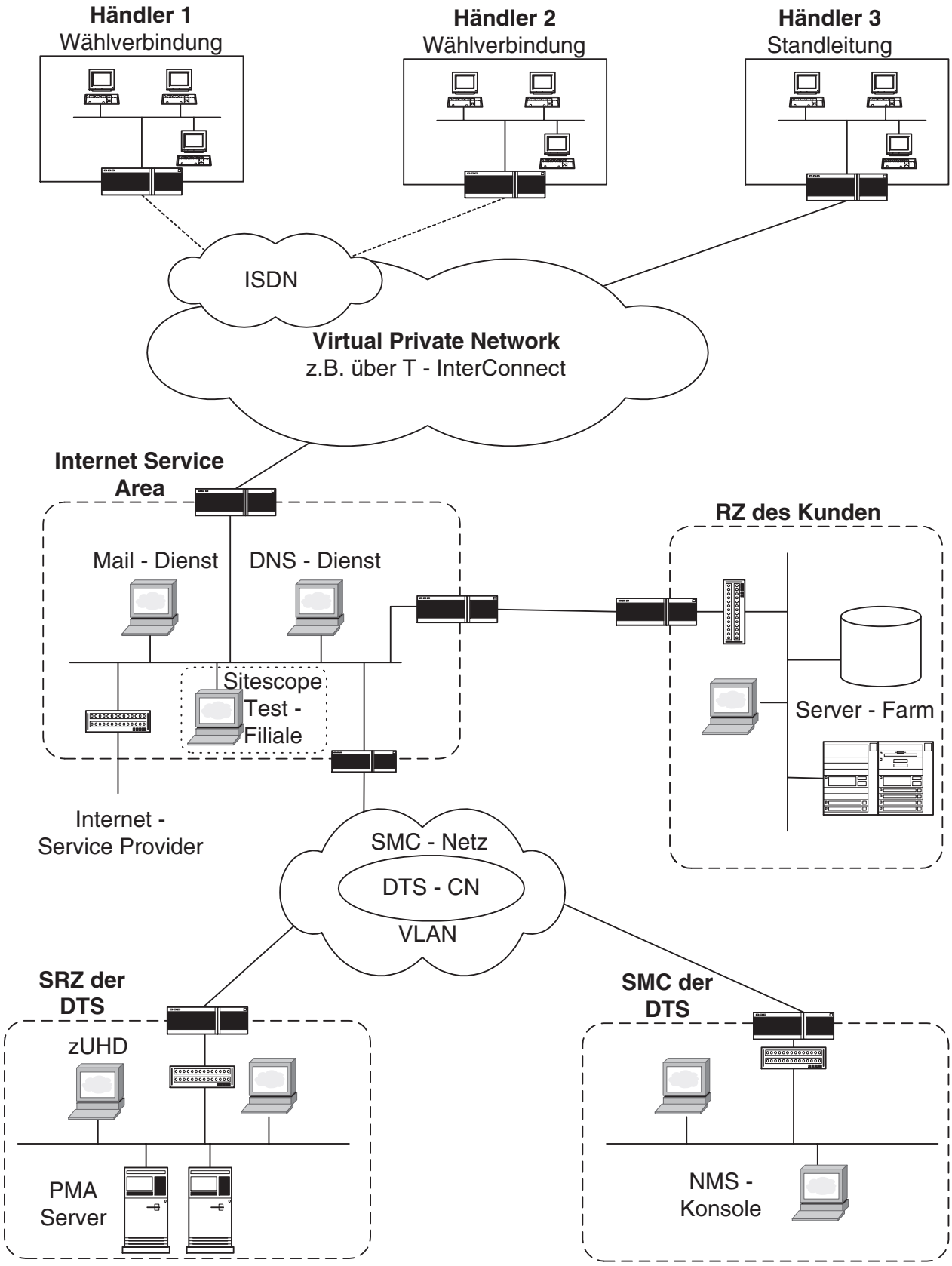

Abbildung 2.2: Die Systemlösung für einen Fahrzeughersteller

- **SMC–Netz**
  Das SMC–Netz verbindet die betrieblichen Einheiten der DeTeSystem.

Es sei an dieser Stelle erwähnt, daß sich für andere Großunternehmen wie Banken, Versicherungen oder Fast–Food–Ketten ein ähnliches Szenario ergeben würde, da es sich in diesen Fällen immer um die Anbindung großflächig verteilter Clients an einen oder mehrere Serverlokationen handelt, die ihrerseits zentrale Dienste anbieten oder Datenhaltung betreiben.

2.2 Service–Level–Management

Die in der Welt der Informationstechnik (IT) in den letzten Jahren zu beobachtende Zunahme von Komplexität und Heterogenität macht eine Planung, Überwachung, Verwaltung und Abrechnung der für diesen Bereich notwendigen Dienste immer schwieriger. Daraus erwuchs in den 90er Jahren der Begriff Service–Level–Management.

2.2.1 Begriff

Grundgedanke dieses Ansatzes ist, daß eine hard– und softwarecorientierte Sicht nicht mehr ausreicht, um die hochkomplexen IT–Syteme eines Unternehmens zu steuern.
Service Level Management geht über die technische Sicht solcher System–Parameter hinaus und hilft, durch zusätzliche Service–Definitionen wie z.B. Reaktionszeit bei Störungsmeldung, den neuen Anforderungen gerecht zu werden.
Die Central Computer and Telecommunication Agency (CCTA) definiert SLM wie folgt [ITIL 2] :

> *Service Level Management (SLM) is the process of managing a delivered IT Service in terms of quality, quantity and cost. ...is formalized by the preparation, agreement and maintenance of formal Service Level Agreements (SLA) which document all the relevant details of an IT service. The Service Level Management can be seen as the bridge between customers and supplier. ...*

Unter einem IT–Service versteht man alle IT–Leistungen, die der Kunde zur erfolgreichen Erledigung seiner Aufgabe (Geschäftsprozesse) benötigt. Es handelt sich hierbei meist um eine Kombination von Hard– und Software sowie Netz– und Telekommunikationsdiensten. Wesentlich ist jedoch, daß sich die Definition ausschließlich aus den Anforderungen des Benutzers oder ganzer Benutzergruppen ergibt.

> *A quality service is a service that lives up to the expectations of costumer. The only possible way to deliver a quality service is by knowing what the customer wants. There is no exception to this. [ITIL 2]*

Ein SLA ist eine schriftliche Vereinbarung zwischen den Kunden, die den geschäftlichen Aspekt eines Unternehmens repräsentiert, und der für die Umsetzung der IT verantwortlichen Institution dieses Unternehmens [McBr 98]. Ziel dieser Vereinbarung ist die Spezifikation dessen, was die unterschiedlichen Benutzergruppen von der IT in Bezug auf Antwortzeit, Systemverfügbarkeit und Prozessquantität von der IT erwarten können [Salm 89]. Solche Benutzergruppen werden meist in Kategorien eingeteilt, die einen unterschiedlichen Service–Level benötigen. Allerdings wird in einem SLA auch definiert, was die IT von dem Kunden z.B. in Bezug auf Systembenutzung erwarten kann.
Durch Service–Level–Agreements entsteht eine neue Schnittstelle zwischen Kunden und Dienstleistern, welche sich nur noch an den vereinbarten Diensten orientiert.
Basierend auf dieser Vereinbarung können beide Parteien ihre Ressourcen planen und einsetzen.
Folgende Komponenten sollte ein SLA enthalten (Auszug) [McBr 98].