Konzeption und Umsetzung einer Gesamtlösung für das Informationsmanagement eines mittelständischen Automobil-Markenvertragshändlers

Diplomarbeit

im Fach Informationsnetze, Kommunikationstechnik, Netzwerkmanagement
Studiengang Informationsmanagement
der
Fachhochschule Stuttgart –
Hochschule der Medien

Markus Vogt

Erstprüfer:	Prof. Dr. Wolf-Fritz Riekert
Zweitprüfer:	Prof. Dr. Christian Rathke

Bearbeitungszeitraum: 01. April 2003 bis 30. Juli 2003

Stuttgart, Juli 2003

Kurzfassung

Die hier vorliegende Arbeit beschreibt die Konzeption und Realisierung einer umfassenden Netzwerklösung für das Informationsmanagement der Firma Auto-Vertieb-Neckar GmbH. Die in dieser Arbeit realisierten Sicherheitsmechanismen gewährleisten den Betrieb eines fehlertoleranten Systems mit hoher Verfügbarkeit. In diese Lösung wird branchenspezifische Software implementiert, die die DV-gestützte Bearbeitung der täglichen Geschäftsprozesse des Automobilhändlers ermöglicht. Das System stellt den zukünftigen Benutzern Anwendersoftware in optimaler Weise zur Verfügung. Es ist außerdem eine investitionssichere Plattform für zukünftige Erweiterungen. Die Umsetzung erfolgt durch Verwendung der Netzwerktopologie Ethernet in Kombination mit den Standardprotokollen für die Kommunikation im Intranet und Internet (TCP/IP).

Schlagwörter: Netzwerk, fehlertolerantes System, Automobilhändler, Verfügbarkeit, Informationsmanagement, Ethernet, Intranet, TCP/IP.

Abstract

This thesis describes the conception and realization of extensive network solutions to handle information management in the Auto-Vertrieb-Neckar GmbH. The mechanisms of security are providing guarantee to run a fault tolerant system in consideration of high availability. The branch specific software used in this diploma thesis enables data processing work with daily business routines. All users of this system will be able to work with specific software tools in optimum ways. Furthermore, this system is a platform to effort future benefits in a safe way. The realization is taking place by using the network topology Ethernet in combination with the standard protocols for intranets and internet (TCP/IP).

Keywords: network, fault tolerant system, car dealer, availability, information management, Ethernet, intranet, TCP/IP.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

SAD	Škoda Auto Deutschland GmbH
AVN	Auto-Vertrieb-Neckar
EDV	Elektronische Datenverarbeitung
IT	Information Technology
VPN	Virtual Private Network
ADSL	Asymmetrical Digital Subscriber Line
TCP	Transmission Control Protocol
IP	Internet Protocol
POP3	Post Office Protocol (Version 3)
SMTP	Simple Mail Transfer Protocol
ETKA	Elektronischer Teile Katalog
ISDN	Integrated Services Digital Network
PC	Personal Computer
LAN	Local Area Network
WAN	Wide Area Network
GAN	Global Area Network
MAN	Metropolitan Area Network
DFÜ	Datenfernübertragung
GUI	Graphical User Interface
PDC	Primary Domain Controller
BDC	Backup Domain Controller
HA	High Availability
CPU	Central Processing Unit
SCSI	Small Computer System Interface
IDE	Integrated Device Electronics
RAID	Redundant Array of Independent Disks
USV	Unterbrechungsfreie Stromversorgung
VNC	Virtual Network Computing
USB	Universal Serial Bus

SAM	Security Account Manager
DHCP	Dynamic Host Configuration Protocol
PPP	Poin to Point Protocol
WINS	Windows Internet Name Service
DNS	Domain Name Server
DAT	Deutsche Automobil Treuhand
SNMP	Simple Network Management Protocol
DV	Datenverarbeitung
CA	Computer Associates
DDS(3)	Digital Data Storage
SQL	Structured Query Language
RIS	Reparatur Informations System
ODBC	Open Database Connectivity
BDE	Borland Database Engine
CLS-ID	Class Identifier

Vorwort

Während meines Studiums an der Hochschule der Medien (HDM) in Stuttgart, arbeitete ich ab dem 3. Semester halbtags als Aushilfe im Teiledienst der Firma Auto-Vertrieb-Neckar GmbH in Korntal-Münchingen. Im Fach Informationsnetze, Kommunikationstechnik, Netzwerkmanagement bei Herrn Prof. Dr. Riekert, erhielt ich erstmalig Einblick in moderne Netzwerktechnologien. Dieses Thema interessierte mich von Beginn an und ich wollte möglichst schnell praktische Erfahrung im Umgang mit EDV und Netzwerken sammeln. Während der Arbeit im Betrieb stellte sich heraus, dass die Geschäftsleitung und die Mitarbeiter unzufrieden mit den vorhandenen EDV-Anlagen waren. Als die Geschäftsleitung beschloss, den Betrieb nach Gerlingen zu verlegen, wurde ein neues Konzept zur Realisierung einer IT-Lösung notwendig. Mit Herrn Jaus, dem Geschäftsführer des Betriebes, sprach ich ein Budget ab und entwickelte ein grobes Konzept für die neue IT-Struktur. Diese Lösung wurde im Zeitraum eines halben Jahres verwirklicht. Die fertige Installation aller Komponenten erwies sich als sicher und zuverlässig, was ausschlaggebend war für die Idee, meine Diplomarbeit über dieses Thema zu schreiben.

Dank gilt allen, die mich bei der Erarbeitung der Diplomarbeit unterstützt haben. Insbesondere allen Mitarbeitern des Betriebes, die geduldig die anfänglichen Kinderkrankheiten der neuen Lösung ertragen haben. Besonderer Dank gebührt Herrn Jaus für die Risikobereitschaft, dieses Projekt einem Neuling zu überlassen und Herrn Prof. Dr. Riekert für die freundliche Unterstützung und Betreuung der Diplomarbeit.

1 Überblick

Die hier vorgestellte Diplomarbeit beschäftigt sich mit der Konzeption und dem Aufbau eines Microsoft-Netzwerkes für die Firma Auto-Vertrieb-Neckar GmbH (AVN). Die Firma AVN ist ein in Gerlingen ansässiger, mittelständischer Škoda-Vertragspartner mit ca. 25 Mitarbeitern. Der jährliche Umsatz beläuft sich auf ca. 6,5 Mio. Euro. Durch den Abschluss einer Vertragspartnerschaft mit der Škoda Auto Deutschland GmbH (SAD) ergaben sich neue Anforderungen an die IT-Infrastruktur. Diese Anforderungen, die Netzwerkbetriebssysteme und Hard- und Software größtenteils vorschreiben, sind im EDV-Betriebskonzept der SAD geregelt. Es galt eine für die Firma AVN möglichst kostengünstige Lösung zu finden. Diese musste erstens den Anforderungen des EDV-Betriebskonzeptes von SAD und zweitens den Anforderungen der Mitarbeiter der Firma AVN an eine moderne EDV-Anlage entsprechen.

Diese Überlegungen liegen der hier vorgestellten Arbeit zugrunde. Dabei werden spezielle Anforderungen in den Abschnitten 2 – 2.3 definiert. Die Zielsetzungen der zu erarbeitenden Lösung werden in Kapitel 2.1 beschrieben. Ausgehend von diesen Zielen, die im nachfolgenden Kapitel im Detail aufgeführt sind und unter Betrachtung des aktuellen Stands der Technik in Kapitel 3 wird die Konzeption von Hard- und Software in Kapitel 4 beschrieben. Basierend auf dieser Konzeption werden in den Kapiteln 5 und 6 Lösungsansätze besprochen. In Kapitel 5 wird zunächst auf die Konfiguration der Serverbetriebssysteme und der serverseitigen Software eingegangen. Mechanismen und Wege für eine größtmögliche Systemsicherheit und die Konfiguration der Domäne werden aufgezeigt. In Kapitel 6 ist das System aus der Sichtweise der Benutzer erklärt. Das Budget für die gesamte Lösung wurde von der Geschäftsleitung vor Beginn des Projektes vorgegeben. Zusammen mit der Anforderungsanalyse im Kapitel 2.3 ergibt sich der Umfang der zu realisierenden Lösung. Aus dem in Kapitel 2.2 erläuterten EDV-Betriebskonzept von SAD ergibt sich die Entscheidungsfindung bezüglich der Auswahl von Microsoft Client- und Serverbetriebsystemen.

Hauptteile dieser Arbeit sind die Beschreibung von Hard- und Software der Clients und Server, sowie die Implementierung aller aktiven Netzkomponenten in Kapitel 4. Die Konfiguration der Server-Betriebssysteme in Kapitel 5 und die Konfiguration der Domäne und der Benutzer werden ebenfalls ab Abschnitt 5 erklärt. Die Realisierung umfangreicher Sicherheitsmechanismen in Abschnitt 5.4 und die Funktionalität der Systemrichtlinien und deren Verwendung in Abschnitt 5.3.3 bilden einen weiteren Schwerpunkt.

Da der Automobilhersteller Škoda ein Tochterunternehmen des Volkswagen Konzerns ist, sind die Kommunikationswege und Kommunikationsmittel in allen anderen Tochterunternehmen der VW-Gruppe ähnlich. Die hier vorgestellte Arbeit steht Systemadministratoren anderer Vertragspartner der Unternehmensgruppe zur Verfügung und kann als Entscheidungshilfe für den Einsatz oder die Anschaffung entsprechender IT-

Lösungen dienen. Eine Zusammenfassung, die den Nutzen der Arbeit beschreibt und einen Ausblick auf zukünftige Weiterentwicklungen gibt, schließt die Arbeit ab.

2 Problemstellung

Unternehmen, die mit der hier vorgestellten Firma AVN vergleichbar sind, planen in der Regel ihre IT-Infrastruktur in Zusammenarbeit mit kleineren DV-Anbietern aus ihrer Region. Nach einer oftmals ungenügenden Analyse ihrer Bedürfnisse, wird die anvisierte Lösung von Technikern installiert. Testphasen und andere Maßnahmen zur Qualitätssicherung werden meistens aus Kostengründen vernachlässigt. Speziell im Bereich Datenintegrität und Datensicherung kann dies kostenintensive Probleme verursachen. Es ist unbedingt erforderlich, die Geschäfts- und Arbeitsprozesse des Unternehmens zu analysieren und eine darauf abgestimmte Lösung zu implementieren. Unternehmensführung und involvierte Mitarbeiter müssen rechtzeitig vor Einführung der neuen Lösung informiert und geschult werden. Eine ausreichend lange Testphase des gesamten Systems muss kalkuliert werden. Um eine nachhaltige Qualitätssicherung für die neue IT-Lösung zu erreichen, wird von Anfang an ein Mitarbeiter der Firma in die Konzeption miteinbezogen. Ausgehend von diesen Überlegungen werden die folgenden Ziele für die neue IT-Lösung definiert.

2.1 Ziele

Schwerpunkt der Zielsetzung ist die Erfüllung und Konformität der Anforderungen, die sich aus dem EDV-Betriebskonzept des Automobilherstellers Škoda Auto Deutschland, im Folgenden häufig mit SAD abgekürzt, ergeben. Im anschließenden Kapitel 2.2 werden auf die grundlegenden Inhalte dieses Betriebskonzeptes eingegangen. Ein weiterer Schwerpunkt ist die Bereitstellung einer Lösung, die größtmögliche Benutzerfreundlichkeit, Sicherheit und einfache Erlernbarkeit bietet. Mit modernen Netzwerktechnologien wird eine 100%ige Vernetzung aller Rechnersysteme des Betriebes erreicht. Dadurch wird dem einzelnen Benutzer eine optimale Client-Umgebung zu Verfügung gestellt. Die Geschäftsleitung erhält einen transparenten Einblick in die tatsächlich anfallenden IT-Kosten des Unternehmens. Folgende Aufzählung beschreibt alle weiteren Ziele:

1. Geeignete Anwendersoftware für die Bearbeitung täglicher Geschäftsabläufe muss ausgewählt und den Benutzern einheitlich zur Verfügung gestellt werden. Soweit möglich wird jede Art von Anwender- oder Branchensoftware in einer Client-Server-Variante implementiert.
2. Das System muss größtmögliche Sicherheit hinsichtlich der Speicherung und Verwaltung unternehmensrelevanter Daten gewährleisten. Dazu müssen Mechanismen für eine netzwerkübergreifende Datensicherung konzipiert werden.
3. Bereitstellung einer Mindestleistung auch im Falle des Versagens von einzelnen Systemkomponenten. Es wird die Erarbeitung eines weitestgehend fehlertoleranten

Systems angestrebt, damit im Falle des Versagens einzelner Komponenten der Geschäftsbetrieb aufrechterhalten werden kann.

4. Der Zugriff auf Konfigurationsoptionen der Clientbetriebssysteme muss durch entsprechende Microsoft-Werkzeuge für die zukünftigen Anwender beschränkt werden. Dadurch werden Systemausfälle, die durch Bedienfehler der User verursacht werden, vermieden. Die Serverbetriebssysteme werden vor dem Zugriff durch normale Benutzer geschützt und dürfen ausschließlich von Administratoren verwaltet werden.
5. Die gesamte Lösung darf einen bestimmten Kostenrahmen nicht überschreiten. Das bedeutet, dass für die Neuanschaffung und den Betrieb der EDV-Anlage die Kosten möglichst gering gehalten werden müssen. Deshalb wird versucht, die bereits vorhandene Hard- und Software in die Planung mit einzubeziehen und Teile der alten Lösung zu migrieren. Die Hardware und Peripheriegeräte, wie Drucker oder Monitore, werden über einen IT-Reseller als Komplettpaket bezogen. Unrentable Geräte werden aus der Systemumgebung entfernt.

Da Neuanschaffungen an Hard- und Software heutzutage bereits nach wenigen Jahren als veraltet gelten, wird für einen mittelständischen Betrieb, wie die Firma AVN, eine investitionssichere Kalkulation benötigt. Grupp (1999, S. 111) führt dazu aus:

> *„Während Hardware aufgrund des überaus schnellen technischen Alterungs-prozesses nach 5-6 Jahren ausgetauscht werden muß, geht man bei einer von Profis erstellten Standartsoftware unter einem Bestimmten Betriebssystem von einer Lebenszeit von 10-15 Jahren aus!“*

Aufgrund der Entwicklungen in den letzten Jahren geht man mittlerweile von einer Hardware-Lebensdauer aus, die zwischen drei und vier Jahren liegt. Mit einer Lebenszeit der Standardsoftware von 10-15 Jahren kann nur dann gerechnet werden, wenn sich die Anforderungen seitens SAD nicht ändern. Aufgrund dieser Überlegungen wird das Budget so geplant, dass die Kosten für Support und Wartung innerhalb des Hardware-Lebenszyklus bereits enthalten sind. Die Anschaffungskosten können auch über Miete oder Leasing abgewickelt werden. Diese Entscheidung bleibt der Geschäftsleitung vorbehalten. Ein Betriebsvergleich mit anderen Škoda Vertragspartnern ergibt, dass die Kosten für die EDV-Anlage nicht mehr als 0.5 % des Jahresumsatzes betragen sollten. Daraus ergibt sich in Rücksprache mit der Geschäftsführung das tatsächliche Budget. Um einen gewissen Spielraum während der Planung der Lösung zu haben, wird die Kalkulation zunächst nicht das gesamte Budget beanspruchen. Die Wartungskosten für die gesamte EDV-Anlage werden durch eine entsprechende Konfiguration der Server und Clients möglichst gering gehalten. Mit der Verwendung eines ADSL[1] Anschlusses werden die Kosten für die Online-Kommunikation überschaubar. Rücklagen für Reparaturen und eventuelle Neuanschaffungen werden berücksichtigt.

[1] ADSL ist im Volksmund auch als DSL bekannt. Diese Technik wird im Glossar erläutert.

2.2 Anforderungen des Automobilherstellers Škoda

Der Vertrieb von Škoda-Fahrzeugen an das Händlernetz wird in Deutschland von der Škoda Auto Deutschland GmbH abgewickelt. Die Abteilung Informationsdienste (IS) von SAD hat zur Regelung des reibungslosen EDV-Ablaufes zwischen dem Škoda-Vertragspartner und dem Automobilhersteller ein EDV-Betriebskonzept erstellt. Dazu schreibt Gottwald (2000, S. 2):

> *„Die Vorgaben dieses Betriebskonzeptes regeln die Zusammensetzung einer einheitlichen EDV-Landschaft auf Seiten der Škoda-Vertragspartner. Das Betriebskonzept beschreibt die dazu notwendigen Vorgaben und sorgt langfristig für eine homogene moderne EDV-Landschaft."*

Für den Austausch von Daten und Information sieht dieses Betriebskonzept eine Anbindung aller Škoda-Vertragspartner über ein Virtual Private Network (VPN), das so genannte Škoda-VPN, an das Intranet von Škoda Auto Deutschland vor. Der Zugriff erfolgt hierbei mittels eines Internet-Browsers. Das Intranet von Škoda Auto Deutschland beinhaltet Softwareanwendungen, die für den Datenaustausch nahezu aller Geschäftsprozesse zwischen SAD und den Vertragspartnern vorgesehen sind. Nachfolgend eine Aufstellung mit namentlicher Nennung der Anwendungen.

1. ***Ersatzteillager:*** Diese Anwendung dient der Abwicklung von Ersatzteil- und Zubehörbestellungen.
2. ***Disposhop:*** Hiermit werden Fahrzeugbestellungen zum Hersteller übermittelt. Der Händler hat die Möglichkeit, Rechnungen und den Lagerbestand von SAD einzusehen.
3. ***Zulassung (Z-Online 3.1):*** Verkaufs- und Zulassungsmeldungen von Škoda Fahrzeugen werden mit dieser Anwendung abgewickelt. Škoda Auto Deutschland stellt sich die Arbeit mit der Anwendung *Zulassung* wie folgt vor. Eine Verkaufsmeldung wird erstellt, sobald ein Vertragsabschluss mit einem Kunden zustande gekommen ist. Wird das Fahrzeug dann zugelassen, wird die betreffende Verkaufsmeldung aufgerufen und in eine Zulassungsmeldung übernommen.
4. ***Gewährleistung (GW-Online 3.0):*** Diese Anwendung wird zur Abwicklung von Gewährleistungs- bzw. Garantieanträgen benötigt.
5. ***R-Online:*** *R-Online* dient der Reklamationsabwicklung von Ersatzteillieferungen. Dazu sind alle beteiligten Stellen wie Škoda Auto Deutschland, der Händler, das Lager und die beteiligten Speditionen im System abgebildet.
6. ***BV-Online:*** Mit dieser Anwendung ist ein Betriebsvergleich mit anderen Händlern durch Eingabe zentraler Daten aus der Buchhaltung möglich.
7. ***SARAH:*** Unterstützt die Mitarbeiter der Abteilung Verkauf beim Datenaustausch und bei der Kommunikation mit der Škoda-Bank. Diese Verkäuferanwendung dient der Konfiguration von Fahrzeugen. *SARAH* bietet Unterstützung

bei der Zuordnung von Ausstattungs- und Motorvarianten zu Fahrzeugmodellen.

Weitere Anwendungen ermöglichen beispielsweise Anmeldungen zu diversen, von SAD angebotenen Schulungen, den Abruf der angefallenen Kosten für die Onlinekommunikation mit SAD und die Bestellung von Literatur oder Prospektmaterial.

Um die Anbindung des Händlers und die Funktion der Anwendungen des Škoda Intranets zu gewährleisten, schreibt das Betriebskonzept die Verwendung bestimmter Hard- und Software verbindlich vor. SAD überlässt es den Vertragspartnern, zwischen einer Einzelplatz- oder Netzwerklösung zu wählen. Die Einzelplatzlösung wird in dieser Arbeit nicht berücksichtigt, da sie den Anforderungen des Betriebes nicht entsprechen würde.

2.2.1 Anforderungen an das Netzwerk seitens des Automobilherstellers

Škoda Auto Deutschland schreibt die Verwendung der Netzwerktopologie Ethernet unter Einsatz der Standardprotokolle für die Kommunikation im Internet und Intranet (TCP/IP) vor. Škoda-Vertragspartner haben die Auswahl zwischen einem hard- oder softwareseitig installierten VPN-Gateway-Router. Die Benutzer des Netzwerkes müssen sich durch Benutzername und Passwort bereits bei der lokalen Anmeldung identifizieren. Microsoft Exchange oder vergleichbare E-Mail-Systeme werden zwar nicht vorgeschrieben, jedoch wird in vielen Geschäftsbereichen die ausschließliche Kommunikation mit E-Mails forciert. Als Mindestanforderung gilt daher der Betrieb von Mail-Clients, die in der Lage sind, POP3 und SMTP, also die gängigen Protokolle für E-Mail-Empfang und Versand, zu verarbeiten.

2.2.2 Anforderungen an die Hard- und Software seitens des Automobilherstellers

Alle von SAD empfohlenen Softwareprodukte können grundsätzlich innerhalb einer vernetzten Umgebung als Mehrplatzsystem betrieben werden. Auf den Arbeitsstationen werden ausschließlich Windows NT 4.0, Windows2000 Professional und Windows XP Betriebssysteme von Škoda Auto Deutschland unterstützt. Als Serverbetriebssystem besteht die Auswahl zwischen Windows NT-Server 4.0 oder Windows2000 Server. SAD schlägt die redundante Verwendung von zwei Domain-Controllern vor. Die Auswahl des Mechanismus, der letztendlich die Daten auf den Servern verteilt, bleibt dem Vertragspartner überlassen[2]. Die einwandfreie Funktion von Anwendungen auf anderen Betriebssystemen, wie zum Beispiel Windows 95 oder 98, wird von SAD nicht garantiert. Online-Kommunikation mit SAD, die auf anderen Betriebssystemen als Windows durchgeführt wird, ist nicht zugelassen. Die Softwareentwicklung und die entsprechenden Tests berücksichtigen ausschließlich die empfohlenen Betriebssysteme

[2] Verschiedene Strategien zur Verwendung von mehreren Servern werden in Kapitel 4.1 beschrieben.

und Netzwerkkomponenten. Die Anwendungen sind für die Darstellung mit einem 17“ Monitor optimiert. Bei Verwendung kleinerer Monitore ist mit Einschränkungen zu rechnen. Die Grafikkarte muss eine Auflösung von 1024x768 Pixeln (High Color) ermöglichen. Bei Verwendung des elektronischen Teilekataloges von SAD, dem ETKA[3], wird eine Auflösung von 1280x1024 Pixeln benötigt. Die Netzwerklösung unterstützt hinsichtlich der Netzwerkkommunikation unterschiedliche Installationsvarianten. Auf Basis des Kommunikationsprotokolls TCP/IP für Netzwerke und Internettechnologie bietet sich hier eine Vielzahl von Integrationsmöglichkeiten in das vorhandene Netzwerk. Die Online-Kommunikation mit SAD ist nur über das Škoda-VPN möglich. Der Dienst wird zu einer Grundgebühr und einem Minutenpreis angeboten. Eine Datenübertragung via Satellit wird von SAD nicht angestrebt. In einigen Gebieten kann eine DSL oder ISDN Flatrate[4] genutzt werden. In welchen Gebieten das möglich ist, muss im Bedarfsfall bei SAD angefragt werden.

2.3 Anforderungsanalyse

Um die Kosten für die Neuanschaffungen auf das Notwendige zu beschränken, erfolgt zunächst eine genaue Analyse der Informationsflüsse des Unternehmens. Alle organisatorischen Bereiche des Unternehmens wie Einkauf, Verkauf, Lager und Geschäftsleitung werden in Betracht gezogen. Zudem werden Kommunikationswege und der Datenaustausch mit Kunden, Lieferanten und Škoda Auto Deutschland untersucht. Hilfreich ist die Analyse der Ablauforganisation einzelner Geschäftsprozesse wie Annahme von Reparaturaufträgen oder Teilelieferungen. Zusammenfassend lassen sich derartige Strukturen auch in einem Organigramm abbilden. Da für die künftigen Benutzer und die Geschäftsleitung die Frage der räumlichen Aufstellung von Clientsystemen und Druckern eine entscheidende Rolle spielt, wird eine Übersicht angefertigt. Abbildung 1 auf Seite 16 zeigt die vorläufige Aufteilung der neuen EDV-Struktur. Anhand der Anforderungsanalyse werden folgende Punkte bestimmt:

1. Kommunikationsmedien
2. Anzahl und Gruppierung der Arbeitsplätze
3. Benötigte PC-Systeme
4. Anzahl der Benutzer
5. Gruppierung der Benutzer
6. Anzahl der Drucker und deren spätere räumliche Aufstellung

---

[3] ETKA wird im Glossar erklärt.

[4] Als Flatrate wird von Internet-Providern wie T-Online oder Arcor die Bereitstellung des Internet-Zugangs zu einem pauschalen Monatpreis bezeichnet.

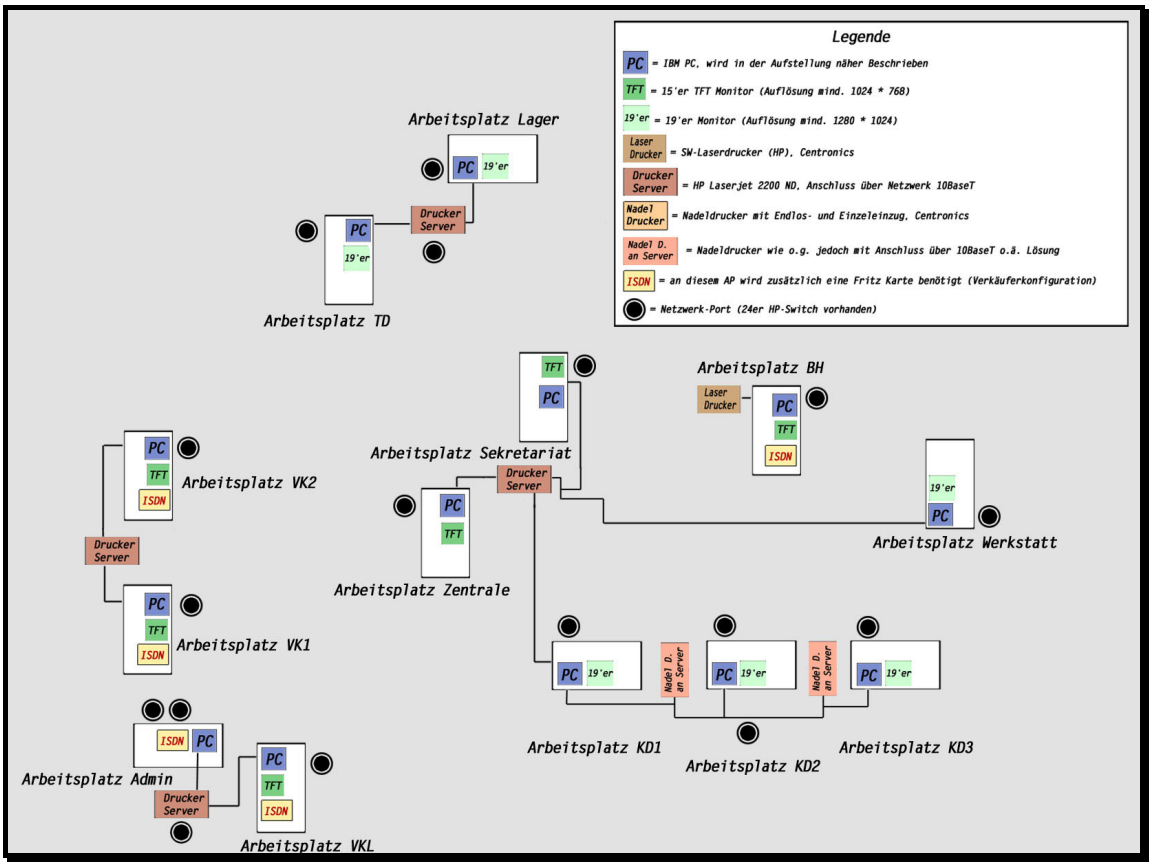

Abbildung 1: Clientsysteme und logisch verbundene Drucker

Anhand der Verbindungslinien in Abbildung 1 wird visualisiert, wie die zukünftigen Benutzer und Arbeitsplätze an die Drucker und Printserver angeschlossen werden. Es handelt sich dabei nicht um eine physische Verkabelung, sondern vielmehr um die zukünftigen Druckereinstellungen der Clients. Durch verschiedenfarbige Symbole werden Netzwerkports, PC-Systeme, Drucker und Monitore versinnbildlicht. Die zukünftigen Benutzer werden am Anfang dieses Projektes zu ihrer Tätigkeit in Verbindung mit der EDV-Anlage befragt. Bedürfnisse und Wünsche der Benutzer lassen sich wie folgt zusammenfassen:

- Die gemeinsame Bearbeitung von Daten und Dokumenten innerhalb der Abteilungen und im gesamten Unternehmen muss ermöglicht werden.
- Die Mitarbeiter benötigen die Möglichkeit der Kommunikation mit E-Mails.
- Die Internetanbindung muss eine große Bandbreite zu Verfügung stellen. Die Anbindung über ISDN erwies sich als zu langsam.
- Die Anwendersoftware muss innerhalb kurzer Zeit erlernbar sein. Entsprechende Hilfefunktionen und Handbücher müssen mitgeliefert werden.
- Das System darf nur sehr geringe Ausfallzeiten durch Wartungsarbeiten oder Fehler verursachen.

- Da die graphische Benutzeroberfläche bei der Dateneingabe von Kunden des Autohauses eingesehen werden kann, muss diese repräsentativ wirken und an das Corporate Design von Škoda Auto Deutschland angepasst werden.
- Seitenstarke Ausdrucke müssen innerhalb kurzer Zeit auf zuverlässigen Druckern zu bewerkstelligen sein. Zuverlässigkeit hinsichtlich Handhabung, Funktion und Verbrauch von Toner und Papier ist erforderlich. Auf Ausdrucken, die an die Kunden des Unternehmens weitergegeben werden, muss das Firmenlogo in Farbe gedruckt werden.

3 Stand der Technik

In diesem Kapitel werden zunächst mögliche Lösungen anderer Škoda-Vertragspartner betrachtet. Nach einem groben Überblick über die verfügbaren Technologien und die bereits vorhandenen Hard- und Software im Unternehmen AVN wird auf mögliche Lösungen für Branchensoftware eingegangen. Gottwald (2000, S. 4) spricht im Betriebskonzept von Škoda Auto Deutschland auch von der Möglichkeit, eine Einzelplatzlösung zu verwirklichen. Durch Gespräche mit anderen Škoda-Vertragspartnern konnte in Erfahrung gebracht werden, dass diese Einzelplatzlösung in der Tat bei einigen Škoda-Händlern realisiert wird. Der Zugang zum Škoda-VPN ist dabei nur von einem einzigen Rechner über eine ISDN-Anbindung möglich. Alle Mitarbeiter des Betriebes teilen sich diesen Arbeitsplatz und nehmen gegebenenfalls Wartezeiten in Kauf. Natürlich sind bei dieser Variante mehrere Rechner im Betrieb vorhanden. Es handelt sich jedoch meistens nicht um Systeme, die in einer Netzwerk- oder Domänenumgebung laufen. Strategien zur Datensicherheit und Systemverfügbarkeit existieren mangels eines Netzwerkes nicht. Die Mitarbeiter haben alle einzelne PCs, die sie selbst verwalten. Der Administrator des Betriebes stellt Branchensoftware, wie das von Škoda Auto Deutschland angebotene Warenwirtschaftssystem Ec@ros[5], zur Verfügung und installiert diese einzeln auf den PCs der Mitarbeiter. Die restliche Anwendersoftware wird ebenfalls vom Administrator des Betriebes lokal auf den PCs installiert. Ein hoher Zeit- und Kostenaufwand ist die Folge. Bei größeren mittelständischen Betrieben kann für den Support einer derartigen Systemlösung eine komplette Personalstelle anfallen.

3.1 Verfügbare Technologien

Rechnernetze lassen sich in zwei große Kategorien einteilen, Local Area Network (LAN) und Wide Area Network (WAN). Diese Einteilung ist für die meisten bestehenden und neu installierten konventionellen Netze und Systemumgebungen auch heute noch sinnvoll. Die Einteilung verliert jedoch zunehmend an Gültigkeit, weil Dienste wie E-Mail von vornherein netzübergreifend konzipiert sind. Kauffels (2002, S. 27) teilt die bekannten Rechnernetze nach folgenden Kriterien ein.

- **WAN**: Klassische Form des Verbindungsnetzwerkes zur Überbrückung von großen Entfernungen. Die Grundstruktur ist meist ein paketvermitteltes Teilstreckennetz mit über Leitungen verbundenen Knotenpunkten. Ein Beispiel dafür ist eine Telefonleitung.
- **LAN**: Lokale Netze und Systeme für den Transfer von Informationen. Einer definierten, gleichberechtigten Anzahl von Benutzern dieser Systeme wird in ei-

[5] Ec@ros wird in Abschnitt 3.3 erklärt

nem räumlich begrenzten Gebiet der Datenaustausch mittels eines Übertragungsmediums ermöglicht.

Weitere, in der Fachliteratur auftretende Bezeichnungen für Rechnernetze sind das Global Area Network (GAN) mit Satellitenverbindungen und das innerstädtische Metropolitan Area Network (MAN), welches mit einem großflächig angelegten LAN vergleichbar ist.

Zum eigentlichen Aufbau des LAN-Netzes kommt in dieser Arbeit die Verbindung des lokalen Netzes mit einem WAN, in Form des Škoda-VPN, und dem Internet hinzu. Im folgenden Abschnitt ist die Soft- und Hardware beschrieben, die im Betrieb bereits vorhanden ist. Um möglichst Kosten sparend zu arbeiten, wird erörtert, ob es sinnvoll ist, die bereits vorhandenen Komponenten in die neue Lösung zu integrieren.

3.2 Vorhandene Hard- und Software im Betrieb

Die vorhandene Hard- und Software des Betriebes ist weder einheitlich noch strukturiert. Die Anforderungen des Automobilherstellers werden in keinem Punkt erfüllt. Folgende Aufstellung gibt einen Eindruck der bestehenden IT-Lösung des Unternehmens:

- In der Systemumgebung werden fünf Workstation-PCs mit unterschiedlichsten Microsoft Betriebssystemen verwendet. Die uneinheitliche Hardware ist nicht dokumentiert.
- Auf einem dieser PCs ist Windows NT Server installiert. Außer dem Betriebssystem hat dieser Rechner aber keine Gemeinsamkeiten mit einem Server. Fünf Lizenzen für den Zugriff der Clients sind vorhanden.
- Eine CD-ROM mit dem Office-Paket in der Version 97 ist vorhanden. Allerdings steht nur eine Lizenz für den gesamten Betrieb zur Verfügung.
- Das Grundmodul der Branchensoftware Werbas mit fünf User-Lizenzen läuft auf dem Server-PC.
- Auf einigen Rechnern ist der elektronische Teilekatalog ETKA in verschiedenen Versionen installiert.
- Auf zweien der Workstation-PCs sind lokale Installationen der CC-Bank-Software Kosyfa[6] zu finden.
- Auf einem Macintosh-Rechner werden die Ausgangsrechnungen für Neuwagen erstellt. Dieser Rechner ist nicht mit dem Netzwerk verbunden.
- Mit veralteten Laser- und Nadeldruckern unterschiedlicher Hersteller werden Rechnungen und Aufträge ausgedruckt. Durch diese teilweise defekten Peripheriegeräte wird kein einheitliches Druckbild erreicht.

---

[6] Kosyfa ist ein Programm der CC-Bank. Es dient zur Anfertigung von Leasing- und Finanzierungsanträgen.

Zusätzlich ist ein neuwertiger Digitalkopierer im Betrieb vorhanden. Der Hersteller dieses Gerätes bietet eine Drucker- und Netzwerkkarte zum nachträglichen Einbau an. Die Ausgangsituation im Betrieb Auto-Vertrieb-Neckar GmbH kann folgendermaßen beschrieben werden. Ein Rechnerverbund mit mehreren Arbeitsplatzrechnern, die unterschiedliche Ausstattung und unterschiedliche Betriebssysteme haben, sind über einen Hub und entsprechende Verkabelung miteinander verbunden. Ein einziger Windows NT Server dient als File-Server für die Datenbanken der Branchensoftware Werbas. Eine NT Domäne mit Domänenbenutzern existiert nicht. Die Zugriffsrechte sind auf den lokalen Betriebssystemen, soweit möglich, hinterlegt. Einige Workstations sind mit den Betriebssystemen Windows 95 oder Windows 98 ausgestattet. Häufige Abstürze der Betriebssysteme und dadurch bedingte Defekte an Datenbanken und Dateien sind die Regel. Eine sichere und strategisch geplante Datensicherung des Netzwerkes wird nicht durchgeführt. Die Benutzer sichern ihre Dateien mittels Disketten oder anderer Speichermedien selbst. Die Kosten für Wartung und Pflege des Systems sind für die Geschäftsleitung unüberschaubar. Besonders hohe Kosten entstehen für die Online-Kommunikation, da jeder Benutzer sich per DFÜ-Einwahlverbindung beim Internet-Provider einwählt. Für alle Mitarbeiter steht nur eine einzige E-Mail Adresse zur Verfügung. Die vorhandenen Installationen sind zum Teil grob fahrlässig und bewirken eine große Verunsicherung der Benutzer im Umgang mit der EDV-Anlage. Es besteht dringender Handlungsbedarf.

3.3 Branchensoftware

Für die Bearbeitung von Abrechnungs-, Betriebs- und Werkstattvorgängen wird eine möglichst einfach zu erlernende, speziell für die Zwecke der Kfz-Branche zugeschnittene Software benötigt. Auch Kundendaten und Betriebsstammdaten müssen mit diesem System verwaltet werden können. Zahlreiche Anbieter platzieren ihre Produkte in diesem Marktsegment. Neben dem Hersteller ADP, der das Produkt DracaR+ entwickelt und vertreibt und nach eigener Aussage Marktführer ist, zeichnet sich DekraData mit der Software Werbas durch eine übersichtliche und modulare Programmierung von Softwarebausteinen aus. Škoda Auto Deutschland bietet allen Vertragshändlern zu relativ günstigen Konditionen das Warenwirtschaftssystem Ec@ros an. Ec@ros wurde vom Hersteller Procar als webbasierte Anwendungsplattform entwickelt. Die Software ist auf die besonderen Bedürfnisse von Škoda-Vertragspartnern im internetbasierten Geschäftsverkehr (Business-to-Business und Business-to-Consumer) ausgerichtet. Zu diesem Zeck wurde Ec@ros in der Programmiersprache Java entwickelt. Eine kostenlose Testversion wurde inklusive dem Webserver Apache[7] installiert und von der Geschäftsleitung ausgiebig getestet. Nach Meinung aller in die Tests involvierten Personen, ist die Bedienung des Programms zu umständlich. Zu verschiedenen Arbeitsschritten des Tagesgeschäftes wurden von den Testpersonen keine entsprechenden

[7] Apache ist ein Webserver für Unix und Microsoft Betriebssysteme. Weiterführende Informationen finden sich auf der Webseite http://www.apache.org. (Letzter Zugriff: 03.07.2003)

Funktionen in der Software gefunden. Da mit der Lösung von DekraData bereits erste positive Erfahrungen gemacht wurden und Lizenzen vorhanden sind, wird dieses System erweitert. Zusätzlich werden weitere Module für den Tagesabschluss und die Kassenfunktion, sowie Schnittstellen zum Teilekatalog ETKA und der Buchhaltungssoftware der DATEV erworben. Die Installation und Konfiguration von Werbas wird in Abschnitt 5.5 auf Seite 56 beschrieben.

4 Konzeption Hard- und Software

In diesem Kapitel wird durch Auswertung der Anforderungen, seitens der zukünftigen Benutzer zum einen und seitens des Automobilherstellers zum anderen, die Auswahl der verwendeten Hard- und Software beschrieben. Aus den verschiedenen Anforderungen können zusammenfassend folgende Schlüsse gezogen werden:

1. Ein vollständiges Server-Betriebssystem muss auf beiden Servern verwendet werden. Entsprechend den Anforderungen des Automobilherstellers ist ein Microsoft Betriebssystem zu verwenden. Eine Alternative zum verwendeten Serverbetriebssystem Windows NT Server wäre der Einsatz von Windows2000 Server oder gar Windows2000 Advanced Server.[8] Da jedoch im Zeitraum der Anschaffung die Lizenzierung von Windows2000 Server noch sehr kostspielig war, fällt letztlich die Entscheidung zu Gunsten von Windows NT Server. Von diesem Betriebssystem ist ohnehin bereits eine Lizenz vorhanden.
2. Um eine benutzerfreundliche Bedienoberfläche auf den Clients zu schaffen, wird ein aktuelles Betriebssystem aus dem Hause Microsoft benötigt. Windows NT kann hier nicht in Betracht gezogen werden, da der Support bzw. die Bereitstellung der Service Packs und anderer Updates von Microsoft zum 30. Juni 2003 eingestellt wurde. Als Nachfolger für Windows NT wurde von Microsoft das Betriebssystem Windows2000 entwickelt, ein würdiger Nachfolger, da dieses Betriebssystem auf NT Technologie basiert.
3. Die zu verwendende Netzwerktopologie ist ein Ethernet in der Ausführung 10/100 BaseT. Das bedeutet, dass alle aktiven Netzwerkkomponenten Übertragungsraten von 10 Megabit pro Sekunde und 100 Megabit pro Sekunde beherrschen müssen. Zur Vereinfachung werden diese Übertragungsraten in allen folgenden Kapiteln mit 10 MBit bzw. 100 MBit benannt.
4. Alle passiven Netzwerkkomponenten müssen ebenfalls für Übertragungsraten von 10 MBit und 100 MBit geeignet sein. Mit passiven Netzwerkkomponenten sind Kabel, Netzwerkanschlüsse oder Patchfelder[9] etc. gemeint.

4.1 Verwendete Hardware der Server

Bevor die exakte Konfiguration der serverseitigen Hardware bestimmt werden kann, wird zunächst die Netzlast des alten Servers ermittelt. Unter Netzlast versteht man die Datenmenge, die innerhalb eines definierten Zeitraums vom Server verarbeitet werden muss. Dies hängt letztendlich vom Umfang der zukünftig installierten Anwendersoft-

---

[8] Auf die exakten Produktbeschreibungen wird hier nicht eingegangen. Sie können jedoch beim Hersteller Microsoft angefordert werden.

[9] Der Begriff Patchfeld wird im Glossar erklärt.

ware ab. Zenk (1995, S. 328) führt aus, dass die effektive Übertragungsgeschwindigkeit weit unterhalb der technischen Übertragungsrate liege. Für Zenk ist dies technisch bedingt. Um die Nettodatenrate zu erhöhen, schlägt Zenk die Verwendung eines leistungsstarken Netzwerkbetriebssystems und schneller File-Server in Verbindung mit schnellen Festplattensystemen vor. In dieser Arbeit wird die zukünftige Netzlast mit Hilfe des alten Servers bestimmt. Es wird die Zeit gemessen, die verstreicht, um eine Datei definierter Größe vom Server auf einen PC zu kopieren. Für die neuen Server werden genügend Ressourcen eingeplant, um den Benutzern neue Installationen mit ausreichender Performance zur Verfügung zu stellen.

Ebenfalls eine wichtige Rolle, um die hard- und softwareseitige Ausstattung der Server bestimmen zu können, spielt die Verfügbarkeit des gesamten Systems. Hohe oder hundertprozentige Verfügbarkeit kann aber nur durch hohe Investitionen realisiert werden. Das steht natürlich im Widerspruch zum vorhanden Budget (siehe Kapitel 2.1). Zur Verfügbarkeit schreibt Raepple (2001, 272):

> *„Überall dort, wo eine sehr geringe Ausfallzeit eines nicht funktionstüchtigen Systems den Verlust von Geld und Ansehen bedeutet, genügt es häufig nicht, Verfügbarkeit alleine über eine hohe Rechen- und Leitungskapazität abzusichern. Hochverfügbarkeit (engl. High Availability, HA) verlangt nach zusätzlichen Schutzmechanismen, die eine nahezu hundertprozentige Ausfallsicherheit garantieren.“*

Im Regelfall können nur durch redundante Hardware-Aufbauten Systeme realisiert werden, die im Falle einer Störung die Funktion über die Paralleleinrichtung fehler- und unterbrechungsfrei ausführen. Durch die Kombination mehrerer Serversysteme wird ein Cluster erzeugt. Durch Cluster werden mehrere eigenständige Server zu einem logischen System, das im Netzwerk unter einer Adresse angesprochen wird zusammengeschlossen. Grundsätzlich erhöht sich die Verfügbarkeit eines Einzelsystems (V1(t)) durch den parallelen Betrieb eines weiteren Systems mit der Verfügbarkeit V2(t) nach der von Raepple (2001, S. 271) definierten Formel:

$$V(t) = V1(t) + V2(t) – (V1(t) * V2(t))$$

Demnach kann die Ausfallzeit von 14 Tagen für ein System mit 95% Verfügbarkeit durch redundante Auslegung auf rechnerisch 21 Stunden (oder 99,75%) verkürzt werden. Hochverfügbare Systeme müssen einen Wert zwischen 99,9% und 99,99% Verfügbarkeit pro Jahr aufweisen, und dürfen somit nur zwischen einer und acht Stunden im Jahr stillstehen. Noch kürzere Ausfallzeiten sind meistens nur mit proprietären Hard- und Software-Lösungen zu erreichen. Bei der redundanten Auslegung eines Systems sind alle seine Komponenten zu berücksichtigen. Dazu zählen das Netzteil, Netzwerkverbindungen, Prozessor, Betriebssystem und Anwendungs-Software. Zwei Mechanismen zur redundanten Weiterführung eines Systems werden unterschieden:

- **Failover-System**: Diese Variante wird im Fachjargon auch als Cold-Standby bezeichnet. Die gängigste Konfiguration wird mit zwei identischen Servern, bei denen nur einer ein Festplattensystem besitzt, hergestellt. Fällt der erste Ser-

ver durch einen Hardwaredefekt aus, wird das Festplattensystem in den zweiten Server montiert. Die Montage lässt sich hierbei durch die Verwendung von Wechselrahmen beschleunigen.

- **Takeover-System**: Diese Lösungen werden oftmals als Standby-Systeme bezeichnet. Beide Server haben ein vollständiges Festplattensystem und sind gleichzeitig am Netzwerk angeschlossen. Durch eine spezielle Software werden die Daten redundant, über eine separate Netzwerkverbindung, in Echtzeit auf beide Server verteilt. Fällt der erste Server aus, zwingt die Software den zweiten Server zur Übernahme des Systems.

Bei Failover-Systemen werden die Anwendungen auf dem zweiten, voll funktionsfähigen System neu gestartet. Takeover-Systeme übernehmen gestartete Anwendungen im laufenden Betrieb. Letztere Variante hat den Vorteil der nonkognitiven Übernahme der von Anwendern gestarteten Netzwerk-Software.

Aus den vorangegangenen Überlegungen und den Anforderungen des Automobilherstellers in Kapitel 2 ergibt sich der zwingende Einsatz von zwei Servern. Die hardwareseitige Bestückung beider Server sollte weitestgehend gleich gewählt werden. Daher macht die Migration des vorhandenen Servers keinen Sinn. Eine Neuanschaffung beider Systeme ist erforderlich. Die Speicherkapazität der Festplattensysteme der beiden neuen Server muss gleich groß sein da, wie im Kapitel 5.4.2 beschrieben, relevante Daten zwischen den Servern über die Netzwerkverbindung ausgetauscht werden. Bei der Konfiguration zweier oder mehrerer Server in einer Domäne, wird ein Server zum primären Domain-Controller (PDC), der oder die anderen zum Backup-Domain-Controller (BDC) (siehe Abschnitt 4.4). Aus den Anforderungen ist erkennbar, dass mehrere Datenbanken und Datenbank-Engines, die sich auf dem Server befinden, von den Clientsystemen abgefragt werden. Der Einsatz eines schnellen Festplattensystems ist daher unabdingbar. Folglich werden für die Server SCSI-Controller vorgesehen. SCSI steht für Small Computer System Interface. Einer der Vorteile gegenüber herkömmlichen IDE-Festplatten liegt darin, dass die angeschlossenen Geräte von einem separaten Chip verwaltet werden und deshalb den Prozessor (CPU) weniger belasten. Tests in verschiedenen Fachzeitschriften ergaben laut Dawicontrol (2003), dass der Geschwindigkeitsgewinn bei Einsatz einer hochwertigen SCSI-Festplatte, je nach Umdrehungszahl (7200 bis 10000 upm), 20 bis 60 Prozent gegenüber einer herkömmlichen Festplatte beträgt. Ein weiterer Vorteil sind die maximal acht respektive 16 Geräte, die sich an einem SCSI-Kanal betreiben lassen. Am IDE Kanal lassen sich hingegen nur zwei Geräte betreiben. SCSI bietet außerdem genügend Anschlussmöglichkeiten für zusätzlich benötigte Peripheriegeräte. Neben Festplatten und CD-Laufwerken, bzw. CD-Recordern, lassen sich auch externe Geräte anschließen. Ein RAID-System mit Level 2 oder Level 5 wäre ebenfalls wünschenswert. RAID-Systeme verteilen Daten eines logischen Laufwerkes auf mehrere Festplatten oder führen, abhängig von der Konfiguration des RAID-Systems, Daten mehrerer Festplatten zusammen. Die Zusätze Level 2 oder Level 5 geben Auskunft über die Konfiguration in Abhängigkeit der Anzahl verwendeter Festplatten des Systems. Aus Kostengründen wird in dieser Arbeit auf

den Einsatz eines RAID-Systems verzichtet. Sollte sich künftig die Anforderung ergeben, eines dieser Systeme nachzurüsten, wäre das in den nachfolgend beschriebenen Konfigurationen mit überschaubarem Aufwand möglich.

Unter Berücksichtigung dieser Überlegungen werden die Server hardwareseitig ausgestattet. In Kapitel 5 wird auf die exakte technische Beschreibung der Komponenten eingegangen. Die Server werden mit zeitgemäßen Prozessoren des Herstellers Intel und SCSI-Festplattensystemen ausgerüstet. Für beide Server werden Bandlaufwerke mit ausreichender Speicherkapazität beschafft. Je Server werden zwei Netzwerkkarten, die eine Datenübertragungsrate von 100MBit unterstützen, verwendet. Damit eine Backupleitung für den Internetzugang konfiguriert werden kann, erhalten beide Server ISDN Steckkarten. Die Größe des Arbeitsspeichers muss ausreichend für die Performance der zu verwendenden Datenbanken sein.

Im Vergleich mit vorgefertigten Servern namhafter Hersteller wie IBM, Hewlett Packard oder Compaq wird deutlich, dass die einzelne Beschaffung und der Zusammenbau der oben aufgelisteten Komponenten deutlich günstiger ist, als der Kauf zweier kompletter Server. Führende Hersteller der Branche bieten mit Ihren Serversystemen für kleinere Unternehmen meist ein durchschnittliches Hardwarepaket, das für vielfältige Einsatzmöglichkeiten verwendet werden kann. Einzelne, wie im Fall dieser Arbeit benötigte Komponenten müssten nachträglich beschafft werden. Bereits eingebaute Komponenten, die zu einem hohen Anschaffungspreis führen, würden nicht benötigt werden.

4.1.1 Aktive Netzkomponenten der Serverumgebung

Die oben beschriebenen Server werden in einer geeigneten Umgebung untergebracht. Durch die einschlägig bekannten Sicherheitsvorschriften für EDV-Anlagen, die jederzeit beim Versicherer nachgefragt werden können, ist der Einsatz eines Serverschrankes[10] notwendig. Außerdem sollten die Serversysteme in einem abschließbaren Raum, zu dem nur eine begrenzte Anzahl von Personen Zutritt hat untergebracht werden. Alle Geräte und Anlagen, die zur Aufrechterhaltung des Netzwerkes dienen werden ebenfalls an diesem Ort aufgestellt. Die Stromversorgung erfolgt zunächst über eine einzelne mit 16 Ampere abgesicherte Stromleitung. Als zweite Komponente zur Aufrechterhaltung der Stromversorgung wird eine unterbrechungsfreie Stromversorgungsanlage (USV) installiert. Eine USV stellt eine überdimensionale Batterie dar, die in der Lage ist, Ausfälle oder Spannungsabfälle des Stromnetzes zu erkennen und automatisch auf Batteriebetrieb umzuschalten. USV-Systeme für kleine bis mittelgroße Netzwerkumgebungen bietet der Hersteller und zugleich Marktführer APC an. In dieser Arbeit wird eine USV mit 1000 Watt verwendet. In Rücksprache mit dem Hersteller des Gerätes ergibt sich aus der angegebenen Stromleistung eine Restlaufzeit der Server und anderer angeschlossener Komponenten von 40-50 Minuten nach Ausfall der Stromversorgung. Die nachfolgend beschriebenen Komponenten werden ebenfalls im Serverschrank untergebracht.

[10] Zur Ausstattung des Serverschrankes siehe Abschnitt 4.1.2

Die eigentliche Netzwerktopologie Ethernet wird durch einen Verteiler, den so genannten Switch oder Hub erzeugt. Ein Switch ist ein spezieller Hub. Der Unterschied ist die Arbeitsweise. Ein Hub empfängt ein Datenpaket und sendet es einfach an jeden seiner Anschlüsse (engl. Port) weiter. Ein Switch hingegen schickt ein Datenpaket nur an den Port, für den das Paket bestimmt ist. Der Vorteil eines Switches liegt in der wesentlich höheren Geschwindigkeit, die durch das intelligente Verteilen der Datenpakete erreicht wird. Diese und die Eigenschaft der Switche, einzelne Ports mit unterschiedlichen Geschwindigkeiten zu betreiben, erhöht den Datendurchsatz im Netzwerk deutlich. Switche sind in der Lage, Kollisionen von Datenpakten zu vermeiden und ermöglichen das gleichzeitige Senden und Empfangen von Datenpaketen. In dieser Arbeit wird daher ein Switch des Hersteller Hewlett Packard mit 24 Ports verwendet.

Aufgrund der räumlichen Trennung des Standortes der Serverkomponenten zum eigentlichen Arbeitsplatz des Administrators, ist der Einsatz einer Lösung zur entfernten Kontrolle (engl. Remote-Access) der Serversysteme zwingend. Man unterscheidet zwei Varianten:

1. Remote-Access auf Softwarebasis, das Netzwerkprotokolle wie beispielsweise das IP Protokoll benutzt. Zur Auswahl stehen Produkte diverser Anbieter. Auch Lösungen zum kostenfreien Download, wie die Software VNC der AT&T Laboratories Cambridge[11] sind eine gängige Variante. Der Nachteil dieses Produktes besteht darin, dass vor dem Zugriff auf das Remote-System, also dem Server, eine Netzwerkverbindung zu diesem bestehen muss. Dadurch ist es nicht möglich, Einblicke in den Bootprozess oder das BIOS zu haben.
2. Eine andere Möglichkeit ist Remote-Access auf Hardwarebasis. Dies wird durch Verwendung von externen Geräten ermöglicht. Bei dieser Variante werden Tastatur-, Maus- und Monitorsignale an einen Sender angeschlossen, der diese durch ein herkömmliches Netzwerkkabel an den zugehörigen entfernten Empfänger schickt. Abbildung 2 auf Seite 27 zeigt die Verkabelung. Signale werden über eine Distanz, abhängig von der Auflösung des Monitors zwischen 75 und 200 Meter Entfernung, übertragen.

[11] Informationen und Download erhält man auf der Website der AT&T Laboratories Cambridge, URL: http://www.uk.research.att.com/vnc/. (Letzter Zugriff: 15.07.2003).

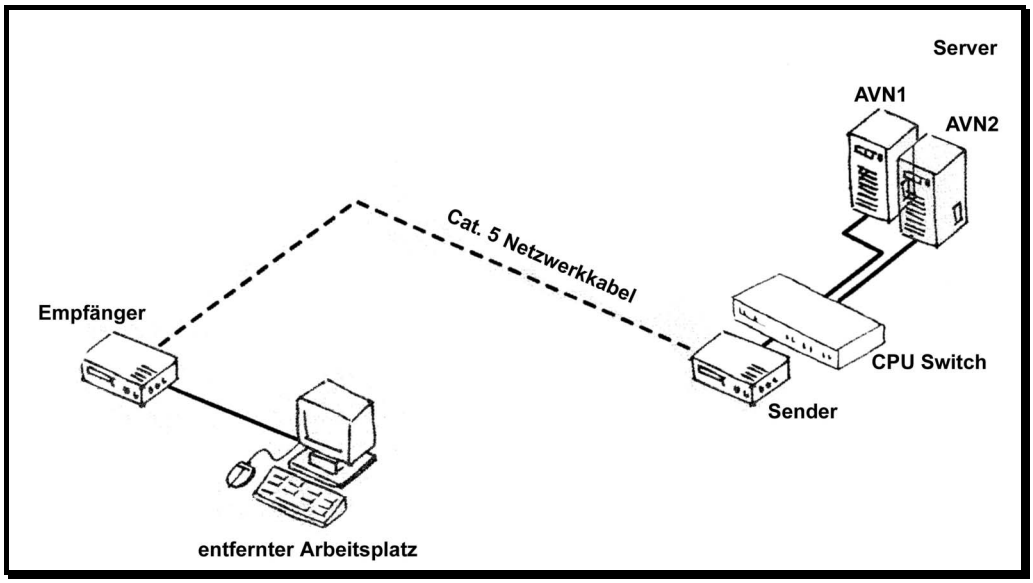

Abbildung 2: Schematische Verkabelung der Remote-Access Lösung

Die Hardware-Lösung mit Remote-Empfänger und -Sender ist hier die bessere Alternative. Obwohl kostenintensiver, wird dadurch der Zugriff auf das BIOS, die Bootsequenz und den DOS-Modus gewährleistet. Insbesondere der Zugriff auf den DOS-Modus der Server wird benötigt, um die Festplatten auf denen das Betriebssystem installiert wird, wie in Abschnitt 5.4.3 erläutert, zu sichern. Bei dem in Abbildung 2 mit CPU Switch bezeichneten Gerät handelt es sich um einen automatischen Umschaltmechanismus, der per Tastenkombination zwischen den Signalen der beiden Server umschaltet.

4.1.2 Serverschrank

Die sichere Unterbringung von EDV-Anlagen, die für die Aufrechterhaltung des Netzwerkbetriebes in einem Unternehmen relevant sind, stellt die erste Stufe zu einem geschützten Unternehmensnetzwerk dar. Alle unter Abschnitt 4.1 beschriebenen Komponenten werden daher in einem speziell für diesen Zweck konstruierten EDV-Schrank untergebracht. Vorteilhaft für die Montage der verschiedenen Geräte ist ein Schrank mit ausreichender Einbautiefe und integrierten vertikalen Schienen, die einen Abstand von 19 Zoll (19“) haben. In Fachzeitschriften und Katalogen werden diese Schränke oftmals als 19er-Rack bezeichnet. Der in diesem Projekt verwendete 19er-Rack-Schrank hat eine Einbautiefe von 80 cm und zusätzliche Auszugfächer, auf denen kleinere Komponenten platziert werden. Aufgrund der hohen zu erwartenden Wärmeabstrahlung der im Serverschrank montierten Geräte, wird ein Lüftersystem angeschlossen. Die Lüfter sorgen für eine konstante Temperatur und einen zirkulierenden Luftstrom, der an der Bodenplatte, vor Eintritt in den EDV-Schrank, durch einen Luftfilter geleitet wird.

4.2 Ausstattung der Clients mit Hard- und Software

Konsequenterweise müsste an dieser Stelle die Konfiguration des Betriebssystems und aller zugehörigen Softwarekomponenten der Server abgehandelt werden. Um jedoch die Wirkung dieser Komponenten auf das Client-Betriebssystem nachvollziehen zu können, wird zunächst auf die Konfiguration der Clients eingegangen. Die Wahl des Betriebssystems fällt auf Microsoft Windows2000 Professional. Das Office Paket wird in der Version 2002 oder besser bekannt unter dem Namen Office XP installiert. Alternativ wäre Office 2000 zu verwenden. Entwicklungen des Herstellers Microsoft werden erfahrungsgemäß innerhalb weniger Jahre durch neue Produkte ersetzt. Microsoft Office 2000 war zum Zeitpunkt der Anschaffung bereits seit 2 Jahren erhältlich. Durch Anschaffung der kostenintensiveren Office 2002 Lizenzen wird eine ausreichende Flexibilität hinsichtlich zukünftiger Anforderungen des Automobilherstellers gewährleistet. Im verwendeten Office Paket sind folgende Einzelkomponenten enthalten:

- Microsoft Word 2002 Version 10. Build 2627
- Microsoft Excel 2002 Version 10
- Microsoft Outlook 2002
- Microsoft Publisher 2002

An die Hardware der Client-Systeme werden keine besonderen Anforderungen gestellt. Es werden lediglich handelsübliche PCs mit zeitgemäßer Ausstattung bezüglich der Arbeitsspeicher und Prozessoren benötigt. Die Netzwerkkarte muss ebenfalls wie die der Server 100 MBit unterstützen. In einigen Fällen ist der Einsatz von 19 Zoll Monitoren, bedingt durch die vom Ersatzteilkatalog ETKA geforderte hohe Auflösung von 1280*1024 Pixeln, zwingend.

In allen Client-Systemen wird identische Hardware verwendet. Die Installation der Software, aller Treiber und des Betriebssystems wird dadurch, wie in Abschnitt 5.4.3 gezeigt, erleichtert. Zusätzliche Geräte wie Scanner, externe Speichermedien, Digitalkameras oder andere Peripheriegeräte können jederzeit an eine USB-Schnittstelle angeschlossen werden. Treiber für diese Geräte werden im Bedarfsfall vom Administrator oder einem autorisierten Mitarbeiter nachgeliefert.

4.3 Entfernte aktive Netzkomponenten

Entfernte aktive Netzkomponenten sind alle Peripheriegeräte, die über einen Ethernetanschluss mit dem Netzwerk verbunden sind. Ein Ziel dieser Arbeit ist die Verbindung nahezu aller Drucker mit dem Netzwerk, um eine freie Verfügbarkeit von Druckressourcen zu schaffen. Printserver sind Hardwarekomponenten, die das Netzinterface auf die Parallelschnittstelle des Druckers umsetzen. Printserver gibt es entweder als Steckkarte zum Einbau in dafür vorbereitete Drucker oder als externe Geräte, an die das Druckerkabel angeschlossen wird. In dieser Arbeit werden beide Varianten benötigt. Damit der Digitalkopierer an das Netzwerk angeschlossen werden kann, wird beim

Hersteller zunächst eine Druckerkarte für dieses Gerät beschafft. Die Druckerkarte ermöglicht den Anschluss von Druckern an den Parallelport des Kopierers. Auf diese Karte wird dann die Netzwerkkarte aufgesteckt. Hiermit steht ein vollwertiger Printserver des Herstellers Kyocera allen Benutzern des Netzwerks zu Verfügung. Für die Druckaufträge der Abteilung Service-Annahme wird eine weitere Printserverlösung benötigt. Reparaturaufträge werden von Nadeldruckern auf Endlospapier, das Durchschläge für die Monteure enthält, gedruckt. Das Original dieser Drucke erhält der Kunde als Anlage zur Rechnung. Da die Nadeldrucker keine Einschubfächer für Netzwerkkarten besitzen, wird ein externer Printserver mit zwei Druckeranschlüssen installiert. Normalerweise dient ein Server zur Bereitstellung der Druckertreiber. Nach der Installation der Drucker auf diesem Server werden die Gerätetreiber für die Benutzer freigegeben. Ein Logon-Skript[12] ordnet die Drucker bei der Anmeldung eines Benutzers an der Domäne dem jeweiligen Clientbetriebssystem zu. Diese Methode gewährleistet eine sehr sichere Verteilung von Druckressourcen über das Netzwerk. Jedoch funktioniert die Zuordnung von Druckertreibern mit herkömmlichen Microsoft-Methoden nicht zufrieden stellend. Der Einsatz von zusätzlicher Software, wie dem Logon-Skript-Prozessor Kixstart[13] wäre nötig, um genügend Parameter für die einwandfreie Funktionalität der Drucker an das Clientbetriebssystem zu übergeben. Da in dieser Arbeit nur wenige Drucker in der Systemumgebung eingesetzt werden, rechtfertigt der relativ geringe Nutzen nicht die zeitaufwendige Entwicklung von Logon-Skripten mit dieser Methode. Die Druckertreiber werden deshalb lokal installiert und mit einer Image-Datei[14] auf die Clientbetriebssysteme verteilt.

4.4 Domäne und Konfiguration der Server

Microsoft sieht bei der Verwendung zweier oder mehrerer Server in einer Domäne folgende Konfiguration vor. Der erste Server ist der Anmeldeserver. Auf ihm melden sich die Clientbetriebssysteme und die Benutzer über das Netzwerk an. Er führt die SAM-Datenbank[15], die Informationen zu den einzelnen Benutzerkonten enthält. Der zweite Server ist der Backup-Server. Alle Benutzereinstellungen, Skript-Dateien und die SAM-Datenbank werden mit diesem Server synchronisiert. Microsoft nennt den Anmeldeserver Primary-Domain-Controller (PDC) und den Backupserver Backup-Domain-Controller (BDC). Damit die Synchronisation in Echtzeit erfolgen kann, muss der BDC ständig am Netzwerk angeschlossen sein und läuft somit als vollständiger Backup-Server neben dem PDC. Die Synchronisation von Skript-Dateien unter den Servern wird im Fachjargon häufig als Replikation bezeichnet. Damit dieser Datenaustausch zustande kommt, wird auf den Servern ein spezieller Dienst, der Verzeichnisreplika-

---

[12] Logon-Skripte sind in Abschnitt 5.3.1 erklärt.

[13] Kixstart wird für die Erstellung umfangreicher Anmeldeskripte benutzt. Weiterführende Informationen sind auf folgender Website erhältlich. URL: http://kixstart.org. (Datum des letzten Zugriffs: 14.07.20003).

[14] Die Image-Dateien werden in Abschnitt 5.4.3 erläutert.

[15] Die SAM-Datenbank wird im Glossar erklärt.

tionsdienst installiert. Die Konfiguration von PDC und BDC erfolgt über eine spezielle Managementoberfläche, die sich Servermanager nennt. Damit bei Ausfall eines Servers der zweite Server problemlos die Domäne, Anwenderprogramme und Datenbanken übernehmen kann, wird, soweit lizenzrechtlich vereinbart, sämtliche Software auf beiden Servern installiert. Dazu zählen die unter Abschnitt 4.4.1 und 4.4.2 beschriebenen Komponenten, sowie die Programme für Service und Verkauf in Abschnitt 5.5 und 5.6. Zur einfacheren Unterscheidung von Domäne, Servern, Clients und anderen Netzkomponenten wird eine Namenskonvention erarbeitet. Die Domäne wird in Anlehnung an den Namen des Betriebes AVNDOM benannt. Tabelle 1 zeigt die schematische Benennung aller Netzwerkkomponenten. Der spätere Netzwerkname entsteht aus den Buchstaben und Zahlen (in Tabelle 1 fettgedruckt) des Standortes, der Domänenzugehörigkeit und einer laufenden Nummer.

Tabelle 1: Namenskonvention

NetBIOS-Name	Domänenzugehörigkeit	Nummer (Anz.)	Beschreibung
A08-VK3	**A**VNDOM	0**8**	Clientsystem des **V**er**k**äuferarbeitsplatzes **3**
A01-PSV	**A**VNDOM	0**1**	**P**rinter**s**er**v**er
A10-BH1	**A**VNDOM	**10**	Clientsystem des **B**uch**h**altungsarbeitsplatzes **1**

Die Server werden außerhalb der Namenskonvention benannt, da eine Identifizierung des Standortes nicht erforderlich ist. Der PDC erhält den Namen AVN1, der BDC erhält den NetBIOS-Namen AVN2. Dembowski (2002, S. 180) sieht das Wichtigste in der NetBIOS-Funktionalität darin, dass die Computer in einem Netzwerk über den jeweiligen Computernamen, also den NetBIOS-Namen, zu identifizieren sind.

4.4.1 Netzwerkdienste und Internetzugang

Škoda Auto Deutschland fordert die Realisierung eines reinen Microsoft-Netzwerkes. Aus diesem Grund werden alle Netzwerkdienste und Protokolle nach den Vorgaben von Microsoft installiert. Die Kommunikation zwischen den Netzkomponenten wird über die Standarddienste *Client für Microsoft Netzwerke* und die *Datei und Druckerfreigabe für Microsoft Netzwerke* abgewickelt. Diese beiden Netzwerktreiber werden in Betriebssystemen von Microsoft mitgeliefert und stellen die grundlegenden Netzwerkfunktionalitäten zur Verfügung. Alle Netzkomponenten erhalten fest zugewiesene IP-Adressen. Das DHCP-Protokoll[16] wird zunächst nicht eingesetzt. In beiden Servern

[16] Das DHCP-Protokoll wird ausführlich im Glossar beschrieben. Zukünftig ist der Einsatz des DHCP-Protokolls zwingend erforderlich. Siehe Abschnitt 5.4.1 und Abschnitt 7.2

sind jeweils zwei Netzwerkkarten vorhanden. Die erste Netzwerkkarte verbindet den Server mit dem Switch und damit mit dem LAN. Über den zweiten Netzwerkadapter wird ADSL im Netzwerk verteilt. SAD bietet verschiedene Möglichkeiten für den Aufbau eines VPN-Tunnels zwischen dem LAN des Betriebes und dem Škoda-Extranet. Der Einsatz eines externen Hardware-Routers ist ebenso zulässig, wie die Verwendung eines softwareseitigen VPN- und Gateway-Servers. Der Support der Hardwarelösung stellte sich als aufwendiger heraus, da SAD Zugriffe auf den Hardware-Router seitens des Administrators des lokalen Netzwerkes nicht zulässt. Bei Ausfall des Routers oder einem Fehler in der Vermittlungsstelle des ADSL-Anbieters müsste telefonisch ein zuständiger Mitarbeiter von SAD verständigt werden, der im Bedarfsfall wiederum den ADSL-Provider verständigt. Alles in allem wären diese Vorgänge viel zu aufwendig und langwierig. SAD biete eine gleichwertige softwareseitige Lösung des Herstellers NCP an. Der lokale Administrator hat bei dieser Variante uneingeschränkten Zugriff auf die Bedienoberfläche. Es handelt sich dabei um ein VPN-Gateway, das einerseits die Vermittlung von ADSL in Form des *Point-to-Point Protokolls over Ethernet* (PPPoE) und andererseits den Aufbau eines definierten VPN-Tunnels zu einem Endpunkt zulässt. Eicker (2003) definiert PPPoE als Protokoll, das bei einer Verbindung über ADSL zum Internet verwendet wird, um das übertragene Datenvolumen zu bestimmen. Bei ADSL handelt es sich technisch gesehen um eine Standleitung, also eine permanente Verbindung. Diese wird in der Regel nach übertragener Datenmenge abgerechnet. Damit die Berechnung auch bei ADSL angewendet werden kann, wurde ein neues Protokoll entwickelt. PPPoE basiert auf zwei gebräuchlichen Standards, den Protokollen PPP und Ethernet. PPP ist das Standardprotokoll beim Aufbau einer Wählverbindung zum Internet-Provider mit Hilfe eines Modems.

Die LAN-seitige IP-Adresse des Servers wird als Standardgateway, also als Zugangspunkt für alle Clients des Netzwerkes, definiert. Die IP-Adresse der zweiten Netzwerkkarte, die direkt mit dem ADSL-Modem verbunden ist, wird als Anfangspunkt des Škoda-VPN verwendet. Abbildung 3 auf Seite 35 zeigt die notwendigen Einstellungen der Netzwerkadapter auf den Client-Betriebssystemen. Zusätzlich bietet die Lösung des Herstellers NCP eine integrierte Firewall und damit Schutz vor Hackerattacken. Eine Firewall ist ein Filter, der Hacker-Angriffe, Viren und unberechtigte Zugriffe auf einen einzelnen Rechner oder ein ganzes Netzwerk verhindert. Firewalls können entweder als reine Software-Lösung installiert werden, oder aber eine Kombination von Soft- und Hardware bilden. Die reine Software-Lösung ist in der Regel auch die billigste und bietet je nach Preisklasse mehr oder weniger effektiven Schutz. Die Firewall, die hier verwendet wird lässt aber keinen Vergleich zu einer speziell für diesen Zweck entwickelten Soft- oder Hardware zu, da die Einstellungsmöglichkeiten bei der Lösung von NCP zu gering sind. Unter Kapitel 7 wird deshalb die künftige Integration einer besseren Variante angesprochen.

4.4.2 Benutzermanager für Domänen

Die Benutzer einer Microsoft-Domäne werden serverseitig im Benutzermanager für Domänen verwaltet. In dieser Arbeit sind grundsätzlich alle Benutzer automatisch Domänen-Benutzer. Eine lokale Anmeldung an Clientsystemen wird nicht erlaubt und durch Entzug der entsprechenden Rechte auf den Clients verhindert. Aus der Analyse aller Geschäftsprozesse des Betriebes können zwei übergreifende Gruppen der Domäne gebildet werden.

1. **Benutzergruppe *Verkauf2000*:** Mitglieder dieser Benutzergruppe arbeiten im Verkaufsbereich und benötigen deshalb identische Einstellungen und den gemeinsamen Zugriff auf spezielle Software des Verkaufsbereiches. Benutzer dieser Gruppe sind unter anderem der Verkaufsleiter und die Verkäufer.
2. **Benutzgruppe *Service2000*:** Mitglieder dieser Gruppe arbeiten weitestgehend im Bereich Service/Auftragswesen und Kundenbetreuung. Dazu zählen unter anderem alle Mitarbeiter der Serviceannahme oder Mitarbeiter des Teiledienstes. Alle Benutzer dieser Gruppe benötigen Zugriff, Lizenzen und entsprechende Rechtevergabe auf die Branchensoftware (siehe Abschnitt 5.5).

Alle weiteren Gruppen sind unter Abschnitt 5.3 erläutert. Teilweise werden individuelle Gruppen für die Verteilung von Systemrichtlinien, wie in Abschnitt 5.3.3 beschrieben, benötigt. Für jeden Benutzer wird ein Home-Laufwerk, wie in Abschnitt 5.3.1 erläutert, auf dem Server freigegeben. Auf diesem Laufwerk speichern die Mitarbeiter des Unternehmens ihre persönlichen Daten. Die Pfade zu diesen Laufwerken und die Pfade zu den Benutzerprofilen werden unter den Konfigurationsoptionen im Benutzermanager für Domänen eingegeben. In Abschnitt 5.3 ist die Realisierung beschrieben.

5 Realisierung

In diesem Kapitel wird die Realisierung der Arbeit beschrieben. Basierend auf den konzeptionellen Überlegungen im vorigen Kapitel 4 werden Methoden und Wege zur Konfiguration der Server erläutert. Zum Verständnis der hier ausgeführten Beschreibungen werden Kenntnisse im Umgang mit dem Serverbetriebssystem Windows NT Server benötigt. Administratives Wissen über die Benutzerverwaltung und Rechtevergabe auf NT- oder Windows2000-Systemen muss dem Leser bekannt sein. Kenntnisse über den Aufbau von NT-Netzwerken und die Struktur der Microsoft Registrierdatenbank sind ebenfalls erforderlich. Lesern, denen diese Begriffe nicht bekannt sind wird empfohlen, dieses Kapitel zu überspringen.

Um die Realisierung der im vorigen Kapitel erstellten Konzeption zu erläutern, wird zunächst in der folgenden Tabelle die exakte technische Beschreibung der Hardware-Komponenten der Server und Clients aufgezeigt. Die Spalten in Tabelle 2 beschreiben die Ausstattung jeweils eines Systems.

Tabelle 2: Hardwareseitige Ausstattung

Komponente	Serversystem	Clientsystem
Prozessor	Zwei Intel Pentium Prozessoren mit je 1000 Mhz	Intel Pentium mit 1,7 Ghz
Hauptplatine	Mainboard des Herstellers A-Open mit entsprechendem Chipsatz zur Verwendung von Doppelprozessoren	Mainboard mit aktuellem Chipsatz
Arbeitspeicher	512 MB SDRAM	128 MB RAM
SCSI-Controller	Adaptec Ultra 160 SCSI-Controller	n.V.
Netzwerkkarte	Zwei NIC´s des Herstellers 3Com mit umfassenden Verwaltungsoptionen (Chip: 3CR990)	NIC für Desktopsysteme des Herstellers 3Com (Chip: 3C905TX)
Festplatte	Zwei SCSI-Festplatten des Herstellers IBM mit einer Speicherkapazität von jeweils 35 GB	30 GB Festplatte des Herstellers IBM

Bandlaufwerk	Hewlett Packard DDS3-Streamer HP C1537A mit einer Speicherkapazität von 24 GB und hardware-seitiger Komprimierung	n.V.
ISDN-Karte	Aktive ISDN-Karte des Herstellers AVM	Fritz-Karte von AVM
Laufwerke	CD-ROM, Floppy	CD-ROM, Floppy

5.1 Zeitplan für die Einführung

In der Firma Auto-Vertrieb-Neckar GmbH existiert bereits eine EDV-Anlage. Sämtliche in dieser Arbeit beschriebenen Komponenten werden daher unabhängig von der alten Anlage installiert und konfiguriert. Erst nach Abschluss aller Arbeiten wird die neue Lösung für den produktiven Betrieb freigegeben. Vorab wird ein mehrtägiger Testlauf mit Benutzern der beiden übergreifenden Gruppen Service2000 und Verkauf2000 durchgeführt. Die Installation der gesamten EDV-Anlage erfolgt in drei Stufen.

1. Die Verkablung von RJ45 EDV-Dosen im Gebäude und der Anschluss des Patchpanels wird von einem Elektrik-Fachbetrieb durchgeführt. Aus Sicherheitsgründen werden Cat. 6 S/STP Kabel verwendet. Diese Kabel sind mehrfach geschirmt und bieten den größtmöglichen Schutz vor Störstrahlung.
2. Nach der Verkabelung des Unternehmens werden die Server und alle anderen Komponenten im Serverschrank in Betrieb genommen.
3. Nach der Installation des ersten Clientsystems wird, wie in Abschnitt 5.4.3 beschrieben, eine Image-Datei der Festplatte erzeugt. Mit diesem Image werden alle weiteren Clientbetriebssysteme aufgesetzt.

5.2 Netzwerkeinstellungen

Die Konfiguration der LAN-Verbindungen wird mit statischer IP-Adressierung vorgenommen. Mit der Subnet-Maske 255.255.255.0 (siehe Abbildung 3, S. 35) wird das Netzwerk als Class-C-Network definiert. Als Standardgateway[17] wird die IP-Adresse des Servers verwendet. Unter der Schaltfläche *Erweitert* werden für die NetBIOS Namensauflösung die WINS-Server eingetragen. Beide Server AVN1 und AVN2 sind als WINS-Server und damit als Push- und Pullpartner konfiguriert. Die Einträge in die Registerkarte sehen folgendermaßen aus:

[17] Das Standardgateway ist die LAN-seitige IP-Adresse der ersten Netzwerkkarte des Servers (Siehe Kapitel 4.4.1)

- 1. WINS-Server: IP-Adresse des PDC = 200.1.104.97
- 2. WINS-Server IP-Adresse des BDC = 200.1.104.99

Als DNS (Domain Name Server) werden die IP-Adressen der DNS-Server der Deutschen Telekom eingetragen. Domänenbenutzer und damit alle Benutzer des Betriebes haben keinen Zugriff auf die Einstellungen der Netzwerkumgebung. Die exklusiven Rechte liegen beim Domänen-Administrator oder einem lokalen Administrator.

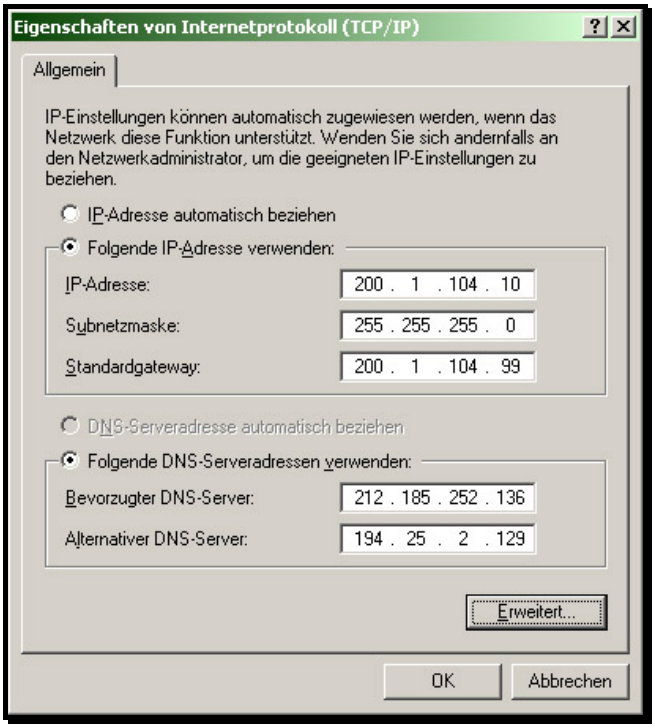

Abbildung 3: Konfiguration der LAN-Verbindung

5.3 Benutzermanagement - Benutzerdaten - Benutzerprofile

Mit dem Benutzermanager des Servers werden in einer WinNT-Domäne alle globalen Gruppen und Domänenbenutzer verwaltet. Microsoft spricht deshalb vom *Benutzermanager für Domänen*. Mit der Installation von WinNT Server werden einige globale Gruppen und Standardbenutzer, wie das Konto des Administrators oder der Gastzugang eingetragen. Insbesondere der Gastzugang ist ein Sicherheitsrisiko und wird deshalb deaktiviert. Abbildung 4 auf Seite 36 zeigt die Konfiguration für die Domäne AVNDOM. Die Domänenbenutzer sind entweder der Gruppe Service2000 oder der Gruppe Verkauf2000 zugeordnet. Damit im Bedarfsfall alle Benutzer angesprochen werden können, sind sie zusätzlich in der Gruppe der Domänen-Benutzer zusammengefasst. Folgende Einstellungen werden in den einzelnen Konten der Benutzer getroffen:

- Pfad für das Profilverzeichnis

- Pfad für das Anmeldeskript
- Pfad für das Basisverzeichnis (Home-Laufwerk)
- Anmeldezeiten werden nur zwischen 05:00 Uhr und 23:00 Uhr gestattet
- Die Clientsysteme, die für den jeweiligen Benutzer verfügbar sind

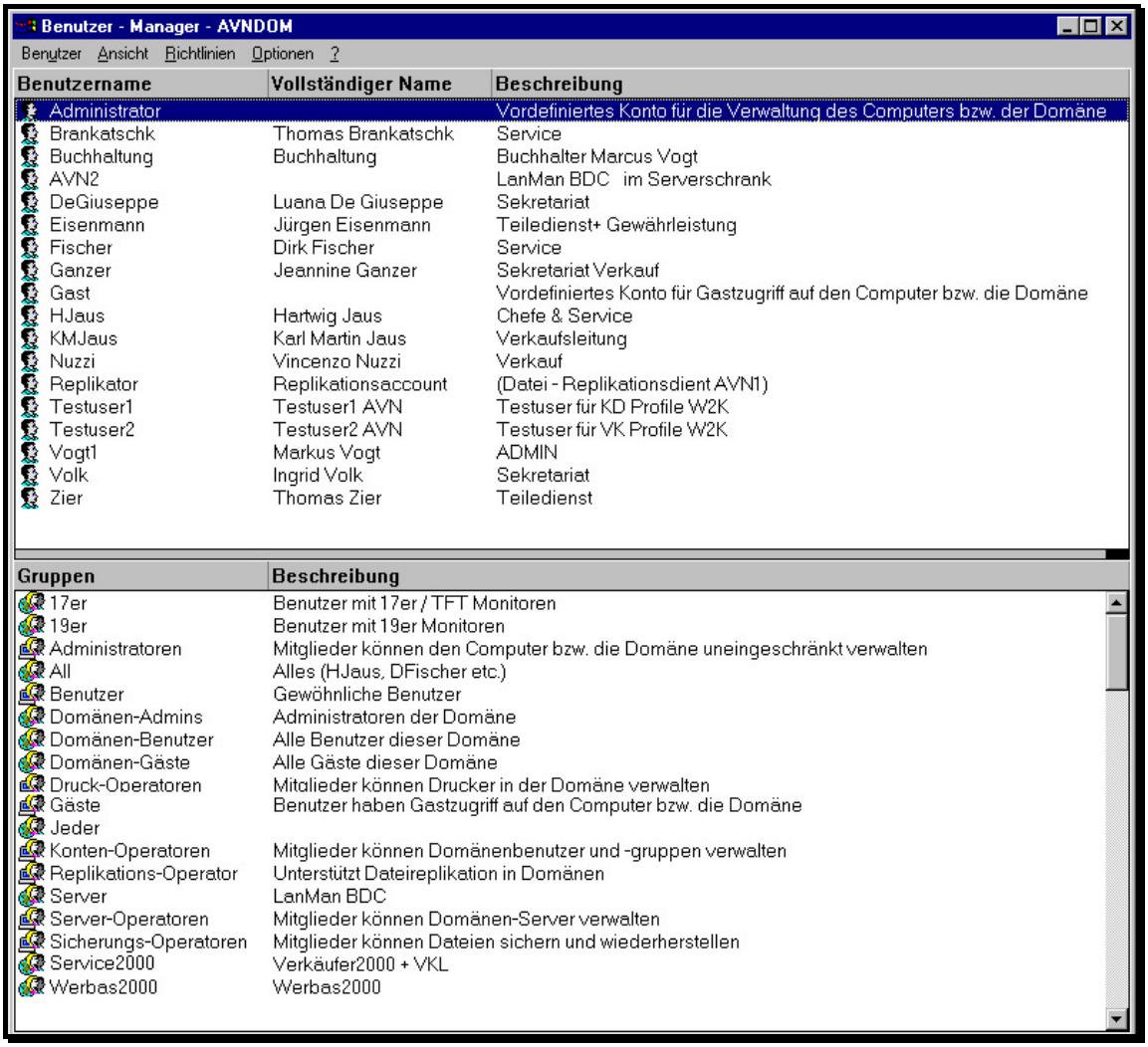

Abbildung 4: Benutzermanager für Domänen

Mitglieder der Gruppe 17er in Abbildung 4 arbeiten an einem 17 Zoll Monitor. Diese Gruppe wird in der Konfiguration der Systemrichtlinien getrennt zu den beiden Haupt-Benutzergruppen angesprochen. Da auf einem 17 Zoll Monitor ein kleineres Hintergrundbild als auf einem 19 Zoll Monitor verwendet wird, müssen in den Pfadangaben der Systemrichtlinien[18] unterschiedliche Dateien als Hintergrundbilder angesprochen werden. Eine weitere Besonderheit ist die Gruppe Server. Mitglieder dieser Gruppe

[18] Die Systemrichtlinien werden in Abschnitt 5.3.3 erläutert. Abbildung 17 auf Seite 67 zeigt das Hintergrundbild auf dem Desktop eines Clientbetriebssystems.

sind das administrative Konto AVN2 und die Domänen-Administratoren. Microsoft schlägt diese Konstellation zur Anmeldung des BDC vor.

5.3.1 Laufwerksfreigaben

Möglichst alle Daten, mit denen auf einem Client gearbeitet werden müssen auf den Laufwerken des Servers gespeichert werden. Damit die künftigen Benutzer auf die Daten zugreifen können, werden entsprechende Netzlaufwerke gemappt und für die jeweiligen Benutzergruppen freigegeben. Die Dateiberechtigungen werden ebenfalls nur auf die Gruppen zugelassen, die tatsächlich mit dem Netzlaufwerk arbeiten. Für das Erstellen (Mappen) von Netzlaufwerken auf den Clients ist es rationeller, ein Anmeldeskript (Logon-Skript) zu erstellen. Abbildung 5 zeigt das Skript der Gruppe Service2000 im Texteditor. Im ersten Teil des Skriptes wird die Uhrzeit des Servers AVN1 ausgewertet und mit dem Clientbetriebssystem synchronisiert. Danach folgen Anweisungen zu den einzelnen Mappings. Im unteren Teil von Abbildung 5 sorgt die Anweisung `wait 15` dafür, dass das Skript für 15 Sekunden angehalten wird. In dieser Zeit wird auf den Clients der Virenscanner aktiviert. Ohne diese Pause führten der gleichzeitige Start des Virenscanners und das aktive Logon-Skript häufig zu Systemabstürzen. Nach dieser Anweisung wird der Mail-Client Outlook durch die Anweisung `start OUTLOOK` aufgerufen. Outlook startet demnach automatisch bei der Anmeldung eines Users an die Domäne und überprüft die E-Mail-Konten. Diese Maßnahme wird eingeführt, da die User in der Vergangenheit oftmals vergaßen, nach Ankunft im Betrieb ihre E-Mail-Konten zu überprüfen. Logon-Skripte werden einem oder mehreren Benutzerkonten oder Benutzergruppen zugeordnet.

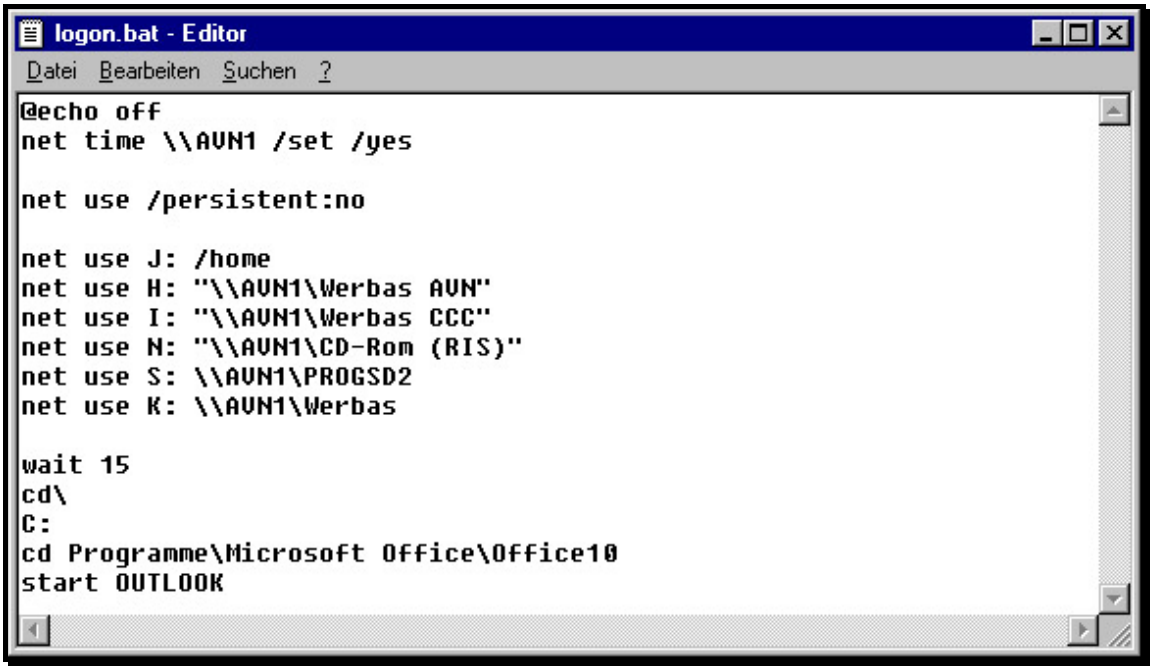

Abbildung 5: Logon-Skript

Administratoren haben aus Sicherheitsgründen ein eigenes Skript. Die Skripte werden bei der Anmeldung eines Benutzers vom Client-Betriebssystem abgearbeitet. Sämtliche Skripte werden im Replikationsordner des Verzeichnisreplikationsdienstes bzw. dem Netlogon-Share gespeichert (siehe Abschnitt 5.3.3.3). Anmeldeskripte werden den Benutzern oder Gruppen im Benutzermanager für Domänen zugeordnet (siehe Abschnitt 5.3, Abbildung 4). Folgende Laufwerke werden durch das Logon-Skript gemappt:

- **Laufwerk J:** Auf diesem Laufwerk speichert der jeweilige Benutzer seine persönlichen Dateien ab. Er besitzt Dateiberechtigungen für das Erstellen, Löschen und Ausführen von Dateien. Jedem Benutzer ist ein separates Laufwerk zugeordnet.
- **Laufwerk H:** Netzlaufwerk der Car Dealer Software *Werbas.* Die Datenbanken der Werbas-Software sind hier und in den enthaltenen Unterordnern hinterlegt.
- **Laufwerk I:** Datenbanken der Software *Werbas*.
- **Laufwerk N:** Freigegebenes CD-ROM Laufwerk des Servers AVN1. Auf der CD-ROM befinden sich Informationen und ein Teilekatalog für die Abwicklung von Reparaturaufträgen.
- **Laufwerk S:** Zentrale Datenbanken aller SilverDAT Anwendungen
- **Laufwerk K:** Additionale Daten zu *Werbas* wie Handbuch und Export-Dateien für andere Anwendungen.

Die Installation der hier erwähnten Anwendersoftware wird in Abschnitt 5.5 und 5.6 erklärt. Zusätzlich wird eine weitere Freigabe auf den Laufwerksbuchstaben X:\ gemappt. Diese Freigabe dient dem Datenaustausch, beispielsweise für Office-Dokumente, der Benutzer untereinander. Für diesen Share werden Rechte für Lese-, Schreib-, Lösch- und Ausführungsvorgänge an alle Benutzer vergeben.

5.3.2 Benutzerprofile

Benutzerprofile werden bei Windows2000 Professional standardmäßig unter folgender Struktur angelegt:

```
C:\Dokumente und Einstellungen\%USERNAME%
```

%USERNAME% ist eine Systemvariable, die für den Namen der oder des Benutzers steht. Für servergespeicherte Profile eignet sich auch jede andere beliebige Verzeichnisstruktur. Auch die standardmäßige Struktur des Servers kann verwendet werden. Wichtig ist, dass für servergestützte Profile eine geeignete Netzlaufwerksfreigabe existiert, beispielsweise \\server\Profiles. In der zugeordneten Struktur ist das Profil mit dem Namen des Benutzers gespeichert. Abbildung 6 auf Seite 40 zeigt, stellvertretend für alle Benutzer, die Struktur des Benutzerprofils für den Benutzer „Brankatschk“. Der Ordnername für das Profil wird nicht durch manuelle Eingabe erzeugt, sondern durch

die entsprechende Systemvariable %USERNAME%. Im Benutzermanager für Domänen wird den Benutzern der Pfad zu ihrem Benutzerprofil mit der Eingabe:

```
\\avn1\Profiles$\%USERNAME%
```

zugewiesen. Nur dieser Eintrag verursacht die Verwendung servergespeicherter Profile für die Benutzer auf den Clientsystemen. Alle Benutzer einer Gruppe müssen sich auf allen in ihrer Gruppe zugelassenen Clientsystemen anmelden können. Aus diesem Grund wird die Outlook-Datendatei in dem Teil des Profils abgespeichert, das auf die entsprechende Laufwerksfreigabe des Servers kopiert wird. Bei der Anmeldung eines Benutzers an die Domäne wird die Datendatei in das lokale Benutzerprofil kopiert. Die Benutzer haben, unabhängig von der Anmeldung am Client, stets ihr eigenes Outlook-Profil zur Verfügung. Nach diesem Schema wird mit allen Dateien verfahren, die standardmäßig von Windows2000 in den Ordnern des Benutzerprofils verankert sind und nicht zum servergespeicherten Profil gehören. Ein weiteres Beispiel ist die Datei mit der Erweiterung *.pab, in der das Adressbuch des Benutzers gespeichert wird. Die Pfadangaben zu diesen Dateien werden durch entsprechende Systemrichtlinien korrigiert[19].

[19] Siehe auch Kapitel 6

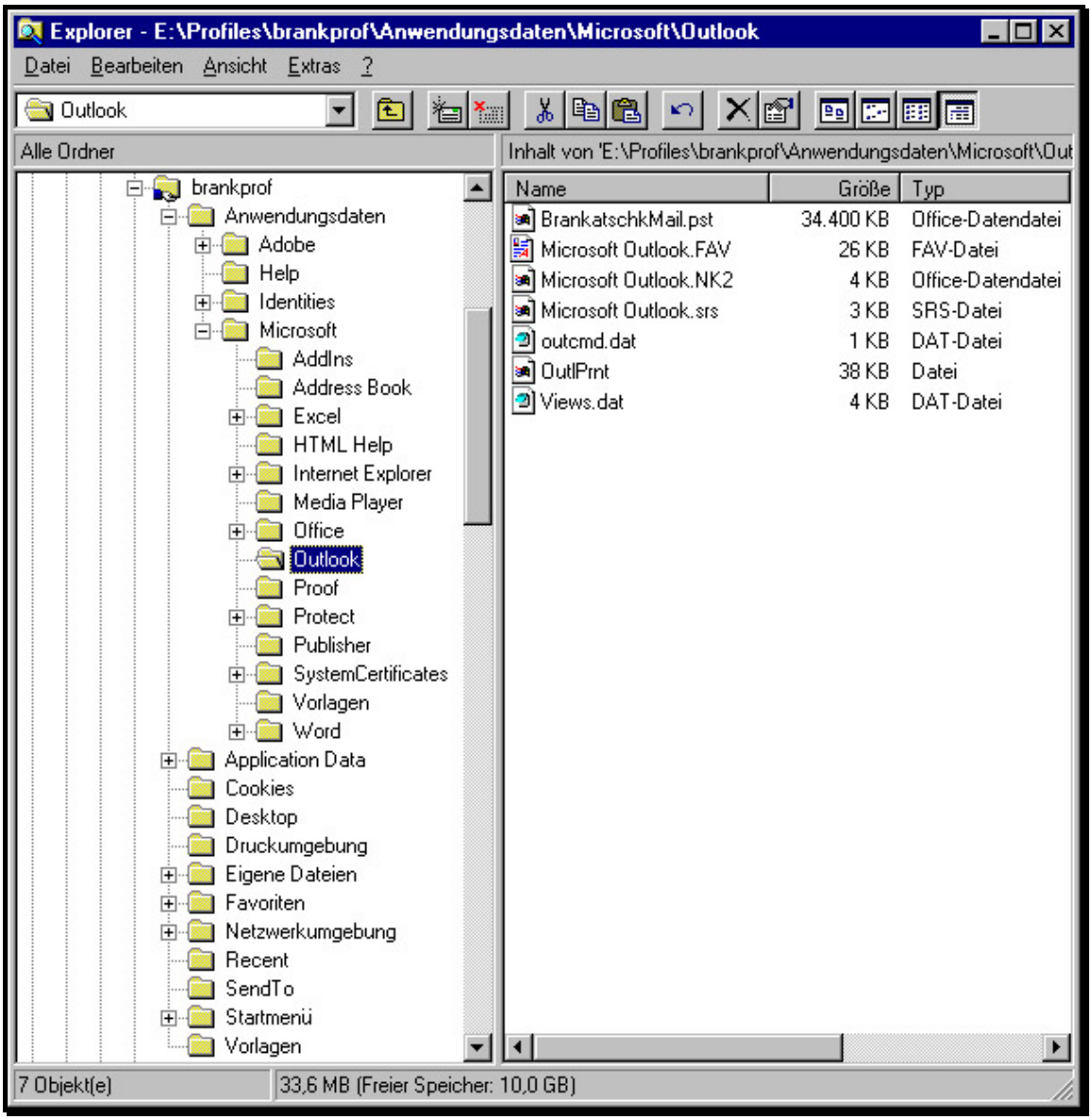

Abbildung 6: Servergespeichertes Benutzerprofil

Abbildung 6 zeigt die Struktur des servergespeicherten Benutzerprofils in einer Ordnerfreigabe des Servers AVN1. Im aktivierten Ordner *Outlook* befinden sich die Datendatei und andere Dateien zur Erzeugung des Mailprofils von Microsoft Outlook. Von Usern wird die Verwendung von servergespeicherten Profilen nicht bemerkt.

5.3.2.1 Zusammenhänge mit Systemrichtlinien

Systemrichtlinien dominieren über Benutzerprofile. Verweise zu Profilen gibt es im Systemrichtlinieneditor unter dem Eintrag *Standard Computer* und im gesamten Zweig des standardmäßigen Benutzers. Sowohl Benutzerprofile, als auch Systemrichtlinien steuern Informationen zu dem Teil der Registrierdatenbank, der für die Einstellungen des angemeldeten Benutzers relevant ist, bei. Auf die Umgebungsvariablen %USERPROFILE% und %SystemRoot%, die die Platzierung des Profils des Benutzers reflektieren, kann referenziert werden. Angewendet werden die Umgebungsvariablen bei-

spielsweise in den Systemrichtlinien im Standardpfad für Programme. Die Variable %SystemRoot% ersetzt immer den Pfad des standardmäßigen Installationsordners eines Microsoftbetriebssystems. Bei Windows NT und Windows2000 Professional ist dies zum Beispiel *C:\WinnNT\.*

5.3.3 Systemrichtlinien

Windows speichert Informationen über seine Konfiguration in einer binären, hierarchisch organisierten Datenbank. Aufbau der ersten Hierarchieebene:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_CONFIG
- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_USER
- HKEY_USERS

Diese Unterteilungen sind nun in weitere Unterschlüssel eingeteilt. Jeder Schlüssel kann weitere Unterschlüssel und Werteinträge enthalten. Diese Werteinträge setzen sich aus drei Teilen zusammen: dem Namen, dem Datentyp und einem zugewiesenen Wert. Die Betriebssysteme Windows NT bzw. Windows2000 Professional erkennen standardmäßig fünf Datentypen. Die Website Winfaq.de[20] liefert bei Bedarf ausführliche Erläuterungen zur gesamten Registrierdatenbank. Systemrichtlinien dienen zur Konfiguration von Rechnern mit Microsoft Betriebssystemen, die sich an einer Domäne anmelden. Beim Anmeldevorgang werden die Einstellungen der Richtliniendatei in die Registrierdatenbank (engl. Registry) des jeweiligen Clients eingelesen bzw. die Registry des Clients wird gemäß der Konfiguration der Systemrichtlinien-Datei, hier NTConfig.pol siehe Abbildung 7, verändert. Zwei wichtige Schlüssel der Registry müssen zum Verständnis unterschieden werden.

1. HKEY_LOCAL_MACHINE
   Unter diesem Schlüssel lassen sich Einstellungen konfigurieren, die für das Betriebssystem und die Software, unabhängig vom angemeldeten Benutzer, gelten.
2. HKEY_CURRENT_USER
   Unter diesem Schlüssel werden Einstellungen festgelegt, die ausschließlich für den angemeldeten Benutzer, unabhängig vom Betriebsystem, gelten.

Die jeweiligen Schlüssel werden im Systemrichtlinien-Editor, der im Lieferumfang von Microsoft Windows NT enthalten ist, durch verschiedene Symbole dargestellt. Für den Zusammenhang HKEY_CURRENT_MACHINE wird ein Computersymbol verwendet und für den Zusammenhang HKEY_CURRENT_USER wird stellvertretend für den User ein Kopfsymbol verwendet. Zusätzlich können Benutzergruppen aus dem Benutzermanager des Servers in den Systemrichtlinien-Editor übernommen werden. Da-

[20] Internet-Adresse im Literaturverzeichnis

durch wird es möglich, Einstellungen für mehrere Benutzer schnell und ohne großen Aufwand zu erstellen. Benutzergruppen werden durch das einschlägig bekannte Symbol von Windows NT für Gruppen dargestellt (siehe Abbildung 7). Einstellungen für Benutzergruppen gelten immer für den Schlüssel HKEY_CURRENT_USER und nicht, wie man vermuten könnte, für den Schlüssel, der alle angemeldeten Benutzer des jeweiligen Clients (HKEY_USERS) betrifft. Um die exakte Wirkung der jeweiligen Systemrichtlinien-Datei auf die Registry zu beurteilen, sollte in jedem Falle vorab die zugehörige Systemrichtlinien-Vorlagendatei in einem Texteditor geöffnet werden (siehe Abbildung 8, S. 46).

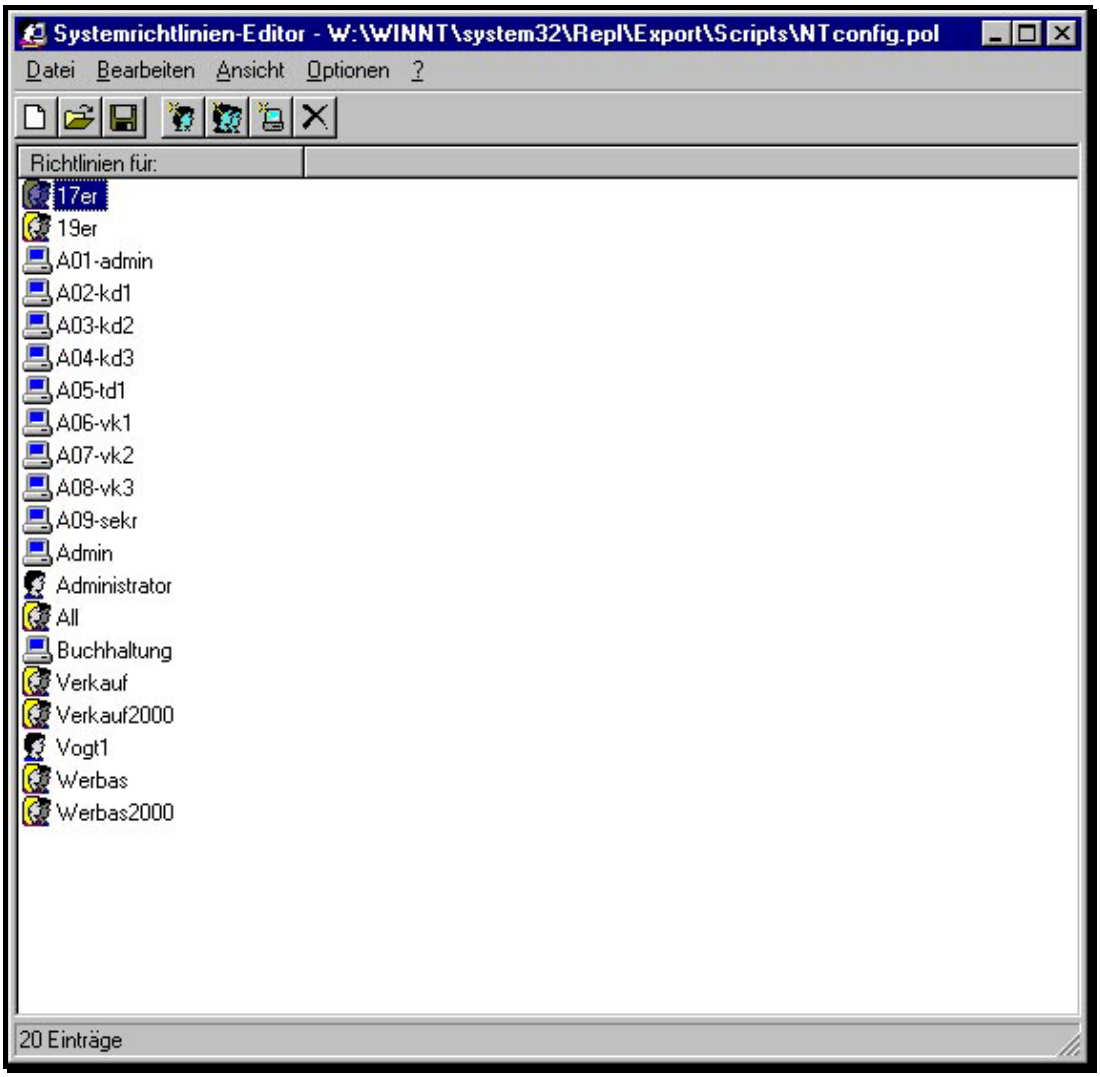

Abbildung 7: Datei NTConfig.pol im Systemrichtlinieneditor

5.3.3.1 Richtlinienvorlagen – ADM Files

Die Systemrichtlinien-Vorlagendateien sind an der Dateierweiterung *.adm, im Folgenden ADM-Dateien genannt, zu erkennen. Zwei ADM-Dateien werden mit der Installa-

tion von Windows NT mitgeliefert. Die Dateien befinden sich nach der Installation im Verzeichnis %Systemroot%\INF.

- Datei Common.adm
- Datei Winnt.adm

Die beiden Dateien sind ergänzend zueinander zu verwenden. Einstellungen in beiden Dateien können sowohl den Schlüssel HKEY_CURRENT_MACHINE, als auch den Schlüssel HKEY_CURRENT_USER betreffen. Mit den Schlüsseln der Registry sind hier die eigentlichen Schlüssel und alle darin enthaltenen Unterschlüssel gemeint. Darüber hinaus werden weitere Vorlagendateien von Microsoft angeboten. Für alle gängigen Office-Pakete sind ADM-Dateien, mit denen beispielsweise der Speicherort für *Eigene Dateien* oder benutzerspezifische Einstellungen für Outlook verändert werden können, kostenlos bei Microsoft erhältlich.

Durch Vorlagen-Dateien kann verhindert werden, dass bestimmte oder alle Benutzer Zugriff auf bestimmte Konfigurationsoptionen des Betriebsystems und der Anwendersoftware des Clients haben. Dadurch wird es möglich, ergänzend zur dürftigen Rechtevergabe des Benutzermanagers für Domänen, Sicherheit gegen Fehlbedienung zu gewährleisten. Winfaq (2003) gibt in folgender Aufstellung einen beispielhaften Überblick über mögliche Konfigurationswerte, die in ADM-Dateien verändert werden können.

1. Systemsteuerung: Einstellen der Systemmöglichkeiten für die Anzeige.
2. Desktop: Festlegen eines Hintergrundbildes.
3. Shell: Beschränken von Einstellungen auf dem Desktop (Suchen, Beenden, Ausführen usw.).
4. System: Deaktivierung des Registrierungseditors und Erstellen einer Liste der erlaubten, vom Benutzer auszuführenden, Windows-Anwendungen, Autostart von bestimmten Anwendungen und Setzen von SNMP-Zielen.
5. Windows NT Shell: Anpassen des Startmenüs und der Desktop Oberfläche, Festlegen von bestimmten Ordnern für die Shell.
6. Windows NT System: Anmeldevorgang, Einlesen der Autoexec.bat, Task-Manager und Anzeigen der Meldungen beim Systemstart.
7. Netzwerk: Umgang mit den Systemrichtlinien, Angabe des Pfades für das Update der Systemrichtlinien.
8. Windows NT Netzwerk: Aktivieren bzw. Deaktivieren der administrativen Laufwerksfreigaben (SHARE$ /LAUFWERK$).
9. Windows NT-Drucker: Deaktivieren des Drucker-Spoolers zur Steigerung der System- und Netzwerkleistung.
10. Windows NT-Remote-Zugriff: Festlegung der Zeiten für wiederholte Versuche, um eine Echtheitsbestätigung von Servern zu bekommen.

11. Windows NT-Benutzerprofile: Löschen zwischengespeicherter Server-Profile.
12. Profilgröße einschränken: Damit wird die Größe für das persönliche Profilverzeichnis (C:\WINNT\PROFILES\ [USER-ID]) festgelegt. Da dieses Verzeichnis bei jeder An- und Abmeldung über das Netzwerk kopiert wird, ist es sinnvoll, dieses auf eine bestimmte Größe zu beschränken. Wird die Größe überschritten, wird der Anwender darauf hingewiesen und kann sich erst abmelden, wenn er das Profilverzeichnis auf die eingestellte Größe anpasst, indem er zum Beispiel Dateien in ein anderes Netzwerklaufwerk kopiert oder Mails löscht.

Unter Verwendung von Microsoft Windows2000 als Clientbetriebssystem wird es erforderlich, die bestehenden Richtlinien-Vorlagendateien von Windows NT Server an die Registry von Windows2000 anzupassen. Microsoft sieht vor, die Systemeinstellungen der Clients mit Windows2000 Betriebsystem über die Gruppenrichtlinie der Windows2000 Domäne zu beherrschen. Die Gruppenrichtlinie ist unter Windows2000 Server als Active-Directory bekannt und stellt ein sehr mächtiges Werkzeug zur Verwaltung von Konfigurationen und Rechtevergabe in einer Windows2000 Domäne dar. Da auf NT-Servern, die in dieser Arbeit verwendet werden, nur mit erheblichem Aufwand ein Windows2000 kompatibles Active-Directory zu realisieren wäre, wird deshalb auf die von Windows NT bekannten Systemrichtlinien zurückgegriffen. Bestimmte Schlüssel der Windows2000 Registrierdatenbank unterscheiden sich stark von der Registry des Betriebssystems Windows NT. Dabei ist im Einzelfall durch Untersuchung und Vergleich der beiden betriebssystemspezifischen Registrys zu bestimmen, an welche Stelle der Windows2000 Registry der gewünschte Windows NT Schlüssel zu platzieren ist. Manche Schlüssel, zugehörige Einträge und davon abhängige Werte sind unter Windows2000 nicht oder nur in veränderter Form zu gebrauchen.

Es lohnt sich im Bedarfsfall ein Blick in das TechNet[21] von Microsoft. In dieser Online-Datenbank werden Lösungen zu microsoftspezifischen Problemen angeboten. Auch das Abbonieren der entsprechenden Whitepapers von Microsoft ist eine lohnende Investition. Prinzipiell besteht die Möglichkeit, jeden der anfangs erwähnten Schlüssel und ihre zugehörigen Unterschlüssel der Windows2000 Registry zu verändern.

5.3.3.2 Systemrichtlinienvorlagen im Texteditor erstellen

Durch Einsatz von Systemrichtlinien in einer Domäne ist es möglich, große Teile der Registry eines einzelnen Clients zu beeinflussen. Microsoft bietet die Möglichkeit, durch Erstellen von selbst programmierten Systemrichtlinien-Vorlagendateien mit Hilfe eines Texteditors, Schlüssel und zugehörige Werte der Client-Registry zu bearbeiten. Die Datei wird im ASCII Format abgespeichert. Durch Einlesen dieser Datei in den Systemrichtlinien-Editor wird der darin enthaltene Quellcode in eine graphische Benutzeroberfläche (engl. Graphical User Interface, GUI) umgewandelt. Durch Bestätigen oder Verwerfen mittels Checkboxen oder Texteingabe können zuvor programmierte

[21] Deutsches Microsoft TechNet. URL: http://www.microsoft.com/germany/technet/. (Datum des Letzten Zugriffs: 15.07.2003)

Werte der Registry aktiviert oder deaktiviert werden. In dieser Arbeit werden Systemrichtlinien-Vorlagendateien selbst erstellt. Ebenso werden von Microsoft erhältliche Vorlagendateien an die Registry von Windows2000 angepasst. Eine Aufstellung aller gängigen Befehle, die in ADM-Dateien Verwendung finden, ist im Internet auf den Webseiten von Winfaq ersichtlich. Abbildung 8 auf Seite 46 zeigt eine in dieser Arbeit verwendete Richtlinien-Vorlagendatei im Texteditor Notepad. In den ersten Zeilen der Datei wird der Schlüssel HKEY_CURRENT_USER durch den Aufruf CLASS USER bearbeitet. Danach wird der Schlüssel HKEY_LOCAL_MACHINE durch den Aufruf CLASS MACHINE editiert. Am Ende der Datei stehen Strings, um die vorab definierten Variablen zu füllen. Abbildung 9 auf Seite 47 zeigt die Auswirkung auf den Systemrichtlinien-Editor.

PolUdpW2K.adm - Editor

Datei Bearbeiten Format ?

```
CLASS USER

CATEGORY "Systemsteuerung und Drucker ect. ausblenden"
CATEGORY "Kontextmenüs des Startmenüs ausblenden"
        POLICY "Kontext Startmenü ausblenden"
                KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                VALUENAME "NoChangeStartMenu"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
        END POLICY

        POLICY "Kontext Start Knopf ausblenden"
                KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                VALUENAME "NoTrayContextMenu"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
        END POLICY
END CATEGORY

        POLICY "Ausblenden: Eigenschaften des Arbeitsplatzes"
                KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                VALUENAME "NoPropertiesMyComputer"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
        END POLICY

        POLICY "Ausblenden: Neue Netzwerkverbindung erstellen"
                KEYNAME "Software\Policies\Microsoft\Windows\Network Connections"
                VALUENAME "NC_NewConnectionWizard"
                  VALUEON NUMERIC 0
                  VALUEOFF NUMERIC 1
        END POLICY

        POLICY "Ausblenden Drucker und Systemsteuerung im Startmenü"
                KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                VALUENAME "NoSetFolders"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
                PART !!INFO1 TEXT
                END PART
        END POLICY

        POLICY "Ausblenden: Neuer Drucker im Startmenü"
                KEYNAME "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
                VALUENAME "NoAddPrinter"
                  VALUEON NUMERIC 1
                  VALUEOFF NUMERIC 0
        END POLICY
END CATEGORY

CLASS MACHINE

CATEGORY "Pfad und Methode für Update der Systemrichtlininen W2K"

        POLICY "Methode"
                KEYNAME "System\CurrentControlSet\Update"
                PART !!NETMODE DROPDOWNLIST
                VALUENAME "UpdateMode"
                ITEMLIST
                  NAME "kein Update"                    VALUE NUMERIC 0
                  NAME "Update mit Standartpfad"        VALUE NUMERIC 1
                  NAME "Update mit definiertem Pfad"    VALUE NUMERIC 2
                END ITEMLIST
                END PART
        END POLICY

        POLICY "Pfad"
                KEYNAME "System\CurrentControlSet\Update"
                PART !!NETPATH EDITTEXT
                VALUENAME "NetworkPath"
                END PART
        END POLICY
END CATEGORY


[strings]
INFO1="Checked = Ausblenden. Blank =  einblenden"
NETPATH="Netzwerkpfad"
NETMODE="Update Methode"
```

Abbildung 8: Datei PolUpdW2K.adm im Texteditor

5.3.3.3 Richtlinienvorlagen-Datei als editierbare Oberfläche

Die erstellte Richtlinien-Vorlagen-Datei, wie in Abbildung 8 auf Seite 46, wird unter der Dateierweiterung *.adm abgespeichert. Durch dieses Dateiformat wird sie als Richtlinien-Vorlagendatei vom Systemrichtlinien-Editor erkannt. ADM-Dateien müssen vor dem Erstellen einer neuen Richtlinie in den Systemrichtlinien-Editor eingelesen werden. Der Systemrichtlinien-Editor interpretiert die eingetragenen Befehle in eine graphische, editierbare Oberfläche (siehe Abbildung 9).

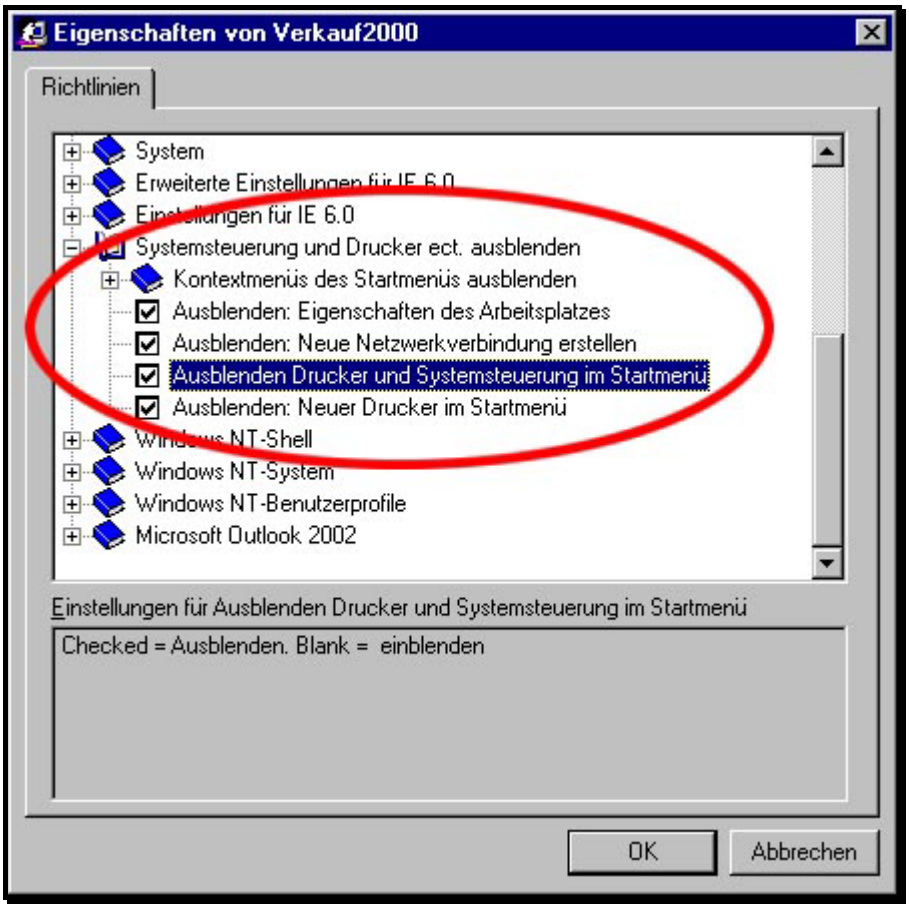

Abbildung 9: Baumstruktur der Datei PolUpdW2K.adm im Systemrichtlinieneditor

Abbildung 9 zeigt die vom Systemrichtlinien-Editor erzeugte Menü-Struktur für die Gruppe Verkauf2000. Diese Gruppe wird durch den Benutzermanager für Domänen erzeugt (Siehe S. 36, Abbildung 4). Diese Ansicht unterscheidet sich nicht von der eines einzelnen Benutzers. Durch die Verwendung von Benutzergruppen im Systemrichtlinien-Editor werden die getroffenen Einstellungen für alle in dieser Benutzergruppe enthaltenen Benutzer gültig.

Diese Einstellungen werden in einer Datei abgespeichert. Damit das jeweilige Client-Betriebssystem die Konfigurationen beim Anmeldevorgang verarbeiten kann, wird die Datei im Netlogon-Share der Domäne bzw. der Server unter der Dateierweiterung *.pol abgespeichert. Der Netlogon-Share ist standardmäßig die Freigabe des Verzeichnis-

ses %Systemroot%\System32\Repl\Import\Scripts. Auf diesen Ordner wirkt der Verzeichnisreplikationsdienst, der die dort abgespeicherten Skriptdateien mit denen des anderen Servers abgleicht und im Bedarfsfall kopiert. Die exakte Konfiguration hängt von den jeweiligen Anforderungen und der Geschwindigkeit des Netzwerkes ab. In einschlägiger Fachliteratur können bei Bedarf Konfigurationsmöglichkeiten nachgelesen werden[22].

5.3.4 Wirkung der Servereinstellungen auf den Client

Über Systemrichtlinien kann vereinbart werden, welche Möglichkeiten in einer Windows NT Umgebung überhaupt nutzbar sind und wie weit die Einflussnahme der Anwender auf die eigene Systemumgebung gestattet ist. In dieser Arbeit werden die Systemrichtlinien auch eingesetzt, um den Benutzern eine einheitliche Bedienoberfläche zu generieren. Bei der Anmeldung eines Benutzers an die Domäne werden die Systemrichtlinien in der Datei NTConfig.pol folgendermaßen auf dem Clientsystem umgesetzt:

1. Bei Anmeldung des Betriebssystems an das Netzwerk wird die Datei NTConfig.pol im Netlogon-Share der Domäne gesucht.
2. Die Einstellungen für den Schlüssel HKEY_LOCAL_MACHINE werden in der Registrierdatenbank des Client-Betriebssystems umgesetzt.
3. Das Betriebssystem des Clients wertet die Einstellungen des Update-Pfads und der Update-Methode (Abbildung 8, S. 46) für Systemrichtlinien aus und gleicht gegebenenfalls die Registry des Clients an.
4. Nach der Anmeldung eines Benutzers (USER) an die Domäne werden die Einstellungen für den Schlüssel HKEY_CURRENT_USER umgesetzt.

Abbildung 10 auf Seite 49 zeigt beispielhaft die Beschränkung von Benutzerrechten. Die Einstellungen für administrative Optionen des Internet Explorers werden vorgeschrieben bzw. deaktiviert. Die Registerkarten *Verbindungen*, *Programme* und *Erweitert* sind deaktiviert und für den Benutzer nicht mehr einzusehen. Die Konfigurationen auf diesen Registerkarten werden von Systemrichtlinien erzeugt.

[22] Zum Beispiel Literaturverzeichnis: Hunt, C. und Thompson, R.B. (1999)

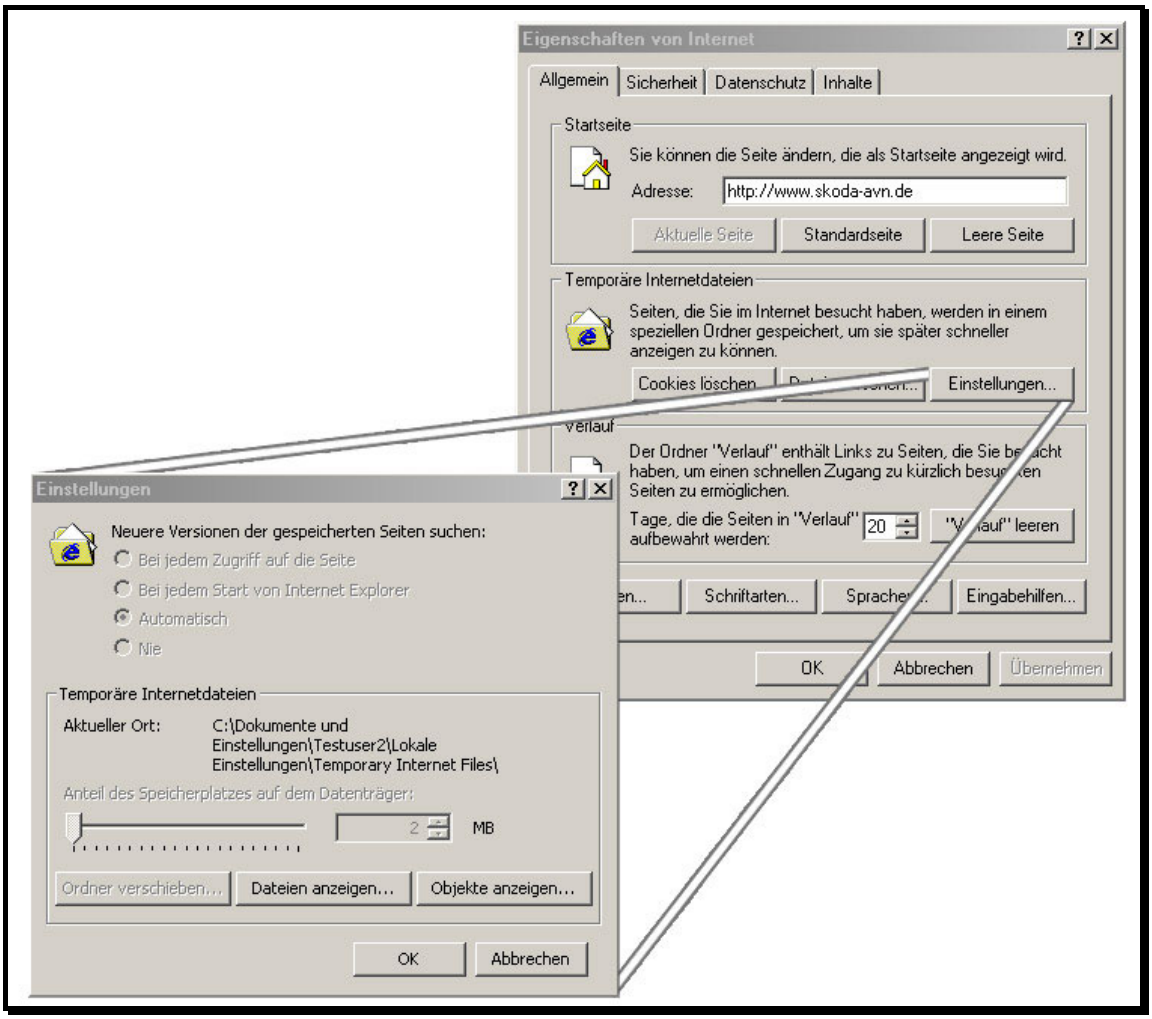

Abbildung 10: Erzwungene Einstellungen des Internet Explorers 6.0

In Abschnitt 6 wird auf die Wirkung der serverseitigen Konfigurationen in Anbetracht der beiden Haupt-Benutzergruppen Service2000 und Verkauf2000 eingegangen.

5.4 Systemsicherheit

Defekte und mutwillige Zerstörungen können durch Einflüsse von außen oder von innen auf das bestehende Netzwerk verursacht werden. Letztlich ergänzen die allgemein[23] bekannten Gefahren durch angebundene Intranets und das Internet die grundsätzlich von innen kommenden Gefahren für die DV-Infrastruktur. Hierzu zählen fehlerhafte oder fehlende Datensicherung und die hohen Schäden durch Bedienungsfehler. Als Gefahren von außen kommen das Eindringen von Hackern aller Art und das Einschleppen von Viren über mitgebrachte Wechselmedien in Betracht. Unter Systemsicherheit wird in diesem Projekt auch das sichere und schnelle Wiederherstellen verlo-

[23] Mit allgemeinen Gefahren sind auch Gefahren durch Viren in E-Mails, wie Würmer oder Trojaner, sowie Gefahren durch versehentliche Installation von kostenpflichtigen DFÜ-Einwahlprogrammen (DIALER) gemeint.

ren gegangener Daten verstanden. Dabei werden sowohl Daten auf den Servern, wie auch die des Betriebssystems berücksichtigt. Letztlich spielt es keine Rolle, ob ein Mitarbeiter wegen fehlender Dateien oder Daten auf dem Server oder wegen eines defekten Clientbetriebssystems seiner Tätigkeit nicht nachkommen kann. Beide Fehler müssen innerhalb eines angemessenen Zeitraumes zu beheben sein. Zusätzlich ist eine individuelle Risikoanalyse nötig, die etwaige sonstige Sicherheitslücken des Netzwerkes aufdeckt. Kauffels (2002, S. 558) führt dazu aus:

> *„Im Rahmen einer Risikoanalyse müssen die Schäden bewertet werden, damit man für Schutz nicht mehr Geld ausgibt, als die Sache überhaupt Wert ist.“*

Kauffels meint damit, dass bewertet werden muss, welche Kosten ein kompletter Systemausfall verursachen würde. Anhand dieser Kosten wird das Budget festgelegt, das zur Anschaffung von Sicherheitsmechanismen verwendet wird.

Persönliche, von Usern auf den Festplatten ihrer jeweiligen Clients abgespeicherte Dateien werden aus der Systemsicherheit abgegrenzt. Alle Mitarbeiter des Betriebes haben die Anweisung, ihre persönlichen Dateien auf den gemappten Netzlaufwerken zu speichern. Für Dateien auf den Festplatten der Clients wird keinerlei Gewähr übernommen. Auf die von außen bestehenden Gefahren wird in dieser Arbeit mit einer Anti-Virus-Software, wie in Abschnitt 5.4.4 beschrieben, und mit der eingebauten Firewall des NCP Secure-Server-VPN-Gateways reagiert (siehe Abschnitt 4.4.1). Gefahren, die von innerhalb des Betriebes drohen werden analysiert und entsprechende Gegenmaßnahmen definiert:

1. Zerstörung der gesamten EDV-Anlage durch Umwelteinflüsse wie Brand, Wasserschaden oder Blitzschlag. Vorsorglich wird der jeweils letzte Datenträger der Datensicherung einer Woche von einem autorisierten Mitarbeiter für eine Dauer von 4 Wochen außerhalb des Betriebes aufbewahrt. Bei Ausfall des Stromnetzes ist die USV in der Lage, den Spannungsabfall zu kompensieren (siehe Abschnitt 4.1.1).
2. Zerstörung oder Defekt der Festplatten, des Netzteils oder der Hauptplatine eines Servers. Die Server sind, wie in den Anforderungen beschrieben, so konfiguriert, dass der Backup-Domain-Controller mit einem überschaubaren Aufwand die Arbeit übernehmen kann[24]. Zusätzlich werden von den Festplatten, auf denen die Betriebssysteme der Server sind Ghost-Image Dateien (siehe Abschnitt 5.4.3) auf einen Datenträger des Bandlaufwerkes gespeichert.
3. Ausfall des Switches. Um diesen Defekt zu kompensieren, wird ein kleinerer und damit kostengünstiger, zweiter Switch mit 8 Ports im Serverschrank installiert.

[24] Auf die Realisierung dieser Funktion wird in Abschnitt 5.4.1 auf S. 51 eingegangen.

4. Zerstörung, Ausfall, irreparabler Absturz eines Client Systems. Alle Clientsysteme sind hardwareseitig identisch. Beim Ausfall eines Systems durch Hardwaredefekt wird die Image Datei auf CD-ROM nach Reparatur der Hardware, wie in Abschnitt 5.4.3 erläutert, erneut installiert. Dasselbe gilt bei Fehlbedienung durch User, die eine Beschädigung des Betriebssystems verursacht. Zur Überbrückung der Ausfallzeit wird ein Ersatzrechner aufbewahrt.

Oben angeführte Szenarien sind Gegenstand des Notfallplans. User bzw. Mitarbeiter des Betriebes bemerken Systemfehler oder Defekte meist dadurch, dass eine oder mehrere Aufgaben nicht mehr bearbeitet werden können. Um Systemausfälle mit geringem Zeitaufwand analysieren zu können und den eigentlichen Fehler zu finden, wird ein Mitarbeiter[25] des Betriebes in den Notfallplan eingewiesen. Anhand von Flussdiagrammen, die für die am häufigsten auftretenden Fehler ausgearbeitet werden, kann der zuständige Mitarbeiter die eigentlichen Fehlerquellen analysieren. Ziel dieser Diagramme ist nicht die tatsächliche Behebung des Problems, sondern das zuverlässige Auffinden des richtigen Ansprechpartners.

5.4.1 Übernahme der Domäne des zweiten Servers AVN2

Bei Hardwaredefekt eines Servers oder eines Softwaredefektes, der nicht durch den zuständigen Mitarbeiter des Betriebes behoben oder analysiert werden kann, wird die gesamte Domäne und alle zugehörigen Installationen vom zweiten Server AVN2 übernommen. Um diesen Prozess zu beschleunigen, werden alle Skript-Dateien und Systemrichtlinien doppelt, mit Einstelllungen bzw. Pfadangaben für beide Server, angefertigt. Eine Batch-Datei, wie in Abbildung 5 auf Seite 37 gezeigt, wird demnach einmal mit den Dateipfaden des ersten Servers AVN1 und mit den Dateipfaden des zweiten Backup-Servers AVN2 abgespeichert. Alle Dateien liegen im Ordner des Verzeichnisreplikationsdienstes. Um Verwechslungen zu vermeiden, werden die Dateien mit unterschiedlichen Dateierweiterungen angelegt, wie beispielsweise die Backupdatei des Logon-Skriptes *logon.bat* mit der Konfiguration des zweiten Servers unter dem Namen *logon.bat2* abgespeichert ist. Im Falle der Übernahme der Domäne durch den zweiten Server AVN2, werden deshalb lediglich die Backup Skript-Dateien umbenannt. Also aus *logon.bat2* wird *logon.bat*. Dasselbe Verfahren wird auf die Datei *NTConfig.pol* angewandt. Das so konfigurierte System arbeitet als Failover-System. Die Benutzer müssen nach Übername des Servers AVN2 alle Client-Systeme neu starten. Die IP-Adressen in den Netzwerkeinstellungen der Clients für das Standardgateway müssen durch den Administrator angeglichen werden. Hier ist der Einsatz des DHCP-Protokolls sinnvoll, da die Einstellungen dieses Protokolls serverseitig verändert werden können und eine eventuelle Umstellung weniger Zeit beansprucht.

[25] Die Aufgaben des Mitarbeiters werden auch in Abschnitt 5.7 beschrieben.

5.4.2 Datensicherung

Die Sicherung aller Daten der Server wird durch zwei Komponenten realisiert. Zum einen wird ein Bandlaufwerk eingesetzt, zum anderen eine Synchronisations-Software, die Benutzerdaten und Datenbanken der installierten Anwenderprogramme auf den zweiten Server AVN2 kopiert. Das Überspielen unternehmensrelevanter Daten auf einen Datenträger des Bandlaufwerkes ist ebenso wichtig, wie die redundante Verteilung der Daten im Netzwerk. Das Bandlaufwerk ist, genauso wie die Festplattensysteme, in der Lage, große Datenmengen aufzunehmen. Der in dieser Arbeit verwendete DDS3-Streamer des Herstellers Hewlett Packard speichert immerhin 24 Gigabyte. Das Speichern und Wiederherstellen von Daten eines Bandlaufwerkes nimmt, bedingt durch den geringeren Datendurchsatz, mehr Zeit in Anspruch, als das Kopieren von Daten auf eine Festplatte eines zweiten Servers im Netzwerk. Der Vorteil eines Bandlaufwerkes liegt darin, dass die Bandkassette, also das Speichermedium und somit der Speicherplatz vergleichsweise billiger ist. Aufgrund des kostengünstigen Speicherplatzes können für die Datensicherung beliebig viele Bänder innerhalb einer Woche oder eines Monates verwendet werden. Festplattensysteme haben den Vorteil der schnelleren Zugriffszeit und des größeren Datendurchsatzes. Da sämtliche servergespeicherten Daten wie Benutzerprofile und Datenbanken ohnehin auf dem Backup-Server AVN2 (BDC) in der jeweils aktuellen Version vorhanden sein müssen, wird eine Kombination beider Sicherungsmöglichkeiten verwendet.

1. Jungbluth (1996, S. 280) empfiehlt bei größeren Netzwerken oder wenn das Backup komfortabler durchgeführt werden soll die Verwendung eines separaten Programms. […] für Windows NT bieten die beiden größeren Hersteller Arcada und Cheyenne Produkte an. In dieser Arbeit wird deshalb die Sicherungssoftware ARCserve des Herstellers Cheyenne verwandt. Sie bietet diverse Möglichkeiten zur Konfiguration von Sicherungsarten. Es wird eine Rotationssicherung mit 8 Bändern erstellt. Das gesamte Festplattensystem des Servers AVN1 wird jeden zweiten Wochentag komplett gesichert. Das jeweils letzte Band der Woche wird weitere vier Wochen aufbewahrt. Der Stand der gesicherten Dateien kann über den Zeitraum eines gesamten Monats zurückverfolgt werden. Da, wie unter dem nachfolgenden Punkt 2 beschrieben, an jedem Wochentag die Festplattensysteme der Server synchronisiert werden, genügt es, die Daten lediglich alle zwei Wochentage auf Band zu sichern.

2. An jedem Wochentag werden bestimmte Daten auf den Festplattensystemen der Server AVN1 und AVN2 miteinander synchronisiert. Alle Datenbanken der Anwendersoftware müssen mit dem Backup-Server abgeglichen werden. Die persönlichen Daten der Benutzer werden durch die administrative Freigabe beider Festplatten der Server miteinander synchronisiert. Da die Ordner der Benutzerprofile bereits freigegeben sind, kann diese Freigabe für die redundante Verteilung genutzt werden.

Die Synchronisation wird mit der Software Allsync des Herstellers Thummerer-Software-Design realisiert. Mit diesem Tool hat man die Möglichkeit, mehrere Profile

für verschiedene Synchronisationsjobs und zugehörige Filter für bestimmte Dateien zu erstellen. Filter werden zum Beispiel für temporäre Daten oder Dateien, die sich im *Papierkorb* befinden eingesetzt. Jeder Synchronisationsjob wird doppelt mit den Inhalten der verschiedenen Festplattensysteme abgeglichen. Allsync erstellt für jeden Kopier- oder Löschvorgang umfangreiche Protokolleinträge. Zwar erlaubt Allsync keine Synchronisation in Echtzeit, jedoch bieten die oben genannten Eigenschaften eine sehr sichere Methode, Daten im Netzwerk redundant zu verteilen. Durch Verknüpfung der verschiedenen Synchronisationsprofile vermeidet man zeitliche Überschneidungen bei der automatisierten Bearbeitung.

Alle unter Abschnitt 5.4.2 beschriebenen Mechanismen zur Datensicherung werden nach Feierabend, in einem Zeitraum, in dem die Benutzer nicht am System angemeldet sind, durchgeführt. Die Anmelderechte der Benutzer werden so vergeben, dass eine Anmeldung am System ausschließlich zwischen 5.00 Uhr und 23.00 Uhr möglich ist. Abbildung 11 zeigt eine Batch-Datei, die durch den Aufruf des Programms *Down.exe* alle Clientsysteme automatisch um 23.00 Uhr abschaltet bzw. „herunterfährt“. Damit die Sicherungssoftware ARCserve Zugriff auf die Datenbanken des Serverbetriebssystems und der Anti-Viren-Software InoculateIT erhält, werden durch eine weitere Batch-Datei verschiedene Dienste des Servers angehalten. Die Datei in Abbildung 12 auf Seite 54 beendet den Verzeichnisreplikationsdienst, den WINS-Dienst und die Dienste von InoculateIT. Weitere Batch-Dateien werden je nach Bedarf erstellt und in die Zeitplanung miteinbezogen.

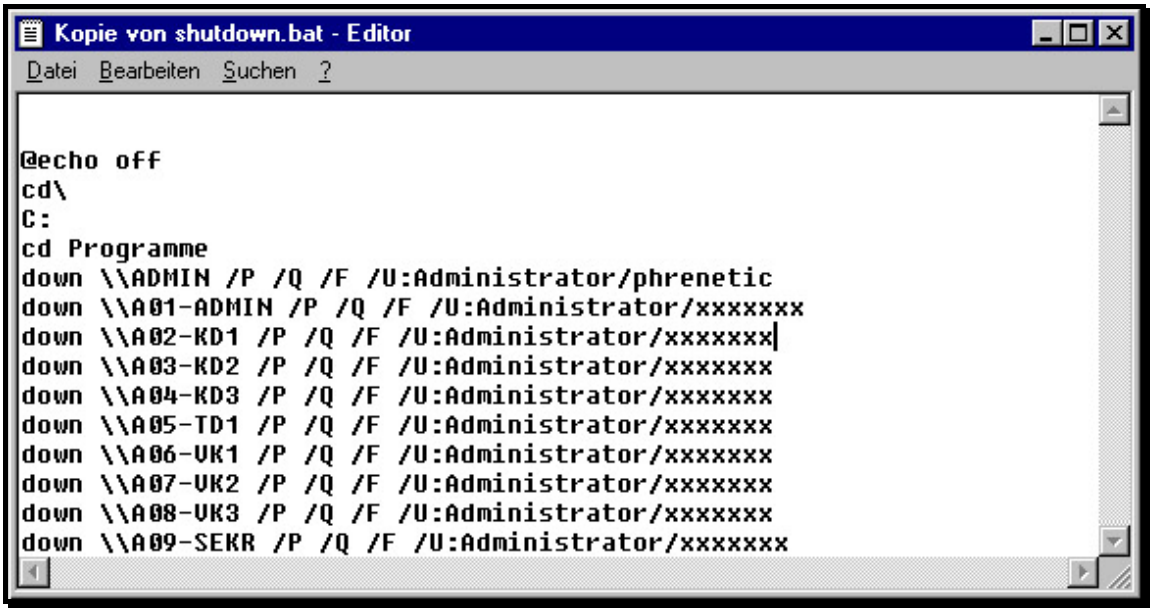

Abbildung 11: Shutdown der Client-Systeme

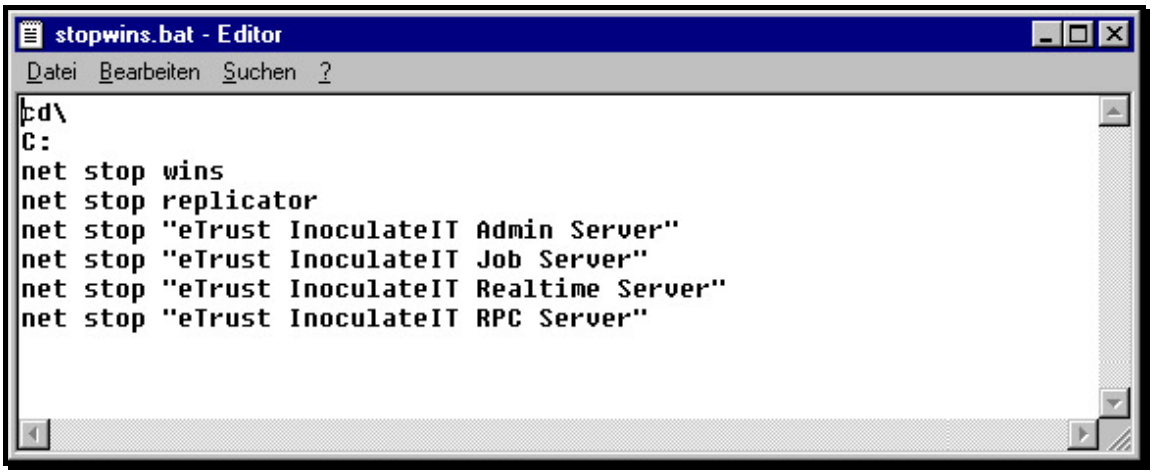

Abbildung 12: Serverdienste

Durch den Aufruf `net stop` in Abbildung 12 werden die serverseitigen Dienste beendet. Nach Durchlauf aller Sicherungsmaßnahmen werden die gestoppten Dienste von einer anderen Batch-Datei mit dem Befehl `net start` wieder gestartet.

5.4.3 Ghost – Images

Eine andere Art der Datensicherung wird durch den Einsatz der Software Norton Ghost des Herstellers Symantec betrieben. Norton Ghost ermöglicht die Sicherung des Inhaltes einer Festplatte oder einer logischen Partition in einer einzigen komprimierten Datei auf einem externen Speichermedium wie einer CD-R oder CD-RW. Diese Datei wird als Image-Datei bezeichnet. Als zusätzliches Feature hat man die Möglichkeit, eine bootfähige DOS-Version auf dem Medium zu platzieren. Durch diese Technik lassen sich zwei Probleme auf einmal lösen:

1. Nach Installation des Betriebssystems, der Anwenderprogramme und aller benötigten Hardware-Treiber auf dem ersten Client, wird von dessen Festplatte eine bootfähige Image-Datei auf eine CD-R gebrannt. Alle weiteren Clients werden anschließend mit dieser Image Datei installiert. Dieser Vorgang wird auch als Klonen bezeichnet. Die Eigenschaften der Netzwerkeinstellungen wie LAN-IP-Adresse und Netzwerkidentifikation (siehe Abbildung 3, S. 35) müssen noch auf den jeweiligen Client abgestimmt werden. Diese Arbeiten sind jedoch weniger zeitintensiv, als eine einzelne manuelle Installation und Konfiguration aller Clientsysteme. Alle Clientsysteme sind durch diese Maßnahme exakt gleich konfiguriert.
2. Trotz aller Anstrengungen zur Beschränkung der Benutzerrechte, besteht die Möglichkeit, dass durch Fehlbedienung eines Benutzers ein Clientbetriebssystem beschädigt wird. Auf der Ghost-Image-Datei ist der Ursprungszustand des Clientbetriebssystems abgespeichert. Sollten Fehler auf den Clients auftreten, müsste keine Zeit in die genaue Analyse und das Beheben des Fehlers investiert werden. Der zuständige Administrator installiert auf die Festplatte des Clients die Ghost-

Image-Datei. Sollte dasselbe Problem wiederholt auftreten, ist mit großer Wahrscheinlichkeit ein Teil der Hardware beschädigt.

Durch den Einsatz dieser Image-Dateien ist der Administrator innerhalb relativ kurzer Zeit in der Lage, Betriebssysteme zu installieren und diese wieder herzustellen. Von den Servern AVN1 und AVN2 wird ebenfalls, nach Installation aller Komponenten, ein Image der Festplatte, die das Betriebssystem enthält, abgespeichert. Da die Datenmenge trotz Komprimierung durch Norton Ghost nicht auf einer CD-R unterzubringen ist, wird die Image-Datei auf einem DDS3-Band erstellt. Für diese Funktion wird eine spezielle Bootdiskette, auf der Treiber für SCSI enthalten sind benötigt. Folgendes Szenario beschreibt den Nutzen dieser Maßnahme:

1. Fehlbedienung des Servers durch den Administrator. Das Betriebssystem wird irreparabel beschädigt. Der Server AVN1 stürzt ab. Das Betriebssystem lässt sich nicht mehr starten.
2. Der Server wird mit einer Bootdiskette, die das Bandlaufwerk am SCSI-Bus unterstützt, im DOS-Modus gestartet.
3. Der Inhalt der primären Partition wird durch die Installation der Image-Datei wiederhergestellt.
4. Gegebenenfalls wird der Inhalt aller anderen Festplatten mit dem DDS3-Band der letzten Datensicherung wiederhergestellt.
5. Wurde die letzte Datensicherung nicht am Vorabend erstellt, werden die aktuellen Datenbestände vom Server AVN2 beschafft. Dazu wird die Software Allsync wie unter Abschnitt 5.4.2 beschrieben, verwendet.

Diese und ähnliche Szenarien und Maßnahmen, um derartige Fehler beheben zu können sind im Notfallplan enthalten. Selbstverständlich kann von einem Mitarbeiter des Autohauses nicht erwartet werden, diese Tätigkeiten selbst zu bewältigen. Allerdings bieten ihm diese Beschreibungen eine Entscheidungshilfe, um den richtigen Ansprechpartner zu verständigen.

5.4.4 Virenschutz

Unzählige Softwarehersteller bieten Lösungen, um ein Netzwerk effizient vor Virus-Attacken zu schützen. Das am weitesten verbreitete Produkt ist sicher die Software Norton AntiVirus des Herstellers Symantec. Theoretisch ist aber der Schutz vor Viren nur die halbe Miete. Da in einem Netzwerk viele Benutzer in viele unterschiedliche Kommunikationsformen und Kommunikationsprozesse außerhalb und innerhalb des LAN eingebunden sind, sollte eine ganzheitliche Lösung wie Norton SystemWorks, die die Funktionen einer Firewall übernimmt oder Schutz vor Spam-Attacken bietet, gewählt werden. Aus Kostengründen wird in dieser Arbeit auf eine derartige Lösung verzichtet. Ebenfalls aus Kostengründen fiel die Wahl der Anti-Virus-Software auf das Produkt InoculateIT Version 6.0 des Herstellers CA. Das Produkt besteht aus einer Komponente, die auf dem Server installiert wird und der Client-Installationsroutine. Die

Datenbanken werden zentral auf dem Server gespeichert und verwaltet. Benutzerrechte können entzogen oder gewährt werden. Je nach Konfiguration werden Funktionen wie das Update der Virussignaturen oder Scanjobs vom Benutzer selbst ausgelöst oder zentral vom Server bzw. Administrator gesteuert.

5.5 Installation der Car-Dealer-Software Werbas

Die bestehenden Datenbanken von Werbas sind in einem Ordner mit der Bezeichnung *\Wali* enthalten. Alle Unterverzeichnisse und zugehörigen Dateien werden in die Laufwerksfreigabe[26] des Werbas-Systems kopiert. Die eigentliche Installation des Systems besteht aus zwei Komponenten:

1. Werbas spricht seine Datenbanken über die Programmiersprache SQL an. Die zugehörige Datenbank-Engine stammt vom Hersteller Pervasive. Die eigentliche Datenbank-Engine wird auf den Servern als Systemdienst installiert und dort gemäß den Herstellerangaben konfiguriert. Die Standardwerte können größtenteils übernommen werden, lediglich die Auswahl der Netzwerkprotokolle seitens der Datenbank-Engine sollte auf die ausschließliche Kommunikation über TCP/IP eingestellt sein.
2. Auf den Clientsystemen wird das Gegenstück zur Datenbank-Engine, der Pervasive-SQL-Datenbankclient installiert.

Um Werbas zu starten, wird auf dem Clientsystem die Datei wpstrq.exe ausgeführt. Diese Datei befindet sich in der Laufwerksfreigabe des Servers. Durch das Ausführen dieser 32Bit Anwendung werden verschiedene Programmunterbibliotheken angesprochen, die mit dem Dienst der Datenbank-Engine verknüpft sind. Durch den Start der Datenbank-Engine auf dem Server wird der Datenbankclient angesprochen. Zur Identifizierung der Lizenz des Clientsystems wird in der Verknüpfung zur Datei wpstrq.exe eine laufende Nummer übergeben. Diese Nummer wird auf jedem Client-System exklusiv vergeben (siehe Abbildung 13, S. 57). Auf allen anderen Clients wird die Installation des Pervasive-SQL-Datenbankclient durch die Ghost-Image-Datei, wie in Abschnitt 5.4.3. erklärt, bewerkstelligt.

Werbas ist eine modular aufgebaute Lösung. Mit dem Erwerb des Grundmoduls stehen dem Betrieb grundlegende Funktionen wie Auftragsbearbeitung, Fahrzeugverwaltung und Kundendatenverwaltung zur Verfügung. Damit Werbas mit anderer, für den Betrieb relevanter Software, Daten austauschen kann, müssen zusätzliche Module neu angeschafft werden. Folgende Werbas-Module und Schnittstellen werden zur Datenübergabe an Programme[27] anderer Hersteller installiert:

---

[26] Die Laufwerksfreigaben werden durch das Logon-Skript auf den Clients gemappt. Siehe Abschnitt 5.3.1.

[27] Im folgenden Abschnitt 5.6 sind alle weiteren Programminstallationen erläutert.

- Modul **Werbas-RIS**: Dieses Modul stellt eine Schnittstelle zu den Datenbanken der Gebrauchtfahrzeugbewertung SilverDAT dar. Fahrzeugdaten können direkt aus SilverDAT importiert werden.
- **Schnittstelle ETKA**: Diese Schnittstelle ermöglicht den Import von elektronisch erstellten Materialscheinen des Ersatzteilkataloges ETKA. In der Abteilung Teiledienst wird so das Erstellen von neuen Aufträgen erleichtert. Die gesammelten Teiledaten und zugehörigen Preise können direkt in den Auftrag des Kunden eingelesen werden.
- **Schnittstelle DATEV**: Durch diese Schnittstelle wird der Kontenrahmen des Herstellers Škoda auf das Werbas Grundmodul angewandt. Alle Buchungen werden nach Tagesabschluss den entsprechenden Konten der Buchhaltung zugeordnet.
- **Schnittstelle Office2002**: Dadurch wird der Export von Formulardaten in Word2002 und Excel2002 ermöglicht. Kundenstamm und Fahrzeugdaten können so für verschiedene Zwecke weiterverarbeitet werden. Dies wird beispielsweise zur Erstellung von Serienbriefen benötigt.

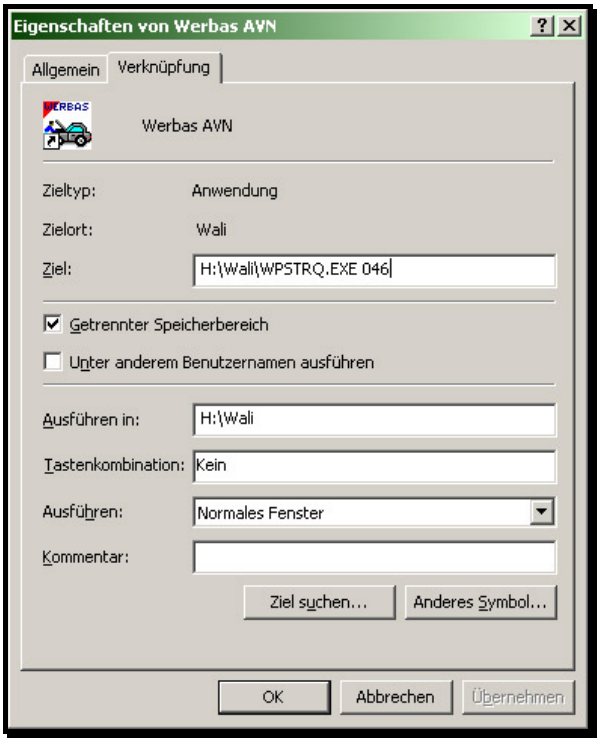

Abbildung 13:Verknüpfung zu wpstrq.exe

Abbildung 13 zeigt die Eigenschaften der Verknüpfung zur Anwendung Werbas. Das Ziel verweist auf die Datei wpstrq.exe im Ordner \Wali in der Netzlaufwerksfreigabe H: auf dem Server AVN1. Die Lizenznummer (hier die Nummer 046) steht nach der Pfadangabe.

5.6 Installation der Anwenderprogramme

Alle weiteren Anwenderprogramme werden jeweils als Client-Server Variante in das System integriert. Hierbei werden auf den Servern immer die zentralen Datenbanken und die Datenbank-Engines verwendet. Auf die Clientbetriebssysteme werden die zugehörigen Datenbank-Clientapplikationen mit Hilfe der Ghost-Image-Datei installiert. Bei fast allen Anwendungen gelingt dies. Der Škoda Ersatzteilkatalog ETKA jedoch wird von SAD nur als Einzelplatzinstallation angeboten. Bei Updates entsteht ein Zeitaufwand von jeweils ca. 20 Minuten, da jeder einzelne Client per CD-ROM aktualisiert werden muss. Bei 5 Clientsystemen auf denen ETKA installiert ist, macht das immerhin 60 Minuten pro Update. Das Problem ist bei SAD bekannt, und die Informationsabteilung arbeitet bereits an einer netzwerkfähigen Version. Bei der im Folgenden beschriebenen Anwender- und Individualsoftware muss im Einzelfall mit dem Hersteller abgeklärt werden, ob etwaige Inkompatibilitäten seines Produktes bekannt sind. Speziell im Verkaufsbereich wird eine große Anzahl von geschäftskritischen Applikationen benötigt. Diese müssen optimal, hinsichtlich der zu verwendenden Datenbanken, aufeinander abgestimmt sein.

SilverDAT ist ein Programm zur Bestimmung des Marktwertes von Gebrauchtfahrzeugen. Es wird von der Deutschen Automobil Treuhand GmbH (DAT)[28] auf CD-ROM ausgeliefert. SilverDAT arbeitet mit einer von der DAT selbstentwickelten Datenbank-Engine. Die Installation ist verhältnismäßig einfach zu bewerkstelligen. Auf der entsprechenden Netzlaufwerksfreigabe der Server werden von CD-ROM die Datenbanken aufgesetzt. Die zugehörigen Softwaretreiber werden automatisch von der Installationsroutine hinzugefügt. Dabei wird ein Ordner erzeugt, der die Installationsroutine für die Clientsysteme enthält. Der Administrator meldet sich am Clientbetriebssystem an und führt diese direkt vom Netzlaufwerk aus. Die Benutzerrechte für diesen Share müssen entsprechend dem geplanten Benutzerzugriff (siehe Abschnitt 6.3) auf Lesen und Ausführen abgeändert werden. Für SilverDAT sind diverse Schnittstellen zu anderen Programmen, wie zum Beispiel für den Export in ODBC-Anwendungen, erhältlich. Die Schnittstelle zur Verkäuferanwendung ProAct wird implementiert.

ProAct unterstützt die Mitarbeiter der Abteilung Verkauf bei der Kundenakquisition und Kundenbetreuung. Eingegebene Datensätze von Kunden werden den Verkäufern zur Erinnerung automatisch von der Software erneut vorgelegt. Diese Individualsoftware wurde von der Firma Kirchhoff Datensysteme im Auftrag von Procar entwickelt. Die Vertragspartner beziehen ProAct von der Firma Procar, die ein IT-Zulieferer von Škoda Auto Deutschland ist. ProAct verwendet die Datenbank-Engine BDE (Borland Database Engine) des gleichnamigen Herstellers. Die Installation läuft nach demselben Schema wie bei der von SilverDAT ab. Der Borland Datenbankclient wird mit der Installationsroutine auf dem Betriebssystem des Clients verankert. Die werksseitigen Einstellungen der BDE werden weitestgehend übernommen. Durch die Schnittstelle zu Sil-

[28] URL: http://www.dat.de (Datum des Letzten Zugriffs: 15.07.2003)

verDAT sind Verkäufer in der Lage, Kundendaten dieser Software zu übernehmen. Die Daten des bewerteten Gebrauchtfahrzeugs werden nur noch einmalig eingegeben.

Kosyfa ist eine Lösung der CC-Bank für die Anfertigung von Leasing- oder Finanzierungsanträgen. Auch hier werden die Datenbanken über die BDE angesprochen. Zu dieser Anwendersoftware wird ausschließlich den Mitarbeitern des Verkaufsbereichs Zugriff gestattet. Die Verkäufer müssen bei der CC-Bank als solche gemeldet sein. Die Besonderheit dieser Software ist der Ablauf des Datenupdates. Um den Kunden des Unternehmens AVN die jeweils aktuellsten Leasing- und Finanzierungskonditionen bieten zu können, werden diese per ISDN-Verbindung zum zentralen Server der CC-Bank vom Verkäufer selbst abgerufen. Die Verbindung wird vom Administrator vor der Auslieferung des Ghost-Images auf dem Clientbetriebssystem erstellt. Alle nötigen Parameter, wie Telefonnummer, Account, Passwort und zu verwendende Protokolle, müssen konfiguriert werden.

MIS (Markt Informationssystem) bietet Marktanalysen für Neuzulassungen, Vertriebs- und Marktströme der Kfz-Branche. Die Installation erfolgt ebenfalls als Client-Server Lösung.

5.7 Einlernen eines Mitarbeiters zur Wartung des Systems

Bereits in der Planungsphase wird ein Mitarbeiter der Firma AVN in alle Entscheidungen mit einbezogen. Der Mitarbeiter erhält Einblick in die Konzeption und wird von Beginn an in administrative Aufgaben, wie die regelmäßige Durchsicht der Ereignisprotokolle der Server, eingewiesen. Er ist für die Kontrolle der Datensicherung auf Vollständigkeit und den Wechsel der DDS3-Bänder zuständig. Škoda Auto Deutschland arbeitet derzeit an innovativen Software-Lösungen für die Vertragspartner. Der Mitarbeiter des Betriebes fungiert hier als Bindeglied zwischen der Abteilung Informationssysteme von Škoda Auto Deutschland und dem externen Administrator des Netzwerkes. Neue Anforderungen und Entwicklungen seitens SAD werden von ihm, soweit möglich, beurteilt und an den Systembetreuer weitergegeben. Software-Updates der implementierten Branchensoftware werden durch diesen Mitarbeiter eingepflegt und verwaltet. Zu diesem Zweck erhält er das Passwort des Domänen-Administrator-Kontos. Regelmäßige Updates bzw. Aktualisierungen der Datenbanken müssen für folgende Programme durchgeführt werden.

- **Werbas**: In unregelmäßigen Abständen werden neue Versionen der Software angeboten. In Rücksprache mit dem Systembetreuer wird im Einzelfall über die Installation entschieden.
- **SilverDAT**: Monatlich werden von DAT neue Daten zur Gebrauchtfahrzeugbewertung veröffentlicht. Der Mitarbeiter erhält den Datenbestand auf CD-ROM und pflegt diesen in die Datenbanken der Server ein.
- **MIS**: Monatliches Update der Marktdaten. Die aktuellen Datenbanken werden ebenfalls auf CD-ROM ausgeliefert.

- **Ersatzteilkatalog ETKA**: Neue Versionen kommen auf CD-ROM in den Betrieb.
- **Kosyfa**: Das Update neuer Konditionsdaten für Fahrzeugleasing und Finanzierung wird von den Verkäufern per DFÜ-Verbindung selbst durchgeführt. Die CC-Bank empfiehlt, diesen Vorgang vor jeder Bearbeitung eines neuen Vertrags durchzuführen.

6 System aus Benutzersicht

Zwei verschiedene Benutzergruppen können auf diesem System arbeiten. Vorteile der einfachen und dennoch effektiven Domänen- und Benutzerverwaltung der Microsof-NT-Domäne kommen den Benutzern des Systems und dem Administrator des Betriebes zu Gute. Benutzer können sich innerhalb ihrer Gruppe an allen verfügbaren Clientsystemen anmelden. Eine einheitliche und übersichtliche Bedienoberfläche gewährleistet ein sicheres Auffinden von gewünschten Programmfunktionen. Dies ist insbesondere bei Verkäuferprogrammen und allen anderen Programmen, die in Gegenwart von Kunden bedient werden von besonderer Wichtigkeit. Ohne den Einsatz von Microsoft Exchange wird ein Servergespeichertes Mail-Profil ermöglicht. Jedem Benutzer, unabhängig von seiner Gruppenzugehörigkeit steht der freie Zugriff zum Internet und zum Škoda-VPN zur Verfügung. Nach dem Start des Clientbetriebssystems müssen sich die Benutzer an der Domäne anmelden. Das erste Kennwort wird vom Administrator vorgegeben. Die Benutzer werden nach der ersten Anmeldung aufgefordert das Kennwort zu ändern. Dieses Verhalten wird im Benutzermanager für Domänen[29] erzeugt. In das Škoda-VPN gelangen die Benutzer durch die Aktivierung einer Verknüpfung des Internet-Explorers. Diese Dateiverknüpfung (Abbildung 14) verweist über das HTTP-Protokoll auf die IP-Adresse des Endpunktes des VPN-Tunnels[30].

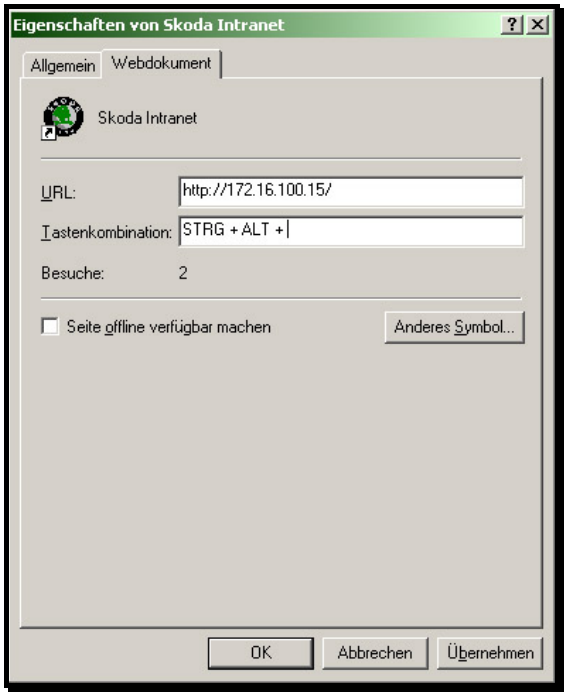

Abbildung 14: Zugriff auf das Škoda-VPN

[29] Benutzermanager für Domänen, siehe Kapitel 5, S. 36.

[30] Der Aufbau des VPN-Tunnels zum Skoda-VPN wird in Abschnitt 4.4.1 beschrieben.

Verknüpfungen im Startmenü und auf den Desktops der Clients bzw. den Benutzerprofilen werden durch Systemrichtlinien erzeugt. Die Benutzer haben die Gewissheit, dass durch Fehlbedienung keine Verknüpfungen gelöscht werden.

Alle nun folgenden Beispiele für die Einstellungen der Clientbetriebssysteme, werden mit denselben Methoden wie in den Abschnitten 5.3.3.1 und 5.3.3.2 beschrieben, erzeugt. Auf dem Server wird dazu immer eine Richtlinienvorlagendatei mit Hilfe des Texteditors erzeugt. Diese Vorlagendatei wird anschließend im Systemrichtlinien-Editor in die Datei NTConfig.pol umgesetzt. In Abschnitt 5.3.3.3 sind die grundlegenden Zusammenhänge erläutert. Das Zusammenwirken mit den Benutzerprofilen ist ein weiterer wichtiger Aspekt.

Für das alte EDV-System war der Support für die Druckereinstellungen und die Druckerkonfiguration mit einem extrem hohen Zeitaufwand verbunden. Die Einstellungen der Druckertreiber wurden oftmals aufgrund von Bedienfehlern durch Benutzer verloren. Beim neuen System muss deshalb der Zugriff auf diese Einstellungen für die Benutzer gesperrt werden. Normalerweise sind die Druckereinstellungen im Startmenü unter *Einstellungen -> Drucker* zu finden. Dieser Order wird durch folgenden Eintrag in der Systemrichtlinienvorlage zur Deaktivierung freigegeben.

```
POLICY "Ausblenden Drucker und Systemsteuerung im Startmenü"
    KEYNAME
    "Software\Microsoft\Windows\CurrentVersion\Policies\Explorer"
   VALUENAME "NoSetFolders"
     VALUEON NUMERIC 1
     VALUEOFF NUMERIC 0
   PART !!INFO1 TEXT
   END PART
END POLICY
```

Der Valuename `NoSetFolders`, der hier die Wertzuweisung ist, bewirkt, dass alle Ordner unter *Startmenü -> Einstellungen* entfernt werden. Der Benutzer hat nun keinen Zugriff mehr auf die Ordner Systemsteuerung, Netzwerk- und DFÜ-Verbindungen und auf den Ordner Drucker. Zum einen wird das so gewünscht, zum anderen kann der Benutzer nun überhaupt keinen Einfluss auf die Druckersteuerung und die Druckaufträge nehmen. Deshalb wird der Druckerordner, mithilfe der CLS-ID[31] dieser Windows-Funktion, direkt im Startmenü wiederhergestellt (siehe Abbildung 16, S. 65). Alle Verknüpfungen des Startmenüs und Verknüpfungen zu den Programmen werden durch folgenden Eintrag in einer anderen Systemrichtlinienvorlagendatei und einer entsprechenden Pfadangabe im Systemrichtlinieneditor, erzeugt. Auf Seite 63 wird der Quellcode gezeigt:

[31] Die Bedeutung von CLS-IDs wird im Glossar beschrieben

```
POLICY !!CustomFolders_StartMenu
   PART !!CustomFolders_StartMenuPath EDITTEXT REQUIRED EXPANDABLETEXT
         DEFAULT !!CustomFolders_StartMenuDefault
         VALUENAME "Start Menu"
     END PART
   END POLICY
```

Die Variable `Default` gibt an, dass die Standardeinstellungen des Windowsbetriebssystems zu verwenden sind, wenn kein Pfad zu einem Ordner der Verknüpfungen enthält angegeben wird. Der Valuename `Start Menu` erzeugt einen Schlüssel der Registrierdatenbank, in dem der Pfad zum Ordner, der die Verknüpfungen des Startmenüs enthält im Systemrichtlinieneditor angegeben werden kann. Der Pfad wird folgendermaßen eingetragen:

```
\\AVN1\W2kstartmenu$
```

Demnach werden alle Verknüpfungen des Startmenüs der Clients in der administrativen Ordnerfreigabe *W2kstartmenu$* erstellt. Der oben erwähnte Ordner der Druckereinstellungen wird durch die Verwendung der CLS-ID dieser Funktion ebenfalls an dieser Stelle eingefügt. Die folgende administrative Ordnerfreigabe enthält die Verknüpfungen für den Aufruf der Programme und der installierten Software des Clientbetriebssystems:

```
\\AVN1\W2kprogravk$
```

Dieser Verweis führt auf den Server AVN1 und dort auf die Ordnerfreigabe *W2kprogravk$*. Die Buchstaben `progra` stehen für die Angabe, dass es sich um den Order für Programmverknüpfungen handelt, die Buchstaben `vk` stehen für die Benutzergruppe Verkauf. Da sich die Programmverknüpfungen der Benutzergruppe Service2000 von denen der Gruppe Verkauf2000 unterscheiden, wird im Systemrichtlinieneditor mit folgendem Eintrag in die Eigenschaften der Systemrichtlinie der zuletzt genannten Gruppe der Verweis auf die entsprechende Ordnerfreigabe erzeugt:

```
\\AVN1\W2kprograsv$
```

`sv` steht hier für die Gruppe Service2000.

Nach demselben Verfahren wird ein weiterer Ordner für Verknüpfungen, die auf den Desktops der Clients angezeigt werden erstellt und freigegeben. Der Eintrag im Systemrichtlinieneditor für die Gruppe Verkauf2000 lautet:

```
\\AVN1\W2kdeskvk$
```

Oder für die Benutzergruppe Service2000:

```
\\AVN1\W2kdesksv$
```

Abbildung 15 auf Seite 64 zeigt den freigegebenen Ordner für die Programmverknüpfungen des Servers ANV1.

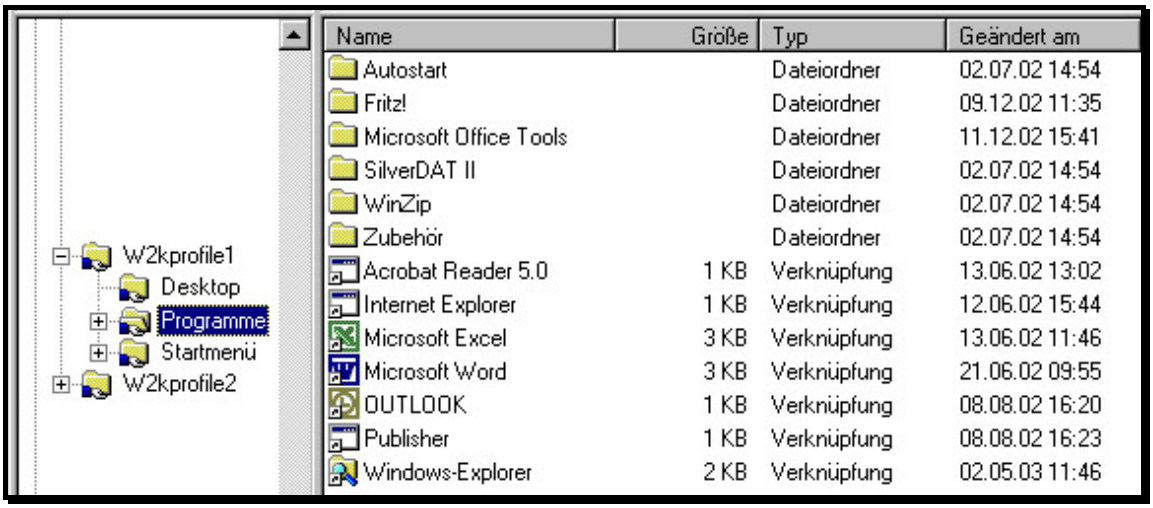

Abbildung 15: Ordnerstruktur für Programmverknüpfungen

Der geöffnete und freigegebene Ordner *Programme* in Abbildung 15 enthält die Programmverknüpfungen und die gesamte Ordnerstruktur des Startmenüs der Clientbetriebssysteme. Abbildung 16 auf Seite 65 zeigt die auf diese Weise erzwungene Struktur des Startmenüs der Benutzergruppe Verkauf2000. Die Unterschiede zur zweiten Benutzergruppe Service2000 werden in Tabelle 3 auf Seite 70 beschrieben.

Abbildung 16 auf Seite 65 zeigt die Druckereinstellungen bzw. den Zugriff auf die installierten Drucker aus der Sicht eines Benutzers der Domänenbenutzergruppe Verkauf2000. Alle Verknüpfungen des Startmenüs werden durch die oben erklärte Pfadangabe im Systemrichtlinieneditor in das Profil des angemeldeten Benutzers eingefügt. Die Verknüpfungen zu den installierten Programmen und der Anwendersoftware werden ebenso durch Eintrag eines Pfades zu einer administrativen Ordnerfreigabe auf dem Server AVN1 erzeugt. Die Gerätetreiber der Drucker werden durch die Installation der Image-Datei[32] lokal hinterlegt.

[32] Image-Datei: siehe Abschnitt 5.4.3

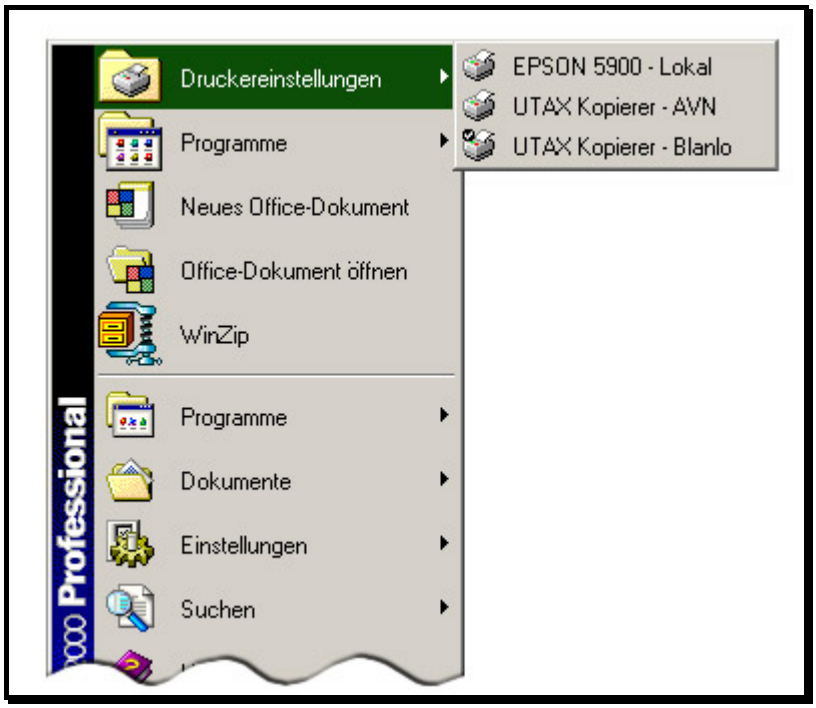

Abbildung 16: Druckereinstellungen aus Sicht der Benutzer

Der Drucker *EPSON 5900 - Lokal* ist ein lokaler Drucker, der an den Arbeitsplätzen der Verkäufer steht. Auf ihm werden Formulare, die von Kunden eingesehen werden müssen, wie Leasing- und Finanzierungsaufträge gedruckt. Die beiden anderen Drucker erlauben Ausdrucke auf dem über das Netzwerk angeschlossenen Kopierer (siehe Abschnitt 4.3 S. 29). Die Einstellungen werden so konfiguriert, dass über den Drucker *UTAX Kopierer - Blanko* der Papiereinzugsschacht mit Blankopapier angesprochen wird. Der Drucker *UTAX Kopierer - AVN* druckt auf Geschäftspapier mit Firmenlogo.

In Abschnitt 2.3 auf Seite 17 wird die Anforderung nach einem einheitlichen Desktop, der das Corporate Design von Škoda Auto Deutschland umsetzt beschrieben. Deshalb wird das Aussehen des Desktops von Systemrichtlinien erzeugt. Die Benutzer haben keinen Einfluss mehr auf Farben, Hintergrundbild und Desktopschemas. Der Eintrag in der Systemrichtlinienvorlagendatei wird folgendermaßen erzeugt:

```
POLICY !!ColorScheme
   PART !!SchemeName                    DROPDOWNLIST
   KEYNAME "Control Panel\Appearance"
   VALUENAME Current                    REQUIRED
   ITEMLIST
   NAME !! AVN256 VALUE !! AVN256
   ACTIONLIST
   KEYNAME "Control Panel\Colors"
   VALUENAME ActiveBorder           VALUE "212 208 200"
   VALUENAME ActiveTitle            VALUE "10 68 6"
   VALUENAME AppWorkSpace           VALUE "128 128 128"
   VALUENAME Background             VALUE "29 139 87"
   VALUENAME ButtonAlternateFace    VALUE "180 180 180"
```

```
   VALUENAME ButtonDkShadow         VALUE "64 64 64"
   VALUENAME ButtonFace             VALUE "212 208 200"
   VALUENAME ButtonHilight          VALUE "255 255 255"
   VALUENAME ButtonLight            VALUE "212 208 200"
   VALUENAME ButtonShadow           VALUE "128 128 128"
   VALUENAME ButtonText             VALUE "0 0 0"
   VALUENAME GradientActiveTitle    VALUE "210 251 208"
   VALUENAME GradientInactiveTitle  VALUE "192 192 192"
   VALUENAME GrayText               VALUE "128 128 128"
   VALUENAME Hilight                VALUE "11 78 7"
   VALUENAME HilightText            VALUE "255 255 255"
   VALUENAME HotTrackingColor       VALUE "0 0 255"
   VALUENAME InactiveBorder         VALUE "212 208 200"
   VALUENAME InactiveTitle          VALUE "128 128 128"
   VALUENAME InactiveTitleText      VALUE "192 192 192"
   VALUENAME InfoText               VALUE "0 0 0"
   VALUENAME InfoWindow             VALUE "255 255 255"
   VALUENAME Menu                   VALUE "212 208 200"
   VALUENAME MenuText               VALUE "0 0 0"
   VALUENAME Scrollbar              VALUE "212 208 200"
   VALUENAME TitleText              VALUE "255 255 255"
   VALUENAME Window                 VALUE "255 255 255"
   VALUENAME WindowFrame            VALUE "0 0 0"
   VALUENAME WindowText             VALUE "0 0 0"
   END ACTIONLIST
   END ITEMLIST
   END PART
   END POLICY
END CATEGORY  ; Desktop
```

Am Anfang dieses Quellcodes wird der Name der Systemrichtlinie erzeugt. Danach folgen die Angaben, welche Farben auf die Desktopeinstellungen angewandt werden. Durch jeweils einen VALUENAME und das dazugehörige VALUE werden die Farbangaben bestimmt. Der VALUE, also der Inhalt des Registrywertes wird durch Zahlen der RGB-Werte angegeben. Abbildung 17 (S. 67) zeigt den auf diese Weise erzeugten Desktop aus Sicht der Benutzer. Das Hintergrundbild wird entsprechend den zugehörigen Benutzergruppen des Benutzermanagers für Domänen[33] durch eine Systemrichtlinie, die die Pfadangabe zur entsprechenden administrativen Freigabe des Servers AVN1 beinhaltet, erzeugt.

[33] In Abschnitt 5.3 (siehe auch Abbildung 4) wird die Konfiguration der Benutzergruppen hinsichtlich dieser Systemrichtlinie beschrieben.

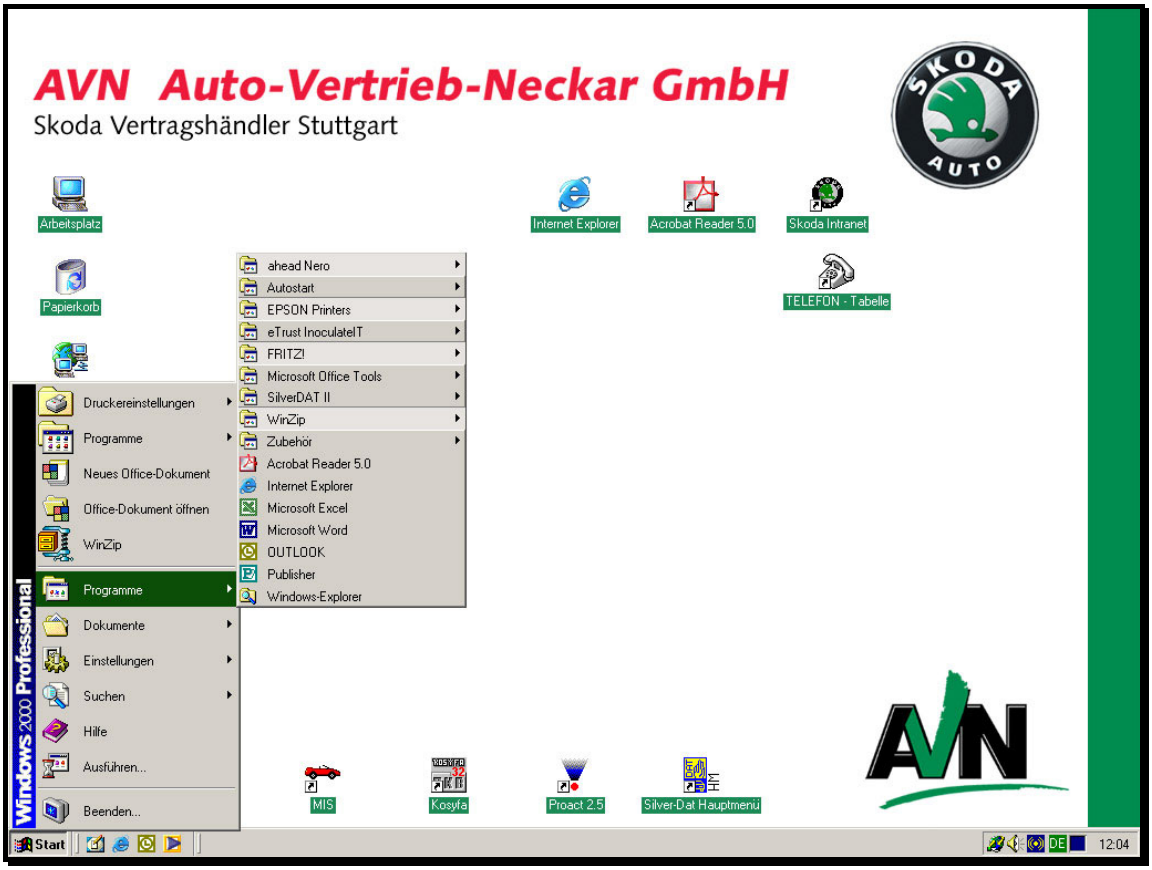

Abbildung 17: Desktop eines AVN-Clients

6.1 Mailprofile

Outlook erzeugt für jeden Benutzer eines Microsoft-Betriebssystems ein Mailprofil in dem E-Mails und persönliche Einstellungen abgespeichert werden. Dieses Profil wird in einer Datei mit der Dateierweiterung *.pst in der Ordnerstruktur seines Benutzerprofils angelegt. Beim Betriebssystem Windows2000 wird diese Datei standardmäßig in folgendem Verzeichnis abgelegt:

```
%SystemRoot%\Dokumente und Einstellungen\%USERNAME%\Local
Settings\Microsoft\Outlook\
```

Dieser Ordner gehört aber nicht zu dem Teil des Benutzerprofils, das auf dem Server gespeichert wird. Daher ist eine Verlagerung dieser Datei nötig. Damit aber die Benutzer den Speicherort in der Datendateiverwaltung von Outlook nicht ändern können, muss die Pfadangabe ebenfalls von einer Systemrichtlinie vorgeschrieben werden. Der Quellcode hierfür sieht folgendermaßen aus:

```
POLICY "Standard Pfad für PST files"
KEYNAME Software\Policies\Microsoft\Office\10.0\Outlook
   PART "Default location for PST files" EDITTEXT
        VALUENAME ForcePSTPath
```

```
   END PART
END POLICY
```

Diese Systemrichtlinie erlaubt die Eingabe eines speziellen Pfades zu einem Ordner, in dem nun das Mailprofil standardmäßig abgespeichert wird. Die Pfadangabe im Systemrichtlinieneditor wird mit diesem Eintrag erzeugt:

```
%SystemRoot%\Dokumente und Einstellungen\%USERNAME%\Anwendungsdaten\
\Microsoft\Outlook\
```

Der Ordner `\Anwendungsdaten` wird in dem Teil des Benutzerprofils gespeichert, der auf dem Server liegt. In Abschnitt 5.3.2 zeigt Abbildung 6 die Ansicht eines servergespeicherten Profils mit dem erzwungenen Speicherort der Datei des Mailprofils eines Benutzers. Damit E-Mails empfangen und versendet werden können, muss noch ein Mailkonto mit Angaben zum Mailserver, POP3- und SMTP-Einstellungen für jeden Benutzer angelegt werden. Die eigentlichen E-Mail-Konten liegen aber nicht auf den Servern des Betriebes, sondern werden entgeltpflichtig von einem Provider, wie zum Beispiel T-Online, zur Verfügung gestellt. Die lokalen Einstellungen für die Benutzer werden von Systemrichtlinien vorgegeben. Durch die oben beschriebenen Maßnahmen wird den Benutzern ein E-Mail-Client geliefert, der zwar keine eigenen Einstellungen hinsichtlich der Konfiguration von anderen E-Mail Konten zulässt, jedoch einen marginalen Aufwand an Support des Administrators erfordert. Alle Konfigurationen sind serverseitig gespeichert und lassen sich von dort aus verwalten.

6.2 Remoteadministration

Der zukünftige Administrator hat die Möglichkeit, über Microsoft NetMeeting die direkte Kontrolle über ein Clientbetriebssystem von einem Arbeitsplatz seiner Wahl zu übernehmen. Auf den Client-Betriebssystemen wird dazu die Remote-Desktop-Freigabe von NetMeeting aktiviert. Über das Zielwahlverzeichnis des Servers, wie in Abbildung 18 auf Seite 69, wählt sich der Administrator in den gewünschten Client ein. Hinter den Namen der Clients in Abbildung 18 verbergen sich ihre IP-Adressen. Für die Anmeldung wird das Administrator-Konto mit dem zugehörigen Kennwort benutzt.

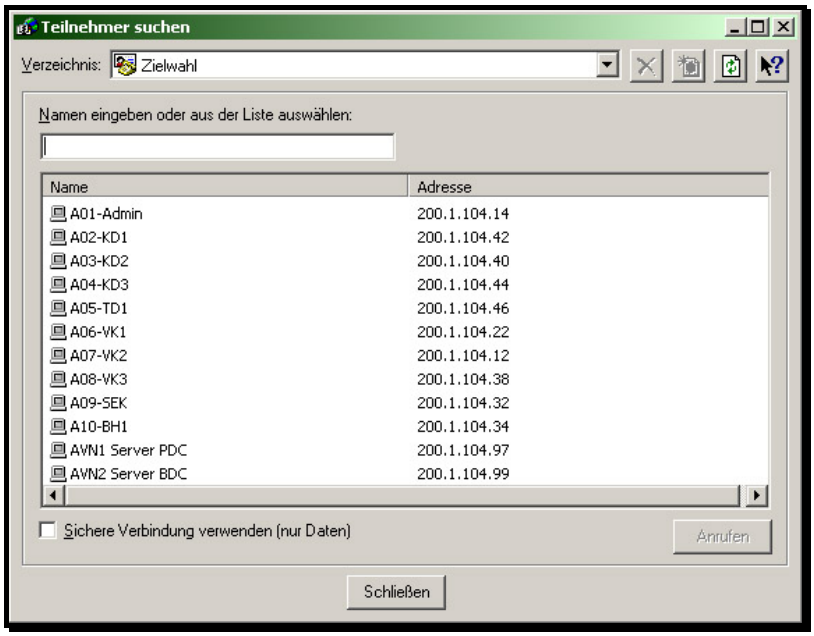

Abbildung 18: Zielwahlverzeichnis des Servers

Für das Remote-Management von InoculateIT6.0 wird auf dem Administrator-Arbeitsplatz die Admin-Konsole der Software installiert. Der Administrator verwaltet ohne direkten Zugriff auf den Server Funktionen wie das Update von Virusdefinitionen oder geplante Virensuchläufe, sowohl auf den Servern als auch auf den Clientsystemen.

6.3 Zugriffsberechtigungen der Benutzergruppen

In diesem Kapitel wird auf die Unterschiede der Benutzergruppen Verkauf2000 und Service2000 eingegangen. Die hardwareseitige Konfiguration der Clientsysteme ist bei beiden Gruppen identisch. Softwareseitig wird durch die Image-Datei ebenfalls die gleiche Konfiguration auf allen Clientsystemen verteilt, jedoch kann nicht allen Benutzern Zugriff auf alle Anwenderprogramme gestattet werden. Folgende Aufstellung erklärt die Gründe:

- Benutzer der Gruppe Verkauf2000 haben keinen Zugriff auf die Car-Dealer-Software Werbas. Lizenzen für Werbas müssen pro Betriebssystem erworben werden. Der Zugriff zur Software funktioniert nur dann, wenn dem dort installierten Datenbankclient (siehe Abschnitt 5.5) eine eindeutige Nummer zugewiesen wird und wenn an dem jeweiligen Rechner ein Hardware-Dongle an der parallelen Schnittstelle des Rechners vorhanden ist. Die Onlinedatenbank der k.u.r.s. mediasystems (2003) definiert den Hardware-Dongle als kleinen Stecker, der ein Verschlüsselungssystem für eine bestimmte Software enthält. Ist er nicht installiert, läuft das Programm nicht. Die einzelnen Lizenzen für Werbas sind recht teuer. Aus diesem Grund werden zu den fünf bestehenden (siehe Kapitel 3) keine weiteren Lizenzen beschafft. Auf den elektronischen Ersatzteilkatalog

ETKA haben Benutzer der Gruppe Verkauf2000 keinen Zugriff, da die Lizenzierung ähnlich wie bei Werbas durch einen Hardware-Dongle geregelt wird.

- Benutzern der Gruppe Service2000 wird der Zugriff auf die verkaufsrelevante Software Kosyfa und ProAct verweigert. Für den Zugriff auf die Software Kosyfa muss der Benutzer bei der CC-Bank als Verkäufer gemeldet sein. Die Anmeldung zu diesem Status wird nur für Mitarbeiter im Verkaufsbereich gemacht. Diese Benutzer erhalten anschließend von der CC-Bank einen Benutzernamen und ein Passwort. Die Software ProAct unterstützt die Mitarbeiter des Verkaufsbereichs hinsichtlich der Kundenbetreuung. Persönliche Daten von Kunden des Autohauses werden mit dieser Software verwaltet. Aus diesem Grund wird auch hier der Zugriff ausschließlich Mitarbeitern des Verkaufsbereichs gestattet.

Damit die jeweilige Software nur von den Mitarbeitern gestartet werden kann, die dazu berechtigt sind, werden die Zugriffsrechte zu den entsprechenden Laufwerksfreigaben des Servers (siehe Abschnitt 5.3.1) beschränkt, bzw. den Benutzergruppen entzogen. Versucht nun ein Benutzer eine Anwendung, auf die er keine Zugriffsberechtigung hat aufzurufen, verursacht das auf dem Clientbetriebssystem eine unschöne Fehlermeldung. Deshalb werden für die zwei Benutzergruppen verschiedene Programmverknüpfungen auf den Client-Betriebssystemen durch die unter Kapitel 6 auf Seite 63 erläuterten Systemrichtlinien verteilt. Die folgende Tabelle zeigt noch einmal, welchen Benutzergruppen welche Programmverknüpfungen zur Verfügung stehen.

Tabelle 3: Programmverknüpfungen

Software	Programmverknüpfungen Benutzergruppe Verkauf2000	Programmverknüpfungen Benutzergruppe Service2000
Werbas	Nein	Ja
Kosyfa	Ja	Nein
ProAct	Ja	Nein
MIS	Ja	Ja
SilverDAT	Ja	Ja
ETKA	Nein	Ja

7 Zusammenfassung – Ausblick

In der hier vorgestellten Arbeit wurde eine moderne Netzwerklösung, die den Anforderungen des Automobilherstellers Škoda und der Firma Auto-Vertrieb-Neckar GmbH entspricht, erarbeitet. Allen Benutzern dieser Lösung stehen moderne Anwendersoftware und neueste Technologien zur Verfügung. Durch die Kombination von Windows2000 Professional als Client-Betriebssystem und Windows NT Server wird die alte EDV-Lösung kostengünstig auf den neuesten Technologiestandard migriert. Dem zukünftigen Administrator des Betriebes steht mit dieser Arbeit eine umfangreiche Dokumentation und Entscheidungshilfe für zukünftige Neuanschaffungen zur Verfügung.

7.1 Erklärung des Nutzens

Mit der Verwendung von zwei Servern und der entsprechenden Konfiguration der Domäne steht dem Unternehmen AVN ein fehlertolerantes System zur Verfügung. Umfangreiche Mechanismen zur Datensicherung und Datenredundanz gewährleisten eine hohe Verfügbarkeit unter Einsatz geringster finanzieller und materieller Mittel. Die serverseitige Konfiguration nahezu aller Benutzeinstellungen benötigt einen minimalen Aufwand an Support durch einen externen Mitarbeiter. Dadurch werden Personalressourcen und damit verbundene hohe Kosten eingespart.

Der Einsatz von netzwerkfähigen Druckern ermöglicht ein schnelles und gezieltes Ausdrucken. Der im Betrieb bereits vorhandene Digitalkopierer wurde mit einer Druck- und Netzwerkschnittstelle ausgestattet. Druckaufträge werden innerhalb kürzester Zeit, selbst im Umfang von mehreren hundert Seiten, abgearbeitet. Alle Drucker der Systemumgebung stehen den Benutzern jederzeit zur Verfügung. Die Nachteile, die bei der Installation und Wartung von lokalen Druckern entstehen sind nicht mehr vorhanden. Über den Druckertreiber des digitalen Kopierers können unterschiedliche Papiereinzüge angesprochen werden. Mit dieser Option sind Ausdrucke auf Geschäftspapier und Blankopapier über ein einziges Gerät möglich.

Die Benutzer der Gruppe Service2000 erhalten durch die Erweiterung der Werbas Car-Dealer-Software ein modernes System, mit dem die Aufgaben des Tagesgeschäftes bearbeitet werden können. Die neuen Schnittstellen zu anderer Anwendersoftware erleichtern die Datenübergabe und vereinfachen den Import von Daten aus anderen Datenbanken. Durch den direkten Import von Daten aus Werbas in die Lohn- und Finanzbuchhaltung DATEV wird die Kontierung erleichtert. Die Datenübergabe an den Steuerberater erfolgt in einheitlicher Weise.

Mitarbeitern der Abteilung Verkauf2000 wird eine einfache und sichere Bedienung verkaufsrelevanter Software ermöglicht. Das schafft Sicherheit bei der Bearbeitung von Kundendaten. Durch die zentrale Verwaltung von Datenbanken der Verkaufssoftware müssen Updates, wie zum Beispiel das Laden von neuen Vertragskonditionen, nur

noch einmalig durchgeführt werden. Sie stehen nach dem Download im gesamten Netzwerk allen Benutzern zur Verfügung. Mit dem Programm ProAct von Procar wird die Kundenbetreuung unterstützt. Die Installation des Markt-Informations-Systems (MIS) liegt zentral auf dem Server und kann vom Verkaufsleiter und den Verkäufern aufgerufen werden. Die Marktanteile und Anzahl der zugelassenen Fahrzeuge kann innerhalb kurzer Zeit bewertet werden.

Die erarbeitete Lösung zeichnet sich durch eine hervorragende Skalierbarkeit hinsichtlich der Verwendung neuer Clientsysteme aus. Neue Mitarbeiter erhalten in kurzer Zeit Zugang zum System. Ermöglicht wird dies durch die temporäre Erstellung so genannter Standardbenutzerprofile, die bei Bedarf einfach in die Laufwerksfreigabe des neuen Benutzerprofils kopiert werden. Die Konfiguration eines neuen Benutzerzugangs bzw. eines neuen Benutzerprofils dauert im Durchschnitt 5 Minuten. Der angelernte Mitarbeiter des Betriebes wird zum lokalen Administrator ernannt und ist in der Lage, diesen Vorgang selbst durchzuführen.

7.2 Zukünftige Erweiterungen

In die hier beschriebene Arbeit sollte zukünftig das Dynamic Host Configuration Protocol (DHCP) integriert werden. Unter Windows NT Server ist das ohne weiteres durch Nachinstallation der entsprechenden Dateien von der CD-ROM des Betriebssystems möglich. Dieses Protokoll weist den Client-Betriebssystemen bei der Anmeldung an eine Windows NT-Domäne die benötigten IP-Adressen dynamisch zu. Hunt und Thompson (1999, S. 127) sprechen von Clients, die keine eigenen IP-Adresse […] haben. Stattdessen fordert ein DHCP-Client beim Systemstart vom DHCP-Server eine IP-Adresse an. Der DHCP-Server besitzt einen Bereich von IP-Adressen, die er Clients zuweisen kann. Wie lange eine IP-Adresse für einen Client gültig ist, hängt von den Einstellungen des DHCP-Servers ab. Durch Einsatz dieses Protokolls wird das Management des Netzwerkes weiter vereinfacht. Insbesondere bei Übernahme eines Backupservers, kann die Umstellung der Domäne und der Clientsysteme durch die schnelle Zuweisung eines anderen, für den zweiten Server gültigen IP-Adressbereich, erfolgen.

Dadurch dass in dieser Arbeit alle Benutzerprofile serverseitig gespeichert werden, kann ein weiteres Feature von Microsoft NT Server eingesetzt werden. Quota-Profile beschränken das Profil eines Benutzers auf eine vom Administrator beliebig festgelegte Größe. Überschreitet das Benutzerprofil die serverseitig vorgeschriebene Größe auf der Festplatte, erhält der Benutzer eine Meldung. Diese Meldung fordert ihn auf, Dateien seines Benutzerprofils zu löschen. So erreicht man eine bessere Verwaltung des vorhandenen Speicherplatzes der Festplattensysteme der Server. Ein weiterer Aspekt ist dabei die Zeit, die nach der Anmeldung eines Benutzers am System verstreicht. Ist das Benutzerprofil zu groß (50-100 Megabyte oder mehr), kann es mehrere Minuten dauern, bis das servergespeicherte Profil auf den Client kopiert wird. In dieser Arbeit werden die Benutzerprofile hauptsächlich durch die E-Mail-Profile von Microsoft Out-

look stark vergrößert. Die oben erwähnte Meldung müsste den Benutzer dann dazu auffordern, E-Mails in Microsoft Outlook zu löschen. Auch das ließe sich durch entsprechende Konfiguration von Systemrichtlinien erzwingen.

Zur verbesserten Absicherung des Systems gegenüber Angriffen aus dem Internet könnte zukünftig eine spezielle Firewall Hardware oder Software eingesetzt werden. Für wirklich effektive Firewallsysteme muss man jedoch mit hohen Anschaffungskosten rechnen. Das steht natürlich im Widerspruch zum kleinen Budget dieser Arbeit. Auch ein serverseitiges Mailsystem wie Microsoft Exchange kann in diese Arbeit problemlos implementiert werden.

Glossar

Business to Business: (Abk. B2B). Bezeichnung für die computergestützte Kommunikation oder Geschäftsabwicklung zwischen Unternehmen.

Business to Customer: (Abk. B2C) Bezeichnung für die computergestützte Kommunikation zwischen Unternehmen und deren Kunden wie etwa bei der Bestellung von Waren über das Internet.

DATEV: in Nürnberg ist Marktführer für Software zur Abwicklung von Finanz- und Lohnbuchhaltung. Der Softwarehersteller bietet Dienste seines Rechenzentrums anderen Unternehmen, insbesondere Anwaltskanzleien und Steuerberatern, an.

ETKA: ist die Abkürzung der Begriffe **e**lektronischer **T**eile **Ka**talog. Er wird von Škoda Auto Deutschland auf CD-ROM an die Vertragspartner ausgeliefert. In den Datenbanken des ETKA sind Preise und Teilenummern aller Škoda Ersatz- und Zubehörteile gespeichert. Die Handhabung ist vergleichbar mit der eines Mikrofiches.

ADSL (DSL): ADSL ist eine neue Technik zur Datenübertragung ins Internet. ADSL (Asymmetric Digital Subscriber Line) bietet viel höhere Geschwindigkeiten, als herkömmliche Methoden wie ISDN oder Modem. Interessant an dieser Technik ist, dass normale zweiadrige Telefonkabel aus Kupfer genutzt werden können. Damit die Sprache von den Daten unterschieden werden kann, wird ein so genannter Splitter eingesetzt, der die verschiedenen Frequenzen für das Telefon von denen des Rechners trennt.

Cat. 5 oder **Cat. 6** Verkabelung bezeichnet die Qualität eines mehradrigen EDV- oder Telephoniekabels bezüglich der Empfindlichkeit gegenüber Störeinwirkungen. Durch die Kategorisierung der Cat. Klassen lassen sich Rückschlüsse auf die größtmögliche zu übertragende Datenmenge und die maximal erlaubte Länge des Kabels ziehen.

SAM-Datenbank: Durch die Sicherheitskontenverwaltung (engl. Security Account Manager) werden die Informationen über Benutzer- und Gruppenkonten eines Windows NT- oder Windows2000 Systems in der Security Account Database, die häufig auch als SAM-Datenbank bezeichnet wird, verwaltet. In einer Domänenumgebung gleicht der erste Domänencontroller (engl. Primary Domain Controller, PDC) die SAM-Datenbank mit allen anderen Domänencontrollern ab.

Patchfeld: Wird im Fachjargon auch als Patchpanel bezeichnet. Dieses Panel hat an der Vorderseite Einschübe für Netzwerkkabel. An der Rückseite werden die Adern der im Gebäude verlegten Netzwerkkabel eingeführt.

Patchkabel: Netzwerkkabel von geringer Länge, mit denen das Patchpanel und der Hub oder Switch im EDV-Schrank angeschlossen werden.

WINS: WINS ist eine verteilte Datenbank auf Internet-Servern mit dem Betriebssystem Windows NT oder einem Nachfolger, in der Paarungen aus IP-Adressen und NetBIOS-

Namen eingetragen sind. Windows-Rechner identifizieren sich beim Start mit ihren NetBIOS-Namen auf dem WINS-Server, so dass andere Windows-Rechner diesen um IP-Adressen anfragen können. Da der WINS-Server über seine IP-Adresse angesprochen wird, kann er auch Auskunft an Rechner geben, die sich in anderen Netzwerksegmenten befinden.

DHCP: Dieses Netzwerkprotokoll ermöglicht die dynamische Konfiguration von IP-Adressen und damit zusammenhängenden Informationen. Es unterstützt die Verwendung von begrenzt vorhandenen IP-Adressen durch zentralisierte Verwaltung der Adresszuordnung über eine Datenbank des Servers. Bei Anmeldung eines Clientsystems an die Domäne bzw. an den DHCP-Server wird eine IP-Adresse für einen bestimmten Zeitraum vergeben.

RGB-Werte, RGB-Farbschema: Das RGB Farbschema ist ein gängiges Schema, das auch in Graphikbearbeitungsprogrammen verwendet wird. Es gibt das Mischverhältnis der Farben Rot, Grün und Blau an.

CLS-ID: Objekte werden von Windows über ihre CLS-ID (Class Identifier) angesprochen. Diese Objekte haben Eigenschaften, z. B. einen Namen, das Icon, ob es sich um einen Shortcut handelt und etliche andere Methoden. Eine Methode ist ein Vorgang, der gestartet wird, wenn mit diesem Objekt gearbeitet wird, zum Beispiel wenn ein Doppelklick mit der Maus auf eine Verknüpfung ausgeführt wird. Damit ein Objekt, welches durch seine CLS-ID repräsentiert wird, eine Methode besitzt, muss natürlich ein Programm vorhanden sein, welches diese Methode ausführt. Alle CLS-IDs sind in der Registrierdatenbank des Windows-Betriebssystems im Schlüssel HKEY_CLASSES-_ROOT angegeben.

Printserver: Ein Rechner oder externes Peripheriegerät im Netzwerk, das den Datenfluss zu einem oder mehreren Druckern steuert und eingehende Druckaufträge in einer Warteschlange verwaltet.

Logon-Skript: Das Logon-Skript ist eine Datei, in der Netzwerkressourcen, wie Drucker oder Ordnerfreigaben, mit Hilfe von DOS-Befehlen den gewünschten Laufwerksbuchstaben zugeordnet werden. Damit diese Skript-Dateien von der DOS-Konsole ausgeführt werden können, werden sie mir der Dateierweiterung *.bat oder *.com abgespeichert.

Literaturverzeichnis

Raepple, M. (2001): Sicherheitskonzepte für das Internet: Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung. 2. Auflage. dpunkt.Verlag. 426 S. ISBN 3-89864-116-3.

Grupp, B. (1999): Das DV-Pflichtenheft zur optimalen Softwarebeschaffung, mitp-Verlag, Bonn. ISBN 3-8266-0493-8. 320 S.

Zenk, A. (1995): Lokale Netze, Kommunikationsplattform der 90er Jahre, LAN-Betriebssystem, Internetworking, Netzwerkmanagement. 3. Auflage. Addison-Wesley Deutschland. ISBN 3-89319-741-9. 884 S.

Dawicontrol (2003): Computersysteme.
URL: http://www.dawicontrol.de/german/html/infoscsi.htm. (Datum des letzten Zugriffs: 03.06.2003).

Eicker, T. (2003): Kleines Lexikon des Internet. URL: http://www.kleines-lexikon.de/w/p/pppoe.shtml. (Datum des letzten Zugriffs: 15.07.2003)

WINFAQ: [Eingangsportal]. URL: http://www.winfaq.de. (Datum des letzten Zugriffs: 20.06.2003).

Kauffels, F.-J. (2002): Durchblick im Netz. 5. Auflage. mitp-Verlag, Bonn.
ISBN 3-8266-0935-2. 693 S.

Dembowski, K. (2002): Netzwerke. Markt+Technik Verlag, München.
ISBN 3-8272-6295-X. 644 S.

Hunt, C. und Thompson, R. B. (1999): Windows NT TCP/IP Netzwerk-Administration. O´Reilly & Associates, Inc.. ISBN: 3-89721-170-X. 512 S.

Jungbluth, T. (1996): Datensicherung: auf Streamern, Wechselplatten und CD-ROM. Carl Hanser Verlag, München Wien. ISBN: 3-446-18610-7, 341 S.

Gottwald, O. (2000): EDV-Betriebskonzept für Škoda Vertragspartner, unveröffentlicht.

k.u.r.s. mediasystems GmbH: Computerhilfen.de URL: http://www.computerhilfen.de/lexikon_anzeiger.php?log=log_h&term=Hardware-Dongle. (Datum des letzten Zugriffs: 14.07.2003).

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Diplomarbeit selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht.

Ort, Datum

Unterschrift