GESIS

IZ InformationsZentrum Sozialwissenschaften

IZ-Arbeitsbericht Nr. 27

IT-Struktur-Konzept des IZ

Daniel Link, Wolf-Dieter Mell

Oktober 2002

InformationsZentrum
Sozialwissenschaften

Lennéstraße 30
D-53113 Bonn
Tel.: 0228/2281-0
Fax.: 0228/2281-120
email: mell@bonn.iz-soz.de
Internet: http://www.gesis.org

ISSN: 1431-6943

Herausgeber: Informationszentrum Sozialwissenschaften der Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V. (ASI)

Druck u. Vertrieb: Informationszentrum Sozialwissenschaften, Bonn
Printed in Germany

Inhalt

1 Vorbemerkungen

1.1 Aufgabenstellung der Organisationseinheit EDV/Org.

Die Abteilung EDV/Org. ist eine Infrastruktur-Abteilung des IZ mit der Aufgabe, die Nutzung und den Einsatz von EDV und Telekommunikation für die Erledigung der Fachaufgaben des Institutes zentral zu koordinieren und zu betreuen.

Hierzu gehören nicht nur die Planung, Beschaffung, Installation und der Betrieb der IT-Infrastruktur (von der Server- und Arbeitsplatz-Hardware über die Betriebssysteme, Dienste und Netzwerkanbindungen bis hin zur Anwendungs-Software auf den Arbeitsplätzen), sondern auch sowohl die Betreuung der fachlichen Projekte hinsichtlich der Auswahl und Nutzung geeigneter IT-Instrumente als auch die Evaluation neuen technischer Optionen hinsichtlich ihres Nutzens zur Erledigung laufender oder neuer Aufgaben in den Fachabteilungen, mit dem Ziel, neue Optionen der sich schnell ändernden IT-Technik innovativ in neue/verbesserte Produkte, Strukturen und Prozesse umzusetzen.

Die besondere Anforderung an diese Aufgabenstellung liegt in der Verantwortung für die Folgen technischer und organisatorischer Entscheidungen auf die Produktivität des Institutes, nicht nur bei der Aufrechterhaltung des störungsfreien Betriebs, sondern auch bei den Entscheidungen über die Zuordnung knapper finanzieller und personeller Ressourcen zu Diensten, Aufgabenbereichen und Personen und bei den Abwägungen zwischen der Durchsetzung organisatorischer und technischer Standardisierung der Betriebsmittel und Betriebsabläufe und der Bewilligung fachlich nachvollziehbarer Sonderlösungen zur Erledigung spezieller Aufgaben.

Das vorliegende Papier befasst sich im Rahmen der Strukturplanung ausschließlich mit der IT-Technik und den damit zusammenhängenden organisatorischen Fragen. Die Konzepte zur Erledigung anderer wichtiger Aufgaben der Abteilung - Beiträge zur Umsetzung neuer IT-Technik in Produkt-, Struktur- und Prozess-Innovationen, Bereitstellung und Pflege von Software für die Fachabteilungen, IT-fachliche Unterstützung der Anwender, inhaltlich-technische Bereitstellung und Pflege des Internet-Angebotes, Bereitstellung IT-basierter Kennziffern etc. - sind Gegenstand separater Untersuchungen.

1.2 Business Value

Zweck des IT-Einsatzes ist es grundsätzlich, einen den IT-Kosten angemessenen Beitrag zur Förderung der Erfolgsfaktoren der Organisation, also ihres Nutzen und Erfolges bei ihren Auftraggebern, Partnern und Kunden zu liefern.

Die zentralen Tätigkeitsfelder des IZ, sein Auftrag, seine Dienste und seine Produkte sind in den Beschlüssen und Positionspapieren der Gremien und der Institutsleitung beschrieben (s. u.a. J. Krause: IZ-Strategiepapier):

Dienstleistungsspektrum des IZ

- Informationssysteme zu sozialwissenschaftlichen Forschungsaktivitäten
  - Datenbank SOLIS zu sozialwissenschaftlicher Fachliteratur
  - Datenbank FORIS zu Projektinformationen
  - Datenbanken zu Forschungseinrichtungen, Fachzeitschriften
  - Englischsprachige Datenbanken/Informationssammlungen zu den osteuropäischen Sozialwissenschaften (Institutionenprofile, Forschungsprojektinformationen, Zeitschriftenprofile, Personen-Datenbank).
  - Nationale und internationale Volltexte im Rahmen des Informationsverbunds Bildung – Sozialwissenschaften – Psychologie (im Aufbau)
  - Virtuelle Fachbibliothek Sozialwissenschaften (mit integrierter Suche von Fachliteratur aus Universitätsbibliotheken, Instituten und den IZ-Literaturdatenbanken).
  - Fachinformationsführer Socioguide und Veranstaltungskalender
- Elektronische und Printprodukte
  - Reihe Sozialwissenschaften im Überblick (Forschungsübersichten gemeinsam mit Fachvertretern zu gesellschaftlich relevanten Themenkomplexen)
  - Reihe Sozialwissenschaftlicher Fachinformationsdienst (soFid) Zweimal im Jahr Nachweis der neuesten Fachveröffentlichungen und Forschungsprojekte zu 28 Themenbereichen
  - Reihe Gesellschaft im Fokus der Sozialwissenschaften mit tagesaktuellen Themenfeldern
  - Newsletter „Social Sciences in Eastern Europe“,
  - State-of-the-Art-Reports und kombinierte Dienste zu den osteuropäischen Sozialwissenschaften wie das Handbuch „Social Sciences in Central and Eastern Europe“
- Serviceleistungen und Koordinationstätigkeit für deutschsprachige Netzwerke der auf Osteuropa gerichteten Forschung sowie für osteuropäische sozialwissenschaftliche Netzwerke
- Internetangebote und -vernetzungen
- Informationsvermittlung auf der Basis internationaler Datenbankrecherchen
- Benutzerfreundliche innovative Softwareentwicklung für sozialwissenschaftliche Dienstleistungen auf der Basis von Standardsoftware
- Workshops, Tagungen, akademische Lehre, Förderung von Nachwuchswissenschaftlern

Aufgabe der IT ist es, die hieraus resultierenden Business-Prozesse zu unterstützen und - durch den geeigneten Einsatz von IT-Instrumenten und -Strukturen - :

- Business-Prozesse zu rationalisieren und den technischen / organisatorischen / personellen Aufwand zu optimieren,
- die Qualität der Ergebnisse von Business-Prozessen zu verbessern,
- Business-Prozesse zu beschleunigen,
- neue Prozesse für alte oder neue Aufgaben zu evaluieren und deren Implementierung technisch und organisatorisch zu unterstützen.

Business-Prozesse in diesem Sinne sind nicht nur die unmittelbaren Arbeitsprozesse zur Erstellung der Dienste und Produkte, sondern alle Aktivitäten, die direkt oder indirekt auf die Förderung von Nutzen und Erfolg des IZ bei seinen Auftraggebern, Partnern und Kunden gerichtet sind, u.a.:

- Prozesse zur Erstellung von Produkten und Diensten,
- Prozesse zur Entwicklung neuer Produkte und Dienste,
- Prozesse in den Beziehungen zwischen dem IZ und seinen Auftraggebern und Kunden (vom Web-Angebot über die Rechnungsstellung bis zur Präsentation auf Tagungen),
- Prozesse in der Zusammenarbeit des IZ mit seinen Partnern (von der Telefon-, E-Mail- und Fax-Unterstützung bis zur Breitstellung von Servern oder Domain-Anmeldungen),
- interne Prozesse (z.B. interne Verwaltung, Organisation und Kommunikation),
- Prozesse zur Bereitstellung von IT-Service und IT-Administration (von der Einrichtung der Accounts, über die Bereitstellung und Pflege der Arbeitspltz-PCs und Server bis zur Steuerung der Internet-Schnittstellen).

Die IT hat hierbei folgende Handdungsoptionen:

- Gestaltung und Bereitstellung von Strukturen:
  - Systemkonzept, Access-Management, Change-Management, Standardisierung,
  - Kommunikation,
  - Datenspeicher,

  - Datenbanken, Dienste, Anwendungen, Verfahren,
  - Mobilitäts-Support,
- Beschaffung, Bereitstellung, Pflege von Hardware, Software, Infrastruktur:
  - Server und Dienste,
  - Arbeitsplätze und Anwendungssoftware,
  - LAN, Internetanbindung, Kommunikationsverfahren,
  - Zubehör,
  - Sicherheit.

Es wird damit gerechnet, dass in den kommenden Jahren folgende Schlüsselfunktionen der Geschäftsprozesse massiv in IT-Verfahren integriert werden:

Funktion	**Beschreibung**	**IZ konkret**
Personalisierung	Integration der Kunden- und Partner-Profile aus den unterschiedlichen operativen Systemen, Multi-Channel-Service auf der Basis personalisierter Kundeninformationen	Weiterentwicklung des Data-Warehouse-Konzeptes, online-Nutzung der Profile für die automatische personalisierte Internet-Kommunikation
Collaboration	IT-gestütze Zusammenarbeit, u.a.: Engineering und Entwicklung, Kunden-Management, Lieferanten/Partner-Management, Dokumenten- Bearbeitung, Projekt-Management, interaktive Besprechungen, etc.	Weiterentwicklung der collaborativen IT-Instrumente und -Verfahren (Videokonferenz, Groupware-Exchange, Produkt-Erstellung (Sofid) etc.) sowie des technischen und organisatorischen Supports für die Kooperations-Projekte des IZ mit externen Partnern

Echtzeit	IT-gestützte Überwachung und Steuerung der Geschäftsaktivitäten durch ereignisgesteuerte Prozesse, Zusammenfassung von separaten Einzelprozessen zu automatisch ablaufenden Gesamtprozessen, u.a.: Produktionssteuerung, Auftragsverwaltung, Lagerverwaltung, Bestellwesen, Verwaltungsvereinfachung, (IT-)Technik-Überwachung	Integration von Vorgangsdaten und Ereignissen in Data-Warehouse-Datenbanken, Weiterentwicklung IT-gestützter Prozessketten, z.B. für Verwaltungsvorgänge, Ersatz manueller Kontrollen und Entscheidungen durch IT-Kontroll-Prozesse
Portale	Integration der unterschiedlichen Anwendungen, einheitliche Oberfläche, Verbindungen zwischen den Anwendungen werden von den Benutzern nicht mehr wahrgenommen. Unternehmensportale sowohl "nach innen" (Intranet) als auch "nach außen", der Fokus von Mitarbeiter und Kunden wird zu einem gesamtheitlichen Ansatz verändert.	Weiterentwicklung der Funktions/Programm-orientierten Menü-Strukturen zu Aufgaben/Ziel-orientierten Prozess-Ketten.
Mobilität	1. Nutzung von Verfahren und Daten von einem beliebigen Netzwerk-Access-point aus, 2. Personalisierung des Zugangs (Oberfläche, Rechte) unabhängig vom Access-point, unabhängig vom Endgerät, 3. Einsatz moderner Verbindungs-Technologien für einen nutzerfreundlichen Netz-Zugang einer großen Bandbreite von Anwendungs-Situationen	Weiterentwicklung 1. des Access-Managements und der Zugangsregeln für das IT-Angebot des IZ, 2. der Oberflächen-Technologie des IT-Angebotes, 3. des Angebotes an Zugangs-technologie, 4. der Sicherheits-Technologie für die Zugangs- und Rechte-verwaltung

Dies wird in den kommenden Jahren (neben den operativen Aufgaben und in Kooperation mit den Fachabteilungen) eine Konzentration der IT auf Datenbank- und Data-Warehous-Technologie, auf Prozess-Integration und auf (Internet-)Kommunikations-Technologie erfordern.

1.3 Grundsätze der IT-Strukturplanung des IZ

Die IT-Strukturplanung des IZ basiert auf folgenden Grundsätzen (s. auch "GESIS IT-Rahmenkonzept und EDV-Investitionsplanung"):

- Alle Arbeitsplätze werden mit einheitlicher PC-Hardware ausgestattet. Hierdurch wird das roll-out, die Behandlung von Störungen und das Change Management erheblich vereinfacht.

- Alle PC-Arbeitsplätze werden in einem gemeinsamen Beschaffungs- und Austausch-Projekt regelmäßig in ca. 3-jährigen Zyklen durch neue Geräte nach dem jeweiligen Stand der Technik ersetzt.

- Betriebssysteme und Anwendungssoftware der PC-Arbeitsplätze werden zentral vorgegeben und gepflegt. Ausnahmen werden nur dort zugelassen, wo dies für Forschungs- und Entwicklungsprojekte unter technischen oder organisatorischen Gesichtspunkten erforderlich ist. Anwendungssoftware wird i.d.R. vollständig auf den Arbeitsplätzen installiert. Die Lizenzverwaltung erfolgt zentral. Die Bereitstellung der dienstlich erforderlichen Software erfolgt - soweit technisch/organisatorisch zweckmäßig und möglich - entweder bei der Auslieferung des Arbeitsplatz-PCs über das Installations-Image oder mit Hilfe von zentral gepflegten Software-Verteilungs-Tools (WinInstall o.ä.). Die individuelle Installation von Software auf den Arbeitsplätzen erfolgt nur in Ausnahmefällen, individueller Download und Installation von Software aus dem Internet ist unerwünscht, wird aber aus übergeordneten organisatorischen Gründen technisch nicht verhindert.

- Für alle Arbeitsplätze (mit wenigen fachlich begründeten Ausnahmen) wird ein einheitliches Standard-Arbeitsplatz-Betriebssystem vorgeschrieben. Wegen der großen Bedeutung des Arbeitsplatz-Betriebssystems für organisatorisch und technisch reibungslose Betriebsabläufe und wegen des erheblichen Aufwandes eines Versionswechsels sowohl für die EDV als auch für die Anwender werden Betriebssystemwechsel mit großer Zurückhaltung geplant und erst nach sorgfältiger Prüfung und Vorbereitung durchgeführt. Arbeitsplatz-Betriebssysteme seit 1990:

1990 - 1994:	MS DOS
1994 - 1997:	MS Windows 3.1 / 3.11
1997 - 2002:	MS Windows 95

In der ersten Jahreshälfte 2002 wurden die Arbeitsplätze nach MS Windows 2000 Prof. migriert.

- Die zentralen Dienste werden durch PC-basierte LAN-Server mit einheitlicher Technologie erbracht. Zur Minimierung der Ausbreitung von Störungen und zur Vereinfachung der Administration wird jeder produktionsrelevante Dienst auf einem eigenen Server installiert. Das gleiche gilt für Forschungs- und Entwicklungsprojekte, auch hier werden jedem Projekt - bei Bedarf und je nach Art der benötigten Dienste - ein oder mehrere dedizierte Standard-Server zur Verfügung gestellt.

- Die PC-basierten LAN-Server für die zentralen IT-Dienste werden wie die PC-Arbeitsplätze in einem zusammenhängenden Beschaffungs- und Austausch-Projekt regelmäßig in ca. 3- bis 4-jährigen Zyklen durch neue Geräte mit den aktuell erforderlichen Leistungsmerkmalen nach dem jeweiligen Stand der Technik ersetzt.

- Das Standard-Server-Betriebssystem des IZ war bis Ende 2001 MS Windows NT und wurde in 2002 auf MS Windows 2000 Active Directory migriert. Andere Betriebssysteme (UNIX, LINUX) werden nur dann eingesetzt, wenn dies aufgrund der Anwendungssoftware für den benötigten Dienst unvermeidbar ist (s. Kap. 1.3.1).

- Ein Sonderfall der Serverkonfiguration ist das aDIS-Anwendungssystem (das Erfassungs- und Pflegesystem für die zentralen IZ-Datenbanken SOLIS und FORIS): Dieses wird als geschlossenes System mit einer Software der Fa. ASTEC und einer ORACLE-Datenbank auf einem Midrange-Server der Fa. Siemens unter UNIX betrieben.

- Die Standardisierung der Arbeitsplatz- und Server-Technologie ermöglicht die Behandlung technischer Störungen nach dem Prinzip der austauschbaren Teile (s.u.), die erforderlichen Komponenten werden systematisch auf Lager gehalten.

- Alle dienstlich relevanten Daten (Dateien und E-Mail) werden auf zentralen Servern gehalten und gepflegt. Dies
  - vereinfacht die Gruppenarbeit,
  - ermöglicht die systematische tägliche Datensicherung,
  - erlaubt den Zugang zu den Daten von unterschiedlichen Arbeitsplätzen/Notebooks aus,

sowohl lokal als auch über remote access, ggf. über das Internet,
- rationalisiert Ersatz/ Rekonfiguration defekter Arbeitsplätze.

- Aus Gründen der Datensicherheit sind alle Platten auf PC-Servern grundsätzlich als Spiegelplatten (RAID-1) konfiguriert. Zusätzlich erfolgt täglich eine Datensicherung aller Server auf die Platten mehrerer zentraler Backup-Server.

- Die beiden lokalen Netze des IZ in Bonn und Berlin verfügen je über ein offizielles C-Netz an IP-Adressen und sind jeweils über einen IZ-eigenen Router/Firewall mit dem Internet (Serviceprovider: DFN-Verein) verbunden. Die Firewalls sind - Stand 2002 - so konfiguriert, dass einerseits alle Arbeitsplätze einen uneingeschränkten Zugang zu allen Internet-Angeboten besitzen, andererseits der Zugriff aus dem Internet mit Hilfe von Filterlisten auf bestimmte IP-Adressen und Ports begrenzt wird (zu den Risiken dieser Technik und zu alternativen Optionen s.u.).

- Das IZ unterstützt den remote access seiner Mitarbeiter auf seine Daten und Dienste einerseits durch IZ-eigene, über Telefon, ISDN und GSM zugängliche RAS-Server, andererseits durch Internet-Zugang über Web-Access-Dienste, z.B. auf die zentralen E-Mail-Server.

1.3.1 Anmerkung: Server-Betriebssystem

Das IZ hat seit 1989 Erfahrungen mit den folgenden Server-Betriebssystemen:

- 1989 - 1999 Mainframe Siemens BS2000
- 1990 - 1995 OS/2
- 1994 - 1998 SCO Unix
- seit 1994 Windows NT
- seit 1995 Linux
- seit 1996 Siemens RM400 Sinix (Unix)
- seit 2000 Windows 2000

Seit 2002 setzt das IZ MS Windows 2000 Active Directory als Standard-Betriebssystem für seine Server ein. Diese Entscheidung basiert auf folgenden Gesichtspunkten:

Im Jahr 1990 wurde bei Einführung der PC-Server-Technologie im IZ eine Grundsatzentscheidung zu Gunsten des damals neuen Server-Betriebssystems OS/2 (der Firmen 3Com, Microsoft und IBM) und gegen das Betriebssystem

Novell getroffen. Die wichtigsten Gründe waren die transparentere Administrierbarkeit auf Intel-PCs und das höhere Einsatzpotenzial für PC-Anwendungen bei OS/2.

Mit dem Ausstieg der Firmen 3Com und Microsoft aus dem OS/2-Konsortium wurde 1995 zu MS Windows NT migriert, da dieses Server-Betriebssystem einerseits mit der installierten OS/2-Infrastruktur weitgehend kompatibel war und als zukunftssicherer eingeschätzt wurde, als die OS/2-Weiterentwickung von IBM.

Die alternative Option einer Migration zu UNIX oder Linux (mit SAMBA) als LAN-Server-Betriebssystem wurde nach unbefriedigenden Erfahrungen mit SCO-Unix (als Internet-Server seit 1994) hinsichtlich Systemstabilität und Administrationsaufwand nicht weiter verfolgt.

Nicht in geeigneter Qualität unter Windows NT verfügbare Dienste - insbesondere für Internet-Anwendungen - wurden seit 1995 als stand-alone-services auf Linux-Servern installiert. Die für das IZ zentrale aDIS-Software wurde wegen der erforderlichen Rechnerleistung als Datenbankanwendung zunächst auf einem Mainframe (Siemens, BS2000) installiert und 1996 auf ein leistungsfähiges UNIX-System migriert.

Die grundlegende Strukturentscheidung, produktionsrelevante Dienste auf jeweils eigenen PC-Systemen zu installieren, hat sich unter wirtschaftlichen, betriebstechnischen und organisatorischen Gesichtspunkten sehr bewährt. Mehrere Versuche der Dienst-Bündelung auf einzelnen Servern wurden wegen Instabilität und organisatorischem Aufwand rückgängig gemacht.

Ebenfalls bewährt hat sich die Entscheidung für MS Windows NT (und seine Nachfolger) als zentrales LAN-Betriebssystem: Die hohe Integration der Arbeitsplatz-Betriebssysteme (Windows) mit dem Server-Betriebssystem und der hohe Grad an gegenseitiger Synchronisation einer beliebigen Anzahl von Servern unter Windows NT (ff) untereinander rationalisiert in erheblichem Umfang die Administration der Benutzer und der Netzwerk-Ressourcen (insbesondere im Vergleich zu dem Administrationsaufwand der bis 2002 betriebenen Linux-Systeme). Die gelegentlich behauptete Instabilität oder Fehlerhaftigkeit von Windows NT kann vom IZ nicht bestätigt werden.

Mit der Verfügbarkeit stabiler Internet-Dienste unter Windows 2000 wurden 2002 die noch im Einsatz befindlichen Internet-Linux-Dienste durch Windows-Server ersetzt.

Für spezielle Anwendungen werden allerdings bei Bedarf auch in Zukunft die erforderlichen Betriebssysteme auf geeigneter Hardware bereitgestellt, diese Systeme sind allerdings i.d.R. nicht in die automatisierte User- und Rechte-Administration sowie in das Access- und Change-Management integriert.

Die Entscheidung des IZ für Windows 2000 als primäres zentrales Server-Betriebssystem wird durch die Untersuchung der Verwaltung des Deutschen Bundestages zu seinem künftigen Betriebssystem für die IuK des Bundestages bestätigt (dargestellt u.a. auf der Euroforum-Konferenz am 9.9.02 in Bonn, Vortrag von Erdmute Rebhan, Leiterin der Zentralen Informationstechnik beim Deutschen Bundestag: "Linux im Deutschen Bundestag"):

In einer umfassenden Untersuchung (2001) wurden dort 5 Infrastruktur-Alternativen einer Nutzwertanalyse unterzogen:

Beschreibung der Alternative	**Nutzwert**	**Rang**
1. Auf allen Servern und Clients wird Windows eingesetzt, bisher unter Linux laufende Systeme werden zu Windows 2000 migriert	7.420	3
2a. Auf den Datei- und Druckservern wird Windows 2000 eingesetzt, Linux-Server bleiben als Dienstserver erhalten, alle Clients nutzen Windows 2000 (ff). Als Verzeichnisdienst wird MS Active Directory eingesetzt.	8.050	1
2b. Auf den Datei- und Druckservern wird Linux eingesetzt, alle Clients nutzen Windows 2000 (ff), Verzeichnisdienst: Open LDAP	7.745	2
3. Auf allen Servern wird ausschließlich Linux, auf allen Clients Windows 2000 (ff) eingesetzt. Verzeichnisdienst: Open LDAP	6.370	4
4. Alle Server und Clients laufen unter Linux.	4.365	5

Das Ergebnis zeigt einen deutlichen Vorrang der moderaten Windows-Server-Option (2a).

Der Ältestenrat des Deutschen Bundestages hat sich allerdings (unter erheblichem politischen Druck) am 14.3.2002 für Alternative 2b (überwiegend Linux-Server) entschieden.

1.4 Evaluation der IT-Struktur 2002

Im Rahmen der Vorbereitung des für Anfang 2002 geplanten Austausches der Server-Hardware und der parallel dazu geplanten Migration des LAN-Betriebssystems auf MS Windows 2000 Active Directory wurde auf Empfehlung des Abteilungsleitung EDV/Org. die Durchführung einer internen Evaluation der IT-Struktur beschlossen, mit dem Ziel, das mittelfristige Entwicklungskonzept zu überprüfen, alternative und neue Optionen zu untersuchen und zu bewerten, die Ergebnisse systematisch zu dokumentieren und hieraus ein Migrationskonzept abzuleiten.

Zur fachlichen und personellen Unterstützung bei der Durchführung dieses Projektes wurde beschlossen, Teilbereiche der Evaluation - insbesondere die Untersuchung der Netzstruktur und der Netzwerksicherheit sowie der sich aus dem Wechsel zu Windows 2000 Active Directory ergebenden Notwendigkeiten, Optionen und Risiken - durch externe Berater bearbeiten zu lassen.

Nach formloser fachlicher Überprüfung mehrerer einschlägiger Beratungsunternehmen wurde dieser Auftrag an die Firma BOV, Essen, vergeben.

Das Evaluations-Projekt startete mit einem kick-off-meeting am 22. Februar 2002. Der abschließende Entwurf des vorliegenden Projektberichtes wurde Ende September 2002 fertiggestellt.

Folgende Personen (in alphabetischer Reihenfolge) waren vorrangig an der fachlichen Erarbeitung der Projektergebnisse beteiligt:

Rolf Beier, IZ
Daniel Link, BOV
Fabian Meissner, BOV
Wolf-Dieter Mell, IZ

2 Stand der IT-Struktur Anfang 2002

Als Ausgangslage soll in den folgenden Kapiteln dieses Abschnittes die IT-Konfiguration des IZ (Stand: Anfang 2002) in ihren entscheidungsrelevanten Strukturkomponenten tabellarisch dokumentiert werden.

2.1 Liste der Netzknoten

Die folgenden Listen dienen der Dokumentation und zeigen tabellarisch die in Bonn und Berlin zum Untersuchungszeitpunkt tatsächlich aktiven Netzknoten und deren Funktionen.

2.1.1 Bonn

IP Domäne: bonn.iz-soz.de
C-Netz: 193.175.238.*
NT Domäne: langroup
Windows 2000 AD Domänen: iz-soz.de, bonn.iz-soz.de

Anzahl Arbeitsplätze: ca. 80

Status-Report Netzknoten nach IP-Adressen (Stand: 30.04.2002, 14 Uhr)

IP-Adresse	Netbios-Name	DNS-Name	Status	Funktion	BS
193.175.238.1	DNS1	dns1	online	AD+DNS IZ-SOZ	W2k
193.175.238.2		dns	online	DNS (extern), DHCP	Linux
193.175.238.3	FTP	ftp	online	FTP, Appl. Server	NT
193.175.238.4		s4	online	aDIS Server	Unix
193.175.238.5		s5	online	Projekt Server FuE	SCO
193.175.238.6		s6, www	online	www.bonn.iz-soz.de	Linux
193.175.238.7		s7, mail	online	SMTP Server	Linux
193.175.238.8					
193.175.238.9	S9	s9	online	SAMBA Server (aDIS)	Linux
193.175.238.10	DNS2	dns2	online	AD+DNS BONN	W2k
193.175.238.11					
193.175.238.12	WGL	wgl	online	Gast: WGL	W2k
193.175.238.13	SERVER1	server1	online	PDC Server langroup	NT
193.175.238.14	FAX1	fax1	online	COM Server	NT
193.175.238.15		firewall	online	CISCO Router	
193.175.238.16	RAS1	ras1	online	RAS Server hybrid	NT
193.175.238.17	RAS2	ras2	online	RAS Server ISDN	NT
193.175.238.18	RAS3	ras3	online	RAS Server analog	W2k
193.175.238.19		lanmeter	online	FLUKE Lanmeter	
193.175.238.20					
193.175.238.21					
193.175.238.22					
193.175.238.23					
193.175.238.24					
193.175.238.25					
193.175.238.26	SERVER16	server16	online	File Server	NT
193.175.238.27					
193.175.238.28	SERVER6	server06	online	Print Server	NT
193.175.238.29	SERVER13S	server13s	online	File Server	NT
193.175.238.30	LEITSTAND	leitstand	online	Netzwerk-Monitor	NT
193.175.238.31	ORACLE01	oracle01	online	DB Server	NT
193.175.238.32	EXCHA3	excha3	online	Exchange Server	W2k

193.175.238.33					
193.175.238.34	ORACLE02	oracle02	online	DB Server	NT
193.175.238.35					
193.175.238.36	EXCHA2	excha2	online	Exchange Server	NT
193.175.238.37		etikett	online	Drucker	
193.175.238.38	JUKEBOX1	jukebox	online	CD-ROM Jukebox	NT
193.175.238.39					
193.175.238.40	FUE01	fue01, gesine	online	Projekt Server	
193.175.238.41					
193.175.238.42		hp-edv	online	Drucker	
193.175.238.43		hp-3og	online	Drucker	
193.175.238.44		hp-4og	online	Drucker	
193.175.238.45		hp-5og	online	Drucker	
193.175.238.46		cl-edv	online	Drucker	
193.175.238.47		cl-3og	online	Drucker	
193.175.238.48		cl-4og	online	Drucker	
193.175.238.49		dev6200		Drucker	
193.175.238.50	SERVER20	server20	online	File Server	W2k
193.175.238.51	SERVER21	server21	online	File Server	W2k
193.175.238.52	SERVER22	server22	online	File Server	W2k
193.175.238.53	SERVER23	server23	online	File Server	W2k
193.175.238.54					
193.175.238.55	BACKUP04	backup04	online	Backup Server	W2k
193.175.238.56	BACKUP01	backup01	online	Backup Server	W2k
193.175.238.57	BACKUP02	backup02	online	Backup Server	W2k
193.175.238.58	BACKUP03	backup03	online	Backup Server	W2k
193.175.238.59	GUIDE	guide	online	Projekt Server	
193.175.238.60					
193.175.238.61	VIBSOZ	vibsoz	online	Projekt Server	
193.175.238.62					
193.175.238.63	IFIS	ifis	online	DB Server sozdb Test	W2k
193.175.238.64					
193.175.238.65	NEWS	news	online	NEWS, WAP Server	NT
193.175.238.66					
193.175.238.67					
193.175.238.68	REPOSITORY	repository	online	Projekt Server	
193.175.238.69	VT-WWW	vt-www, volltextserver	online	Projekt Server	
193.175.238.70	VT-APP	vt-app	online	Projekt Server	
193.175.238.71	TRANSFER	transfer, carmen	online	Projekt Server	
193.175.238.72					
193.175.238.73					
193.175.238.74					
193.175.238.75		www.priub.org	online	Gast: AFB	
193.175.238.76	GESINE2	gesine2, sozdb	online	DB Server sozdb Prod.	W2k
193.175.238.77	ONORDER	onorder	online	DB Server onlineorder	W2k
193.175.238.78	LISTSERV	listserv	online	Listserv Server	W2k
193.175.238.79	JOELIST	listserv.joe-list.de	online	Gast: Joe-Liste	W2k
193.175.238.80		hub	online	Nortel Passport Hub	
193.175.238.81					
193.175.238.82					
193.175.238.83					
193.175.238.84					
193.175.238.85					

193.175.238.86					
193.175.238.87					
193.175.238.88					
193.175.238.89					
193.175.238.90					
193.175.238.91					
193.175.238.92	OH-ACBF0D1		online	Arbeitsplätze	W95
193.175.238.93				mit festen	
193.175.238.94				IP-Adressen	
193.175.238.95					
193.175.238.96	SI-ACBF0DA		online		W95
193.175.238.97					
193.175.238.98					
193.175.238.99					
193.175.238.100					
193.175.238.101					
193.175.238.102	MO-ACBF11F		online		W95
193.175.238.103					
193.175.238.104					
193.175.238.105	SOE		online		W2k
193.175.238.106					
193.175.238.107					
193.175.238.108					
193.175.238.109					
193.175.238.110					
193.175.238.111					
193.175.238.112					
193.175.238.113					
193.175.238.114					
193.175.238.115	HELLWEG	hellweg	online		Linux
193.175.238.116					
193.175.238.117					
193.175.238.118					
193.175.238.119					
193.175.238.120					
193.175.238.121					
193.175.238.122					
193.175.238.123					
193.175.238.124					
193.175.238.125					
193.175.238.126					
193.175.238.127					
193.175.238.128					
193.175.238.129	PETER...		online		W2k
193.175.238.130					
193.175.238.131					
193.175.238.132					
193.175.238.133					
193.175.238.134					
193.175.238.135					
193.175.238.136					
193.175.238.137					
193.175.238.138					

193.175.238.139					
193.175.238.140					
193.175.238.141		index	online	temp. Projekt Server	Linux
193.175.238.142					
193.175.238.143					
193.175.238.144					
193.175.238.145	SF-ACBF0DF		online		W95
193.175.238.146					
193.175.238.147					
193.175.238.148					
193.175.238.149					
193.175.238.150					
193.175.238.151					
193.175.238.152					
193.175.238.153					
193.175.238.154					
193.175.238.155					
193.175.238.156	SONT4		online		NT
193.175.238.157					
193.175.238.158					
193.175.238.159					
193.175.238.160					
193.175.238.161					
193.175.238.162					
193.175.238.163					
193.175.238.164					
193.175.238.165					
193.175.238.166					
193.175.238.167					
193.175.238.168					
193.175.238.169					
193.175.238.170		zv1		Projekt Server	
193.175.238.171		elvira2			
193.175.238.172	ELVIRA1	elvira1, intra	online		OS/2
193.175.238.173		elvira4			
193.175.238.174				Arbeitsplätze	
193.175.238.175				mit festen	
193.175.238.176				IP-Adressen	
193.175.238.177					
193.175.238.178					
193.175.238.179					
193.175.238.180					
193.175.238.181					
193.175.238.182	KH-P600-02		online		W2k
193.175.238.183					
193.175.238.184					
193.175.238.185				DHCP	
193.175.238.186	TH-P600-01		online	IP-Adress-Bereich	W2k
193.175.238.187	ZS-ACBF133		online		W95
193.175.238.188			online		
193.175.238.189	SM-ACBF0ED		online		W95
193.175.238.190					
193.175.238.191	ZS-P600-01		online		W2k

193.175.238.192					
193.175.238.193					
193.175.238.194	HG-P600-01		online		W2k
193.175.238.195					
193.175.238.196					
193.175.238.197	WA-P600-01		online		W2k
193.175.238.198	RO-P600-01		online		W2k
193.175.238.199					
193.175.238.200					
193.175.238.201					
193.175.238.202					
193.175.238.203					
193.175.238.204	HY-001F807		online		W95
193.175.238.205	AD020306		online		W95
193.175.238.206	MR		online		W2k
193.175.238.207	JK-X21-01		online		W2k
193.175.238.208					
193.175.238.209					
193.175.238.210					
193.175.238.211	HY-ACBF11A		online		W95
193.175.238.212	ML-P600-01		online		W2k
193.175.238.213					
193.175.238.214	HE-ACBF137		online		W95
193.175.238.215					
193.175.238.216					
193.175.238.217	SB-ACBF0E8		online		W95
193.175.238.218	SK-P600-01		online		W2k
193.175.238.219	GB-ACBF0FB		online		W95
193.175.238.220					
193.175.238.221	MUE-WIN2000		online		W2k
193.175.238.222					
193.175.238.223					
193.175.238.224					
193.175.238.225	MT-ACBF122		online		W95
193.175.238.226	RAS3		online		
193.175.238.227	NE-P600-01		online		W95
193.175.238.228	JM-ACBF12A		online		W95
193.175.238.229					
193.175.238.230					
193.175.238.231					
193.175.238.232					
193.175.238.233					
193.175.238.234	RJE761-ACBF10		online		W95
193.175.238.235	SC-9B90700		online		W95
193.175.238.236	KN-ACBF0F1		online		W95
193.175.238.237	LE-ACBF149		online		W95
193.175.238.238					
193.175.238.239					
193.175.238.240	BL-P600-01		online		W2k
193.175.238.241	UR-P600-01		online		W2k
193.175.238.242	SI-ACBF11B		online		W95
193.175.238.243	ZM-ACBF0D3		online		W95
193.175.238.244					

193.175.238.245					
193.175.238.246	BACKTAPE		online		W2k
193.175.238.247	MS-P600-01		online		W2k
193.175.238.248	BA-P600-01		online		W2k
193.175.238.249	FB-ACBF135		online		W95
193.175.238.250	AE-302EBCC		online		W95
193.175.238.251					
193.175.238.252					
193.175.238.253	MUE-AA0F5AB		online		W95
193.175.238.254	JK-ACBF134		online		W95

2.1.2 Berlin

IP Domäne: berlin.iz-soz.de
C-Netz: 193.175.239.*
NT Domäne: dbln
Windows 2000 AD Domäne: berlin.iz-soz.de

Anzahl Arbeitsplätze: ca. 20

Status-Report Netzknoten nach IP-Adressen (Stand: 03.05.2002, 10 Uhr)

IP-Adresse	**Netbios-Name**	**DNS-Name**	**Status**	**Funktion**	**BS**
193.175.239.1	IZ	iz	online	File Server Print Server DHCP Server	W2k
193.175.239.2		dns	online	DNS (extern)	Linux
193.175.239.3	EXCHABLN	exchabln	online	Exchange Server	W2k
193.175.239.4	DNS3	dns3	online	AD+DNS BERLIN	W2k
193.175.239.5					
193.175.239.6					
193.175.239.7					
193.175.239.8					
193.175.239.9					
193.175.239.10					
193.175.239.11		r-bln-lan	online	CISCO Router	
193.175.239.12					
193.175.239.13					
193.175.239.14					
193.175.239.15	WWP2	wwp2	online	Web-Server	W2k
193.175.239.16					
193.175.239.17					
193.175.239.18					
193.175.239.19					
193.175.239.20	DSBLN1	DSBLN1	online	PDC dbln File Server RAS Server	NT

193.175.239.21					
193.175.239.22	DSBLN3	ftp	online	BDC dbln, RAS Server	NT
193.175.239.23		dsbln4	online	Web-Server	W2k
193.175.239.24					
193.175.239.25					
193.175.239.26			online	Web-Adresse	
193.175.239.27			online	Web-Adresse	
193.175.239.28			online	Web-Adresse	
193.175.239.29			online	Web-Adresse	
193.175.239.30	WWWSBLN	WWWSBLN	online	WWW-Statistik	NT
193.175.239.31			online	Web-Adresse	
193.175.239.32			online	Web-Adresse	
193.175.239.33			online	Web-Adresse	
193.175.239.34			online	Web-Adresse	
193.175.239.35			online	Web-Adresse	
193.175.239.36					
193.175.239.37					
193.175.239.38					
193.175.239.39					
193.175.239.40					
193.175.239.41					
193.175.239.42					
193.175.239.43					
193.175.239.44					
193.175.239.45					
193.175.239.46					
193.175.239.47					
193.175.239.48					
193.175.239.49					
193.175.239.50					
193.175.239.51					
193.175.239.52					
193.175.239.53					
193.175.239.54					
193.175.239.55					
193.175.239.56					
193.175.239.57					
193.175.239.58					
193.175.239.59					
193.175.239.60			online	Web-Adresse	
193.175.239.61			online	Web-Adresse	
193.175.239.62			online	Web-Adresse	
193.175.239.63			online	Web-Adresse	
193.175.239.64			online	Web-Adresse	
193.175.239.65			online	Web-Adresse	
193.175.239.66			online	Web-Adresse	
193.175.239.67					

193.175.239.68					
193.175.239.69					
193.175.239.70		www	online	www.berlin.iz-soz.de	
193.175.239.71			online	Web-Adresse	
193.175.239.72			online	Web-Adresse	
193.175.239.73			online	Web-Adresse	
193.175.239.74			online	Web-Adresse	
193.175.239.75					
193.175.239.76					
193.175.239.77					
193.175.239.78					
193.175.239.79					
193.175.239.80					
193.175.239.81					
193.175.239.82					
193.175.239.83					
193.175.239.84					
193.175.239.85					
193.175.239.86					
193.175.239.87					
193.175.239.88					
193.175.239.89					
193.175.239.90					
193.175.239.91					
193.175.239.92					
193.175.239.93					
193.175.239.94					
193.175.239.95					
193.175.239.96					
193.175.239.97					
193.175.239.98					
193.175.239.99					
193.175.239.100	WWP	wwp	online	www.gesis.org	W2k
193.175.239.101					
193.175.239.102					
193.175.239.103					
193.175.239.104					
193.175.239.105					
193.175.239.106	LXAS	LXAS	online	Linux: Oracle Appl. Server SAMBA	Linux
193.175.239.107					
193.175.239.108					
193.175.239.109					
193.175.239.110					
193.175.239.111					
193.175.239.112					
193.175.239.113	DK-PC600-1	DK-PC600-1	online		W95/98
193.175.239.114					

193.175.239.115					
193.175.239.116					
193.175.239.117					
193.175.239.118					
193.175.239.119					
193.175.239.120				DHCP	
193.175.239.121				IP-Adress-Bereich	
193.175.239.122					
193.175.239.123					
193.175.239.124					
193.175.239.125					
193.175.239.126					
193.175.239.127					
193.175.239.128					
193.175.239.129					
193.175.239.130	NTS2	NTS2	online		
193.175.239.131	HB2	hb2	online		W95/98
193.175.239.132			online		
193.175.239.133					
193.175.239.134		sw-pc600-1			
193.175.239.135		we-pc600-1			
193.175.239.136		wk			
193.175.239.137	NTS3	nts3	online	Web Server	W2k
193.175.239.138	BR-T22-01	br-t22-01	online		W2k
193.175.239.139	NTS2	nts2	online	Backup Server RAS Server	W2k
193.175.239.140	NBK-EI	nbk-ei	online		
193.175.239.141					
193.175.239.142					
193.175.239.143	MX-PC600-01	mx-pc600-01	online		W2k
193.175.239.144					
193.175.239.145					
193.175.239.146					
193.175.239.147					
193.175.239.148					
193.175.239.149					
193.175.239.150					
193.175.239.151					
193.175.239.152		nbk-berlin			
193.175.239.153					
193.175.239.154					
193.175.239.155					
193.175.239.156					
193.175.239.157					
193.175.239.158					
193.175.239.159					
193.175.239.160					
193.175.239.161					

193.175.239.162					
193.175.239.163					
193.175.239.164					
193.175.239.165					
193.175.239.166					
193.175.239.167					
193.175.239.168					
193.175.239.169					
193.175.239.170					
193.175.239.171					
193.175.239.172					
193.175.239.173					
193.175.239.174					
193.175.239.175					
193.175.239.176					
193.175.239.177					
193.175.239.178					
193.175.239.179					
193.175.239.180	EI_OS2	EI_OS2	online		OS/2
193.175.239.181					
193.175.239.182					
193.175.239.183					
193.175.239.184					
193.175.239.185					
193.175.239.186					
193.175.239.187					
193.175.239.188					
193.175.239.189					
193.175.239.190					
193.175.239.191					
193.175.239.192					
193.175.239.193					
193.175.239.194					
193.175.239.195					
193.175.239.196					
193.175.239.197					
193.175.239.198					
193.175.239.199					
193.175.239.200	MK-PC600-1	mk-pc600-1	online		W2k
193.175.239.201					
193.175.239.202					
193.175.239.203					
193.175.239.204					
193.175.239.205					
193.175.239.206		bu-pc600-1			
193.175.239.207		kc-pc600-1			
193.175.239.208	RR-PC600-1	RR-PC600-1	online		W95/98
193.175.239.209	IZ2	iz2	online	DB Server	W2k

193.175.239.210	WWE	wwe	online	DB Server	W2k
193.175.239.211		sd-pc600-1			W2k
193.175.239.212					
193.175.239.213	LA-PC600-1	la-pc600-1	online		W95/98
193.175.239.214					
193.175.239.215	TT-PC600-1	tt-pc600-1	online		W95/98
193.175.239.216	gast1-pc600-1	gast1-pc600-1	online		W95/98
193.175.239.217		gast4-pc600-1			
193.175.239.218	SN-PC600-1	sn-pc600-1	online		W2k
193.175.239.219					
193.175.239.220					
193.175.239.221	EI	ei	online		W95/98
193.175.239.222					
193.175.239.223					
193.175.239.224					
193.175.239.225					
193.175.239.226					
193.175.239.227					
193.175.239.228					
193.175.239.229					
193.175.239.230					
193.175.239.231					
193.175.239.232					
193.175.239.233					
193.175.239.234					
193.175.239.235					
193.175.239.236					
193.175.239.237					
193.175.239.238					
193.175.239.239					
193.175.239.240					
193.175.239.241					
193.175.239.242					
193.175.239.243					
193.175.239.244					
193.175.239.245					
193.175.239.246					
193.175.239.247					
193.175.239.248					
193.175.239.249					
193.175.239.250					
193.175.239.251					
193.175.239.252					
193.175.239.253				Drucker	
193.175.239.254			online	Drucker	

2.2 Netzstruktur

2.2.1 Topologie

An den Standorten Bonn und Berlin gibt es jeweils ein LAN, mit sternförmiger Cat-5-Verkabelung, dem Transportprotokoll Ethernet 10/100 und je einem Switch-Hub 10/100 MBit/sec.

Es wird darauf hingewiesen, dass die Switch-Hub-Technik (bei der Datentransporte durch den Switch unmittelbar vom sendenden auf den empfangenden Port geleitet werden) einerseits eine erhebliche Verbesserung der Bandbreite des Gesamtnetzes bewirkt, andererseits allerdings die zentrale Überwachung des Datenverkehrs auf dem Gesamtnetz z.B. durch Performance-Monitore oder durch Intrusion Detection Systeme erschwert (s. hierzu Kap. 3.4).

Das LAN in Bonn ist über einen CISCO-Router 2610 und eine Telefon-Standleitung mit 2 MBit/sec an einen Gigabit-Internet-Knoten des DFN-Vereins angeschlossen.

Das LAN in Berlin ist über einen CISCO-Router 2611 mit 10 MBit/sec. an das Netz der Humboldt-Universität Berlin angeschlossen und hat damit ebenfalls Zugang zum Gigabit-Internet des DFN-Vereins.

Beide Standorte verfügen je über ein offizielles C-Netz an IP-Adressen:

Bonn: 193.175.238.*
Berlin: 193.175.239.*

Jedem aktiven Netzknoten wird statisch oder dynamisch (DHCP) mindestens eine IP-Adresse aus diesem Bereich zugewiesen.

Beide Router sind als Firewalls konfiguriert, mit folgenden grundlegenden Regeln:

- Netzknoten mit IP-Adressen aus den C-Netzen 193.175.238.* und 193.175.239.* haben jeweils uneingeschränkten Durchgriff auf das andere Netz. Dies ermöglicht eine unbehinderte Kommunikation zwischen den beiden Standorten.

- Alle Netzknoten innerhalb der LANs haben über ihren Firewall jeweils unbeschränkten Zugriff auf alle Internet-Angebote, soweit nicht andere vorgelagerte Router/Firewalls dies beschränken.

Nutzungseinschränkungen für die Mitarbeiter (z.B. Internet-Nutzung für private Zwecke) werden organisatorisch vermittelt.

- Der Zugriff aus dem Internet auf Netzknoten innerhalb des LANs wird über Filterregeln auf explizit zugelassene IP-Adressen und Ports beschränkt.

Die Standard-Internet-Domäne des IZ hat den Namen "iz-soz.de".

Das Subnetz "bonn.iz-soz.de" (DNS-Server: 193.175.238.2) verwaltet vorrangig den IP-Adressbereich in Bonn, das Subnetz "berlin.iz.soz.de" (DNS-Server: 193.175.239.2) verwaltet vorrangig den IP-Adressbereich in Berlin.

Auf dem DNS-Server 193.175.238.2 in Bonn werden insgesamt folgende Domänen verwaltet:

primary	iz-soz.de	Stamm-Domäne IZ-Soz
primary	bonn.iz-soz.de	Sub-Domäne IZ-Soz
primary	sowinet.de	Projekt
primary	so-wi-net.de	Projekt
primary	joe-list.de	Gast-Domäne
primary	infoconnex.de	Projekt
primary	info-connex.de	Projekt
primary	sowiport.de	Projekt
primary	osteuropa-netzwerk.de	Projekt
primary	osteuropa-verbund.de	Projekt
primary	vibsoz.de	Projekt
primary	priub.org	Gast-Domäne
secondary	berlin.iz-soz.de 193.175.239.2	Sub-Domäne IZ-Soz

2.2.2 Bonn

IP Domäne: bonn.iz-soz.de
C-Netz: 193.175.238.*
Windows NT Domäne: langroup
Windows 2000 AD Domänen: iz-soz.de, bonn.iz-soz.de

Serverstruktur:

Betriebssystem	Windows Domäne	Funktion, Dienste	Anzahl
Windows 2000	iz-soz	AD, DNS	1
Windows 2000	bonn	AD, DNS	1
Windows 2000	bonn	File-Server + Backup	8
Windows 2000	bonn	Exchange-Server	1

Windows NT	langroup	PDC	1
Windows NT	langroup	BDC, File-Server	2
Windows NT	langroup	BDC, Print-Server	1
Windows NT	langroup	Exchange-Server	1
Windows NT	langroup	sonstige zentrale Dienste	9
Unix		aDIS Server	1
Linux	langroup	SAMBA	1
Linux		DNS (extern), DHCP	1
Linux		SMTP (Frontend)	1
NT / 2000 / OS/2 / Linux	bonn / langroup	Projekt-Server	13
Windows / Linux		Server von Gästen	3
		Summe	**45**

Anzahl Arbeitsplätze: ca. 80

Standardbetriebssystem:	Windows 95 in 2002: Windows 2000 Prof.	
einzelne Arbeitsplätze:	Windows NT Client	
ein Arbeitsplatz:	Linux	
Standard-Anmeldedomäne:	Windows 95	=> langroup
	Windows 2000	=> bonn

Anmerkungen:

- Alle Benutzer der Domäne langroup wurden mit ihrer SID-History in die Domäne bonn übernommen.
- Zwischen den Domänen bonn und langroup sind Windows-Trusts eingerichtet, so dass alle Benutzer auf alle Ressourcen in beiden Domänen zugreifen können, sofern sie dazu berechtigt sind.
- Der zentrale File-Service inkl. Backup und der zentrale E-Mail-Service (Exchange) wurden im 1. Quartal 2002 auf neuen Servern unter Windows 2000 in der Domäne bonn installiert und in Produktion genommen. Die restlichen Dienste auf alten Servern in der Domäne langroup werden Zug um Zug umgestellt, abschließend wird die Domäne langroup gelöscht.
- DNS für die Domänen iz-soz.de und bonn.iz-soz.de war bis Mitte 2002 wie folgt organisiert:
  Im Internet registriert ist der DNS-Server 193.175.238.2 (BS: Linux).
  Die beiden AD-Domänen besitzen je einen eigenen (internen) DNS-

Dienst für die von ihnen betreuten Zonen, externe Adressauflösung erfolgt über den DNS-Server 193.175.238.2.

- DHCP:
  Der DHCP-Dienst läuft z.Z. auf dem DNS-Server 193.175.238.2.
  Adressbereich: 193.175.238.185 - 254
  Standard DNS: 193.175.238.2
  Standard Gateway: 193.175.238.15
  Subnetzmaske: 255.255.255.0

- Der E-Mail-Dienst war bis Mitte 2002 wie folgt organisiert:
  Im Internet für bonn.iz-soz.de registriert ist der SMTP-Server 193.175.238.7 (BS: Linux).
  Über die aliases-Datei dieses Servers werden alle E-Mail-Accounts für Mitarbeiter des IZ in Bonn an den Exchange-Server excha3.bonn.iz-soz.de (BS: Windows 2000) weitergeleitet, der als interner Mail-Server dient. Der E-Mail-Dienst auf excha3 ist in AD integriert. Die Mitarbeiter verwenden in aller Regel Outlook (Arbeitsgruppen-Modus) als Mail-Client. Ausgehende E-Mail des Exchange-Servers wird an den SMTP-Server 193.175.238.7 geleitet und von dort an die Empfänger-Server gesendet
  Zusätzlich werden auf dem SMTP-Server Postfächer für externe Gäste verwaltet, denen E-Mail-Adressen unter der Domäne bonn.iz-soz.de zugeteilt wurden. Diese Post verbleibt auf dem SMTP-Server und wird per IMAP oder POP3 bearbeitet.
  Auf allen E-Mail-Servern wurde die Proxy-Funktion abgeschaltet, ausgehende Post wird nur dann bearbeitet, wenn sie von einem Client mit einer IP-Adresse aus dem Bereich 193.175.238.* gesendet wurde.
  Der alte E-Mail-Server excha2 (BS: Windows NT) in der Domäne langroup verwaltet z.Z. noch die "Öffentlichen Ordner" des Exchange-Systems, dies wird bis Ende 2002 umgestellt.
  Excha3 ist über das Internet Firewall-gesichert auf folgenden Ports zugänglich:
  - 110 (POP3) Mail-Client
  - 135 (EPMAP) für Outlook-Client
  - 139 (NETBIOS-SSN) für Outlook-Client
  - 143 (IMAP) Mail-Client
  - 80 (WWW) Web-Mail Outlook
  - 950 - 1299 für Outlook-Client

2.2.3 Berlin

IP Domäne: berlin.iz-soz.de
C-Netz: 193.175.239.*
NT Domäne: dbln
Windows 2000 AD Domäne: berlin.iz-soz.de

Liste der Server

IP- Adresse	DNS-Name	Funktion	BS	Bemerkung
193.175.239.4	dns3	AD + DNS BERLIN	W2k	
193.175.239.2	dns	DNS Server (extern)	Linux	
193.175.239.1	iz	File Server Print Server DHCP Server	W2k	 DHCP-Bereich: .120-.250
193.175.239.139	nts2	Backup Server RAS Server	W2k	
193.175.239.209	iz2	DB Server	W2k	Oracle, Web-Angebot
193.175.239.100	wwp	Web Server (iis)	W2k	WWW.GESIS.ORG
193.175.239.15 193.175.239.23 193.175.239.70 193.175.239.71 193.175.239.72 193.175.239.73 193.175.239.74	wwp2	 Web Server (apache) Web Server (iis)	W2k	1 Server mit 7 IP-Adressen und mehreren Teil-Webs Projekte: Foris, SOFO, ProEastE, InEastE www.Berlin.iz-Soz.de (alt) Hosts (externe Gäste) German_microdata_lab SowiNet OENetzwerk
193.175.239.137	nts3	Web Server(Tomcat)	W2k	Zeitschriftendatenbank
   193.175.239.210 193.175.239.60 193.175.239.61 193.175.239.62 193.175.239.63 193.175.239.64 193.175.239.65	wwe	Web Server (iis)	W2k	1 Server mit 7 IP-Adressen und mehreren Teil-Webs EntwicklungsServer Gesis Schulung BerlinWeb BonnWeb ExternWeb ToolsWeb TestWeb
193.175.239.3	exchabln	Exchange Server	W2k	
193.175.239.20	dsbln1	PDC dbln File Server (alt) RAS Server	NT	
193.175.239.22 193.175.239.26	dsbln3	BDC dbln RAS Server interner Web-Server		
193.175.239.11		CISCO Router		

Anzahl Arbeitsplätze: ca. 20
Standardbetriebssystem: Windows 98
in 2002: Windows 2000 Prof.

Anmerkungen:

- Die Windows 2000 AD Domäne "Berlin" wurde Ende 2001 aus lokalen technischen Gründen unabhängig von der NT Domäne "dbln" als Child-Domäne von "iz-soz.de" installiert. Benutzernamen und deren Eigenschaften in "Berlin" konnten aus technischen Gründen nicht aus "dbln" übernommen werden, sondern wurden neu eingerichtet. Zwischen "berlin" und "dbln" besteht keine Trust-Beziehung.

- Zwischen den AD-Domänen "berlin.iz-soz.de", "bonn.iz-soz.de" und "iz-soz.de" bestehen bidirektionale, transitive Vertrauensstellungen.

- Alle zentralen Dienste einschließlich E-Mail (Exchange) (ausgenommen der externe DNS-Server unter Linux) wurden unter Windows 2000 kurzfristig entweder neu in "berlin" installiert oder aus "dbln" in die neue Domäne übernommen. "berlin" ist die Produktions-Domäne.

- Die verbliebenen "dbln"-Dienste (RAS und internes Web) werden in 2002 Zug um Zug übernommen, anschließend wird "dbln" abgeschaltet.

- DNS für die Domäne berlin.iz-soz.de war bis Mitte 2002 wie folgt organisiert:
  Im Internet registriert ist der externe DNS-Server 193.175.239.2 (BS: Linux). Die AD-Domäne besitzt einen eigenen (internen) DNS-Dienst (DNS3: 193.175.239.4) für die von ihr betreute Zone berlin.iz-soz.de, die Informationen werden mit dem zentralen AD-Server für iz-soz.de (DNS1: 193.175.238.1) repliziert, die externe Adressauflösung erfolgt über den DNS-Server 193.175.239.2.

- DHCP:
  Der DHCP-Dienst läuft unter Windows 2000 auf dem Server "iz" 193.175.239.1.
  Adressbereich: 193.175.239.120 - 250
  Standard DNS: 193.175.239.4
  Standard Gateway: 193.175.239.11
  Subnetzmaske: 255.255.255.0

- Der E-Mail-Dienst ist wie folgt organisiert:
  Im Internet für berlin.iz-soz.de registriert ist der Exchange-Server "exchabln" 193.175.239.3.
  Der E-Mail-Dienst ist in AD integriert, der Server "exchabln" repliziert mit dem Exchange-Servern in Bonn "excha3" und "excha2".
  Innerhalb des LAN und bei RAS-Zugang wird von den Mitarbeitern des IZ als Mail-Client Outlook (Arbeitsgruppen-Modus) verwendet. Über das Internet sind Firewall-gesichert die Ports SMTP, POP3 und IMAP zugänglich.

- Der Standort Berlin ist wegen seiner schnellen Internet-Anbindung zentraler Standort der Server für das öffentliche WWW-Angebot der GESIS.
  Es werden WWW-Dienste für mehrere unterschiedliche Internet-Domänen bereitgestellt, u.a. gesis.org, sowinet.de, osteuropa-netzwerk.de.
  Die meisten dieser Zonen werden nicht auf den DNS-Servern in Berlin, sondern auf den DNS-Servern anderer GESIS-Standorte verwaltet.
  Zur Einrichtung von Teilwebs mit jeweils eigener URL, eigener IP-Adresse und eigenem WWW-Root-Verzeichnis für die unterschiedlichen Angebote und Domänen wurde den meisten WWW-Servern mehrere IP-Adressen zugewiesen.

2.3 Spezielle Strukturkomponenten

2.3.1 aDIS-Verfahren

Das Verfahren aDIS ist eine Client-Server-Anwendung zur Erfassung, Pflege und Auswertung der bibliographischen und Forschungsinformationen für die IZ-Datenbanken SOLIS und FORIS einschließlich deren Randdatenbanken.

Die - Stand 2002 - für die Produktion verwendete Verfahrensversion der Software aDIS wurde Anfang 1999 auf einer Anfang 1996 installierten Midrangeanlage Siemens RM 400-730 gemeinsam mit dem DB-System Oracle 8 in Betrieb genommen.

Die Maschine läuft unter dem UNIX-Dialekt Reliant UNIX 5.44 und ist über Ethernet 10Base-T mit dem LAN verbunden.

Über NFS wird das Dateisystem eines Linux-Servers integriert, welches gleichzeitig per SAMBA in den Windows-Domänen verfügbar ist. Auf die-

sem Speicherplatz werden Output-Dateien der aDIS-Benutzer abgelegt, die auf den Arbeitsplätzen mit Windows-Tools weiter bearbeitet werden können.

Der aDIS-Client ist eine Telnet-ähnliche, Masken-orientierte 16-Bit-Anwendung.

Wegen der erheblichen Komplexität der fachlichen Anforderungen an die Anwendung ist - Stand 2002 - kein technisch und fachlich geeignetes Nachfolgesystem in Aussicht.

2.3.2 Telefonanlage

Das IZ setzt als Telefonsystem in Bonn und Berlin jeweils eine Anlage der Fa. Siemens Typ HICOM ein.

Dieser Anlagentyp kann grundsätzlich mit einem LAN gekoppelt werden, um Telefon-/Faxdienste von Windows-Clients aus zu bedienen und um Wartungs- und Pflegearbeiten an der Anlage von einem PC-Arbeitsplatz aus durchzuführen.

Die Nutzung dieser Optionen soll Mitte 2002 implementiert werden.

2.3.3 GSM, GPRS, WAP

Seit 1996 wird im IZ routinemäßig GSM-Technik für die mobile Datenübertragung in Kombination mit Notebooks eingesetzt. Zur Standardisierung der Anschlusstechnik und des Zubehörs wurde von der EDV grundsätzlich eine einheitliche Handy-Technik zentral bereitgestellt und in Zyklen von ca. 2 Jahren technisch modernisiert.

Einsatzzweck dieser Geräte ist neben der mobilen telefonischen Erreichbarkeit vorrangig die Bereitstellung eines mobilen Datenkanals für den Anschluss von Notebooks sowohl an das Internet als auch über die IZ-eigenen RAS-Dienste an das LAN des IZ. Hierzu werden seit 1996 alle Notebooks des IZ mit der erforderlichen Hard- und Software-Anschlusstechnik für das jeweilige Standard-Handy des IZ ausgestattet.

Stand Anfang 2002 waren im IZ 12 D-Netz-Mobiltelefone im Einsatz. Die seit 2001 eingesetzten Geräte (Siemens S/ME45) sind sowohl WAP- als auch GPRS-geeignet.

Das GPRS-Protokoll (General Packet Radio Service) ist als Vorläufer von UTMS eine Paket-orientierte Datenübertragungstechnik in Funk-Netzen mit einer Tarifierung entsprechend der übertragenen Datenmenge, unabhängig von der Übertragungszeit. Dies ermöglicht z.B. eine stressfreie Bearbeitung von E-Mail ohne den Druck zeitabhängiger Übertragungskosten. Zusätzlich erfolgt die Datenübertragung auf mehreren parallelen Datenkanälen, so dass Übertragungsraten mit 2-4-fach höherer Geschwindigkeit gegenüber der GSM-Standard-Übertragungsrate von 9,6 kBit/sec erreicht werden können.

GPRS bietet einen unmittelbaren Zugang zum Internet über einen Router des jeweiligen Telefon-Providers (für das IZ: D2-Vodafone), dem Endgerät wird hierbei von einem DHCP-Service des Providers eine individuelle IP-Adresse zugewiesen. Da das IZ - Stand 2002 - nicht über eigene GPRS-fähige RAS-Zugänge verfügt, muss der Zugang zu IZ-Diensten mittels GPRS über das Internet, begrenzt durch die Filterliste des Firewalls, erfolgen. Ist der Zugang zu Firewall-geschützten internen Daten des IZ erforderlich, so kann alternativ eine Standard-GSM-Verbindung zu einem RAS-Server des IZ hergestellt werden.

Das IZ wird die Entwicklung der UTMS-Technologie beobachten und frühzeitig testen.

Seit 2000 wird im IZ mit dem Einsatz von WAP (Wireless Application Protocol) experimentiert, einem Internet-Protokoll ähnlich http zur Präsentation von Informationen auf Mobiltelefonen und PDAs. Die Angebote werden auf Standard-WWW-Servern bereitgestellt (z.B. MS IIS), Der Abruf erfolgt mit speziellen, in den mobilen Endgeräten i.d.R. als Firmware eingebauten Browsern. Das IZ betreibt für Testzwecke eine kleine inoffizielle WAP-Site.

Die kommerziellen WAP-Angebote konzentrieren sich bisher auf mobilinteressante Informations-Dienste mit hohem Aktualitätsgehalt und ggf. regionaler Fokussierung, z.B. Wetter, Verkehr, Nachrichten, Börse, Sport.

Das IZ erprobt in seiner WAP-Site u.a. ein zentrales Telefonverzeichnis, aus dem mit WAP-Technik unmittelbar ein Anruf initiiert werden kann.

Für offizielle WAP-Produkte aus dem inhaltlichen Fokus des IZ konnte bisher kein Bedarf festgestellt werden.

2.4 Netzwerksicherheit

2.4.1 Firewall

Als Trennung zwischen den lokalen LANs und dem Internet werden im IZ Firewalls mit Filterlisten eingesetzt. Details hierzu wurden bereits in Kap. 2.2 dargestellt.

2.4.2 Virenschutz

Zum Schutz gegen Viren, die z.B. über E-Mails oder den Besuch kontaminierter Internetseiten ins Netzwerk gelangen könnten, sind Virenschutzprogramme in einem zweistufigen Konzept im Einsatz:

- Auf den Exchange Servern kommt McAfee Groupshield zum Einsatz. Damit wird der Inhalt von eingehenden E-Mails auf Viren etc. überprüft.

- Auf den einzelnen Arbeitsplatzrechnern wird McAfee VShield, auf den Fileservern NetShield verwendet. Damit wird verhindert, dass Viren auf Arbeitsplätzen aktiviert werden oder in das Netzwerk und auf die Fileserver gelangen.

Die Signaturdateien der Virenscanner werden systematisch aktualisiert:

- GroupShield und NetShield: Täglicher automatischer Update,

- VShield: Update durch Logon-Skript, aktualisiert bei Bedarf durch den System-Administrator.

2.5 Datensicherung, Behandlung von Störungen

Die Zielkonzepte für den Daten-Backup und die Behandlung von Störungen sind in Kap. 3.3 beschrieben. Sie basieren im Wesentlichen auf den Erfahrungen der vergangenen Jahre und sind Weiterentwicklungen erprobter Strategien entsprechend dem Stand der Technik.

Wegen ihrer besonderen Bedeutung für den störungsfreien Betrieb wurden die erforderlichen Routinen und Geräte in der ersten Phase der Migration Anfang 2002 implementiert. Diese Maßnahmen waren zum Zeitpunkt der Berichtserstellung bereits abgeschlossen.

2.6 Access- und Change-Management

Access- und Change-Management beschreibt Prozeduren und Techniken zur Behandlung folgender Anforderungen:

- Installation von Betriebssystem und Anwendungssoftware auf einem Arbeitsplatz-PC,
- Installation zusätzlicher Anwendungssoftware und regelmäßiger Änderungen (Fahrpläne etc) auf Arbeitsplatz-PCs,
- Statusüberprüfung und Installation von Updates (Signaturdateien für Virusprüfung, Updates von Systemsoftware etc.) auf Arbeitsplatz-PCs,
- Anlegen eines neuen Benutzers und eines neuen Postfachs, Ändern der Gruppenzugehörigkeiten und sonstiger Eigenschaften eines Benutzers.
- Austausch der Hardware eines Arbeitsplatz-PCs,
- Anmelden eines Anwenders an "seinem" Arbeitsplatz-PC, Herstellen der Anwender-spezifischen Umgebung,
- Anmelden eines Anwenders an einem anderen Arbeitsplatz-PC ("moving user"), Herstellen der Anwender-spezifischen Umgebung,
- Bereitstellung der erforderlichen Zugangsschnittstellen, Rechte, Zugangsprofile und Updates für Anwender mit Notebooks ("traveling user") und folgenden alternativen Standorten:
  - "Heimat-LAN" (IZ-Domäne Bonn oder Berlin),
  - LAN der jeweils anderen IZ-Domäne (Berlin oder Bonn),
  - Standort außerhalb des IZ mit Zugang zum nationalen/internationalen Telefon/ISDN/GSM/GPRS-Netz,
  - Standort außerhalb des IZ mit Zugang zu einem fremden LAN.

2.6.1 Access-Management

Die Authentifizierung eines Benutzers in den IZ-LANs Bonn und Berlin erfolgt über folgende Parameter

- Benutzername
- Windows NT / Windows 2000 - Domäne
- Passwort

Alle Benutzer sind nach organisatorischen und fachlichen Gesichtspunkten einer oder mehreren Benutzergruppen zugeordnet. Die Vergabe von Zugriffsrechten auf Netzwerk-Ressourcen erfolgt i.d.R. für Benutzergruppen.

Der Standard-Zugang erfolgt über den Ethernet-LAN-Anschluss des jeweiligen Standortes.

Die Authentifizierung erfolgt durch den für die Domäne zuständigen Domänen-Controller.

In den Domänen LANGROUP und BONN ist für alle Benutzerkennungen (Ausnahmen: Administrator- und Test-Kennungen) im Benutzer-Profil bei einer LAN-Anmeldung die Ausführung eines zentralen Skriptes (logw95.bat) zwingend vorgeschrieben.

Bei Anmeldung an die Domäne BONN:

```
 .....
echo verbinden mit Server20
net use n: /d
net use n: \\server20\dosapps
if not exist n:\tools\logw2k.bat goto :fehler1

n:
cd \tools
call logw2k.bat
c:
goto :ende

:fehler1

 .....

:ende
```

Die zentral gepflegten Prozeduren
N:\tools\logw2k.bat (für Anmeldungen an BONN),
N:\tools\logw95.bat (für Anmeldungen an LANGROUP)

haben die Aufgabe, bei einer Anmeldung

- die Standard-Verbindung zwischen Netzwerk-Verzeichnissen und Plattenbuchstaben nach der Nomenklatur des IZ herzustellen:
  - N: Programme und Software-Quellen (read-only),
  - G: gemeinsame Daten (read/write für Benutzergruppen)
  - U: Home-Directory des Benutzers (read/write)

- die Ausführung vorgeschriebener Programme zu erzwingen, u.a. die Update-Prozedur der McAfee-VirusScan-Software.

Beispiel logw2k.bat:

```
 .....
:script
echo 1 Mappen der LAN-Platten
net use g: /d
net use g: \\server22\gruppe-1
net use u: /d
net use u: \\server23\%username%

n:
cd \software-quellen\antivirus-programme\virusscan95_Mcafee\sdat-akt
echo 2 Update VirusScan

sdat4200 /silent

:ende
```

Neben dem lokalen Ethernet-LAN-Anschluss stehen den IZ-Mitarbeitern folgende Zugänge für den Remote-Access zur Verfügung:

- RAS-Zugang über das Telefonnetz (analog, ISDN, GSM).
  Die RAS-Server sind ohne Firewall direkt mit dem LAN verbunden. Es erfolgt eine 2-stufige Authentifizierung:

  1. Prüfung von Benutzername und Passwort auf RAS Zugangsberechtigung, ggf. wird ein Rückruf eingeleitet.
     Nach erfolgreicher Verbindung wird dem Arbeitsplatz vom RAS-Server die IP-Adresse (aus dem zentralen DHCP-Pool), DNS- und Gateway-Information zugewiesen.

  2. Bei einem Windows-Arbeitsplatz wird anschließend eine Authentifizierung der Anmelde-Informationen des Arbeitsplatzes (Benutzername, Passwort, Domäne) versucht.
     Bei erfolgreicher Authentifizierung stehen dem Anwender die LAN-Ressourcen entsprechend seinen Berechtigungen zur Verfügung.
     Ohne Authentifizierung stehen dem Anwender (genau wie ohne Authentifizierung am LAN) nur die anonym nutzbaren TCP/IP-Ressourcen, u.a. DNS und Internet-Zugang über den Gateway zur Verfügung.

- Zugang über das Internet, unabhängig von der Art des Internet-Anschlusses, über den Firewall. Der Firewall filtert anhand der Quell- und Ziel-IP-Adresse und des Zielports die Durchgriffserlaubnis, i.d.R. nur auf die öffentlichen Internet-Dienste.
  Zwei Sonderfälle:

3. Die Quell-IP-Adresse stammt aus dem C-Netz des jeweils anderen IZ-Standortes, in diesem Fall erlaubt der Firewall vollen Durchgriff auf alle LAN-Ressourcen.

4. Einzelne TCP/IP-Dienste erlauben - sofern der Firewall den Durchgriff auf die erforderlichen Ports zulässt - die individuelle Authentifizierung des Anwenders über Internet-Protokolle, bei Erfolg ist anschließend der Zugriff auf geschützte / persönliche Datenbereiche dieses Dienstes möglich.
   Beispiele (LAN Bonn):
   - E-Mail (POP3, IMAP, Outlook-Web-Access, Outlook-Client)
   - FTP (geschützte Verzeichnisse auf dem FTP-Server)
   - Listserv (Listserver-Pflege über WWW Port 80)
   - Terminalserver (remote Wartung von Windows 2000 Servern, standardmäßig durch Firewall gesperrt),
   - Telnet (nur in Sonderfällen im Firewall zugelassen)
   - aDIS-Client (nur für ASTEC-Quell-IP-Adressen im Firewall zugelassen).

Die Software-Installation und die Profilverwaltung auf den Arbeitsplätzen und Notebooks ist (Stand Anfang 2002) Geräte-basiert und statisch. D.h.:

- Alle benutzer-spezifischen Installationen und Einstellungen - u.a. die Konfiguration des Profils für Outlook - erfolgen nur auf dem jeweiligen Gerät.
  Ausnahmen:

  - Die Verbindung mit dem Home-Directory des Benutzers erfolgt bei Logon durch das Skript.

  - Einzelne Anwendungen (u.a. InfoLog, Office-Anwendungen, IExplorer, Netscape) speichern Profil-Informationen in konfigurierbare Dateien. Werden diese Profil-Dateien im Home-Directory angelegt, sind sie Geräte-unabhängig zugreifbar.

- Wechselt der Benutzer auf einen anderen Arbeitsplatz, so müssen dort die Profil-Informationen und die noch nicht vorhandenen Software-Module (von den o.g. Ausnahmen abgesehen) erneut installiert werden.

2.6.2 Change-Management

Der Änderungsdienst basiert auf folgenden Austauschzyklen der zugrundeliegenden Hardware:

- PC-Arbeitsplätze und Notebooks werden systematisch im Block alle ca. 3 Jahre ausgetauscht.
  Die Anfang 2002 eingesetzte Arbeitsplatz-Hardware wurde Ende 1999 beschafft.
  Die aktuell im IZ eingesetzten Notebooks wurden im Block mit einheitlicher Ausstattung Mitte 2001 beschafft.

- PC-Server werden in mehreren Funktionsblöcken im Mittel alle 4 Jahre ausgetauscht. Der überwiegende Anteil der z.Z. produktiven Server wurde Anfang 2002 beschafft.

Zum Change-Management sind (Stand Anfang 2002) folgende Verfahrens-Komponenten verfügbar:

- Auf der Grundlage einer einheitlichen Arbeitsplatz-Hardware erfolgt die Installation von Betriebssystem und einem Grundbestand der Anwendungssoftware durch die Übernahme eines Images (DriveImage) (der PC wird mit einer speziellen FD gestartet, mit dem LAN verbunden und das Image wird von einem LAN-Server geladen).

- Die Installation zusätzlicher Software erfolgt - soweit entsprechender Mehrfachbedarf vorliegt - mit Hilfe des Verfahrens "WinInstall", welches auf Benutzeranforderung zentral erstellte Musterinstallationen auf den Arbeitsplatz kopiert.

- Sonstige im Einzelfall benötigte Software wird individuell installiert.

- Vom IZ für den Standort Bonn beschaffte CD-ROMs inkl. aller Software-Quellen werden dort zentral auf einem CD-ROM-Server (Jukebox mit 200 Plätzen) verwaltet und können von dort aus genutzt werden. Sonstige Software-Quellen (überwiegend Downloads) werden auf File-Servern gesammelt und von dort aus genutzt.

- Die Neuanlage und der Änderungsdienst von Benutzerkonten am Standort Bonn erfolgt wegen der Parallelität der 2 Domänen BONN und LANGROUP 2-stufig:

1. Neue Benutzerkonten werden zunächst auf dem PDC der NT-Domäne LANGROUP angelegt,

2. Das Konto wird mit Hilfe des Tools "Active Directory Migrationsprogramm" in das Active Directory des DC der Domäne BONN übertragen, auf diesem Wege wird eine gemeinsame SID-History für das Konto in beiden Domänen erzeugt.
   Anschließend werden auf dem DC der Domäne BONN die E-Mail-Parameter für Exchange 2000 konfiguriert.
   (Bei der Einrichtung eines E-Mail-Accounts ist zur Erreichbarkeit aus dem Internet darauf zu achten, dass auf dem Frontend-SMTP-Server eine entsprechende Weiterleitung auf den Server "excha3.bonn.iz-soz.de" und im E-Mail-Konto des Benutzers eine zugehörige SMTP-Adresse eingerichtet wird.)

3. Änderungen an einem Konto (Passwort, Gruppenzugehörigkeiten etc) müssen bis zur Abschaltung von LANGROUP parallel in beiden Domänen erfolgen.

- Da es sich sowohl bei den beiden Konten eines Benutzers in LANGROUP und BONN als auch bei den Gruppen trotz SDI-History um Windows-technisch zwei separate Konten bzw. Gruppen handelt, müssen bis zur Abschaltung von LANGROUP bei den Sicherheitseinstellungen pro Ressource die gewünschten Berechtigungen aus beiden Domänen eingetragen werden.

- Die Installation und Konfiguration der Server erfolgt wegen der geringen Stückzahl pro Funktionsgruppe i.d.R. individuell. Die Basis-Installation von Windows 2000 Server auf der z.Z. aktuellen Hardware-Konfiguration wird allerdings i.d.R. durch eine Image-Übertragung von einem File-Server mit anschließendem Sysprep erheblich beschleunigt und vereinfacht.

3 Konzepte und Entwicklungs-Optionen

3.1 Active Directory

3.1.1 Vorbemerkungen

Der folgende Abschnitt des Dokuments befasst sich mit dem Soll-Zustand der künftigen Active Directory Umgebung. Diese ist in ihrer Grundstruktur bereits realisiert und produktiv, erfordert aber in Teilbereichen eine Überarbeitung. Daher wird hier nicht der Ist-Zustand dieser neuen Umgebung dokumentiert, sondern der geplante Soll-Zustand.

Zum Zeitpunkt der Dokumentation sind drei Active Directory-Domänen aktiv und produktiv. In jeder der drei Domänen „iz-soz.de“, „bonn.iz-soz.de“ und „berlin.iz-soz.de“ ist jeweils nur ein Domänencontroller aktiv. Im Folgenden werden die Soll-Zustände mit jeweils zwei Domänencontrollern je Domäne beschrieben. Dies stellt aus Gründen der Redundanz und der Sicherheit der Daten eine Grundvoraussetzung für den Betrieb einer Windows 2000 Active Directory Umgebung dar. Die verwendeten Namen der Domänencontroller in diesem Dokument werden, abweichend von der realen Benennung, zur besseren Lesbarkeit wie folgt vergeben:

Domäne	Name in der Dokumentation	Realer Name
iz-soz.de	Root1	DNS1
	Root2	DNS1A
bonn.iz-soz.de	Bonn1	DNS2
	Bonn2	DNS2A
berlin.iz-soz.de	Berlin1	DNS3
	Berlin2	DNS3A

3.1.2 Logischer Aufbau und Struktur des Active Directory

3.1.2.1 Das Domänenmodell im Überblick

3.1.2.1.1 Die Domäne „iz-soz.de“

Die Domäne „iz-soz.de“ bildet die Root-Domäne des gesamten Active Directory. Sie ist der zentrale Konfigurationspunkt für alle Einstellungen des Acti-

ve Directory. Innerhalb dieser Domäne werden keine neuen Objekte über die standardmäßig vorhandenen hinaus angelegt. Produktive Ressourcen wie Benutzerkonten, Freigaben, Drucker oder ähnliche werden in den untergeordneten Domänen angelegt.

3.1.2.1.2 Die Domäne „bonn.iz-soz.de“

Die Domäne „bonn.iz-soz.de“ ist die Domäne in der die Benutzer- und Computerkonten für die Mitarbeiter des Standortes Bonn angelegt werden. In dieser werden auch große Teile der für alle Mitarbeiter, einschließlich der Berliner, notwendigen Objekte und Freigaben erstellt, die innerhalb der gesamten Organisation verwendet werden. Dieser Standort beheimatet den überwiegenden Teil der Ressourcen (Datenbanken, Servern, Speicherplatz etc.).

3.1.2.1.3 Die Domäne „berlin.iz-soz.de“

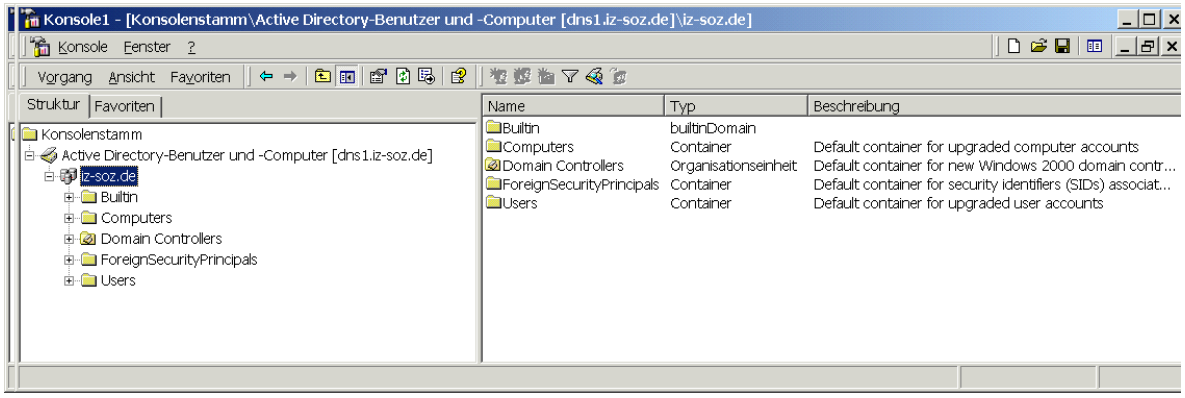
Die Domäne „berlin.iz-soz.de“ ist die Produktivumgebung der Berliner Mitarbeiter. Aus Gründen der Organisation und der Sicherheit ist dieses System getrennt von der Benutzerumgebung der Mitarbeiter in Bonn. Am Standort Berlin sind große Teile der Webserver beheimatet, da an diesem Standort eine Internetanbindung von 10 MBit zur Verfügung gestellt wird.

Durch die Trennung der Domänen ergibt sich einerseits eine Minimierung des Risikos eines unbeabsichtigten Zugriffs auf das Active Directory – Schema, andererseits können administrative Grenzen strenger gezogen werden.

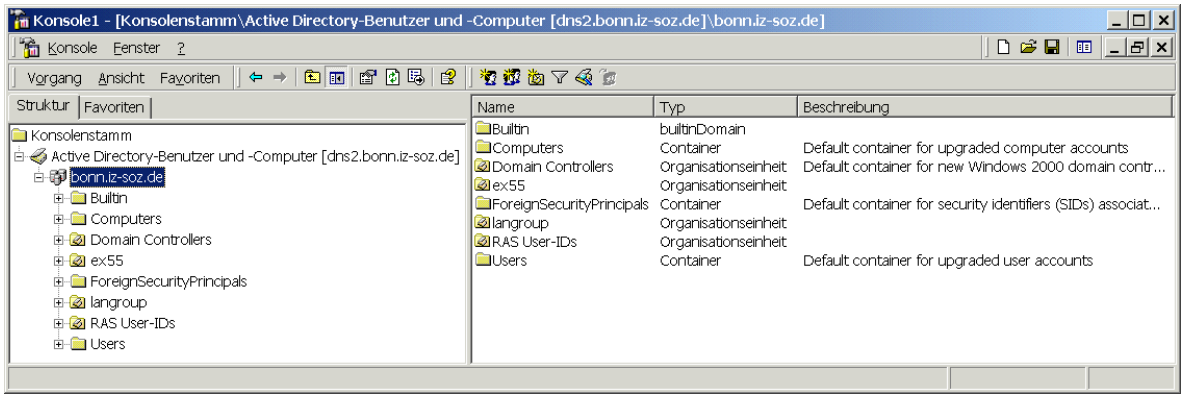
3.1.2.2 Organisatorischer Aufbau der Domänen

Die Unterteilung der Domäne in Organisationseinheiten (OUs) erleichtert die Verwaltung und sorgt für eine übersichtliche Darstellung der Struktur. Sofern nicht technisch oder organisatorisch notwendig, wird die Zahl der OUs so gering wie möglich gehalten.

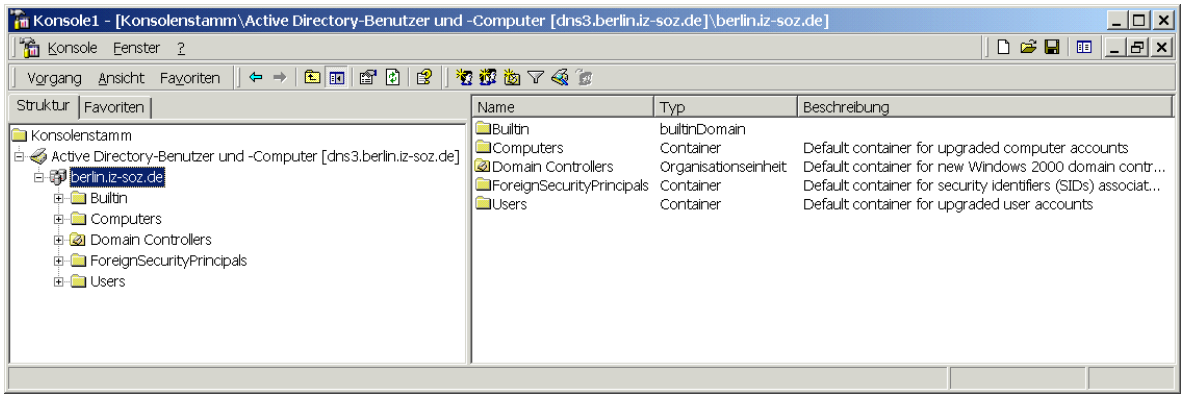
In der Root-Domäne „iz-soz.de“ sind ausschließlich die Standard-OUs vorgesehen. Eine Übersicht bietet die folgende Grafik:



Für die Domäne "bonn.iz-soz.de" wurden zusätzliche OUs angelegt. Diese dienen zur Aufnahme spezieller Benutzer- und Computerkonten. Eine Übersicht bietet die folgende Grafik:



Zum Zeitpunkt der Dokumentation waren für die Domäne "berlin.iz-soz.de" keine weiteren OUs angelegt. Eine Übersicht bietet die folgende Grafik:



OUs werden nicht nur zur Verwaltung und Organisation von Benutzer- und Computerkonten verwendet. Mit Hilfe von OUs können Benutzern und Computern Gruppenrichtlinien zugeordnet werden. Mit Gruppenrichtlinien kön-

nen sehr weitgehende Konfigurationen von Computern- oder Benutzerrechten verwaltet und eingerichtet werden.

Die Entwicklung und Anwendung von Gruppenrichtlinien wird gesondert behandelt.

Zum Zeitpunkt der Dokumentation waren außer den Standard-Gruppenrichtlinien für die jeweilige Domäne und die OU „Domain Controllers“ keine weiteren Richtlinien erstellt und angewendet.

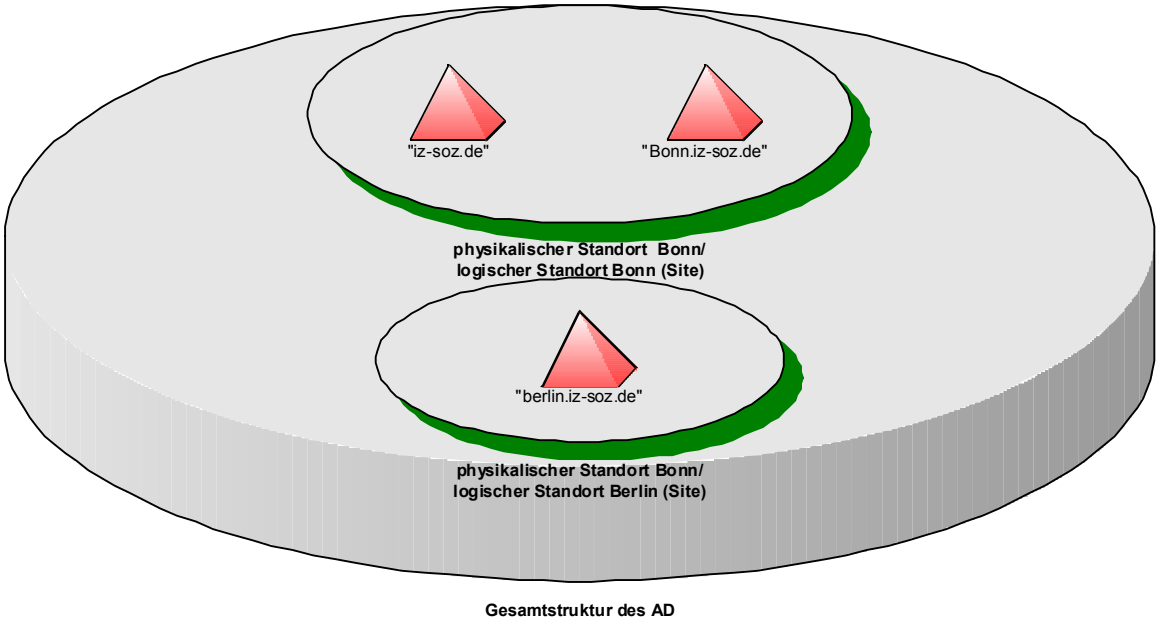
3.1.3 Physischer Aufbau und Struktur des Active Directory

3.1.3.1 Der Forest

Die physischen Standorte der Domänen befinden sich an den Standorten Bonn und Berlin. Am Standort Bonn befindet sich gegenwärtig ein Domänencontroller der Domäne „iz-soz.de“ Root1, sowie ein Domänencontroller der Domäne „bonn.iz-soz.de“ Bonn1. Am Standort Berlin befindet sich ein Domänencontroller der Domäne „berlin.iz-soz.de“ Berlin1.

Zur Steuerung der Replikation zwischen den beiden physischen Standorten werden eigene „Sites“ konfiguriert. Jedes Teilnetz erhält eine eigene Site. Dadurch lassen sich die Zeiten, in denen Replikationsverkehr stattfindet, definieren.

Die folgende Grafik verdeutlicht den Aufbau des Active Directory mit seinen räumlichen und logischen Verknüpfungen.



3.1.3.2 Die Root-Domäne „iz-soz.de“

Die Domäne „iz-soz.de“ bildet die Forest-Root-Domäne für das gesamte Active Directory. Ihre Aufgabe besteht darin, der zentrale Konfigurationspunkt für alle weiteren Domänen zu sein. Innerhalb der Domäne werden außer den beiden Domänencontrollern keine weiteren Member-Server oder Clients vorhanden sein. Die durch die Installation der Domäne erstellten Benutzerkonten und –gruppen werden nicht durch weitere Konten ergänzt, es sei denn zu administrativen Zwecken des gesamten Forests.

Name der Domäne:	iz-soz.de
Funktion:	Forest Root Domäne
Child-Domains:	2 (Bonn und Berlin)
Anzahl DCs	2 (Root1 und Root2)
Anzahl GCs	2 (Root1 und Root2)
Explizite Trusts:	Keine (aktuell LANGROUP)

3.1.3.3 Die Domäne „bonn.iz-soz.de“

Die Domäne „bonn.iz-soz.de“ befindet sich physisch am Standort Bonn und wird auch nur dort von den Mitarbeitern zur Authentifizierung genutzt. Diese

Domäne ist die Produktivdomäne für alle Mitarbeiter und Ressourcen, die nicht in Berlin angesiedelt sind.

Name der Domäne:	bonn.iz-soz.de
Funktion:	Produktivdomäne Benutzer in Bonn
Child-Domains:	Keine
Anzahl DCs	2 (Bonn1 und Bonn2)
Anzahl GCs	2 (Bonn1 und Bonn2)
Explizite Trusts:	Keine (nach der vollständigen Migration)

3.1.3.4 Die Domäne „berlin.iz-soz.de“

Die Domäne „berlin.iz-soz.de“ befindet sich physisch in den Räumen der Berliner Außenstelle. In dieser Domäne werden alle benötigten Ressourcen bereitgestellt, die zum Betrieb vor Ort notwendig sind. Darüber hinaus sind in Berlin, bedingt durch die bessere Anbindung ans Internet auch zahlreich Webserver beheimatet. Durch das Einrichten einer eigenen Domäne werden Sicherheitsrisiken minimiert, die beispielsweise durch unbeabsichtigte Dateizugriffe bei Nutzung einer gemeinsamen Domäne mit den Benutzern der „bonn.iz-soz.de“ entstehen könnten.

Name der Domäne:	berlin.iz-soz.de
Funktion:	Produktivdomäne Benutzer in Berlin
Child-Domains:	Keine
Anzahl DCs	2 (Berlin1 und Berlin2)
Anzahl GCs	2 (Berlin1 und Berlin2)
Explizite Trusts	Keine (nach der vollständige Migration)

3.1.3.5 Verteilung der Global Catalog Server

Durch die Installation des Active Directory wird der erste Server der ersten Domäne automatisch zum Global Catalog Server. In dieser ersten, wie auch in allen weiteren Domänen, müssen neue Server explizit als Global Catalog Server konfiguriert werden. Da Abfragen auf den Global Catalog sehr häufig erfolgen, empfiehlt es sich, mehr als einen Global Catalog Server im Netzwerk zur Verfügung zu stellen. Die Verteilung der Server auf die Domänen ergibt sich wie folgt:

3.1.3.5.1 Root-Domäne „iz-soz.de“

Der erste Domänencontroller „Root1“ in der Domäne „iz-soz.de“ wird durch die Installation des Active Directory zum Global Catalog Server (GC). Nach Installation von „Root2“ wird auch dieser als Global Catalog Server konfiguriert. Das Betriebsmastertoken „Infrakstruktur-Update-Master“ verbleibt auf dem Server „Root1“.

3.1.3.5.2 Child-Domäne „bonn.iz-soz.de“

Der Domänencontroller „Bonn1“ der „bonn.iz-soz.de“ ist nach seiner Installation kein Global Catalog Server. Aus Gründen der Performance wird der Server zum Global Catalog Servern konfiguriert. Hieraus ergibt sich eine erhöhte Replikationslast, da im Global Catalog Objekte sowie deren Attribute aus allen Domänen der Gesamtstruktur gespeichert werden. Dennoch entsteht durch die ausreichend hohe Bandbreite innerhalb des LAN am Standort Bonn keine Beeinträchtigung anderer Netzwerkdienste oder eine für die Benutzer erhöhte Antwortzeit der Server. Nach Installation von „Bonn2“ wird auch dieser als Global Catalog Server konfiguriert.

3.1.3.5.3 Child-Domäne „berlin.iz-soz.de“

In der Domäne „berlin.iz-soz.de“ ist zunächst nur der erste Domänencontroller „Berlin1“ als Global Catalog Server konfiguriert. Damit werden Abfragen über die WAN-Verbindung nach Bonn unterbunden und die verfügbare Bandbreite nicht unnötig belastet. Die Replikation der Global Catalog Daten erfolgt auf Attributebene, die Datenmenge ist sehr gering. Nur bei einer Änderung des Schemas erfolgt eine vollständige Replikation des Global Catalog mit hohem Datenaufkommen. Diese Änderungen werden sehr selten sein. Nach Installation von „Berlin2“ wird auch dieser als Global Catalog Server konfiguriert.

3.1.3.6 Die Positionierung der FSMO (Betriebsmasterrollen)

Innerhalb der Gesamtstruktur eines Active Directory gibt es zwei Betriebsmasterrollen, die nur einmal vorhanden sind:

1. Schemamaster
2. Domain Naming Master

Diese sind für alle in einem gemeinsamen Active Directory vorhandenen Domänen zuständig und daher von besonderer Wichtigkeit.

Nach der Installation des ersten Domänencontrollers liegen diese beiden Rollen auf dem Server „Root1“ in der Domäne „iz-soz.de“.

3.1.3.6.1 Betriebsmasterrollen pro Domäne

Innerhalb jeder einzelnen Domäne eines Active Directorys gibt es drei weitere Betriebsmasterrollen, die jeweils unabhängig von anderen Domänen vorhanden sein müssen. Diese sind:

1. Relative ID Master
2. PDC-Emulator
3. Infrastructure Update Master

Die Rolle des Infrastructure Update Master und der Global Catalog sind miteinander inkompatibel. Diese beiden Funktionen dürfen nicht auf einer Maschine vereint sein. Sobald mehr als ein Domänencontroller innerhalb einer Domäne installiert wird, ist diese Betriebsmasterrolle auf diesen zu verschieben.

Eine Ausnahme von dieser Regel bildet die Situation, dass alle Domänencontroller innerhalb einer Domäne die Rolle des Global Catalog Server innehaben. In diesem Fall entfällt die Funktion des „Infrastrukturmasters“; gleichwohl ist ein Server je Domäne Inhaber dieses Betriebsmaster-Tokens. Das heißt, dass es in den entsprechenden Konfigurationsdialogen nach wie vor einen Server mit der Rolle des „Infrastrukturmasters“ gibt, dieser diese Rolle aber de facto nicht ausführt. Da alle Domänencontroller des Active Directory des IZ-Soz gleichzeitig als Global Catalog Server konfiguriert sind, tritt der oben beschriebene Fall ein.

Hinweis:

Sollte in einer der Domänen ein weiterer Domänencontroller installiert werden, der nicht als Global Catalog Server fungiert, so muss die Betriebsmasterrolle des Infrastructure Update Masters auf diesen Server verschoben werden. Sollte dies nicht geschehen, werden Replikationsfehler innerhalb der Domäne auftreten. Diese werden in der Ereignisanzeige der Server angezeigt. Der KCC (Knowledge Consistency Checker), der für die automatische Erstellung von Replikationsverbindungen der Server untereinander zuständig ist, kann bei falscher Verteilung der Betriebsmasterrollen seine Aufgabe nicht ausführen.

3.1.3.7 Domänenmodi

3.1.3.7.1 Gemischter Modus

Beim Betrieb einer Windows 2000 Domäne gibt es unterschiedliche Betriebsarten (Modi). Der so genannte gemischte Modus erlaubt den Betrieb von Windows 2000 Domänencontrollern und Windows NT 4.0 BDCs innerhalb einer Domäne. Dabei nehmen die NT 4.0 BDCs nur „passiv“ an der Verwaltung der Domäne teil. Das heißt, Benutzer können sich an diesen Servern authentifizieren, weitere Aufgaben fallen diesen Servern nicht zu. Die „aktive“ Verwaltung einer Domäne liegt im gemischten Modus immer bei einem oder, sofern vorhanden, mehreren Windows 2000 Domänencontrollern.

3.1.3.7.2 Einheitlicher Modus

Im Gegensatz zum gemischten Modus erlaubt der einheitliche Modus ausschließlich den Betrieb von Windows 2000 Domänencontrollern. Server unter Windows NT 4.0 können keine Authentifizierungen vornehmen. Der Mechanismus, der im gemischten Modus diese Server mit den aktuellsten Informationen versorgt, wird im einheitlichen Modus deaktiviert. Das Umschalten des Betriebsmodus einer Domäne ist nur von gemischt auf einheitlich möglich und **nicht** reversibel.

Alle Domänen innerhalb des Active Directory der IZ-Soz werden im einheitlichen Modus betrieben. Der Domänenmodus wird unmittelbar nach der Installation des ersten Domänencontrollers umgestellt.

3.1.3.8 Aufbau und Verteilung von DNS

Da sich die Domänen „iz-soz.de“ und „bonn.iz-soz.de“ physisch am gleichen Standort befinden und über ein LAN mit 100 MBit verbunden sind, reicht es aus, wenn in der Root-Domäne „iz-soz.de“ zwei DNS-Server installiert werden. Die Server der „iz-soz.de“ sind auch für die Domäne „bonn.iz-soz.de“ autoritativ. Für die Zone „berlin.iz-soz.de“ werden zwei weitere DNS-Server eingesetzt. Die Autorität dieser Zone wird von der „iz-soz.de“ auf diese beiden Server delegiert.

Als DNS-Server kommen die Windows 2000 eigenen DNS-Dienste zum Einsatz. Diese werden auf den Domänencontrollern „Root1“ und „Root2“ installiert. Für die Domäne „berlin.iz-soz.de“ werden diese Dienste auf den Servern „Berlin1“ und „Berlin2“ installiert.

Die DNS-Zonen „iz-soz.de“ und „bonn.iz-soz.de“ werden als Active Directory integrierte Zonen konfiguriert. Durch die doppelte Auslegung der DNS-Server in der Domäne „iz-soz.de“ ist für eine Redundanz der DNS-Daten gesorgt, da bei Ausfall eines Servers der verbliebene Server über identische Informationen verfügt. Für Abfragen von Clients in Bonn auf Rechner in Berlin wird die Zone „berlin.iz-soz.de“ als sekundäre Standardzone von den Servern „Berlin1“ und „Berlin2“ importiert. Diese Server informieren über eventuelle Updates innerhalb dieser Zonen.

Um Zugriffe ins Internet zu ermöglichen wird auf den Servern „Root1“ und „Root2“ eine Weiterleitung auf den öffentlichen DNS-Server in Bonn „dns.bonn.iz-soz.de“ konfiguriert.

Die Zone „berlin.iz-soz.de“ wird als Active Directory-integrierte Zone auf den Servern „Berlin1“ und „Berlin2“ angelegt. Um auf Abfragen aus der Zone „iz-soz.de“ oder „bonn.iz-soz.de“ antworten zu können wird hierfür eine sekundäre Standardzone von den Servern „Root1“ und „Root2“ importiert. Diese Server informieren über eventuelle Updates innerhalb dieser Zonen.

Um Zugriffe ins Internet zu ermöglichen wird auf den Servern „Berlin1“ und „Berlin2“ eine Weiterleitung auf den öffentlichen DNS-Server „dns.bonn.iz-soz.de“ in Bonn konfiguriert (s. Kap. 4.1.2 Frontend-Struktur).

Um umgekehrte Namesauflösungen (IP-Adresse => Namen) zu ermöglichen wird auf den DNS-Servern „Root1“ und „Root2“ eine Active Directory-integrierte Reverse-Lookupzone für den Bereich 193.175.238.x eingerichtet. Diese erlaubt dynamische Updates. Um diesen Vorgang auch für IP-Adressen aus dem Berliner Subnetz zu ermöglichen wird auf den Servern „Berlin1“ und „Berlin2“ ebenso eine Active Directory-integrierte Zone für das Subnetz 193.175.239.x eingerichtet. Auch diese lässt dynamische Updates zu. Auf „Root1“ und „Root2“ wird jeweils eine sekundäre Standardzone eingerichtet, die von den Servern aus Berlin geladen wird. Ebenso wird auf den „Berlin1“ und „Berlin2“ jeweils eine sekundäre Standardzone mit den Informationen aus dem Bonner Netzwerk geladen.

Server	Zone(n)	AD integriert	Weiterleitung	Server für Domäne
Root1	iz-soz.de, bonn.iz-soz.de	ja	Öffentlicher DNS-Server Bonn	iz-soz.de, bonn.iz-soz.de
Root2	iz-soz.de, bonn.iz-soz.de	ja	Öffentlicher DNS-Server Bonn	iz-soz.de, bonn.iz-soz.de
Berlin1	berlin.iz-soz.de	ja	Öffentlicher DNS-Server Bonn	berlin.iz-soz.de
Berlin2	berlin.iz-soz.de	ja	Öffentlicher DNS-Server Bonn	berlin.iz-soz.de

3.1.3.9 Sitekonzept

Sites werden unter Windows 2000 zur Regelung des Replikationsverkehrs eingerichtet. Durch Konfigurieren von Sites und sogenannten Siteconnectoren kann die logische Verwaltung des Active Directory auf die vorhandene physische Infrastruktur des Netzwerks angepasst werden. Auf diese Weise lässt sich verhindern, dass tagsüber schmalbandige Verbindungen zur Replikation genutzt werden, was unter Umständen höhere Antwortzeiten bis hin zu Timeouts zur Folge hätte. Ein solches Szenario impliziert eine Einschränkung der Benutzer.

Stattdessen kann die Replikation so gesteuert werden, dass sie außerhalb der üblichen Arbeitszeiten stattfindet und tagsüber den Benutzern die volle Bandbreite des Netzwerks zur Verfügung steht.

Da sich die beiden Domänen „iz-soz.de“ und „bonn.iz-soz.de“ physisch am gleichen Standort in Bonn befinden, besteht keine Notwendigkeit für diese Domänen eigene Sites zu konfigurieren. Es bleibt bei dem bei der Installation des Active Directory automatisch angelegten Standort, mit der Bezeichnung „Standardname-des-ersten-Standortes“. Dieser wird in „Bonn“ umbenannt. Für diesen Standort wird das Subnetz 193.175.238.x eingerichtet.

Für den Standort Berlin wird ein weiterer Standort eingerichtet. Dieser wird auch mit „Berlin“ bezeichnet. Diesem wird das Subnetz 193.175.239.x zugeordnet.

Die Aufteilung in unterschiedliche Standorte wird nicht nur zur Steuerung der Replikation verwendet, sondern ist im weiteren Verlauf auch für die Steuerung der Clients über Gruppenrichtlinien notwendig (Client- und Changemanagement s.u.).

3.1.4 DHCP

Zur automatischen Vergabe von IP-Adressen an die Clients in einem Netzwerk wird DHCP eingesetzt. Damit entfällt das manuelle Zuweisen von IP-Adressen. In Windows 2000 sind neue Funktionalitäten implementiert worden, die, sofern notwendig, für unterschiedliche Computer im gleichen Segment unterschiedliche Einstellungen vergeben können.

Als Server wird in Bonn „Root1“ verwendet. Damit die Clients bei einem Ausfall des DHCP-Servers nicht automatisch Adressen aus dem privaten Adressbereich 169.x.x.x verwenden und somit nicht mehr auf die Server im Adressbereich 193.175.x.x zugreifen können, wird über eine Einstellung in der Registrierungsdatenbank APIPA (Automatic Private IP Adressing) auf allen Clients deaktiviert. Damit behalten alle Clients ihre per DHCP erhaltene IP-Adresse so lange, bis die Leasedauer abgelaufen ist. Innerhalb dieser Zeit ist normales Arbeiten möglich:

Um APIPA zu deaktivieren muss die Registrierungsdatenbank um folgenden Eintrag ergänzt werden:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"IPAutoconfigurationEnabled"=dword:00000000
```

In Berlin übernimmt „Berlin1“ die Aufgabe des DHCP-Servers. Die Clients werden ebenso wie in Bonn manipuliert, damit sie ihre IP-Adresse behalten, falls der Server nicht antwortet.

Standort	Server	Adressbereich	Adresspool	Reservierungen
Bonn	Root1	193.175.238.x	193.175.238.165 – 193.175.238.254	
Berlin	Berlin1	193.175.239.x	193.175.239.120 – 193.175.239.254	

3.1.5 WINS

Als weiterer Netzwerkdienst wird WINS installiert. Für Windows 2000 Clients ist DNS der erste und standardmäßig verwendete Dienst zur Auflösung von Namen zu IP-Adressen. Windows 98 oder Windows NT 4.0 Clients verwenden jedoch primär NetBIOS zur Namensauflösung. Durch die Installation von WINS kann die Netzwerkperformance dieser Clients gesteigert wer-

den. Weiterhin wird das Netzwerk von regelmäßigen Broadcasts entlastet, die ohne WINS zur Namensauflösung verwendet würden.

Als WINS-Server kommen in Bonn "Root1" und "Root2", in Berlin "Berlin1" und "Berlin2" zum Einsatz.

Am Standort Bonn sind die Server "Root1" und "Root2" als Push/Pull-Partner konfiguriert. Am Standort Berlin sind die Server "Berlin1" und "Berlin2" als Push/Pull-Partner konfiguriert. Zwischen den beiden Standorten sind die Server "Root1" und "Berlin1" ebenfalls als Push/Pull-Partner konfiguriert. Mit dieser WINS-Konfiguration ist eine Auflösung der NetBIOS-Namen aller Rechner innerhalb des Active Directory möglich, ohne mehrfache Replikationen der WINS-Datenbank zwischen den Standorten durchzuführen.

Die Informationen über die WINS-Server müssen auf allen Servern manuell in den Netzwerkeinstellungen eingetragen werden, die Clients erhalten diese über DHCP zugeordnet. Die WINS-Datenbank ist dynamisch und bedarf keiner besonderen Pflege. Lediglich statische Einträge müssen beachtet werden, falls sich diese ändern. Falsche Einträge können an dieser Stelle zu einer Verringerung der Performance führen, da die Clients mit fehlerhaften Informationen versorgt werden und diese dann wieder auf Broadcasts zurückgreifen.

3.1.6 Das Schema des Active Directory

3.1.6.1 Das Standardschema von Microsoft

Mit der Installation des Active Directory wird das Standardschema von Windows 2000 installiert. Durch zusätzliche Softwareprodukte kann dieses Schema erweitert werden. Da das Schema für das gesamte Active Directory gültig ist, wirkt sich die Installation von Software die das Schema verändert, auf alle Domänen innerhalb des Active Directory aus. Dies gilt auch, wenn diese Software in einer untergeordneten Domäne installiert wird. Daher müssen vor einer solchen Installation die möglichen Auswirkungen und Probleme sorgfältig geprüft und die Konsequenzen geplant werden. Eine Veränderung des Schemas zieht zwingend eine vollständige Replikation des gesamten Global Catalogs nach sich.

Das Schema welches im IZ zum Einsatz kommt wird nicht durch individuelle Anpassungen oder Programmierungen verändert. Die Installation von Exchange 2000 erweitert das Schema zwar, dennoch werden auch hier keine

individuellen Anpassungen vorgenommen, sondern nur die Standardveränderungen, die Exchange 2000 selbständig vornimmt.

3.1.6.2 Microsoft Exchange 2000 und Active Directory

Innerhalb des Active Directory existiert eine Exchange-Organisation. Die Benutzer am Standort Bonn verwenden den Exchange-Server „Excha3“, die Benutzer in Berlin den Server „Exchabln“.

Exchange 2000 verwaltet keine eigene Benutzerdatenbank wie die Vorgängerprodukte, sondern legt seine Daten im Active Directory selbst ab. Durch die Installation von Exchange 2000 wird die Zahl der Attribute und Objekte des Active Directory mehr als verdoppelt. Diese Veränderung des Schemas zieht, wie weiter oben erwähnt, eine komplette Replikation des Schemas zwischen allen Domänencontrollern der Gesamtstruktur sowie der kompletten Datenbanken aller GCs nach sich.

Nach der Installation von Exchange 2000 werden Aufgaben wie das Erstellen, Löschen oder Verschieben von Postfächern über die Verwaltungskonsole "Active Directory-Benutzer und -Computer" erledigt. Dies ist die augenscheinlichste Veränderung durch die Schemaerweiterung. Die Eigenschaften des Objekts „Benutzer“ werden durch eine Vielzahl neuer Karteireiter sowie zusätzliche Optionen im Kontextmenü erweitert (man beachte bei Bedarf in der Konsole "Active Directory-Benutzer und -Computer" im Menü "Ansicht" die Funktion "Erweiterte Funktionen").

3.1.7 Verteilung der FSMO (Betriebsmasterrollen)

Durch die Installation von Windows 2000 Active Directory liegen die Betriebsmasterrollen jeweils auf den ersten in der Domäne installierten Domänencontrollern. Um die Ausfallsicherheit gegen den Totalausfall einer ganzen Domäne zu erhöhen, werden die Rollen auf mehrere Server verteilt.

3.1.7.1 Die FSMO in der Domäne „iz-soz.de“

In der Domäne „iz-soz.de“ sind durch die Installation folgende Rollen und Funktionen auf dem ersten Server angelegt:

- Schemamaster
- Domain Naming Master
- PDC-Emulator

- RID-Master
- Infrastructure Update Master
- Global Catalog Server

Da der zweite Domänencontroller ebenfalls Global Catalog Server konfiguriert wird, entfällt die Funktion der Rolle des Infrastructure Update Masters. Das entsprechende Betriebsmaster-Token verbleibt auf dem ersten Domänencontroller (siehe oben). Die Verteilung der Rollen und Funktionen in dieser Domäne ergibt sich demnach wie folgt:

Rolle/Funktion	Root1	Root2
Schemamaster	X	
Domain Naming Master	X	
PDC-Emulator	X	
RID-Master	X	
Infrastructure Update Master	X	
Global Catalog Server	X	X

3.1.7.2 Die FSMO in der Domäne „bonn.iz-soz.de“

Beide Domänencontroller der Domäne „bonn.iz-soz.de“ werden Global Catalog Server. Die Rolle des Infrastructure Update Masters verbleibt auf „Bonn1“ (siehe oben). Eine Aufteilung der weiteren, domäneninternen Rollen führt hier zu keiner Steigerung der Performance und unterbleibt deswegen.

Alle Rollen und Funktionen der Server in der Tabelle:

Rolle/Funktion	Bonn1	Bonn2
Schemamaster	nicht vorhanden	nicht vorhanden
Domain Naming Master	nicht vorhanden	nicht vorhanden
PDC-Emulator	X	
RID-Master	X	
Infrastructure Update Master	X	
Global Catalog Server	X	X

3.1.7.3 Die FSMO in der Domäne „berlin.iz-soz.de“

Um die Domäne „berlin.iz-soz.de“ weitgehend unabhängig von Abfragen über die WAN-Verbindung zu machen, werden beide Domänencontroller dieser Domäne als Global Catalog Server eingerichtet. Eine Aufteilung der weiteren, domäneninternen Rollen führt hier zu keiner Steigerung der Performance und unterbleibt deswegen. Die Rolle des Infrastructure Update Masters verbleibt auf „Berlin1“ (siehe oben).

Die Verteilung der Rollen und Funktionen ist aus der folgenden Tabelle ersichtlich:

Rolle/Funktion	Berlin1	Berlin2
Schemamaster	nicht vorhanden	nicht vorhanden
Domain Naming Master	nicht vorhanden	nicht vorhanden
PDC-Emulator	X	
RID-Master	X	
Infrastructure Update Master	X	
Global Catalog Server	X	X

3.1.8 Änderungen am Active Directory (Change Management)

Änderungen des Active Directory treten relativ häufig auf, sind aber in zwei unterschiedliche Klassen einzuordnen. Einerseits sind dies inhaltliche Veränderungen der vorhandenen Objekte und Attribute durch Füllen, Leeren oder Verändern der entsprechenden Datenfelder.

Andererseits betrifft dies Änderungen an der zu Grunde liegenden Struktur des Schemas. Während eines solchen Prozesses werden dem Active Directory – Schema neue Objekte hinzugefügt, beispielsweise der Exchange – Informationsspeicher als Active Directory-Objekt, oder bestehenden Objekten werden neue Attribute hinzugefügt, beispielsweise der Ort des zugeordneten Exchange-Postfachs als Attribut des Benutzerobjekts.

3.1.8.1 Änderungen des Active Directory Inhalts

Dieser Abschnitt beschreibt Änderungen, die sich nur auf den Inhalt des Active Directory beziehen. Das Schema bringt eine große Anzahl vorgefertigter Objekte mit, die zur Verwaltung einer Domäne in aller Regel ausreichen. Die Attribute dieser Objekte können vollständig oder nur zum Teil mit Werten

gefüllt werden. Zur Bearbeitung dieser Werte gibt es verschiedene Methoden, wobei üblicherweise die Verwaltungstools der Microsoft Management Console (MMC) verwendet werden. Innerhalb dieser Konsolen kommen so genannte Snap-Ins zum Einsatz. Das sind Module, die zur Verwaltung einzelner Dienste wie „DNS“ oder der Objekte in „Active Directory Benutzer und Computer“ benötigt werden. Um sie zu verwenden, sind entsprechende Benutzerberechtigungen notwendig. Die Konsolen für fast alle Verwaltungsvorgänge werden auf den Domänencontrollern automatisch installiert. Diese sind unter „Start/Programme/Verwaltung“ zu finden. Eine Zusammenstellung von mehreren Snap-Ins in einer eigenen Konsole ist ebenso möglich.

Um die Verwaltungstools von einer Workstation im Netzwerk verwenden zu können, müssen diese ggf. manuell installiert werden. Dazu muss die Datei „adminpak.msi“ ausgeführt werden. Diese findet sich auf der Windows 2000 Server CD im Verzeichnis i386 oder unter C:\Winnt\System32\ auf den Domänencontrollern.

Es gibt zwei verschiedene Stufen der Active - Directory - Replikation. Sicherheitsrelevante Veränderungen des Inhalts, wie zum Beispiel die Sperrung eines Benutzerkontos, werden sofort repliziert. Alle anderen, nicht sicherheitskritischen, Veränderungen werden innerhalb des Standardzyklus von maximal 15 Minuten repliziert.

Die Replikationszyklen zu Domänen in anderen Sites werden über Siteconnectoren konfiguriert.

3.1.8.2 Änderungen des Active Directory Schemas

Änderungen am Schema des Active Directory unterscheiden sich sowohl in ihrer Häufigkeit als auch in ihrer Komplexität von „normalen“ Veränderungen des Active Directory, in Form von Änderungen oder Neuanlegen von Objekten. Zur Schemaänderung sind spezielle Benutzerberechtigungen notwendig. Änderungen am Schema lassen sich nicht mehr rückgängig machen, neu angelegte Objekte oder Attribute können lediglich deaktiviert werden. Häufige Veränderungen und deren Zurücknahme führen zu unnötiger Vergrößerung des Active Directory und bergen die Gefahr von Fehlfunktion oder totaler Zerstörung des Active Directory.

Von manuellen Veränderungen abgesehen kann das Schema auch durch Installation von neuen Softwareprodukten verändert werden. Hierbei werden neue Attribute und Objekte angelegt, die für die Verwendung dieser Software

notwendig sind. Durch die Installation von Exchange 2000 wird die Anzahl der Objekte und Attribute des Active Directory mehr als verdoppelt.

3.1.9 Management des Active Directory

3.1.9.1 Anbindung der DCs an einen zentralen Zeitdienst

Zeitsynchronisation unter Windows 2000 ist ein elementarer Bestandteil des Active Directory. Ohne Zeitsynchronisation würden die Systemzeiten der einzelnen Server nach einer gewissen Zeit mehr oder weniger stark voneinander abweichen. Überschreiten die Abweichungen eine Schwelle von fünf Minuten, ist keine Replikation möglich. Weiterhin werden Kerberos-Tickets, die zur Authentifizierung verwendet werden, ungültig, sobald ihr Zeitstempel des ausgebenden Servers um fünf oder mehr Minuten vom empfangenden Server abweicht. Daher ist die Zeitsynchronisation unter Windows 2000 hierarchisch durch das gesamte Active Directory aufgebaut, wobei der erstinstallierte Domänencontroller automatisch als Zeitserver für das lokale Netzwerk gilt. Um dessen Zeit zu synchronisieren, wird dieser auf eine externe Zeitquelle konfiguriert. Dazu wird ein Zeitserver der Physikalisch Technischen Bundesanstalt in Braunschweig verwendet.

Weitere Informationen hierzu finden sich in der technischen Referenz Technet:

- Q224799: Basic Operations of the Windows Time Service
- Q216734: How to Configure an Authoritative Time Server in Windows 2000

3.1.9.2 Remote Administration des Active Directory

Die meisten Aufgaben, die täglich bei der Administration anfallen, lassen sich auch über das Netzwerk und die Verwendung der standardmäßigen Snap-Ins der Konsole erledigen. Einige Tätigkeiten können nur bei lokaler Anmeldung am Server ausgeführt werden, zum Beispiel die Installation neuer Software. Dafür bietet sich die Verwendung der Terminaldienste an. Eine Anmeldung an einem Server über die Terminal-Services gleicht einer lokalen, interaktiven Anmeldung am Server selbst. So ist die Installation von Software möglich, ohne physisch Zugriff auf den Server zu haben. Aus diesem Grund sind auf allen Servern die Terminal-Services installiert, die eine lizenz- und kostenfreie Fernwartung über das Netzwerk ermöglichen.

3.1.9.3 Administration über Snap-Ins der MMC

Die Microsoft Management Console (MMC) ist eine neue Umgebung zur Administration von Windows 2000. Im Gegensatz zu Windows NT 4.0 werden hier keine einzelnen, starren Verwaltungsinstrumente in einer GUI angeboten. Die MMC selbst bietet keine eigene Funktion, sondern stellt den äußeren Rahmen für die einzelnen Verwaltungsmodule bereit. Damit ist es möglich, je nach Benutzer eigene Konsolen zusammenzustellen, die nur die wirklich benötigten Module enthalten, oder auch alle gewünschten Module in einer einzigen Umgebung vereinen. Mit der Installation des Active Directory werden alle zur Verwaltung notwendigen Snap-Ins in jeweils einer eigenen Konsole zur Verfügung gestellt. Neu installierte Software bringt häufig eigene, neue Snap-Ins mit sich.

Aus Gründen der Sicherheit wird das Snap-In zur Verwaltung des Schemas nicht standardmäßig zur Verfügung gestellt, sondern muss manuell nachregistriert werden.

Die geschieht über den Kommandozeilenbefehl:

regsvr32 schmmgmt.dll.

Danach steht auch der Zugriff auf das Schema über ein Snap-In zur Verfügung. Weitere Information zu diesem Thema enthalten die folgenden Technet-Artikel:

- Q229691: How to Enable Domain Controllers to Modify the Schema
- Q268655: Active Directory Schema Snap-In Does Not Connect to the Operations Master

3.1.10 Muster-Konfiguration der Server

3.1.10.1 Root1

Bereich	Name	Wert
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.238.1
	DNS-Server	193.175.238.1
	WINS-Server	193.175.238.1, 193.185.238.20
Netzwerk Dienste		
	DNS	
	DHCP	
	WINS	

OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Konf. DNS		
	DNS-Server für	Zone „iz-soz.de“, Active Directory integriert Domäne „bonn.iz-soz.de“, dyn. Updates zugelassen
	Weiterleitung	193.175.238.2
	Delegation	Zone „berlin.iz-soz.de“ auf Berlin1 und Berlin2
	Root-Hints	Löschen aller Verweise auf Root-Server
	Reverse Lookup	193.175.238.1 Active Directory integriert, Update-Notification an Berlin1 und Berlin2, dyn. Updates zugelassen 193.175.239.4 Standard Secondary von Berlin1 und Berlin2
W32Time		
	NTP-Server	ptbtime1.ptb.de (194.95.250.35) Es wird geprüft, statt dessen eine lokale Funkuhr einzusetzen
Active Directory		
	Betriebsmasterrollen	Schema-Master, Domain Naming Master, Infrastructure-Update-Master, PDC-Emulator, RID-Master, Global Catalog Server

3.1.10.2 Root2

Bereich	**Name**	**Wert**
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.238.20
	DNS-Server	193.175.238.20
	WINS-Server	193.175.238.1, 193.175.238.20
Netzwerk Dienste		
	DNS	
	WINS	
OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Konf. DNS		
	DNS-Server	Übernahme der Daten aus dem Active Directory
	Weiterleitung	193.175.238.2

	Root-Hints	Löschen aller Verweise auf Root-Server
W32Time		
		Synchronisation mit Root1
Active Directory		
	Betriebsmasterrollen	Global Catalog Server

3.1.10.3 Bonn1

Bereich	Name	Wert
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.238.10
	DNS-Server	193.175.238.1, 193.175.238.20
	WINS-Server	193.175.238.1, 193.175.238.20
OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Active Directory		
	Betriebsmasterrollen	Infrastructure-Update-Master, PDC-Emulator, RID-Master, Global Catalog Server

3.1.10.4 Bonn2

Bereich	Name	Wert
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.238.21
	DNS-Server	193.175.238.1, 193.175.238.20
	WINS-Server	193.175.238.1, 193.175.238.20
OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Active Directory		
	Betriebsmasterrollen	Global Catalog Server

3.1.10.5 Berlin1

Bereich	Name	Wert
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.239.4

	DNS-Server	193.175.239.4
	WINS-Server	193.175.239.4, 193.175.239.7
Netzwerk Dienste		
	DNS	
	DHCP	
	WINS	
OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Konf. DNS		
	DNS-Server für	Zone „berlin.iz-soz.de“, Active Directory integriert, dyn. Updates zugelassen
	Weiterleitung	193.175.238.2
	Weitere Zonen	Standard Sekundäre Zone für „iz-soz.de“
	Root-Hints	Löschen aller Verweise auf Root-Server
	Reverse Lookup	193.175.238.1 Active Directory integriert, Update-Notification an Root1 und Root2, dyn. Updates zugelassen
Active Directory		
	Betriebsmasterrollen	PDC-Emulator, RID-Master, Infrastructure-Update-Master, Global Catalog Server

3.1.10.6 Berlin2

Bereich	Name	Wert
Betriebssystem		Windows 2000 Server, SP3
Netzwerk		
	IP-Adresse	193.175.239.7
	DNS-Server	193.175.239.7
	WINS-Server	193.175.239.4, 193.175.239.7
Netzwerk Dienste		
	DNS	
	WINS	
OS		
	DS-Datenbank	C:\Winnt\NTDS\
	DS-Logfiles	C:\Winnt\NTDS\
Konf. DNS		
	DNS-Server für	Zone „berlin.iz-soz.de“, Active Directory integriert
	Weiterleitung	193.175.238.2
	Weitere Zonen	Standard Sekundäre Zone für „iz-soz.de“
	Root-Hints	Löschen aller Verweise auf Root-Server
Active Directory		
	Betriebsmasterrollen	Global Catalog Server

3.2 E-Mail, Exchange, Outlook

Die E-Mail ist neben Telefon und persönlichen Gesprächen inzwischen die wichtigste Kommunikationsform des IZ, sowohl für den internen Informationsaustausch als auch im Kontakt mit externen Partnern, Kunden und Lieferanten.

Neben der Verwaltung der elektronischen Post bieten moderne, unternehmens-orientierte E-Mail-Systeme zusätzlich ein umfangreiches Spektrum von Groupware-Funktionen und von Integrations-Schnittstellen zu anderen Kommunikations-Diensten und -Geräten.

Nach dem Stand der Technik sind hierbei die beiden Systeme

IBM Lotus Notes und
Microsoft Exchange/Outlook

technisch und in ihrer Marktverbreitung führend.

Nachdem 1994 das LAN-Betriebssystem von vormals OS/2 auf Windows NT umgestellt worden war, wurden 1998 Microsoft Exchange (als Mail-Server) und Microsoft Outlook (als Mail-Client im Arbeitsgruppen-Modus) als Nachfolger eines einfachen SMTP/POP3-basierten E-Mail-Systems eingeführt.

Der Vorteil von Exchange/Outlook gegenüber konkurrierenden Systemen besteht unter den Randbedingungen des IZ u.a. in

- der Integration in die User-, Zugriffs- und Rechte-Verwaltung des LAN-Betriebssystems Windows NT/2000,
- der Integration in das Standard-Anwendungs-Paket des IZ Microsoft Office,
- der einheitlichen und zentralen Verwaltung einer großen Anzahl wichtiger Struktur- und Groupware-Komponenten, u.a.:
  - Persönliche / öffentliche Ordner,
  - Postfächer,
  - Kalender,
  - Kontakte, Adressbücher,
  - Aufgaben,
  - Notizen, Entwürfe,
  - Groupware-Funktionen, u.a.:
    Zugriffsrechte und Sekretariatsfunktionen für

die Bearbeitung fremder Postfächer,
gemeinsame Terminverwaltung,
sequentielle Bearbeitung von Office-Dokumenten,
Vergabe und Überwachung von Aufgaben,

- der Integration von Exchange/Outlook-Schnittstellen in UMS-Anwendungen (unified messaging service) anderer Produkte, u.a.
  - Handy (u.a. Siemens: Organizer, Telefonbuch),
  - PDA (Personel Digital Assistant: E-Mail, Adressen, Office),
  - Telefonanlage (u.a. Siemens Hicom: Adressen, Telefon/Fax).

Ein erheblicher Teil dieser Optionen wird - Stand 2002 - im IZ produktiv genutzt, weitere Funktionen (u.a. Groupware-Kalender) werden erprobt, in Planung befinden sich u.a. der Einsatz von PDAs und die Integration von Telefonanlage und LAN (s.u.).

3.3 Spezielle Strukturkomponenten

3.3.1 aDIS-Verfahren: nächste Schritte

Für das aDIS-Verfahren ist (s. Kap. 2.3.1) - Stand 2002 - ein Upgrade der Anwendungssoftware nicht absehbar und funktionell auch nicht dringend. Zur mittelfristigen Stabilisierung dieser für das IZ existenziellen Anwendung ist deshalb geplant, in 2002 die veraltete Server-Hardware Siemens RM 400 unter weitgehender Beibehaltung der Betriebs- und Anwendungssoftware gegen eine kompatible aber technisch modernere und leistungsfähigere Maschine auszutauschen.

3.3.2 Telefonanlage: Kopplung mit dem LAN

Die Telefon-Situation des IZ zeichnet sich - Stand 2002 - dadurch aus, dass an den beiden Standorten Bonn und Berlin IZ-eigene, kompatible Telefon-Anlagen des Typs Siemens Hicom HG1500 installiert sind.

Für diesen Anlagentyp können durch eine Anbindung an die jeweiligen LANs folgende zusätzlichen Dienste bereitgestellt werden:

- zentrale Administration beider Telefonanlagen über einen zentralen Server inkl. der individuellen Konfigurierung der Telefon-Funktionen wie Anrufübernahme, Tastenprogrammierung etc.,
- zentrale Gebührenerfassung und -auswertung,

- einheitlicher Nummern-Plan für Bonn und Berlin und Ergänzung jedes Telefonanschlusses um einen individuellen (virtuellen) Faxanschluss durch Einführung einer einheitlichen Fax-Einwahl-Ziffer für alle Telefonnummern des IZ, Senden und Empfangen von Fax erfolgt über Exchange/Outlook (s.u.),
- unified messaging über eine Schnittstelle zu Exchange/Outlook mit folgenden ergänzenden Funktionen des Outlook-Client:
  - Multimedia-Mailbox, Verwaltung von Sprachnachrichten,
  - Senden und Empfangen von Faxnachrichten,
  - Computergestützte Telephonie (CTI):
    wählen aus Outlook-Adressbüchern,
    Verwaltung eingehender und ausgehender Telefonate,
  - Nutzung aller UMS-Funktionen (z.B. Voice-Mailbox) auch außerhalb des IZ über das Internet.

Die Realisierung dieser Funktionen ist für Mitte 2002 projektiert und erfordert neben dem technischen Anschluss der Telefonanlagen an die lokalen LANs die zentrale Installation von zwei zusätzlichen Servern (CTI-Server, UMS-Server) unter Windows 2000, die Kommunikation zwischen Servern und Telefonanlagen erfolgt über TCP/IP-Intranet/Internet.

Die zentrale Administration und Konfiguration der beiden Telefonanlagen durch (die hierfür zuständigen) IZ-Mitarbeiter mit Hilfe einer benutzerfreundlichen Windows-Anwendung wird voraussichtlich eine erhebliche Vereinfachung und Beschleunigung der Erledigung von Änderungsanforderungen aus dem Haus bewirken. Für Änderungsanforderungen musste bisher - in Ermangelung geeigneter Benutzerschnittstellen der Telefonanlagen - in vielen Fällen externes Service-Personal beauftragt werden.

Von den Outlook-gestützten UMS/CTI-Funktionen, dem individuellem Fax und der Internet-Bedienbarkeit dieser Optionen wird eine Vereinfachung und Beschleunigung der Telefon-basierten Kommunikation der Mitarbeiter erwartet, insbesondere in den Aufgabenbereichen mit intensiver Telefon-/Fax-Kommunikation. Soweit es sich überschlägig feststellen lässt, überlappt sich diese Nutzergruppe sowohl mit den intensiven E-Mail-Anwendern als auch mit der Mitarbeitergruppe, die - z.B. über Notebooks - von externen Standorten aus und über das Internet auf ihre IZ-E-Mail zugreifen.

Die Nutzung der Windows/Outlook-Adressobjekte als CTI-Telefonbuch bietet darüber hinaus weitere Möglichkeiten zur Standardisierung der Adressen-

verwaltung im IZ einschließlich der Option, LDAP-Online-Adressbücher Internet-öffentlich bereitzustellen.

3.4 Netzstruktur und Netzwerksicherheit

3.4.1 Allgemeine Netzwerksicherheit

Alle Computer im Netzwerk des IZ haben öffentlich IP-Adressen. Im Standort Bonn sind dies Adressen aus dem Bereich 193.175.238.x, in Berlin aus dem Bereich 193.175.239.x. Dadurch, dass für die Adressierung der Rechner im lokalen Netzwerk öffentliche Adressen verwendet werden, sind diese prinzipiell auch über das Internet und damit als Angriffsziel für Missbrauch und Datenzerstörung erreichbar.

Um die Gefährdung zu reduzieren, sind sowohl in Bonn als auch in Berlin zwischen dem Interzugang und dem lokalen Netzwerk Cisco-Router eingebaut worden. Diese können über konfigurierbare Skripte eingehende und ausgehende Datenpakete nach ihrer Quell- und Zieladresse und den Portnummern filtern. Der Transfer sowohl von innen nach außen als auch von außen nach innen kann dadurch auf dedizierte Dienste beschränkt werden.

3.4.2 Weitergehende Optionen

Um die Sicherheit des Netzwerks zu erhöhen und die Möglichkeit des Missbrauchs von Ressourcen zu verhindern stehen weitere technische Maßnahmen zur Verfügung:

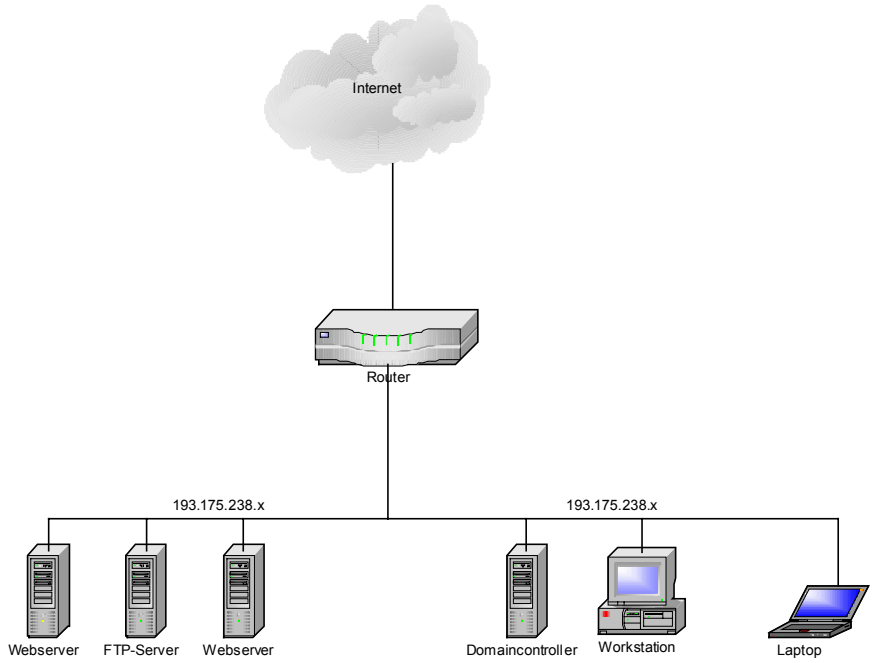
3.4.2.1 DMZ (DeMilitarisierte Zone)

Da alle Rechner im Netzwerk des IZ, sowohl am Standort Bonn als auch in Berlin, zur Zeit über offizielle IP-Adressen verfügen, sind diese auch prinzipiell über die IP-Adressierung ansprechbar. Dieser Umstand stellt grundsätzlich eine Gefährdung des lokalen Netzwerks an beiden Standorten dar. Durch die Trennung zwischen öffentlich erreichbarem Bereich und dem lokalen Netzwerk kann diese Gefährdung verringert werden.

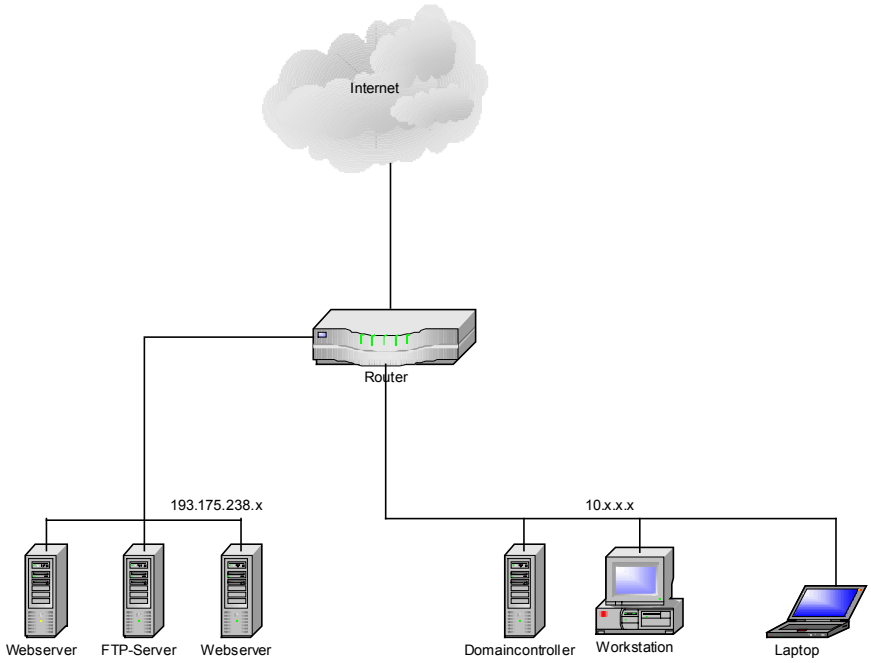
Mit der bereits vorhandenen Hardwareausstattung ließe sich diese Trennung wie folgt realisieren:
In beide Router wird je ein weiteres Netzwerkmodul eingebaut. Mit Hilfe dieses Netzwerkmoduls wird dem LAN der Zugriff ins Internet ermöglicht, während das vorhandene interne Interface alle Anfragen aus dem Internet in

das Segment der öffentlich erreichbaren Server weiterleitet. Die IP-Adressen innerhalb des LANs werden zeitgleich auf einen privaten Adressbereich umgestellt. Damit sind Zugriffe auf diesen Teil des Netzwerks von außerhalb nicht mehr möglich,

Die folgenden zwei Grafiken verdeutlichen den Unterschied:



Vor der Umstellung befinden sich öffentlich erreichbare Server und das lokale Netzwerk in einem Adressbereich.



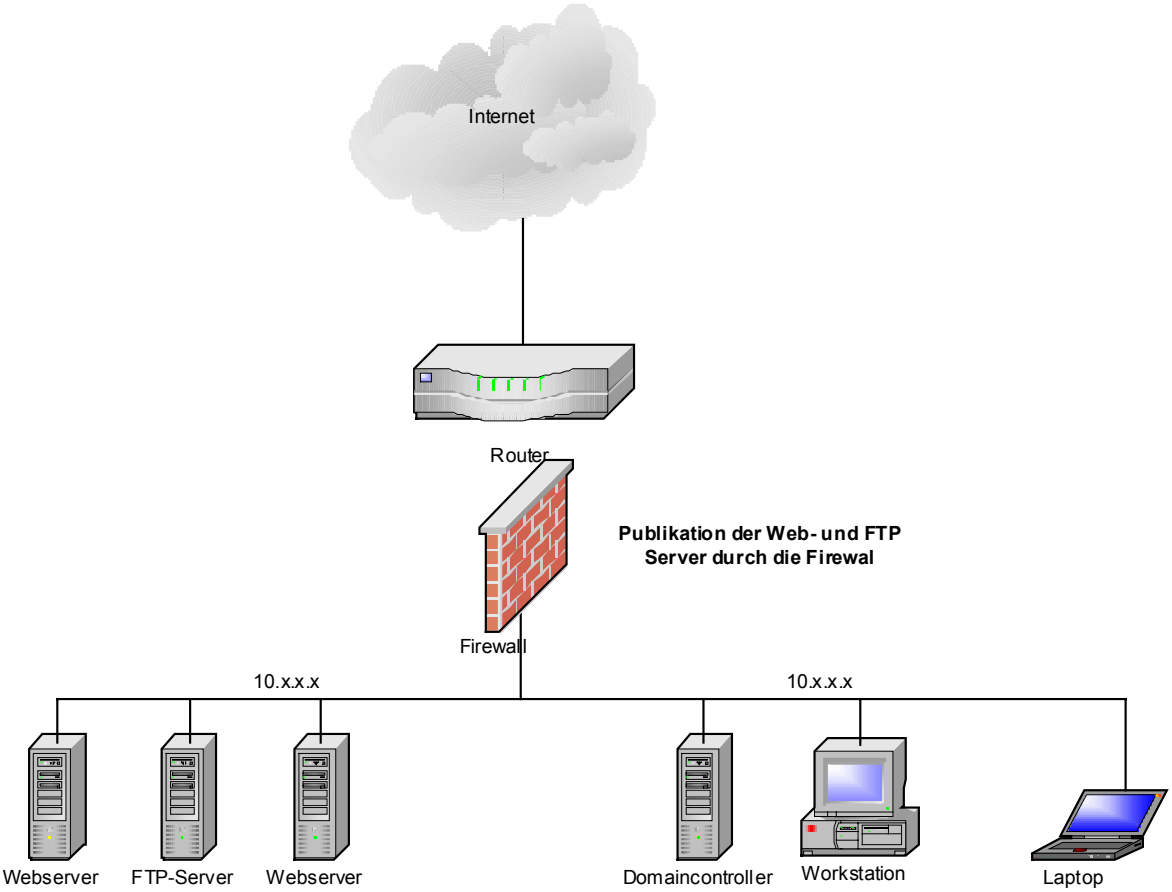
Nach der Umstellung befinden sich die öffentlichen Server in einer DMZ, die physisch wie logisch vom lokalen Netzwerk getrennt ist.

3.4.2.2 Firewall mit Adresskonvertierung

Eine weitere Möglichkeit stellt der Einsatz eines dedizierten Firewalls mit Adresskonvertierung dar. Dabei werden alle Rechner an den Standorten Bonn und Berlin mit privaten IP-Adressen ausgestattet. Dadurch sind sie nicht mehr direkt aus dem Internet erreichbar. Da aber z.B. die Web- und FTP-Server auch weiterhin erreichbar sein müssen, werden diese durch Serververöffentlichung des Firewalls publiziert. Durch diese Konfiguration ist sichergestellt, dass alle lokalen Arbeitsstationen auf die Web- und Projektserver zugreifen können, sich diese aber alle in einem privaten Adressbereich befinden.

Durch den Einsatz geeigneter Software auf einem dedizierten Server, z.B. Microsoft ISA-Server oder Firewall 1 lässt sich eine weitere Anforderung realisieren: Durch MAPI-Veröffentlichung können die Benutzer des IZ-Netzwerks auch über das Internet auf den Exchange-Server zugreifen und damit arbeiten, wie bei einer lokalen Anmeldung.

Zur Verdeutlichung folgende Grafik:



3.4.2.3 Einrichten eines VPN (Virtuelles privates Netzwerk)

Zur Sicherung des Replikationsverkehrs der Active Directory Umgebung über die Internetverbindung zwischen Bonn und Berlin, sollte ein Virtuelles Privates Netzwerk eingerichtet werden. Dadurch werden Daten, die innerhalb des Netzwerks ausgetauscht werden, verschlüsselt übertragen.

Dies kann voraussichtlich durch geeignete Konfiguration der vorhandenen Router realisiert werden.

3.4.2.4 Intrusion Detection - Intrusion Response

Während es sich bei Firewalls und DMZ bildlich gesprochen um "Schutzzäune" handelt, die grundsätzlich einen unbefugten Zugang verhindern sollen, und Adresskonvertierung darüber hinaus einen "Sichtschutz" darstellt, der den externen Einblick in interne Strukturen erschweren soll, sind Intrusion Detection Systeme (IDS) mit "Alarmanlagen" vergleichbar, die einen erfolgten (oder vermuteten) Einbruch melden sollen, und Intrusion Response Sys-

teme (IRS) mit den zugehörigen "Reaktions-Systemen", im Extremfall mit "Selbstschussanlagen".

Nach dem Stand der Technik werden für Intrusion Detection (ID) - die Diagnose eines irregulären Vorgangs innerhalb des LAN, z.B. eines Versuchs, von außerhalb des Netzes unerlaubt oder mit irregulären Inhalten auf einen Server innerhalb des Netzes zuzugreifen - folgende Methoden verwendet (vergl. hierzu u.a. die Studie der debis IT Security Services von 1998: Helden und Karsch: "Grundlagen, Forderungen und Marktübersicht für Intrusion Detection Systeme (IDS) und Intrusion Response Systeme (IRS)"):

- Mit Hilfe eines spezialisierten Servers ("Sniffers") werden alle Datenpakete auf dem gesamten Netz oder einem Netzsegment mitgelesen und inhaltlich nach Zeichenketten ("Signaturen") durchsucht, die für unerlaubte Funktionen typisch sind.
  Hierdurch können insbesondere solche Einbruchsversuche identifiziert werden, bei denen versucht wird, auf öffentlich zugänglichen Servern (z.B. WWW-Server) über den regulären Port (z.B. Port 80) mit Hilfe spezieller Input-Zeichenketten irreguläre Effekte zu erzielen, z.B. einen Software-Fehler ("Sicherheitslücken") zu nutzen, der das System in einen unerwünschten Zustand versetzt.
  Hinweis:
  Bei Verwendung von Switch-Hubs in Ethernet-LANs muss darauf geachtet werden, dass der "Sniffer" an ein Ethernet-Segment angeschlossen wird, in das auch die zu untersuchenden Datenpakete übertragen werden. I.d.R. ist dies das gleiche Segment, mit dem der Internet-Router an den Switch-Hub angeschlossen wird, hierzu ist ein u.U. zwischengeschalteter, zusätzlicher Non-Switch-Hub erforderlich.

- Eine spezielle Anwendung der "Sniffer"-Technik sind Proxy-Server mit Zeichenkettenanalyse. Diese werden im Datenstrom - i.d.R. als Gateways oder Router - zwischen dem Internetzugang und dem potentiellen Angriffsziel positioniert und analysieren die Datenpakete bevor sie an das Ziel weitergeleitet werden. Bei Verdacht auf ID kann dann ggf. die Verbindung unterbrochen werden.

- Die Zustandsdaten der gefährdeten Systeme (Ereignis-Logs, Performance-Daten, Betriebsmittel-Verbrauch etc.) werden systematisch in Log-Dateien gesammelt und daraufhin überprüft, ob einzelne Zustandsveränderungen oder Ketten von Ereignissen auf einen unerwünschten Vorgang, z.B. mehrfaches versuchtes Login mit ungültigem

Passwort oder das unerwartete Starten/Beenden von Diensten, schließen lassen. Die Analyse erfolgt durch einen Server auf der Grundlage von "Regeln", die verdächtige Zustände beschreiben.

In der o.g. debis-Studie von Helden und Karsch werden folgende Angriffsmethoden einschließlich der vorbereitenden Informations-Beschaffung über das Angriffsziel unterschieden:

- TCP Port Scans
  - active / half open / stealth
- UDP Port Scans
- finger, ruser, netstat, rstatd, sysstat, identd, rwho, nbstat
- IP-Fragmentierung
- falsche IP-Parameter
- SYN mit unerreichbarer Quelladresse
- CPU-Angriff mittels Telnet (Windows NT)
- IIS-Angriff mittels Telnet (Windows NT)
- ICMP-Angriffe:
  - ICMP Redirect
  - ICMP Destination Unreachable
  - ICMP Echo Request
  - ICMP Zeitstempel
  - ICMP Tunnel
- Spoofing:
  - IP Spoofing
  - TCP-Sequenznummernvorhersage
  - DNS Spoofing
  - RIP Spoofing
  - WWW Spoofing
- Source Routing
- Session Hijacking
- Flooding
  - Mail Flooding
  - SYS Flooding
  - System Log Flooding
  - Data Flooding
  - finger Flooding
- DNS-Angriff
  - Cache Verunreinigung
- NIS Angriff
- FTP Angriff

aktiver / passiver FTP-Angriff
Brute-Force Angriff
HTTP Angriff
SMB Crash
NFS Angriff
SENDMAIL Angriff
Mail Spoofing
Angriff auf das Authentisierungssystem
Lauschangriff
Erraten von Passwörtern
Viren, Trojanische Pferde, Würmer
Hintertüren
Sicherheitslücken (z.B. Reaktion auf spezielle Input-Zeichenketten)
Java, Cookies, ActiveX, CGI, MIME

Die meisten dieser Angriffstechniken können mit Firewalls und Filterlisten nicht verhindert werden, da zugelassene IP-Adressen und reguläre Ports verwendet werden. Ein zweites Problem besteht darin, dass komplexe Angriffe häufig in mehreren, aufeinander aufbauenden Schritten erfolgen, wobei jeder Teilschritt für sich genommen unschädlich und häufig von regulären Transaktionen kaum zu unterscheiden ist.

Erfolgreiche Angriffe auf IT-Systeme bewirken in den meisten bekannten Fällen auf dem angegriffenen System oder von dort aus auf einem anderen Zielsystem einen "Denial-of-Service", die Beendigung oder die intensive Störung von Diensten, häufig den Absturz des angegriffenen Rechners.

Die Antwortmaßnahmen auf einen (vermuteten) Einbruch haben folgende mögliche Ziele:

- Identifizieren des Angreifers,
- Schutz vor weiteren Schäden,
- Beheben der entstandenen Schäden.

Folgende automatische, halbautomatische oder manuelle Maßnahmen sind möglich:

- Gegenangriff auf den Angreifer (z.B. Denial-of-Service-Angriff) (rechtlich problematisch),

- Abschottung
  Schließen der betroffenen TCP/IP-Ports
  Terminieren von Programmen und Diensten,
  Sperren der angreifenden IP-Adresse,
  Sperren von Benutzeraccounts.
- Identifizieren des Angreifers
  Protokollierung,
  Umlenken des Angriffs in eine "Gummizelle",
  Identifikation des angreifenden Rechners mit DNS,
  Benachrichtigung eines CERT,
  Benachrichtigung des Administrators der angreifenden Maschine.

Für beide Diagnosetechniken: "Sniffer mit Signaturscan" und "Zustands-Log mit Regelprüfung" werden geeignete Produkte auf dem Markt angeboten. Es ist geplant, u.a. folgende Systeme auf ihre Eignung für einen Einsatz im IZ zu überprüfen:

(Produktbeschreibungen unter Verwendung von Texten der Anbieter aus dem Internet.)

"Sniffer mit Signaturscan" u.a.:
RealSecure der Firma IIS

RealSecure Network Sensor runs on a dedicated system that monitors network traffic for attack signatures – definitive identifiers that an intrusion is underway. Attack recognition, incident response, and intrusion prevention occur immediately, with full customization of signatures and response capabilities.

RealSecure Workgroup Manager provides centralized, scalable management, configuration, reporting, and real-time alarming for all RealSecure Sensors. The Workgroup Manager is based on a three-tiered architecture, and natively supports an enterprise database, MSDE or Microsoft SQL.

Automatic product updates. Self-installing *X-Press Update*™ product enhancements for RealSecure's attack signature database and program code ensure that the latest network security information is available and active. In addition, RealSecure sensors are remotely upgradeable, including full release updates.

RealSecure erzeugt bei Identifizierung eines signifikanten Datenblocks einen spezifischen Alert, mit dem sowohl automatische Aktionen gestartet als auch Meldungen (z.B. per e-Mail) gesendet werden können.

"Zustands-Log mit Regelprüfung" u.a.:
Kane Secure Enterprise der Firma Intrusion.Com

Audit events provide extensive data for both security and system administration. These events come from logs accumulated by the system being monitored, or directly from the system being monitored on an event-byevent basis. KSE standardizes the format of events into a *Virtual Record* (VR). The VR is forwarded to the KSE Manager's Analysis Engine. The Analysis Engine uses a sophisticated expert system to detect attack signatures by employing parsing and pattern matching techniques. The audit events and derived events are inserted into the KSE Database. The KSE Console is used for Security Administration, Reporting and Analysis.

The KSE 4.0.4 software product performs analyses of computer system audit data and ancillary data. During this process, it

- discovers security relevant events that may be evidence of attacks against information stored on, processed on, or transmitted by computers.
- gathers and processes audit log information from many platforms in a timely manner, and presents it in an organized, easy-to-use format.

The goal of KSE is to provide the capability to process a wide range of data in an effective manner.
KSE has the following four main components:

- Database
- Manager
- Console
- Agents

Eine allgemeine Form der Technik "Zustands-Log mit Regelprüfung" bieten zentralisierte Event-Monitore, u.a.:

Microsoft Operations Manager (MOM)

Microsoft Operations Manager 2000 delivers enterprise-class operations management by providing comprehensive event management, proactive monitoring and alerting, reporting, and trend analysis. The Application Management Pack—the extensive product support knowledge base included in Microsoft Operations Manager—is the key to helping reduce the day-to-day support costs associated with running applications and services in a Microsoft Windows®–based IT infrastructure. As a key part of any successful Windows 2000 Server or Microsoft .NET Enterprise Server deployment, Microsoft Operations Manager 2000 management packs provide the operational knowledge necessary to keep mission-critical applications and systems running smoothly.

MOM ist die Weiterentwicklung eines Vorläuferproduktes der Firma NetIQ. Microsoft liefert als vorgefertigte Regelsätze "management pack modules" für einen großen Bereich von Diensten (u.a. IIS, Exchange) und Überwachungsaufgaben, u.a. auch ein Paket zur Integration der Alerts des "sniffer"-Systems RealSecure.

3.4.3 Abwägung, Empfehlung

Die organisatorischen und technischen Vor- und Nachteile der Schutz-Optionen

- Firewall mit Filterliste
- DMZ
- Firewall mit Adresskonvertierung
- Intrusion Detection

müssen unter den Gesichtspunkten

- organisatorische Erfordernisse
- Bedrohungspotential, Sicherheitsrisiken
- Organisatorischer, technischer Aufwand

beurteilt und gegeneinander abgewogen werden.

3.4.3.1 Organisatorische Erfordernisse:

In Bonn haben von den rund 150 Netzknoten rund 45 Serverfunktionen. Rund 20 Server - überwiegend Projekt-Server - müssen aus dem Internet über unterschiedliche Ports zugänglich sein.

Anzahl, Einrichtung, Konfiguration und Pflege vor allem der Projekt-Server ist hochgradig dynamisch und erfordert den ungehinderten physischen und DV-technischen Zugriff der Projekt-Mitarbeiter auf ihre Server einschließlich der LAN-Kommunikation zwischen den Projekt-Arbeitsplätzen und den Servern auf Administrator-Ebene.

Die Server kommunizieren über vielfältige Protokolle und Ports miteinander, sowohl DV-organisatorisch (z.B. Active Directory Replikationen), als auch fachlich (z.B. Datentransfer Backup, Datentransfer zwischen den Datenbanken).

Die Arbeitsplätze kommunizieren mit allen Servern über vielfältige Protokolle und Ports.

Die Arbeitsplätze benötigen aus prinzipiellen Gründen zur Erledigung der Fachaufgaben einen unbehinderten Zugriff auf das Internet. Zwar lassen sich im Einzelfall die Zugriffsanforderungen aufgabenbezogen eingrenzen, die Summe der Anforderungen umfasst aber das komplette Zugriffsspektrum und

die Arbeitsplätze lassen sich - wegen der IP-Adressvergabe per DHCP - nicht ausreichend scharf aufgabenbezogen identifizieren.

Fazit:

Die technische Isolierung der Server mit Internet-Zugang von den übrigen Netzknoten im Sinne einer DMZ ist organisatorisch nicht ohne erhebliche Arbeitsbehinderungen realisierbar.

Wegen der organisatorisch erforderlichen, TCP/IP-technisch nahezu unbehinderten Kommunikation zwischen den Netzknoten innerhalb des lokalen Netzes ist es auf der Ebene des TCP/IP-Protokolls praktisch nicht zu verhindern, dass sich geeignete automatisierte Angriffsroutinen innerhalb des Netzes ausbreiten und aus dem lokalen Netz auf das Internet zurückwirken. Die Verhinderung solcher Angriffe erfordert Abwehrmaßnahmen auf systemtechnischer Ebene (Kontrolle der aktiven Dienste, Port-Überwachung etc.) und im Bereich der Inhaltskontrolle (Virenprüfung. Intrusion Detection etc.).

3.4.3.2 Bedrohungspotential, Sicherheitsrisiken:

Nach dem Stand der bekannten Hacker- und Viren/Würmer/Trojaner-Strategien ergibt sich folgendes Bedrohungspotential:

- Reguläre Dienste (z.B. E-Mail oder FTP) werden von externen Benutzern für nicht-IZ-dienstliche Zwecke genutzt, z.B.
    - Verteilen von Spam-Mail über die E-Mail-Server des IZ,
    - Missbrauch des FTP-Dienstes als Relay für die Verteilung von Software.
    - Vortäuschung von offiziellen IZ-E-Mail-Adressen als Absender von Spam-Mail.
- Infizierte Dateien werden automatisch vorwiegend über E-Mail (aber auch über andere Download-Quellen) publiziert, i.d.R. mit einer oder mehreren der folgenden Wirkungen:
    - Die infizierte Datei versucht sich mit Hilfe der lokal verfügbaren E-Mail-Adressbücher an weitere Adressaten zu versenden.
    - Die infizierte Datei erzeugt bei Aktivierung Schäden an den ihr zugänglichen Ressourcen.

  - Die infizierte Datei verwendet bei Aktivierung den Wirt-PC als Host für die Verbreitung innerhalb des lokalen Netzes und/oder für Angriffe auf andere Internet-Ziele.

- Hacker suchen - i.d.R. mit Hilfe von Scan-Automaten - über das Internet nach DV-Systemen mit den für den geplanten Angriff benötigten offenen Internet-Ports und speziellen für diesen Angriff erforderlichen "Sicherheitslöchern" der installierten Software. Werden zusätzlich Authentifizierungs-Informationen benötigt, so wird versucht, diese mit Hilfe automatisierter "Schlüssel-Hacker" zu bestimmen. Bei einem erfolgreichen Einbruch in das DV-System werden Programme an geeigneter Stelle in das System importiert oder vorhandene Programme/Dateien modifiziert und deren Aktivierung initialisiert. i.d.R. mit einer oder mehreren der folgenden Wirkungen:

  - Das implantierte Verfahren arbeitet automatisch und erzeugt bei Aktivierung Schäden an den ihm zugänglichen Ressourcen.

  - Das implantierte Verfahren arbeitet automatisch und verwendet bei Aktivierung den Wirt-PC als Host für die Verbreitung innerhalb des lokalen Netzes und/oder für Angriffe auf andere Internet-Ziele.

  - Das implantierte Verfahren öffnet bei Aktivierung einen Input-Port auf dem Wirt-PC um dann vom Verursacher über das Internet ferngesteuert zu werden, i.d.R., um gezielt die o.g. Wirkungen zu erzeugen.

- Hacker nutzen eine reguläre, für die Systemadministration vorgesehene Schnittstelle (z.B. RAS, Telnet, SSH, FTP) für den Zugang zum lokalen Netz und häufig auf "konventionellem" Wege beschaffte Authentifizierungsinformationen zur Manipulation.

D.h., es bestehen folgende Sicherheitsrisiken, für die jeweils die zugehörigen technisch möglichen Gegenmaßnahmen aufgelistet werden:

- Missbrauch von E-Mail- oder FTP-Diensten:
  Gegenmaßnahmen:
  - Abschalten der E-Mail-Relay-Funktion,
  - Einschränkung der Zugriffsrechte für anonymen FTP,

  - Reduzieren der über das Internet erreichbaren SMTP- und FTP-Ports (u.a. durch Firewall-Filterlisten oder durch Frontend / Relay-Systeme) auf das organisatorisch erforderliche Minimum,
  - gegen die missbräuchliche Nutzung fremder E-Mail-Absender-Adressen ist keine Gegenmaßnahme bekannt.

- Schädliche Dateien gelangen über E-Mail, Download oder andere Dateiimport-Methoden auf einen Netzknoten und werden dort aktiviert.
  Gegenmaßnahmen:
  - zentrale und dezentrale Virusprüfung eingehender E-Mail und sonstiger Datei-Importe,
  - zentrale Frontend / Relay-Systeme für den Datenaustausch mit dem Internet mit umfangreicher Virus-Prüfung.

- Schädliche Dateien werden über offene Ports und "Sicherheitslöcher" aktiver Dienste über das Internet auf Netzknoten implantiert und aktiviert.
  Gegenmaßnahmen:
  - Deaktivieren von nicht zwingend erforderlichen offenen Ports,
  - Filterliste des Firewalls reduziert die zugänglichen Ports,
  - Schließen bekannter "Sicherheitslöcher" erforderlicher öffentlicher Dienste,
  - da die bei "Port-Hacking" importierten oder modifizierten Dateien i.d.R. keine Viren enthalten, sind Virusprüfungen unwirksam,
  - Intrusion Detection Systeme, sowohl "Sniffer mit Signaturscan" als auch "Zustands-Log mit Regelprüfung", hierbei sollen Verfahrens-Muster automatisierter Hacker-Routinen erkannt und, wenn möglich, blockiert werden.
  - die Verschärfung interner Regeln zur Verschleierung von Authentifizierungsinformationen (häufiger Passwortwechsel etc.) hat sich wegen der hochwirksamen automatischen "Schlüssel-Hacker" als vergleichsweise wenig wirksam erwiesen.

- Authentisierungsinformationen werden "konventionell" oder durch "Abhören" des Verkehrs über das Internet ausgeforscht und missbraucht.
  Gegenmaßnahmen:
  - Für den Datenverkehr zwischen den LANs in Bonn und Berlin: Einrichtung eines VPN,
  - organisatorische Regelungen zur Sicherung der Vertraulichkeit, u.a. keine Passwortübermittlung per E-Mail.

  - wenige, einheitliche, im lokalen Kontext "sprechende" Passworte sind vermutlich sicherer als viele, verschiedene, komplexe Passworte, da schriftliche Passwort-Listen ein Sicherheitsrisiko darstellen.

- "Infektionen" auf einem Netzknoten breiten sich auf andere Knoten des lokalen Netzes aus und werden (auch) von dort aus aktiv.
  Gegenmaßnahmen:
  - Minimieren der offenen Ports pro Netzknoten,
  - ständig mitlaufende Virusprüfungen auf allen Netzknoten,
  - systematische Kontrolle offener Ports, aktiver Dienste und entsprechender Zustandsveränderungen auf allen gefährdeten Systemen, z.B. durch Intrusion Detection Systeme vom Typ "Zustands-Log mit Regelprüfung",
  - Intrusion Detection Systeme vom Typ "Sniffer mit Signaturscan" und Überwachung des Datenverkehrs auf dem gesamten LAN (technische Probleme bei Switch-Hubs).

3.4.3.3 Zusammenfassung, Empfehlungen

Aus dem gesagten ergibt sich für die spezielle Situation des IZ:

- Die Isolierung der "Internet-Server" von den übrigen Netzknoten im Sinne des DMZ-Konzeptes ist aus den dargestellten organisatorischen Gründen mit angemessenem Aufwand nicht realisierbar.

- Die Adresskonvertierung im Sinne des Konzeptes "Firewall mit Adresskonvertierung" zu Schutz der Netzknoten vor unbefugtem Zugriff aus dem Internet ist wenig wirksam, da
  - zu viele Netzknoten einen publizierten Kanal zum Internet benötigen und damit potenziell angreifbar sind,
  - die Ausbreitung von "Infektionen" innerhalb des Netzes nicht behindert wird.

- Es verbleiben folgende Handlungsoptionen:
  - Einrichtung eines VPN zwischen Bonn und Berlin zur Sicherung des IZ-internen Datenverkehrs gegen "Abhören",
  - zentral gepflegte, systematisch aktualisierte und ständig mitlaufende Virusprüfung auf allen Netzknoten, vor allem auf den E-Mail-Servern.

- zentral gepflegte Adress- und Port-Filterlisten auf den Firewalls, um den Umfang der aus dem Internet zugänglichen offenen Ports zu kontrollieren und zu minimieren. Parallel hierzu kontrollierte Deaktivierung nicht-benötigter Ports auf allen Netzknoten und Vermeidung der Aktivierung empfindlicher Dienste (Telnet u.ä.).
- Frontend/Proxy-Systeme für besonders gefährdete Dienste, u.a.:
  - E-Mail (SMTP)-Frontend,
  - DNS-Frontend
  - WWW-Proxy.

  E-Mail- und DNS-Frontend haben die Aufgabe, die internen produktiven Dienste vor dem unmittelbaren Zugriff von Hackern zu schützen. Eine noch offene Frage bei Einsatz eines E-Mail-Frontend ist die Realisierung von E-Mail-Client-Zugriffen über das Internet ohne direkten Zugang zum "verdeckten" produktiven E-Mail-Server.

  Ein WWW-Proxy bietet einen graduell besseren Schutz der Arbeitsplätze insbesondere vor Viren etc., ist aber aus den o.g. organisatorischen Gründen kein Weg zur Vermeidung unmittelbarer Internet-Durchgriffe der Arbeitsplätze.
- Installation von Intrusion Detection Systemen, sowohl "Sniffer mit Signaturscan" als auch "Zustands-Log mit Regelprüfung". Diese Technik ist die einzige, welche für die besonders gefährdeten öffentlichen Internet-Dienste einen - wenn auch beschränkten - zusätzlichen Schutz bietet.

Fazit und Empfehlung:

- Das aktuell eingesetzte Verfahren "Firewall mit Filterliste" ist eine brauchbare "erste Verteidigungslinie" gegen unbefugten Zugriff auf die IT-Ressourcen des IZ. Es muss darauf geachtet werden, dass die Filter-Politik des IZ nicht durch individuelle Port-Öffnungen für einzelne Arbeitsplätze oder Projekt-Server durchlöchert wird.

- Das aktuell eingesetzte mehrstufige Verfahren von NAI/McAfee zum Schutz gegen Viren (GroupShield auf den Mail-Servern, VShield auf allen Arbeitsplätzen, NetShield auf allen Servern) und dessen Update-Technik hat sich bewährt (im Zeitraum 2.1.02-15.5.02 wurden von GroupShield 246 Viren in eingehenden E-Mails identifiziert und ge-

löscht, im gleichen Zeitraum wurde kein Virenangriff auf einen Arbeitsplatz oder Server festgestellt).

- Die aktuell eingesetzte Frontend-Technik für E-Mail/SMTP und DNS wird hinsichtlich ihres Nutzens überprüft und ggf. mit aktualisierter Software fortgeführt.

- Aufwand und Nutzen der Einführung eines WWW-Proxy-Dienstes wird geprüft.

- Der Stand der Technik sowie Aufwand und Nutzen von Intrusion Detection Systemen wird geprüft. Nach dem Stand der vorliegenden Informationen müssen zwei Techniken untersucht werden:
  - "Sniffer mit Signaturscan", z.B. RealSecure, im Ethernetsegment des Internet-Routers,
  - "Zustands-Log mit Regelprüfung", z.B. MOM, sowohl zur Aufdeckung von Missbrauch als auch zur allgemeinen, zentralen Betriebsüberwachung.

- Es sind organisatorische und technische Verfahren zur systematischen Überwachung der aktiven Ports und Dienste auf allen Netzknoten zu evaluieren und einzuführen.

3.5 Datensicherung, Störungs- und Desaster-Management

3.5.1 Backup, Desaster-Management

3.5.1.1 Backup-Server und Backup-Checkliste

Die Datensicherung der Server des IZ erfolgt grundsätzlich auf die Platten von Backup-Servern. Diese Technik hat gegenüber der Datensicherung auf Bänder den Vorteil, vollständig und ohne Medienwechsel automatisierbar zu sein.

Das IZ Bonn verfügt - Stand Mitte 2002 - über eine Gruppe von 4 Backup-Servern (Windows 2000) mit je 8 Datenplatten als RAID-5-Strip, pro Server rund 0,5 TB Speicherplatz, zusammen rund 2 TB Backup-Speicherplatz. Die Server-Gruppe ist außerhalb des Rechnerraumes in einem geschlossenen Kellerraum des Gebäudes USV-gesichert aufgestellt.

Den Backup-Servern sind jeweils die Sicherungen bestimmter Produktions-Server zugeordnet, Stand Mitte 2002 Bonn:

- Backup01: Server21, Server22
- Backup02: Server20, Server23
- Backup03: DC-Server, Exchange, Datenbank-Server,
- Backup04: Projekt-Server, Sonstige Server.

Das Desaster-Management - die Vorsorge gegen den Totalausfall von Servern als Folge von Einbruch, Feuer, sonstigen Zerstörungen in den Rechnerräumen - wird grundsätzlich auf die Rekonstruierbarkeit produktionsrelevanter Daten beschränkt. Nach Abschätzung der Wahrscheinlichkeiten für das Eintreffen der unterschiedlichen Risiko-Szenarien wird darauf verzichtet, "Ersatzrechenzentren" vorzuhalten.

Am Standort Bonn wird die Vorsorge auf Schäden im zentralen Rechnerraum des IZ beschränkt. Für Schäden über mehrere Stockwerke des Gebäudes (z.B. Brand) und Ausfall der Backup-Server kann auf Grund des Datenvolumens nur für ausgewählte Datenbereiche mit Hilfe wöchentlich oder monatlich erstellter Abzüge auf Bandkassetten und deren Lagerung in einem feuersicheren Safe Vorsorge getroffen werden.

Das Desaster-Management für den Standort Berlin schließt wegen fehlender räumlicher Voraussetzungen bei einer Zerstörung des dortigen Rechnerraumes die Rekonstruktion der betroffenen Daten aus.

Eine systematische und zeitnahe Remote-Datensicherung auf die Backup-Server des jeweiligen anderen Standortes ist wegen des großen Datenvolumens nach dem Stand der Technik nicht realisierbar.

Bei größeren Katastrophen, z.B. Schaden an den Gebäuden in Bonn oder Berlin mit Verlust der dortigen Infrastruktur, müssen die Produktionsdatenbanken aus den Replikaten der Datenbanken sowohl an den anderen Standorten als auch bei den Produkt-Partnern (GBI etc.) oder aus elektronischen Produkten (z.B. CD-ROM) wieder hergestellt werden.

Für Backup und Restore aller produktiven Server des IZ wird eine Backup-Checkliste mit den erforderlichen Maßnahmen, Kontrollen und Zeitplänen sowie den hierfür verantwortlichen Personen erstellt.

Die folgenden Abschnitte beschreiben in Stichworten die Backup-Maßnahmen der zentralen Servergruppen:

3.5.1.2 Backup der Domänencontroller

Alle Server sind mit Spiegelplatten mindestens für die Systemplatten ausgestattet. Beim Ausfall einer Festplatte übernimmt die zweite Festplatte ohne Verzug den Betrieb und stellt damit die Funktionsfähigkeit des Servers sicher. Nach dem Defekt einer Platte muss diese ausgetauscht und der Spiegelsatz wieder hergestellt werden. Daher ist eine regelmäßige Kontrolle des Zustandes des Spiegelsatzes wichtig, um den Betrieb nicht durch einen weiteren Ausfall zu gefährden.

Die Systempartitionen aller Domänencontroller aller Domänen des Active Directory sollten mindestens einmal pro Woche über das Tool Ntbackup.exe gesichert werden. Diese Sicherung kann in eine lokale Datei erfolgen, die dann ihrerseits auf die Backupserver gesichert wird. Um einen Domaincontroller nach einem Ausfall wieder herzustellen, wird eine Windows 2000 Standardinstallation durchgeführt und anschließend über NTBackup.exe der Systemstatus wieder hergestellt.

Da auf den Domänencontrollern keine Nutzdaten liegen, ist keine Sicherung von Nutzdaten erforderlich.

3.5.1.3 Backup der Fileserver

Die Fileserver des IZ besitzen für die Nutzdaten eine gespiegelte RAID-1 Konfiguration. Dadurch sind die Daten während des Betriebes bestmöglich gegen Ausfall einer Platte geschützt.

Die Fileserver des IZ werden täglich auf die Backupserver gesichert. Dabei wird initial eine vollständige Sicherung der Datenbestände durchgeführt. Anschließend werden nur veränderte Dateien auf die Backupserver kopiert.

Die Datensicherung erfolgt mit Hilfe von XCOPY durch Replizierung der kompletten Datenstruktur. Auf dem Quell-Server gelöschte Dateien bleiben auf dem Backup-Server erhalten. Hierdurch wird es möglich, versehentlich gelöschte oder z.B. durch Viren zerstörte Dateien mit geringem Aufwand wieder herzustellen. Diese Funktion hat sich in den vergangenen Jahren als der Hauptnutzen des Backup-Verfahrens bewährt.

Die Steuerung und Überwachung des Backups der Fileserver erfolgt durch Prozedur-Skripte.

3.5.1.4 Backup von Exchange 2000

Der Exchange-Dienst verfügt über folgende Basis-Sicherungen:

- Die Platten-Konfiguration des Servers ist vollständig RAID-1 gesichert.
- Versehentlich oder absichtlich gelöschte Postfächer werden Software-gesteuert zunächst für einen konfigurierbaren Zeitraum (z.B. 30 Tage) deaktiviert und können in diesem Zeitraum erneut aktiviert oder einem anderen/neuen User zugewiesen werden. Nach Ablauf der Sperrfrist werden die deaktivierten Postfächer entgültig entfernt.

Für die Sicherung der Exchange-Daten stehen zwei Methoden zur Verfügung:

- Mit dem Exchange-Dienstprogramm EXMERGE werden die einzelnen Postfächer der Benutzer in separate PST-Dateien gesichert, die dann auch einzeln sowohl auf den Arbeitsplätzen als auch auf dem Server wieder hergestellt werden können.
- Mit dem Windows-Dienstprogramm NTBACKUP werden sowohl die Exchange-Datenbanken als auch die Systemumgebung paketweise gesichert. Mit NTBACKUP gesicherte Exchange-Datenbanken können nur komplett inkl. aller im Sicherungspaket enthaltenen Postfächer wieder hergestellt werden. Dies ist - Stand 2002 - die aktuell eingesetzte Sicherungs-Methode im IZ.

Die Wiederherstellung eines defekten Exchange-Servers ist wegen der hohen Integration in die Active Directory Struktur ein aufwendiger Vorgang, der von Microsoft in speziellen Dokumenten beschrieben wird (s. ergänzende Dokumentation des IZ).

Die zukünftige Backup-Strategie für die Exchange-Server wird unter Berücksichtigung der Problem-Risiken voraussichtlich aus folgenden Komponenten bestehen:

- Regelmäßige, z.B. wöchentliche, Vollsicherung mit NTBACKUP in getrennten Paketen für die Systemumgebung und die Datenbanken.
- Tägliche Sicherung aller Postfächer mit EXMERGE, ggf. in mehreren Versionen, z.B. pro Wochentag.

3.5.1.5 Backup sonstiger Server

Für die sonstigen Server ist es i.d.R. ausreichend, je nach Änderungsintensität der Nutzdaten in regelmäßigen Abständen - z.B. wöchentlich - Systemumgebung und Nutzdaten mit NTBACKUP zu sichern.

Bei den Oracle-Datenbank-Servern erfolgt zusätzlich - abhängig von der Änderungsintensität eine tägliche oder wöchentliche Datenbank-Sicherung mit Oracle-Tools.

Die Sicherungs-Strategie für die Projekt-Server wird von den Projekt-Verantwortlichen abhängig von den Server-Daten definiert.

3.5.2 Behebung von Störungen

3.5.2.1 Hardwareprobleme bei PC-Servern

Alle PC-Server der gleichen "Beschaffungsgeneration" bestehen einheitlich aus folgenden identischen Komponenten:

- Prozessorturm:
  2 SCSI-Adapter mit externem Ausgang
  je einer Platte auf Wechselrahmen pro SCSI-Adapter
  FD- und CD-ROM-Laufwerk,

- Plattenturm:
  mit bis zu 4 SCSI-Platten auf Wechselrahmen in Reihe.

Die aktuell 2002 eingesetzten Platten haben eine Kapazität von 36 oder 72 GB.

Ein Server mit geringem Plattenplatzbedarf besteht aus dem Prozessorturm mit den beiden Platten (Software-RAID-1).

Ein Fileserver besteht aus einem Prozessorturm und 2 Plattentürmen (Software-RAID-1).

Die Backupserver bestehen aus einem Prozessorturm und 2 Plattentürmen (Plattentürme als gemeinsamer RAID-5-Strip).

Bei hardwaretechnischen Problemen werden der mutmaßlich defekte Prozessorturm (ohne die Wechselplatten), der Plattenturm (ohne die Wechselplatten) oder die Platte gegen ein Ersatzgerät aus dem Ersatzteillager ausge-

tauscht. Die Lauffähigkeit eines defekten Servers kann mit diesem Verfahren i.d.R. innerhalb von 60 Minuten wieder hergestellt werden.

Mutmaßlich defekte Serverkomponenten werden anschließend zunächst durch eigenes Personal überprüft und anschließend bei Bedarf an eine Servicefirma übergeben.

3.5.2.2 Problembeseitigung bei PC-Arbeitsplätzen

Alle PC-Arbeitsplätze der gleichen "Beschaffungsgeneration" sind technisch identisch.

Die Standard-Softwareinstallation sowohl des Betriebssystems als auch der Standard-Anwendungssoftware erfolgt über ein einheitliches zentral vorproduziertes Image (Powerquest DriveImage) mit anschließendem Sysprep. Der PC wird zur Installation mit einer speziellen Boot-FD gestartet, mit dem LAN verbunden und das Image wird von einem LAN-Server geladen. Zusätzliche Software wird zentral per WinInstall vorkonfiguriert und kann bei Bedarf auf die Arbeitsplätze kopiert werden.

Bei einem mutmaßlich hardwaretechnischen Problem mit einem PC-Arbeitsplatz wird der PC komplett gegen ein Ersatzgerät ausgetauscht und eine Standard-Softwareinstallation vorgenommen.

Es wird geprüft, zukünftige Arbeitsplätze mit Wechselplatten auszustatten, um bei Hardwareproblemen die Austauschgeräte ohne erneute Softwareinstallation in Betrieb nehmen zu können.

Bei mutmaßlich softwaretechnischen Problemen wird das Image reinstalliert und eine Standard-Softwareinstallation durchgeführt.

Dieses Verfahren setzt voraus, dass alle Anwendungsdaten prinzipiell auf LAN-Servern gehalten werden, dass sich auf den lokalen Platten der Arbeitsplätze nur System- und Anwendungssoftware befindet und dass diese Software mit geringem organisatorischem Aufwand rekonstruiert werden kann.

Zur Vereinfachung der Rekonstruktion wird geprüft, in welchem Umfang lokale Profile von Betriebssystem und Anwendungen auf zentralen Servern gehalten werden können, um sie dort entweder direkt zu nutzen oder sie von dort bei Anmeldung eines Arbeitsplatzes zu laden.

Eine weitere Rekonstruktionsmethode für Arbeitsplätze unter Windows 2000 besteht darin, die Originalplatte mit NTBACKUP zu sichern, auf dem Aus-

tausch-PC eine Basis-Installation von Windows 2000 durchzuführen und anschließend die Originaldaten mit NTBACKUP zu importieren. Hierdurch werden alle Benutzerdaten und -Einstellungen auf dem Austausch-PC rekonstruiert. Der Reiz dieses Verfahrens besteht u.a. darin, dass Original-PC und Austausch-PC nicht mehr technisch identisch sein müssen, da die Hardware-relevanten Treiber durch die initiale Windows-Installation bereitgestellt werden. Das Verfahren eignet sich deshalb u.a. für den Austausch alter Arbeitsplatz-Hardware gegen technisch aktuelle unter Beibehaltung der individuellen Software-Installation auf dem Arbeitsplatz.

3.6 Access- und Change-Management

Aus dem Einsatz von Windows 2000 Active Directory und Windows 2000 Prof. ergeben sich für das Access- und Changemanagement zusätzliche Optionen in Ergänzung zu den in Kap. 2.6 dargestellten Verfahren.

Folgende Funktionskomplexe des Betriebssystems Windows 2000 sind von besonderem Interesse:

- IntelliMirror,
- Gruppenrichtlinien

(Die Texte zu IntelliMirror und Gruppenrichtlinien wurden in Teilen der Hilfe-Funktion von Windows 2000 entnommen).

IntelliMirror:

IntelliMirror ist eine in Windows 2000 enthaltene Gruppe von leistungsfähigen Funktionen für die Verwaltung von Änderungen an Desktop und Konfiguration.

- Verwaltung der Benutzerdaten:
  Unterstützt das Spiegeln von Benutzerdaten auf dem Netzwerk sowie das Anfertigen lokaler Kopien von ausgewählten Netzwerkdaten.

- Installieren und Warten von Software:
  Ermöglicht die zentrale Verwaltung der Installation, der Wartung, der Aktualisierung und der Entfernung von Software durch die Administratoren.

- Verwaltung der Benutzereinstellungen:
  Ermöglicht die zentrale Definition von Einstellungen für die Arbeits-

umgebung von Benutzern und Computern durch die Administratoren. Umfasst außerdem das Spiegeln der Benutzereinstellungen auf dem Netzwerk.

- Remoteinstallationsdienste:
  Vereinfacht die Einrichtung und die Konfiguration. Ermöglicht außerdem die Remoteinstallation auf Computern im gesamten Unternehmen.

Die zentrale (und für die Nutzung im IZ interessante) Funktion von IntelliMirror ist die Spiegelung und Synchronisation von Datenbereichen auf dem Arbeitsplatz-PC mit Datenbereichen auf LAN-Servern für folgende Anwendungen:

- Offline-Verfügbarkeit von LAN-Daten:
  Dateien oder Verzeichnisse auf LAN-Servern werden auf die lokale Platte des Arbeitsplatz-PC (oder des Notebooks) kopiert, beide Versionen werden systematisch und automatisch synchronisiert. Dem Benutzer wird dieser Datenbereich auch bei offline-Betrieb präsentiert, als ob er online mit dem LAN-Server verbunden wäre. Die Synchronisation geänderter Dateien erfolgt konfigurierbar beim Anmelden oder Abmelden des Arbeitsplatzes am LAN und/oder auf Anforderung.
  Die Einrichtung und Konfigurierung erfolgt durch den Benutzer auf dem Arbeitsplatz und ist nur für diesen Arbeitsplatz-PC wirksam.

- Lokale Datenbereiche auf dem Arbeitsplatz-PC, u.a. "Eigene Dateien" können auf einen LAN-Server verschoben werden und sind dann für diesen Benutzer von beliebigen Arbeitsplätzen aus zugänglich.
  Die Einrichtung und Konfigurierung erfolgt durch den Benutzer und ist bei jeder Anmeldung des Benutzers auf einem beliebigen Arbeitsplatz-PC wirksam.

- Systemprofile und lokale Einstellungen (inkl. Outlook-Profile und Desktop-Einstellungen) können auf LAN-Servern gepuffert werden. Der Update der Serverdaten erfolgt bei Abmeldung des Benutzers. Bei Anmeldung des Benutzers auf einem beliebigen Arbeitsplatz, werden seine Serverdaten mit dem Benutzer-spezifischen Profil auf den Anmelde-Arbeitsplatz geladen.
  Die Einrichtung und Konfigurierung erfolgt durch den Systemadministrator unter Active Directory entweder individuell oder mit Hilfe von Gruppenrichtlinien (s.u.).

- Bei Anmeldung eines Benutzers wird anhand der lokalen Profile des Arbeitsplatz-PCs überprüft, ob alle diesem Benutzer zugeordneten Programme auf dem Arbeitsplatz-PC installiert sind. Bei Bedarf werden fehlende Programme automatisch nachinstalliert.
  Die Einrichtung und Konfigurierung erfolgt durch den Systemadministrator unter Active Directory entweder individuell oder mit Hilfe von Gruppenrichtlinien (s.u.), die Installations-Quellen müssen im MSI-Format vorliegen.

Gruppenrichtlinien:

Gruppenrichtlinien sind ein MMC-Snap-In (Microsoft Management Console) in Windows 2000, mit dessen Hilfe das Verhalten des Benutzerdesktops festgelegt wird. Für die Konfiguration der Desktopeinstellungen wird ein Gruppenrichtlinienobjekt verwendet, das der Administrator mit Hilfe der Gruppenrichtlinie erstellt.

Ein Gruppenrichtlinienobjekt ist eine Zusammenstellung von Einstellungen für Gruppenrichtlinien. Gruppenrichtlinienobjekte werden auf der Domänenebene gespeichert und wirken sich auf Benutzer und Computer an Standorten, in Domänen und Organisationseinheiten aus. Außerdem verfügt jeder Windows 2000-Computer über eine einzige lokal gespeicherte Gruppe von Einstellungen, die als lokales Gruppenrichtlinienobjekt bezeichnet wird.

Mit den Gruppenrichtlinieneinstellungen werden die verschiedenen Komponenten der Desktopumgebung definiert, die durch einen Systemadministrator verwaltet werden, beispielsweise die Programme, die den Benutzern zur Verfügung stehen sollen, die Programme auf dem Desktop des Benutzers und die Optionen im Menü Start.

Die Gruppenrichtlinien umfassen Einstellungen für die Benutzerkonfiguration (wirkt sich auf Benutzer aus) und die Computerkonfiguration (für Computer).

Mit den Gruppenrichtlinien und deren Erweiterungen können folgende Ausgaben ausgeführt werden:

- Verwalten der Richtlinien, die auf Registrierungseinträgen beruhen, über administrative Vorlagen:
  Bei den Gruppenrichtlinien wird eine Datei mit Registrierungseinstellungen erstellt, die in die Registrierungsdatenbank in den Teil für den Benutzer oder den lokalen Computer geschrieben werden. Benutzer-

profileinstellungen für Benutzer, die sich an einer bestimmten Arbeitsstation oder einem bestimmten Server anmelden, werden unter
HKEY_CURRENT_USER (HKCU)
in die Registrierung geschrieben, computerspezifische Einstellungen unter
HKEY_LOCAL_MACHINE (HKLM).

- Zuweisen von Skripten:
(beispielsweise für das Hoch- und Herunterfahren des Computers sowie für das An- und Abmelden).

- Umleiten von Ordnern
aus dem Ordner Dokumente und Einstellungen (auf dem lokalen Computer) an einen Netzwerkpfad.

- Verwalten von Anwendungen
(Zuweisen, Veröffentlichen, Aktualisieren, Reparieren).

- Festlegen von Sicherheitsoptionen

Die Benutzerrichtlinien (Einstellungen unter Benutzerkonfiguration in den Gruppenrichtlinien) werden beim Anmelden eines Benutzers abgerufen.

Die Einstellungen für die Computerrichtlinien befinden sich unter Computerkonfiguration; diese Richtlinien werden beim Starten des Computers abgerufen.

Benutzer und Computer sind die *einzigen* Typen von Active Directory-Objekten, die Richtlinien erhalten. Insbesondere auf die Sicherheitsgruppen werden keine Richtlinien angewandt. Stattdessen dienen die Sicherheitsgruppen aus Leistungsgründen zum Filtern der Richtlinien für die Zugriffssteuerung (ACE-Eintrag).

Die Richtlinien werden in der nachstehenden Reihenfolge angewandt:

1. Eindeutiges lokales Gruppenrichtlinienobjekt
2. Gruppenrichtlinienobjekte für den Standort, in der Reihenfolge, die vom Administrator festgelegt wurde
3. Gruppenrichtlinienobjekte für die Domäne, in der Reihenfolge, die vom Administrator festgelegt wurde

4. Gruppenrichtlinienobjekte für die Organisationseinheit, von der größten bis hinunter zur kleinsten Einheit (von der übergeordneten zur untergeordneten Einheit), in der Reihenfolge, die vom Administrator in den einzelnen Ebenen der Organisationseinheiten festgelegt wurde.

Bei Abweichungen in den Richtlinien überschreiben die Richtlinien, die zu einem späteren Zeitpunkt angewandt werden, standardmäßig die zuvor angewandten Richtlinien. Wenn keine Abweichungen in den Einstellungen auftreten, werden sowohl die zuerst angewandten Richtlinien als auch die späteren Richtlinien berücksichtigt.

Die Vererbung von Richtlinien, die im Regelfall von einem übergeordneten Standort, einer höheren Domäne oder einer Organisationseinheit übernommen würden, kann deaktiviert werden. Dies erfolgt entsprechend auf der Ebene der Standorte, der Domänen bzw. der Organisationseinheiten.

Bei Richtlinien, die im Normalfall von Richtlinien in untergeordneten Organisationseinheiten überschrieben würden, kann auf der Ebene der Gruppenrichtlinienobjekte die Einstellung Kein Vorrang festgelegt werden.

3.7 Organisatorisches Service-Konzept

Aus den als bekannt vorausgesetzten TCO-Studien (Total Cost of Ownership) (s. u.a. Vortrag von Wolf-Dieter Mell: "Kennzahlen für das IT-Personal", WGL EDV-AG, 4. - 5. Mai 2000, Halle) ergibt sich für die Organisation der IT-Service-Aufgaben (von der Planung über Installation und Betrieb bis zur Hotline) in kleinen Organisationen (weniger als 150 Mitarbeiter) folgendes Dilemma:

- TCO-Untersuchungen am Beispiel der GESIS-Institute zeigen, dass für die Erledigung der erforderlichen IT-Dienstleistungen (ohne Programmierung und unter Berücksichtigung der aktuell gegebenen technischen Ausstattung der Einrichtungen) eine Personalkapazität von rund
  1 qualifizierter IT-Mitarbeiter pro 15 Anwender
  benötigt wird.
  Bei einem Stand von ca. 90 Anwendern im IZ (Bonn und Berlin) (inkl. Hilfskräfte und Gäste) entspricht dies einem Bedarf von 6 qualifizierten IT-Mitarbeitern (ohne Programmierer-Anteile).
  De facto verfügt die Abteilung EDV/Org. - Stand 2002 - über ein Potenzial von 4,8 Mitarbeitern, von denen ein Anteil von ca. 1,8 Mitarbeitern wichtige Programmieraufgaben erledigen.

Mit der verbleibenden Personalkapazität von 3 Mitarbeitern könnten im Prinzip ca. 50% der erforderlichen IT-Dienstleistungen erbracht werden.

- Für den effektiven IT-Service wird ein breites und gleichzeitig fundiertes fachliches know-how benötigt, von der Beschaffung und Wartung der eingesetzten Hardware über Planung, Installation und Konfiguration mehrerer Betriebssysteme in einer komplexen Netzwerkumgebung, bis zu Auswahl, Einführung und Beratung umfangreicher Anwendungssoftware.
  Einschlägige IT-Kompetenz erfordert bei der gegenwärtigen dynamischen Technologie-Entwicklung Spezialisierung und kontinuierliches Training in einem pro Mitarbeiter relativ engem individuellen Kompetenz-Segment.
  Um die aktuell im IZ eingesetzte System-Konfiguration zu betreuen werden u.a. folgende Spezialkenntnisse benötigt:
  - Windows NT, Windows 2000 Active Directory,
  - Internet-Dienste (DNS, FTP, WWW etc.), Exchange 2000,
  - allgemeine und spezielle LAN-Dienste (File/Print, RAS etc.)
  - Linux, Unix, NFS, SAMBA
  - LAN-Technologie, Internet-Technologie, Router, Sicherheit,
  - Arbeitsplatz-Betriebssysteme (Windows 95 / 98 / 2000 / NT),
  - Oracle: Installation, Konfiguration, Administration,
  - MS Office Anwendungssoftware,
  - Spezielle Standard-Anwendungssoftware (Corel, Adobe etc),
  - Spezielle fachliche Anwendungssoftware (aDIS, Buchhaltung, Personal, KLR etc.),
  - PC-Hardware (Planung, Konfiguration, Installation, Wartung),
  - Telekommunikations-Technologie, Telefon/ISDN/DSL/ATM, Modems, GSM/GPRS, Handy-/PDA-Integration.

  Es ist offensichtlich, dass bereits für die genannten 12 grundlegenden Kompetenz-Bereiche sich keine vollständige qualifizierte Abdeckung mit 6 oder weniger Mitarbeitern erreichen lässt, wobei die Akquisition qualifizierten Personals durch Stellenkegel und Besoldungsregeln mit typischen Eingruppierungen für EDV-Mitarbeiter zwischen BAT V und BAT II zusätzlich erschwert wird.
  (Es wird darauf hingewiesen, dass dies kein spezielles Personalproblem des IZ, sondern ein grundsätzliches Problem kleiner Organisationen ist.)

Das IZ verfolgt zur Lösung dieser Probleme folgendes Service-Konzept:

- Die Summe der erforderlichen, durch die Abt. EDV/Org. zu erbringenden IT-Serviceleistungen wird in drei Bereiche gegliedert:
  - Planung, Koordination und Beschaffung,
  - 1st Level Support:
    Routine-Aufgaben, Helpdesk, Problemdiagnose,
    Benutzerbetreuung,
  - 2nd Level Support:
    Sonstige Service-Aufgaben, insbesondere: Expert-Support,
    zeitlich umfangreiche und fachlich komplexe Installations- und
    Konfigurationsaufgaben, Hardware-Wartung.

- Die Bereiche Planung, Koordination und Beschaffung sowie der 1st Level Support werden im Rahmen der verfügbaren fachlichen Kompetenzen und Personal-Ressourcen durch die Abteilungsleitung und die eigenen Mitarbeiter erledigt.

- Der 2nd Level Support wird entweder im Einzelauftrag oder über Service-Verträge durch externe Firmen erbracht.

- Im Einzelfall und i.d.R. nur bei FuE-Projekten wird die technische Betreuung von Software und/oder Servern den fachlich zuständigen Mitarbeitern unmittelbar übertragen, sofern diese über das erforderliche Fachwissen und das dafür notwendige Zeitbudget verfügen. Die Richtlinienkompetenz der EDV-Abteilung bleibt dadurch unberührt.

4 Migrationskonzept

4.1 Strukturkonzept

4.1.1 Eckwerte

Aus den dargestellten Zustandsdaten und Entwicklungs-Optionen ergeben sich folgende Eckwerte für die mittelfristige IT-Strukturplanung der Netze des IZ in Bonn und Berlin:

- Die grundlegende Topologie der beiden Netze wird nicht verändert:
  - Alle Netzknoten erhalten eine IP-Adresse aus dem Pool der dem jeweiligen Standort zugeordneten offiziellen C-Netze.

  - Die Kommunikation mit dem Internet erfolgt pro Standort über je einen Router/Firewall mit Filterregeln für IP-Adressen und Ports.

  - Die Kommunikation der beiden Standorte erfolgt über das Internet. Durch geeignete Filterregeln in den Firewalls erhalten beide Netze jeweils einen uneingeschränkten Durchgriff auf das andere Netz.

- Der Ansatz, die zentralen IT-Dienste durch PC-basierte LAN-Server mit einheitlicher Technologie und jeweils eigenem Server pro produktionsrelevantem Dienst zu erbringen, hat sich für das Anforderungsprofil des IZ organisatorisch und technisch bewährt und wird beibehalten. Die alternative Option, die Dienste auf wenigen zentralen Servern zusammenzufassen, wird wegen der damit verbundenen erhöhten Störanfälligkeit bei geringerer administrativer Flexibilität mittelfristig nicht weiter verfolgt.

- Beide Netze werden durch folgende Maßnahmen gegen Missbrauch und unbefugten Zugriff durch Außenstehende gesichert:

  - Geeignete organisatorische Maßnahmen zur Erhaltung der Vertraulichkeit und Verlässlichkeit von Account- und Passwort-Informationen,

  - Explizite, Account-gestütze Zugriffsregeln auf alle internen Daten,

  - Filterregeln in den Routern/Firewalls,

  - VPN (Virtuelles privates Netzwerk) mit verschlüsselter Datenübertragung zwischen den Netzen Bonn und Berlin,

  - mehrstufiger Schutz aller Server und Arbeitsplätze gegen Viren etc. durch automatischen Viren-Scan auf allen Geräten nach dem Stand der Technik und mit kurzfristig aktualisierten Viren-Signaturen,

  - Intrusion Detection der Kommunikation über die Router-Schnittstellen mit Hilfe von Systemen des Typs "Sniffer mit Signaturscan",

  - Zustandsüberwachung der Dienste und Funktionen mit Hilfe von Systemen vom Typ "Zustands-Log mit Regelüberprüfung",
  - Frontend-Technik für E-Mail/SMTP und DNS.

- Nach dem Stand der Technik bestehen Restrisiken vor allem für die Integrität der öffentlichen Internet-Dienste (DNS, WWW, FTP, E-Mail/SMTP, E-Mail/Clients, Listserver, News). Diese könnten - nach dem Stand der Technik - jeweils nur durch massive Einschränkung des Dienstumfanges reduziert werden.
  In Abwägung zwischen der weiteren Erhöhung der Netzwerksicherheit durch zusätzliche Maßnahmen einerseits und den hierdurch entstehenden Nutzungsbehinderungen andererseits werden im Interesse einer Minimierung des personellen und technischen Aufwandes für die Realisierung von Internet-Projekten verbleibende potentielle Sicherheitslücken beobachtet und - wo möglich, z.B. durch Software-Updates - reduziert, Restrisiken aber in Kauf genommen.

- Der Datentransport innerhalb der Netze erfolgt über das vorhandene Cat-5-Kabelsystem mit Ethernet 100Base-T. Die Notwendigkeit für einen Wechsel zu höheren Übertragungsraten oder Glasfaser-Verkabelung ist mittelfristig nicht absehbar. Der Einsatz Funk-basierter Datenübertragung, z.B. Bluetooth oder WLAN wird überprüft und bei Bedarf implementiert.

- Das LAN-Betriebssystem wird vollständig und einheitlich auf - mittelfristig - Windows 2000 Active Directory migriert.

- Als Arbeitsplatz-Betriebssystem wird einheitlich ab 2002 Windows Prof. eingesetzt. Entscheidungen über Migrationen auf Nachfolge-Betriebssysteme erfolgen restriktiv unter dem vorrangigen Gesichtspunkt der Einheitlichkeit nach technischen und fachlichen Erfordernissen.

- Alternative Betriebssysteme werden nur dann produktiv eingesetzt, wenn dies zur Nutzung spezieller Software oder Betriebssystemeigenschaften unumgänglich ist oder wenn die Migration eines Alt-Systems einen unverhältnismäßigen Aufwand erzeugen würde.

- Die Speicherung produktiver Daten erfolgt - nach wie vor - aus Gründen der Datensicherheit und der kooperativen Nutzung grundsätzlich auf zentralen File-Servern. Sofern dies aus Gründen der Performance

oder der offline-Nutzung erforderlich ist, können auf den Arbeitsplätzen lokale, mit den zentralen Daten synchronisierte Kopien angelegt werden.

- Zur Verbesserung des Betriebsmittel-Managements und zur Überwachung der Zustands-Daten von Diensten und Ressourcen wird ein Überwachungs-Systems vom Typ "Zustand-Log mit Regelprüfung" evaluiert und bei Erfolg implementiert.

- Zur Rationalisierung des Change-Managements werden technische Veränderungen an den Arbeitsplätzen (u.a. Wechselplatten), der Einsatz zusätzlicher Betriebssystem-Optionen (IntelliMirror / Gruppenrichtlinien: Verschiebung lokaler Profile auf LAN-Server, automatische Software-Installation etc.), alternative Verfahren der zentralen Bereitstellung von Software (z.B. ON Command CCM) etc. evaluiert und bei Erfolg implementiert.

- Die Integration der Kommunikationsdienste durch UMS (Unified Messaging Service) wird verstärkt. Hierzu werden einerseits Telefonfunktionen mit LAN-Diensten gekoppelt, andererseits die unterschiedlichen Kommunikationsfunktionen auf Basis der zentralen Plattform Exchange/Outlook zusammengefasst. Als ergänzende mobile Schnittstelle zu UMS wird neben dem Einsatz von Notebooks die Nutzung von GSM/GPRS/UMTS-Technologie (Handy) und PDAs (Personel Digital Assistant) evaluiert.

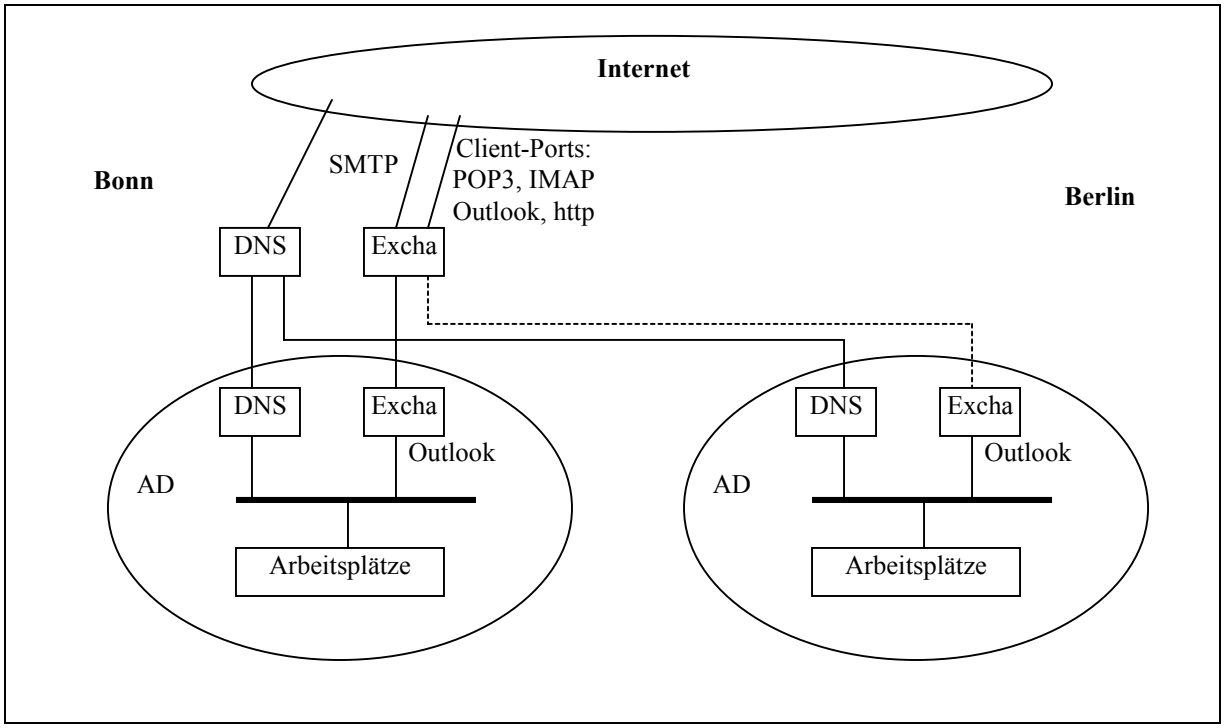
- Es werden Methoden weiterentwickelt, Zugangstechniken, Datenstrukturen und Zugriffsrichtlinien so zu organisieren, dass Mitarbeiter mit den erforderlichen Account-Informationen über öffentliche Netze - wo möglich über das Internet - auf die relevanten Teile ihrer Produktionsdaten zugreifen können, ohne dass hierdurch die Netzwerksicherheit gefährdet wird.

- Die Backup-Strukturen werden so konfiguriert, dass Produktionsdaten des gestrigen Tages auf Anwendungsebene wieder hergestellt werden können, sowohl bei inhaltlichen Problemen (defekte, gelöschte Daten), als auch bei Hardwaredefekten.
  Das Desaster-Management am Standort Bonn wird auf Schäden im zentralen Rechnerraum des IZ beschränkt. Für Schäden über mehrere Stockwerke des Gebäudes (z.B. Brand) und Ausfall der Backup-Server kann auf Grund des Datenvolumens nur für ausgewählte Datenbereiche

mit Hilfe wöchentlich oder monatlich erstellter Abzüge auf Bandkassetten und deren Lagerung in einem feuersicheren Safe Vorsorge getroffen werden.
Das Desaster-Management für den Standort Berlin schließt wegen fehlender räumlicher Voraussetzungen bei einer Zerstörung des dortigen Rechnerraumes die Rekonstruktion der betroffenen Daten aus.

4.1.2 Frontend-Struktur

Für die Internet-Dienste DNS und E-Mail werden Frontend-Server konfiguriert, um die Produktions-Server gegenüber dem Internet abzuschirmen.



1. DNS:
   - Innerhalb der Active Directory Strukturen in Bonn und Berlin gibt es einen AD-integrierten DNS-Dienst für die Zonen iz-soz.de, bonn.iz-soz.de und berlin.iz-soz.de, dieser hat keine Verbindung zum Internet und verweist für die Namensauflösung auf den zentralen Frontend-DNS.

- Der zentrale Frontend-DNS wird auf einem Server unter Windows 2000 (stand alone am Standort Bonn) konfiguriert und im Internet als zuständiger DNS-Server für die jeweiligen Zonen publiziert.
  Der Frontend-DNS ist für alle Zonen primäre Internet-Referenz, die dem IZ zugewiesen worden sind (s. Kap. 2.2.1), einschließlich der Zonen iz-soz.de, bonn.iz-soz.de und berlin.iz-soz.de.
  Der Frontend-DNS hat (aus Sicherheitserwägungen) keine Verbindung zu den AD-Servern, alle Zonen werden auf diesem Server separat manuell gepflegt. Für die Subdomänen von iz-soz.de werden nur die Hosts auf diesem Server publiziert, die aus dem Internet sichtbar sein müssen (diese Hosts müssen parallel dazu auch in die Filterlisten der Firewalls in Bonn und Berlin eingetragen werden).

2. E-Mail, Exchange:

   - Innerhalb der Active Directory Strukturen gibt es jeweils AD-integrierte Exchange-Server in Bonn und Berlin. Diese halten alle Anwendungsdaten (Postfächer, öffentlichen Ordner), haben keine Verbindung zum Internet und kommunizieren mit dem zentralen Frontend-Exchange-Server. Für den Zugriff der Arbeitsplätze wird auf diesen Servern als einziges Client-Protokoll Outklook/MAPI installert.

   - Der Frontend-E-Mail-Server wird als Exchange-Enterprise-Server unter Windows 2000 konfiguriert. Er hält keine Anwendungsdaten.
     Durch geeignete MX-Einträge in den DNS-Servern ist dieser Frontend der zentrale SMTP-Zugangspunkt für alle Domänen des IZ. Der Frontend-Exchange verteilt eingehende E-Mail auf die zuständigen Postfach-Server.
     Der Frontend-Exchange ist ebenfalls zentraler Zugangspunkt für Client-Zugriffe auf alle IZ-Postfächer aus dem Internet, vorgesehen sind die Protokolle: POP3, IMAP, POP3S, IMAPS, Outlook/MAPI, http.

   - Geplanter Standort des Frontend-Exchange ist Bonn. Sollte sich (wider Erwarten) die 2 MBit Internet-Verbindung in Bonn mittelfristig als Engpass für den E-Mail-Verkehr mit Berlin erweisen, kann entweder der Frontend-Exchange nach Berlin portiert oder dort ein zweiter Frontend-Exchange installiert werden.

4.1.3 Server und Dienste

Die folgenden Tabellen beschreiben die vorgesehene mittelfristige Server- und Dienste-Struktur:

4.1.3.1 Bonn

Dienstbereich	Anz. Server	Dienst / Server	Anmerkungen
Internet Gateway	1	Router, Firewall	CISCO, Firewall mit Filterliste
RAS	2	RAS-Server: 2*4*analog, 2*4*ISDN	analog, ISDN, GSM
Internet Frontend	1	DNS Frontend	W2k DNS, Bonner Zonen
	1	E-Mail Frontend	W2k Exchange zentral
AD Controller, s. Kap. 3.1.10	1	AD, DNS, NTP	Root1, iz-soz.de
	1	AD, DNS	Root2
	1	AD	Bonn1, bonn.iz-soz.de
	1	AD, WINS, DHCP	Bonn2
E-Mail	1	Exchange	excha3, zentraler E-Mail-Dienst Standort Bonn, 72 GB netto
File/Print	4	File-Server	je 4*72 GB netto
	2	Print-Server	"neue" und "alte", s/w, color Stockwerks-Drucker
aDIS	1	aDIS-Server	Unix Midrange-System
	1	aDIS-File-Server	Linux Samba, W2k-Schnittstelle
Datenbanken	4	Oracle SQL	SOZDB etc.
sonstige Dienste	n	CD-ROM Jukebox, Listserver, News, WAP-IIS FTP, Com-Modem Intranet	dedizierte Server für spezielle Dienste

Telefon-LAN-Integration	2	UMS, CTI	2 W2k-Server in Domäne iz-soz.de
ID / IR	3	Intrusion Detection, Leitstand	z.B. RealSecure, MOM, Netzwerk-Monitor
Projekte	n		Projekt-Server
Gäste	1	WGL-Internet	W2k, www.wgl.de
	1	AFB	Linux, www.priub.org
	1	Joe-List	W2k Listserver, www.joe-list.de
Backup	4	Backup	je 7 * 72 GB

4.1.3.2 Berlin

Dienstbereich	**Anz. Server**	**Dienst**	**Anmerkungen**
Internet Gateway	1	Router, Firewall	CISCO, Firewall mit Filterliste
RAS	1	RAS-Server: 4*analog, 4*ISDN	analog, ISDN, GSM
Internet Frontend	1	DNS Frontend	W2k DNS Berliner Zonen
AD Controller, s. Kap. 3.1.10	1	AD, DNS, WINS, DHCP	Berlin1, berlin.iz-soz.de
	1	AD, DNS	Berlin2, ggf. = DNS-Frontend
E-Mail	1	Exchange	exchabln, zentraler E-Mail-Dienst Standort Berlin, 72 GB netto
File/Print	2	File-Server	je 4*72 GB netto
	1	Print-Server	"neue" und "alte", s/w, color Stockwerks-Drucker
Datenbanken	2	Oracle SQL	SOZDB etc.

sonstige Dienste	n	CD-ROM Jukebox, Listserver, FTP, Intranet	dedizierte Server für spezielle Dienste
GESIS, Internet	3	externe WWW Server	externes Angebot
	2	interne WWW Server	Entwicklung, Statistik
ID / IR	2	Intrusion Detection, Leitstand	z.B. RealSecure, MOM, Netzwerk-Monitor
Projekte	n		Projekt-Server
Backup	1	Backup	7 * 72 GB

4.2 Aktivitäten-Liste und Zeitplan

4.2.1 Aktivitäten-Liste

Die folgende Tabelle enthält die nach Aufgabenbereichen gegliederte Liste der erforderlichen Aktivitäten und die geplanten Ziel-Termine für deren Erledigung:

		Aktivität	**Ziel-Termin**
1.		**IT-Struktur-Konzept**	
	1.1	Vorinformation, Konzeptrichtlinien, Evaluationsbeschluss	2001 Q4
	1.2	Evaluation/Revision, Erstellung des Berichtes	2002 Q2
	1.3	IT-Struktur-Konzept: Beratung, Abstimmung, Beschluss	2002 Q3
2.		**Migration LAN-Betriebssystem**	
	2.1	Test, Evaluation Windows 2000 AD	2001 Q3
	2.2	Gerätebeschaffung Server Migrationsphase 1 (Gerätetyp: "2001")	2001 Q4
	2.3	Einführung Windows 2000 AD, Parallelbetrieb NT	2002 Q1
	2.4	Gerätebeschaffung Server Migrationsphase 2 (Update Gerätetyp auf "2002", Test von Prototypen)	2002 Q3

	2.5	Umsetzung Struktur-Konzept, Feinanpassung	2002 Q3
	2.6	Gerätebeschaffung Server Migrationsphase 3	2002 Q4
3.		**Migration Arbeitsplatz-Betriebssystem**	
	3.1	Test, Evaluation Windows 2000 Prof.	2001 Q3
	3.2	W2kP: Festlegung der neuen Softwareumgebung, Einrichtung der Migrations-Tools (Image, WinInstall)	2001 Q4
	3.3	W2kP: Installation auf den neuen Notebooks	2001 Q4
	3.4	W2kP: Start und Test der Migration der Arbeitsplatz-PCs	2002 Q1
	3.5	W2kP: Abschluss der Migration der Arbeitsplatz-PCs	2002 Q4
4.		**Server-Upgrade aDIS-System**	
	4.1	neuer aDIS-Server: Planung, Upgrade-Konzept, Geräteauswahl und -beschaffung	2002 Q2
	4.2	neuer aDIS-Server Installation und Test	2002 Q3
5.		**Telefon-LAN-Integration**	
	5.1	UMS, CTI Evaluation, Herstellergespräche	2001 Q4
	5.2	UMS, CTI Entscheidung: Technik, Konfiguration, Lieferant, Beschaffung	2002 Q2
	5.3	UMS, CTI Installation	2002 Q3
6.		**Intrusion Detection Systeme, Monitoring**	
	6.1	ID/IR: Evaluation Stand der Technik, Softwaretests	2002 Q3
	6.2	ID/IR Entscheidung: Technik, Konfiguration, Lieferant, Beschaffung	2002 Q4
	6.3	ID/IR Installation, Parametrierung, Produktions-Tests	2003 Q1
7.		**Access- und Change-Management**	
	7.1	Gruppenrichtlinien, IntelliMirror: Tests	2002 Q4
	7.2	GR: Entscheidung über die zu nutzenden Optionen	2003 Q1
	7.3	GR: Detail-Konfiguration, Implementierung	2003 Q2

8.		**Austausch Arbeitsplatz-PCs**	
	8.1	Neue PC-Generation: Vorbereitung, Mengengerüst, Konfigurationsanforderungen	2002 Q4
	8.2	Test von PC-Prototypen, Einrichtung der Migrations-Tools, Entscheidung, Beschaffung	2003 Q1
	8.3	Austausch der Arbeitsplatz-PCs	2003 Q2-3

4.2.2 Zeitplan

Die folgende Tabelle enthält die nach Ziel-Termin sortierten Einzelaktivitäten:

		Aktivität	**Ziel-Termin**
	2.1	Test, Evaluation Windows 2000 AD	2001 Q3
	3.1	Test, Evaluation Windows 2000 Prof.	2001 Q3
	1.1	Vorinformation, Konzeptrichtlinien, Evaluationsbeschluss	2001 Q4
	2.2	Gerätebeschaffung Server Migrationsphase 1 (Gerätetyp: "2001")	2001 Q4
	3.2	W2kP: Festlegung der neuen Softwareumgebung, Einrichtung der Migrations-Tools (Image, WinInstall)	2001 Q4
	3.3	W2kP: Installation auf den neuen Notebooks	2001 Q4
	5.1	UMS, CTI Evaluation, Herstellergespräche	2001 Q4
	2.3	Einführung Windows 2000 AD, Parallelbetrieb NT	2002 Q1
	3.4	W2kP: Start und Test der Migration der Arbeitsplatz-PCs	2002 Q1
	1.2	Evaluation/Revision, Erstellung des Berichtes	2002 Q2
	4.1	neuer aDIS-Server: Planung, Upgrade-Konzept, Geräteauswahl und -beschaffung	2002 Q2
	5.2	UMS, CTI Entscheidung: Technik, Konfiguration, Lieferant, Beschaffung	2002 Q2
	1.3	IT-Struktur-Konzept: Beratung, Abstimmung, Beschluss	2002 Q3
	2.4	Gerätebeschaffung Server Migrationsphase 2 (Update Gerätetyp auf "2002", Test von Prototypen)	2002 Q3

	2.5	Umsetzung Struktur-Konzept, Feinanpassung	2002 Q3
	4.2	neuer aDIS-Server Installation und Test	2002 Q3
	5.3	UMS, CTI Installation	2002 Q3
	6.1	ID/IR: Evaluation Stand der Technik, Softwaretests	2002 Q3
	2.6	Gerätebeschaffung Server Migrationsphase 3	2002 Q4
	3.5	W2kP: Abschluss der Migration der Arbeitsplatz-PCs	2002 Q4
	6.2	ID/IR Entscheidung: Technik, Konfiguration, Lieferant, Beschaffung	2002 Q4
	7.1	Gruppenrichtlinien, IntelliMirror: Tests	2002 Q4
	8.1	Neue PC-Generation: Vorbereitung, Mengengerüst, Konfigurationsanforderungen	2002 Q4
	6.3	ID/IR Installation, Parametrierung, Produktions-Tests	2003 Q1
	7.2	GR: Entscheidung über die zu nutzenden Optionen	2003 Q1
	8.2	Test von PC-Prototypen, Einrichtung der Migrations-Tools, Entscheidung, Beschaffung	2003 Q1
	7.3	GR: Detail-Konfiguration, Implementierung	2003 Q2
	8.3	Austausch der Arbeitsplatz-PCs	2003 Q2-3

5 Zusammenfassung

In Vorbereitung eines geplanten routinemäßigen Serveraustausches parallel zu einer geplanten Migration des LAN-Betriebssystems auf Windows 2000 Active Directory wurde Anfang 2002 eine interne Evaluation der IT-Struktur des IZ durchgeführt mit dem Ziel, das mittelfristige Entwicklungskonzept zu überprüfen, alternative und neue Optionen zu untersuchen und zu bewerten, die Ergebnisse systematisch zu dokumentieren und hieraus ein Migrationskonzept abzuleiten. Die Untersuchungen wurden fachlich und personell durch Mitarbeiter der Beratungsfirma BOV (Essen) unterstützt.

Der vorliegende Untersuchungsbericht besteht aus 4 Teilen:

In Kapitel 1 werden, bezugnehmend auf die Aufgabenstellung der EDV, insbesondere die bestehenden mittelfristigen Grundsätze der IT-Strukturplanung des IZ auf der Grundlage des GESIS IT-Rahmenkonzeptes zusammengefasst. Diese betreffen vor allem Regeln für die einheitliche Ausstattung der Ar-

beitsplätze und Server zur Vereinfachung des Störungs- und Change-Managements.

In Kapitel 2 wird der Stand der IT-Struktur Anfang 2002 in Bonn und Berlin dokumentiert. Neben der aktuellen Topologie und der Serverstruktur werden spezielle Strukturkomponenten (u.a. das aDIS-Verfahren), sowie die bisherigen Konzepte zur Netzwerksicherheit, zur Datensicherung und Störungsbehandlung sowie zum Access- und Change-Management beschrieben.

In Kapitel 3 werden für die Kernbereiche dieser Struktur weiterführende Konzepte und Entwicklungs-Optionen untersucht und beurteilt. Im Mittelpunkt stehen dabei einerseits eine geeignete Dienste-Struktur für das LAN-Betriebssystem Windows 2000 Active Directory, eine umfassende Auseinandersetzung mit Optionen zur Erhöhung der Netzwerksicherheit (vor allem gegen unbefugten Zugriff aus dem Internet) sowie organisatorische und technische Maßnahmen zur Behandlung und Behebung von Störungen.

In Kapitel 4 werden als Folgerung aus dieser Analyse zunächst die Eckdaten der zukünftigen mittelfristigen IT-Strukturplanung und - daraus abgeleitet - die erforderliche Server- und Dienste-Struktur tabellarisch erfasst. Das Realisierungskonzept wird dann in Form einer Aktivitäten-Liste und eines Zeitplanes für die zwei Jahre vom 3. Quartal 2001 bis zum 3. Quartal 2003 zusammengestellt.