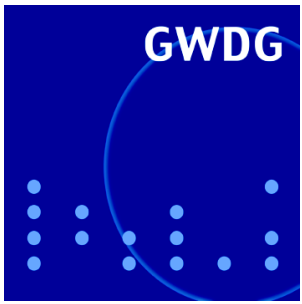


GWDG-Bericht Nr. 66

Dietmar Bussmann,
Andreas Oberreuter
(Hrsg.)

19. und 20. DV-Treffen der Max-Planck-Institute

20. - 22. November 2002
19. - 21. November 2003
in Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Dietmar Bussmann, Andreas Oberreuter (Hrsg.)

19. und 20. DV-Treffen der Max-Planck-Institute

20. - 22. November 2002
19. - 21. November 2003
in Göttingen

Dietmar Bussmann, Andreas Oberreuter (Hrsg.)

19. und 20. DV-Treffen der Max-Planck-Institute

20. - 22. November 2002
19. - 21. November 2003
in Göttingen

GWDG-Bericht Nr. 66
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg
D-37077 Göttingen
Telefon: 0551-201-1510
Telefax: 0551-21119
E-Mail: gwdg@gwdg.de

Satz: Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Druck: Offset- und Dissertationsdruck Kinzel, Göttingen-Weende

ISSN 0176-2516

Inhalt

Vorwort

In dem vorliegenden Band sind einige Beiträge des 19. und 20. DV-Treffens der Max-Planck-Institute, abgehalten bei der GWDG in Göttingen, enthalten.

Eine vollständigere (elektronische) Zusammenstellung der Vorträge findet man in dem beschriebenen IT-Portal der MPG des ersten Artikels unter „DV-Treffen der Institute“.

Das Thema Sicherheit war bei beiden DV-Treffen eine vorrangige Angelegenheit, der sich inzwischen auch die IT-Sicherheitszentrale der GWDG angenommen hat. Neben Virenschutz gehören natürlich u. a. auch ein solide Datensicherung und eine vorausschauende Langzeitarchivierung dazu, die jeweils mit einem Beitrag hier vertreten sind.

Dass wissenschaftliches Arbeiten nicht mehr ohne EDV auskommt, ist mittlerweile als allgemein bekannt vorauszusetzen. So ziehen Portale und Content-Management-Systeme ein, um die Kommunikation und Kooperation zu verbessern, aber auch EDV-Dienstleistungszentren mit entsprechendem Informationsmanagement, wie es bspw. die GWDG anbietet, gehören dazu.

Die weitaus meiste Zeit verbringt der Administrator aber immer noch in den Routineinstallationen der unzähligen Arbeitsplatzsysteme. Diesem Thema widmet sich u. a. der letzte Beitrag, der wie gesagt auch nur eine Auswahl aus dem Gesamt-Portfolio der Vorträge darstellt.

Als (Mit-)Veranstalter möchten wir einmal mehr feststellen, dass wir, wie auch schon in den letzten Jahren, eine bestens vorbereitete Tagungsumgebung nutzen konnten, welche uns die Mitarbeiter der GWDG, koordiniert durch Herrn Otto, sowie das MPI für biophysikalische Chemie mit seinen Räumlichkeiten zur Verfügung gestellt haben. Herzlichen Dank!

Für die rege Teilnahme, die vielfältigen Beiträge und fruchtbare Diskussionen von allen Teilnehmern sei ebenso gedankt. Die gleiche Resonanz wünschen wir ebenso dem Team 2004.

Bonn, Heidelberg, 19.10.2004 Andreas Oberreuter, Dietmar Bussmann

Teil 1: Beiträge vom 19. DV-Treffen

IT-Portal der MPG

Wilfried Grieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Geschichte des IT-Portals

Die Idee eines IT-Portals für die Max-Planck-Gesellschaft wurde am 15. und 16. Januar 2002 auf einem Workshop in Heidelberg geboren. Es sollte alle IT-relevanten Themen beherbergen. Von der GWDG wurde vorgeschlagen, das Portal mit Hilfe von Lotus Notes zu realisieren. Die Gründe dafür waren:

- eine schnelle Realisierung
- eine mehrjährige Erfahrung mit dem System
- eine mögliche Nutzung des Lotus-Notes-Datenbanksystems
- die automatische Generierung von WWW-Seiten aus der Datenbank heraus ohne zusätzlichen Programmieraufwand

Auf Grund dieser Tatsachen erhielt die GWDG den Auftrag, das IT-Portal mit Lotus Notes zu realisieren. Federführend für das Projekt in der Generalverwaltung ist Herr Dr. F. Zite-Ferenczy, das Lotus-Notes-Design stammt von Frau S. Greber.

Bereits Anfang Februar 2002 konnte der erste Prototyp des IT-Portals der Max-Planck-Gesellschaft online geschaltet werden.

2. URL des Portals

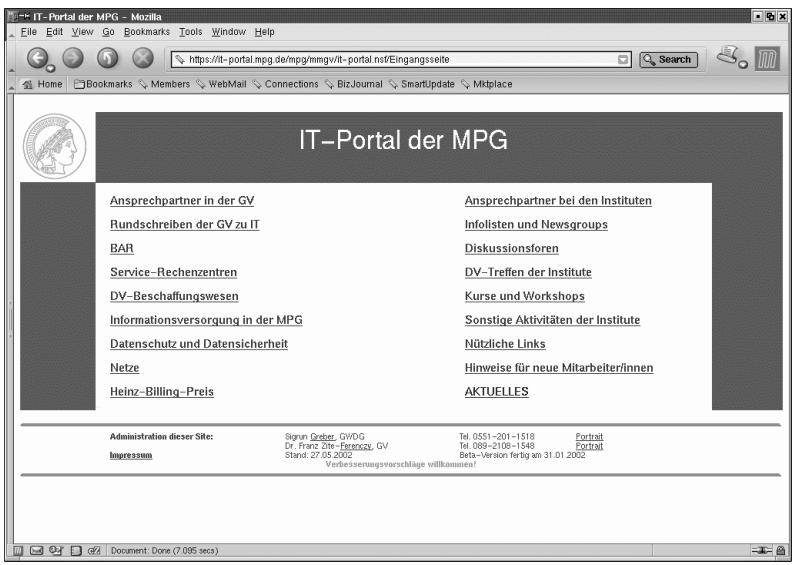
Der URL des Portals lautet:

https://it-portal.mpg.de

Der Zugang steht jedem Rechner offen, der über eine IP-Adresse aus der Max-Planck-Gesellschaft verfügt, sich also im MPG-Intranet befindet. Zusätzlich ist der Zugriff ssl-verschlüsselt, so dass die übertragenen Daten nicht abgehört werden können.

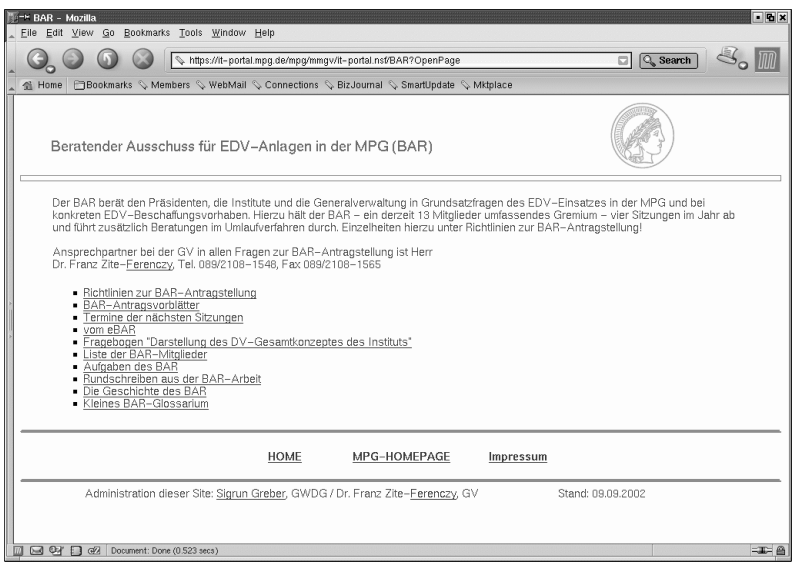
3. Zum Inhalt des Portals

Die Startseite des Portals ist gleichzeitig das Inhaltsverzeichnis:



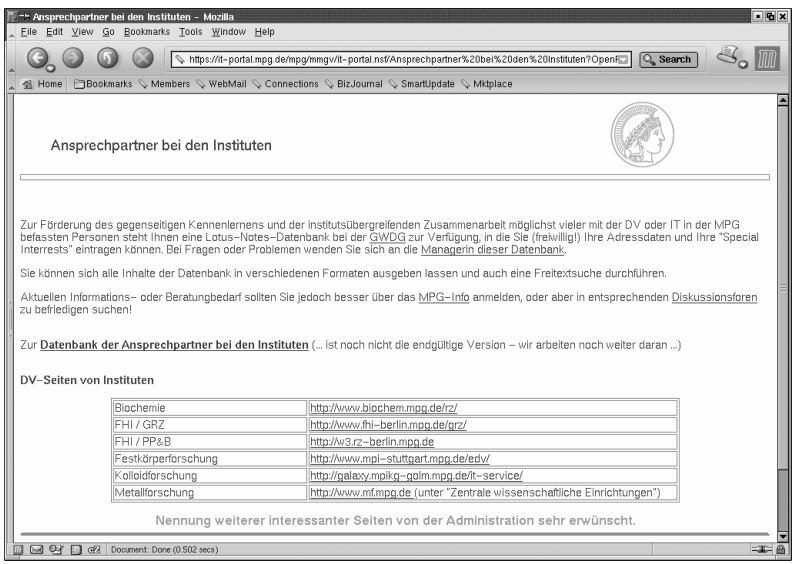
Insbesondere sind die Rundschreiben der Generalverwaltung enthalten, die den IT-Bereich betreffen:

Weiter sind im Portal die für einen Antrag beim BAR benötigten Dokumente und Hinweise enthalten:



Auch Datenschutz und Datensicherheit ist thematisiert:

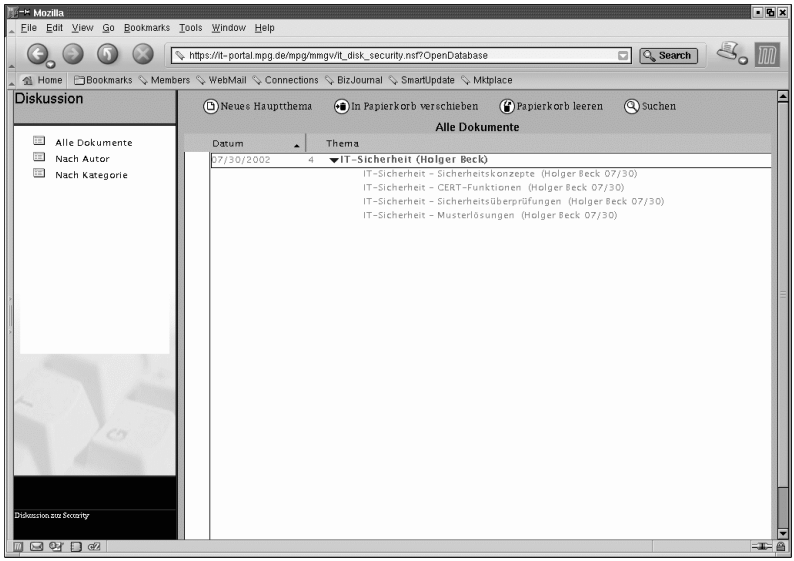
Ansprechpartner für den IT-Bereich in den einzelnen Max-Planck-Instituten können sich selber in das Portal eintragen:



Wichtig sind natürlich auch die aktuellen Ankündigungen, die von Herrn Ferenczy gepflegt werden:

Zum Informationsaustausch sind Diskussionsforen eingerichtet:

Ein Beispiel dafür ist das Forum zur IT-Security:



Die IT-Sicherheitszentrale der GWDG

Holger Beck

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Einleitung

Wie den meisten bekannt sein dürfte, hat sich der BAR bzw. die Task-Force „IT-Sicherheit“ des BAR intensiv mit dem Thema IT-Sicherheit befasst. Als ein Ergebnis hat man die GWDG gebeten, ein Konzept zu entwickeln, das als Grundlage für die Einrichtung einer MPG-weiten IT-Sicherheitszentrale dienen kann. Die GWDG hat daraufhin auf der BAR-Sitzung am 08.03.02 die erarbeiteten Vorstellungen für die Umsetzung dieses Konzeptes dargestellt. Der BAR hat dem Konzept der GWDG zugestimmt und seine volle Unterstützung zugesagt.

Die GWDG hat jetzt begonnen, die Funktionen einer IT-Sicherheitszentrale vorzubereiten und entsprechend umzusetzen. Die hier anfallenden Aufgaben sind teils theoretisch bis konzeptioneller, teils aber auch pragmatischer Art.

2. Inhaltliche Konzeption

Die GWDG plant, zunächst folgende Schwerpunkte beim Auf- bzw. Ausbau des Sicherheitsbereichs zu setzen:

2.1 IT-Sicherheitskonzepte

Ein sehr allgemeines und umfassendes Thema, bei dem die GWDG zu Prinzipien eines Sicherheitsprozesses beraten wird. Durch die vorgestellten Musterlösungen wird die Umsetzung in das jeweilige Institutsumfeld vereinfacht, allerdings ist mit Einführung und konsequenter Überwachung der festgelegten Sicherheitsrichtlinien ein nicht unerheblicher Aufwand verbunden.

2.2 CERT-Funktionen

Vernetzte Systeme werden von einer immer mehr ansteigenden Flut immer neuer Sicherheitslücken geplagt. Manche wünschen sich hier ein MPG-CERT. Die GWDG vermeidet diese Bezeichnung, denn CERTs gibt es schon einige und die GWDG kann mit den größeren Einrichtungen nicht konkurrieren, wenn man den vollen Funktionsumfang erwartet - ganz abgesehen davon, dass man das Rad ja auch nicht immer neu erfinden muss. Einige Funktionen eines CERT wird die GWDG aber übernehmen müssen und wollen.

2.3 Sicherheitsüberprüfungen

Der Wunsch nach prophylaktischen Security-Scans durch eine vertrauenswürdige Institution (z.B. GWDG) scheint bei etlichen Instituten ganz oben auf den Prioritätslisten zu stehen. Die GWDG stellt einen solchen Dienst jetzt zur Verfügung.

2.4 Musterlösungen zu Einzelproblemen

Hier gibt es Anfragen zu einigen sicherheitsrelevanten Teilbereichen. Die GWDG kann hier sicherlich nicht alles gleichzeitig auf den Weg bringen. Die Reihenfolge, in der die GWDG die vorliegenden Anfragen bearbeiten wird, soll hier noch bestimmt werden. Das lässt also noch ein bisschen Spielraum für konkrete Wünsche durch die Institute.

3. Personelle Konzeption

Die IT-Sicherheitszentrale wird zunächst von einem Kernteam getragen, zu dem einige GWDG-Mitarbeiter (Andreas Ißleiber, Bodo Gelbe, Holger Beck, Hossein Sheikhikhou und Michael Reimann) und ein Mitarbeiter aus der Max-Planck-Gesellschaft (Dietmar Bussmann) gehören.

Zusätzliche GWDG-Mitarbeiter für spezielle Aufgaben werden nach Bedarf eingesetzt. Kollegen aus der MPG oder der Universität Göttingen sind als freiwillige Mitarbeiter willkommen. Bei Bedarf ist auch der Einkauf von externem Expertenwissen vorgesehen.

Die IT-Sicherheitszentrale ist per E-Mail unter itsz@gwdg.de zu erreichen.

4. IT-Sicherheitskonzepte

Hier geht die GWDG vom Grundschutzhandbuch (GSHB) des BSI (Bundesamt für Sicherheit in der Informationstechnik) aus. Dieses ist nicht nur auf Papier erhältlich, sondern steht auch im Internet zur Verfügung (http://www.bsi.bund.de/gshb/deutsch/menue.htm).

Auf den ersten Blick mag man sich von dem (auf Papier drei Aktenordner dicken) GSHB erschlagen vorkommen. Aber letztlich ist es ein Standard, an dem man nicht vorbeikommt.

Wir sehen in diesem Ansatz wesentliche Vorteile:

- Wir können sofort mit einem umfassenden Konzept starten.
- Das Konzept stammt von einer anerkannten Autorität.
- Das GSHB steht online zur Verfügung und ist somit auch immer online aktualisiert.
- Das GSHB ist gut organisiert und strukturiert.
- Das GSHB verfolgt ein Baukastenprinzip.
- Unsere (MPG) eigenen Ergänzungen, Konkretisierungen, Musterlösungen wären zusätzliche Bausteine
- und lassen sich dann auch online mit dem GSHB verknüpfen.

Das GSHB hat nur den Anspruch, Empfehlungen für den Schutz bei „normalen“ Sicherheitsanforderungen zu geben. Das tut es allerdings recht umfassend. Bei höherem Sicherheitsbedarf müssen wir selbst darüber hinaus gehende Lösungen suchen.

Das GSHB gibt aber nicht nur Empfehlungen zu bestimmten Komponenten eines IT-Systems, sondern beginnt mit allgemeinen Überlegungen über Sicherheitskonzepte. Ein Punkt soll hier hervorgehoben werden: Sicherheit basiert auf einem Prozess. Damit ergibt sich auch eine Aufgabe für die MPG und für jedes einzelne Institut (unabhängig von, unterstützt durch und parallel zu den Arbeiten der GWDG als IT-Sicherheitszentrale):

Der IT-Sicherheitsprozess

Das GSHB stellt diesen im Wesentlichen aus folgenden Schritten dar (aus http://www.bsi.bund.de/gshb/deutsch/b/20.htm):

- Initiierung des IT-Sicherheitsprozesses
  - Erstellung einer IT-Sicherheitsleitlinie (eine allgemeine, eher politische Zielsetzung der Leitungsebene)
  - Einrichtung eines IT-Sicherheitsmanagements (zunächst eine organisatorische Aufgabe)
- Erstellung eines IT-Sicherheitskonzepts
  - IT-Strukturanalyse
  - Schutzbedarfsfeststellung
  - IT-Grundschutzanalyse
  - ggf. ergänzende Sicherheitsanalyse
  - Realisierungsplanung
- Umsetzung
- Aufrechterhaltung im laufenden Betrieb

Wichtige Erkenntnis aus dieser Darstellung ist, dass IT-Sicherheit von der Leitungsebene initiiert, getragen und aktiv unterstützt werden muss. IT-Sicherheit ist auch nicht das Flicken von Löchern, die gerade mal aktuell und in aller Munde sind. Es ist eben ein Prozess, der auch eine gewisse Organisation voraussetzt.

Die GWDG kommt erst da intensiver ins Spiel, wenn es um Unterstützung bei der Erstellung des konkreten Konzepts geht. Aber auch da kann die GWDG nur beraten. Die Strukturanalyse wie auch eine Schutzbedarfsfeststellung müssen primär durch die Betreiber bzw. Nutzer des IT-Systems erfolgen.

In der Annahme, dass sich viele Szenarien in der MPG wiederholen, kann die GWDG voraussichtlich am ehesten mit Musterlösungen für bestimmte (wiederkehrende) Teilbereiche helfen.

5. CERT-Funktionen

Im Rahmen des Konzepts IT-Sicherheitszentrale taucht immer wieder der Begriff MPG-CERT auf. Die GWDG ist sicherlich nicht in der Lage ist, alle Funktionen, die man bei einem CERT erwartet, zu übernehmen. Insbesondere das Austesten von allen Sicherheitsproblemen oder der dazu gehörenden Lösungen mit der von einem CERT zu erwartenden Vollständigkeit wäre wohl kaum zu leisten.

Die GWDG wird daher nur einen Teil der CERT-Funktionen übernehmen können. Geplant ist vor allem:

- Erstellung von Übersichten zu Sicherheitsproblemen und deren Lösungen (sprich Patches und Workarounds) für ausgewählte Systeme (sprich in der MPG relevante Bereiche) auf der Basis der von den bekannten CERTs oder von Herstellern veröffentlichten Informationen
- Bereitstellung von Patches auf Servern der GWDG (als Kopie dessen,was die Hersteller zur Verfügung stellen) für ausgewählte Systeme
- Alarmierung bei besonders dringenden oder wichtigen Sicherheitsproblemen auf der Basis von Informationen wie oben. Dabei wird das ein Dienst (wie bisher auch schon auf der Mailing-Liste „MPG-Info“ praktiziert) sein, bei dem die GWDG nach eigenem Dafürhalten und ohne jegliche Gewähr, dass für jeden alle relevanten Informationen auf diesem Wege verteilt werden, über die Auswahl der weitergeleiteten Informationen entscheidet. Wer die Garantie haben will, dass er wirklich alle möglicherweise relevanten Informationen erhält, wird auf die Hersteller, Security-Listen und CERTs verwiesen.
- Sammelstelle für Informationen über Sicherheitsvorfälle bei der MPG (freiwillige Meldungen, auf Wunsch auch Anonymisierung)

Gewünscht wird auch eine Hilfe bei Sicherheitsvorfällen durch die GWDG. Im Rahmen ihrer Möglichkeiten wird die GWDG auch das leisten. Nur kann die GWDG hier keine Garantien über Antwortzeiten und Verfügbarkeiten übernehmen. Insbesondere bei größeren „Epidemien“ über die MPG verteilt oder auch umfangreichen Vorfällen an einer Stelle könnte die GWDG aufgrund der Quantität der Anforderungen bei begrenzter eigener Kapazität nicht mehr in der Lage sein, die gewünschten Dienste im gewünschten Umfang zu erbringen.

6. Sicherheitsüberprüfungen

Ein weiterer unter der Rubrik IT-Sicherheitszentrale von der GWDG erwünschter Dienst sind Sicherheitsüberprüfungen durch die GWDG.

Sicherheitsüberprüfung heißt hier nicht die Prüfung von USV-Anlagen oder Feuerlöschern, sondern das Scannen von Rechnern auf mögliche Unsicherheiten bis zum (vorher abgesprochenen) Versuch eines Einbruchs in das IT-System eines MPIs.

Diesen Dienst bei der GWDG zu suchen, mag manchen MPIen sympathischer sein, als eine fremde Firma zu beauftragen. Immerhin gehört die

GWDG ja doch (hälftig) zur MPG und man kennt sich oder hat prinzipiell ein gewisses Vertrauensverhältnis. (Ein externer Dienstleister könnte dafür vielleicht weniger vorbelastet oder unvoreingenommener an die Arbeit gehen.)

Dei GWDG plant, diesen Dienst möglichst bald zur Verfügung zu stellen. Vorkenntnisse sind bei der GWDG durchaus vorhanden. Möglicherweise allerdings nicht in der Tiefe, die manche kommerziellen Anbieter haben. Als Hacker hat sich bei der GWDG wirklich ernsthaft noch niemand versucht. Ob die Mehrzahl der kommerziellen Anbieter solcher Dienste mehr können, als die üblichen Scan-Tools einzusetzen, wäre allerdings auch erst zu klären. Die GWDG muss (und will) ihr Know-How hier möglicherweise noch verbreitern.

Die GWDG nutzt zur Prüfung auf Schwachstellen verschiedenen Tools

- primär Nessus (Linux, Open Source)
- Retina Security Scanner von eEye (kommerzielle Software)
- LANGuard Network Security Scanner von GFI (kommerzielle Software)

Die Überprüfungen erfolgen in der Regel von Göttingen aus, aus dem GWDG-Netz heraus (das möglicherweise an Firewalls der MPIe privilegiert ist) oder aus einem eigenem Class-C-Netz der GWDG (also für die Firewalls der MPIe ein Fremdnetz). Bei Bedarf kann eine Sicherheitsüberprüfung auch lokal in Instituten erfolgen, so dass der Scanner hinter der Firewall des MPIs eingesetzt wird und auch nur lokal ausnutzbare Schwachstellen entdecken kann (in der Regel wird das wohl nicht nötig sein).

Wer eine solche Sicherheitsüberprüfung bei der GWDG bestellen darf, ist noch nicht endgültig entschieden. Aus rechtlichen Gründen wird es wahrscheinlich nötig sein, nur Anforderungen durch den geschäftsführenden Direktor oder ausdrücklich hierfür bevollmächtigte Personen zu akzeptieren.

7. Musterlösungen zu Einzelproblemen

Die GWDG wird Musterlösungen zu ausgewählten und für die MPG relevanten Bereichen ausarbeiten.

Einige Anfragen liegen bereits vor. Andere Dinge ergeben sich schon aufgrund der Verbreitung und der Wichtigkeit im Bereich IT-Sicherheit. Auf der Liste stehen bei uns insbesondere

- Windows-Betriebssystem
- Internet Explorer

- MS Outlook (in seinen Varianten)
- Mail-Systeme einschließlich Web-Mail
- Firewalls (einschließlich Paketfilter auf Routern)
- Netzwerkstrukturen in Bezug auf Sicherheit
- VPN (Virtual Private Network)
- PKI (Public Key Infrastructure)
- SSH-Implementationen
- Linux-Betriebssysteme

Etwas langwieriger ist von den obigen Punkten sicherlich PKI. Das haben auch wir noch nicht und müssen es, wenn der Rückgriff auf externe Anbieter nicht sinnvoller ist, erst aufbauen. Hier könnte also eine längere Vorlaufzeit nötig sein.

Diese Musterlösungen sind verfügbar unter

- http://www.gwdg.de/service/sicherheit

oder bei rein MPG-internen Informationen unter

- https://it-portal.mpg.de (z.B. Diskussionsforum zur IT-Sicherheit)

Sophos Anti-Virus – Lizenzen und mehr ...

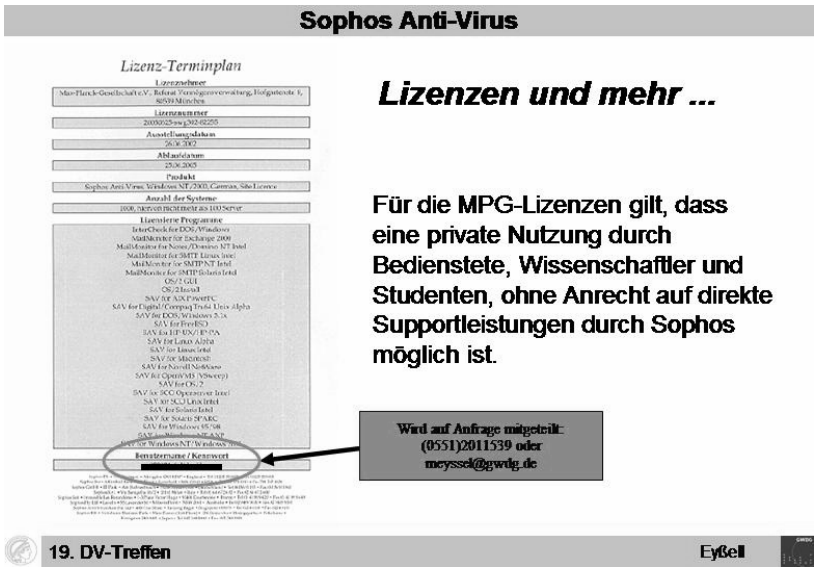
Manfred Eyßell

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Lizenz für Sophos Anti-Virus

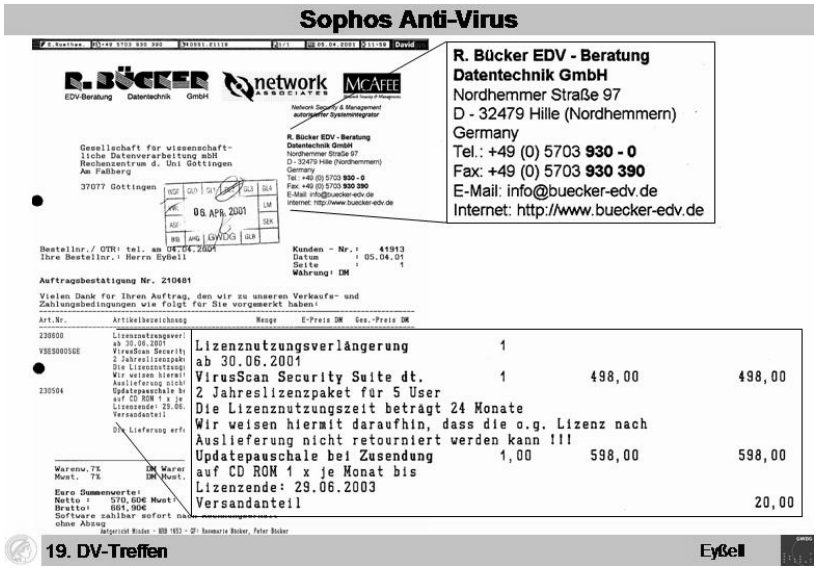
Seit 26. Juni 2002 ist ein von der Generalverwaltung der MPG abgeschlossener Lizenzvertrag mit der Firma Sophos Plc in Kraft. Das Ablaufdatum ist der 26. Juni 2005.

Lizenziert sind für die Institute der MPG die Produkte „*Sophos Anti-Virus*“ und „*MailMonitor*“ für alle gängigen Betriebssysteme. Für das Programm „*Enterprise Manager*“ ist nur eine Lizenz zum Gebrauch in der Generalverwaltung beschafft worden. Gegen eine zusätzliche Gebühr können Institute auch die Lizenz für den „*Enterprise Manager*“ erwerben.



2. Lizenz für McAfee abgelaufen

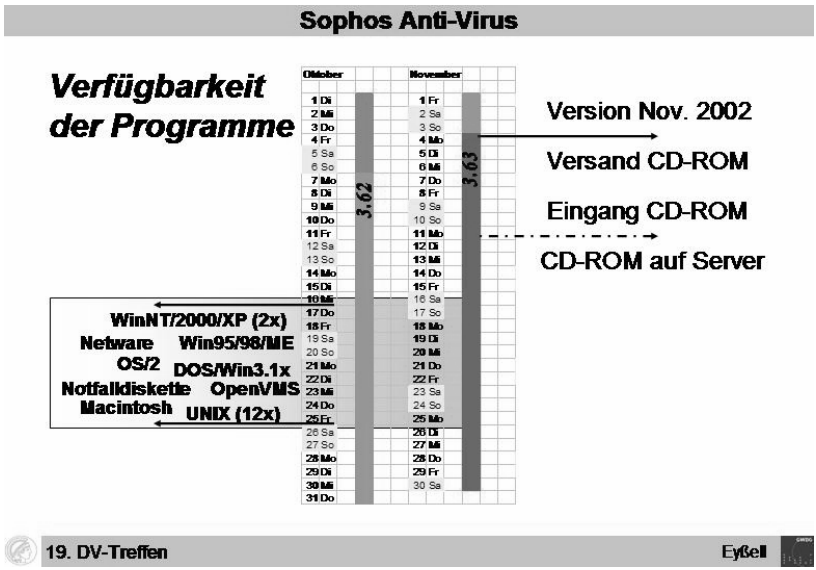
Die bisher in den Max-Planck-Instituten genutzte Antiviren-Software „*McAfee*“ ist mit dem 30. September 2002 abgelaufen. Die GWDG wird für ihre interne Nutzung – und um auch in Zukunft zum Einsatz dieser Software Unterstützung geben zu können – eine kleine Anzahl von Lizenzen dieses Produkts behalten. Den Max-Planck-Instituten, die weiterhin McAfee einsetzen wollen, kann z. B. der Lieferant der GWDG empfohlen werden:



3. Der Einsatz von Sophos Anti-Virus

Mit dem Einsatz des Programmsystems Sophos Antiv-Virus hat die GWDG mittlerweile ein halbes Jahr Erfahrung. Die Qualität der Software bezüglich Erkennung und Beseitigung von Computerviren ist, wie zu erwarten war, gut. Umständlich und leider nicht perfekt zu realisieren ist ein automatisches Programm-Update, wie es eigentlich monatlich durchgeführt werden müsste.

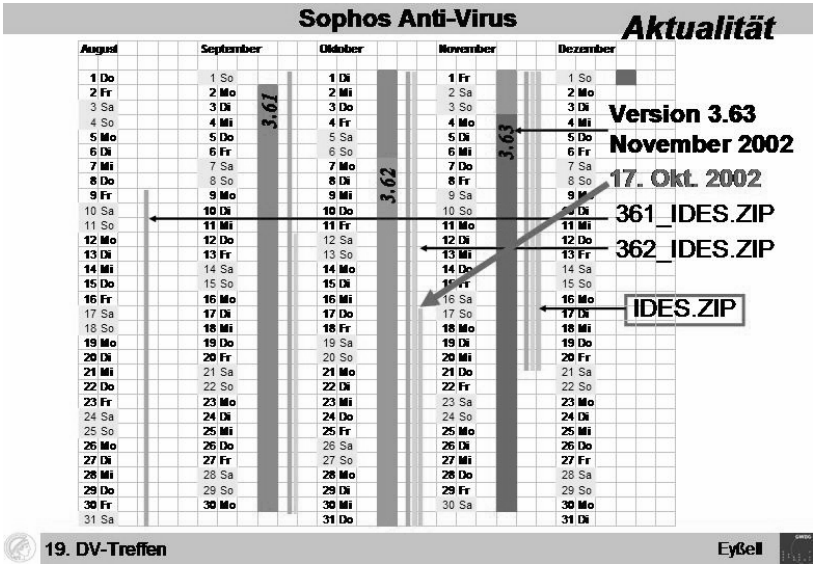
Für das Funktionieren der Virenerkennung ist absolut notwendig, sämtliche bekannten Virenkennungen im eigenen System integriert zu haben. Da die Veränderungen in der Funktionsweise von Viren und Würmern auch die Weiterentwicklung der Virenerkennungs-Software erforderlich macht, gibt Sophos monatlich eine neue Programmversion heraus, die installiert werden muss. In diese Programmversion sind alle Virenkennungen eingearbeitet, die bis zum Fertigstellungstermin bekannt sind. Sie sind in den Dateien VDL.DAT enthalten.



Während der Erscheinungstermin der Software jeweils der erste Montag im Monat ist, liegt der Fertigstellungstermin meist schon in der vorletzten Woche des Vormonats. Von diesem Zeitpunkt an (Datum der Datei VDL.DAT) muss man sämtliche anschließend veröffentlichten Virenkennungsdateien seinem System hinzufügen: sie brauchen nur in das Sophos-Verzeichnis abgelegt werden.

Versäumt man das Umstellen auf eine neue Monatsversion, darf es nicht sein, dass man die Erweiterung um Virenkennungsdateien mit der aktuellen gepackten Datei „IDES.ZIP“ durchführt, denn dann entsteht eine Lücke bei den Virenkennungen, weil IDES.ZIP nur die seit der Fertigstellung der aktuellen Monatsversion hinzugekommenen Signaturen enthält. In diesem Fall muss man die Datei „xxx_IDES.ZIP“ laden, wobei xxx die Versionsnummer derjenigen Monatsversion ist, die man gerade einsetzt. Diese enthält dann sämtliche Virenkennungen ab deren Fertigstellungsdatum. Auf der Folie ist der 17. Oktober das Fertigstellungsdatum der Version SAV 3.63 und die Datei „IDES.ZIP“, die von Sophos ständig aktualisiert wird, versorgt einen mit den ab 17. Oktober erschienenen Virensignaturen. Diese Datei wird nach der Fertigstellung der Version 3.64 weiter um Virenkennungen ergänzt und bekommt am Erscheinungstag der Version 3.64 den Namen

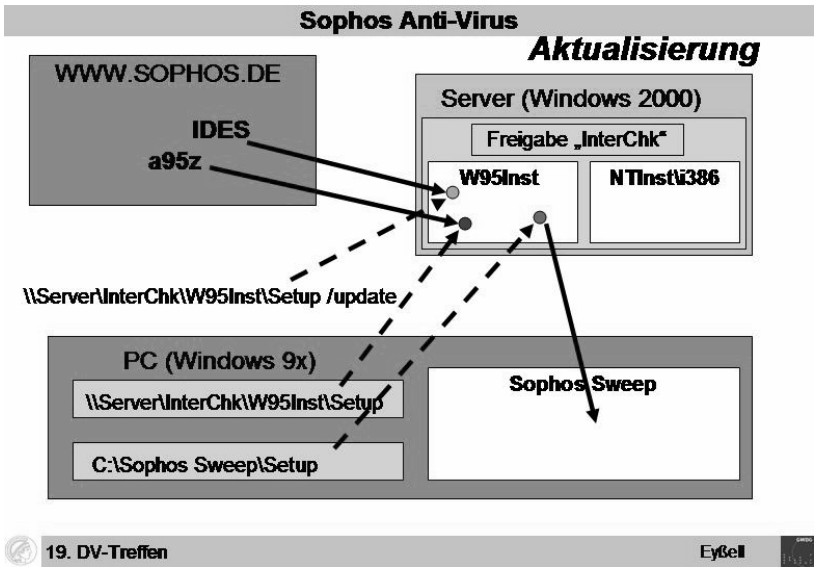
„363_IDES.ZIP“. Diese muss man verwenden, solange man nicht auf die Monatsversion 3.64 umgestellt hat.



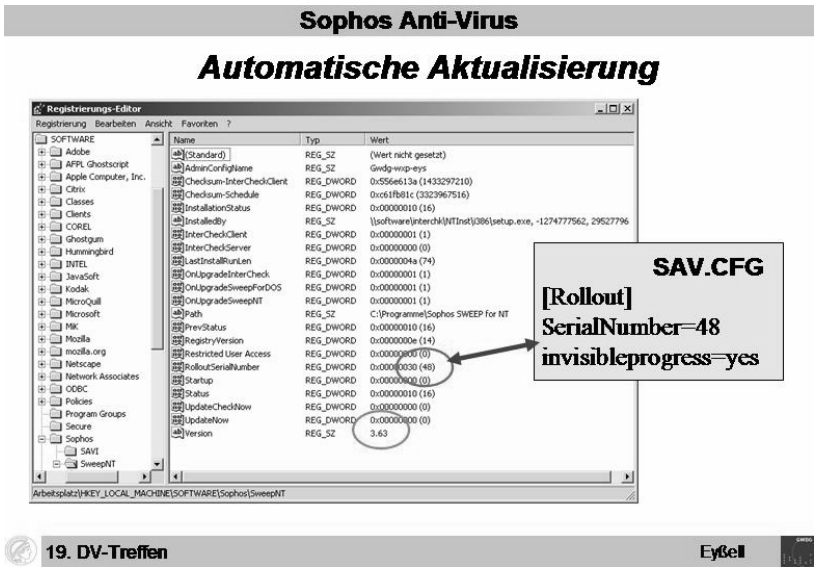
Auf dem Intranet-Server „S-WWW.GWDG.DE“ der MPG wird die GWDG stets nach Lieferung der Monats-CD von Sophos deren Inhalt ablegen. Wollten wir hier ein wirklich aktuelles Angebot machen, müssten wir ab Monatsmitte täglich prüfen, ob eines der etwa 20 Produkte neu ist, dieses per Hand herunterladen, um es dann auf den Intranet-Server zu kopieren. Auch aktuelle Virenkennungen wollen wir auf dem Intranet-Server aus praktikabilitätsgründen nicht anbieten.

Sowohl das Herunterladen von Virensignaturdateien (.IDE-Dateien) vom Web-Server der Firma Sophos als auch das Holen des monatlich neu erscheinenden kompletten Programms lässt sich leicht mit einer Kommandodatei realisieren. Damit jedoch Arbeitsplatzrechner, die an ein zentrales Installationsverzeichnis angeschlossen sind, neben den Virenkennungsdateien auch die Programme einwandfrei automatisch aktualisieren, ist auf dem Server im Zentralen Installationsverzeichnis ein „Setup“ erforderlich, das – wenn man nicht den „Enterprise Manager“ eingesetzt hat – nur manuell (im Dialog) durchgeführt werden kann.

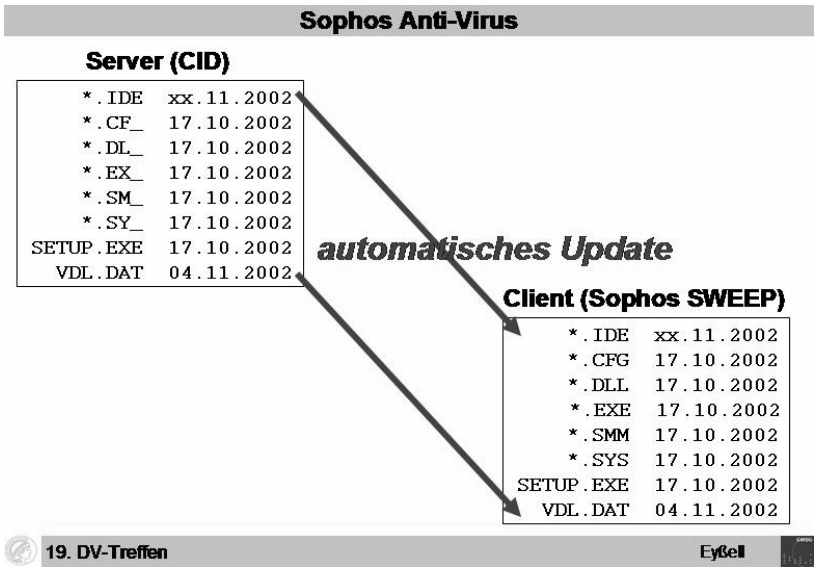
4. Automatische Aktualisierung über ein Zentrales Installationsverzeichnis



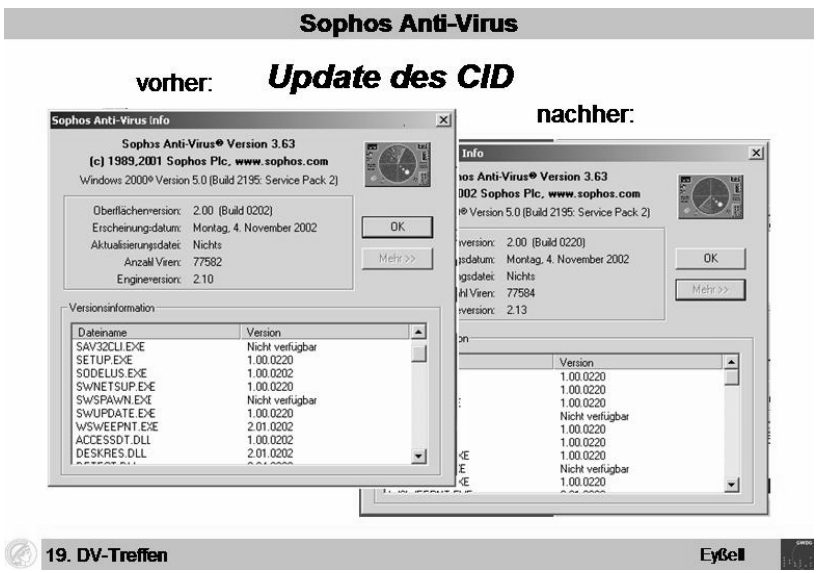
Die GWDG pflegt ein Zentrales Installationsverzeichnis auf ihrem PC-Netz-Server „Software" für die Betriebssysteme „Windows 9x" (W95Inst) und „Windows NT" (NTInst\i386). In ihm werden sowohl die Programme als auch die Virensignaturdateien aktuell gehalten. Während es dazu notwendig ist, im jeweiligen Zentralen Installationsverzeichnis das Kommando „Setup" im Anschluß an das Laden einer neuen Monatsversion zu geben, ist eine solche manuelle Tätigkeit an den angeschlossenen Arbeitsplatzrechnern nicht erforderlich.



Die Arbeitsplatzrechner vergleichen in bei der Installation festgelegten Zeitabständen die mit jeder Aktualisierung im Zentralen Installationsverzeichnis um Eins erhöhte „Rollout Number“, die in ihrer Registrierungsdatenbank geführt wird, mit der entsprechenden Nummer in dar Datei „SAV.CFG“ im Zentralen Installationsverzeichnis. Ist letztere größer, muss sich der Arbeitsplatzrechner die neuen Dateien holen.

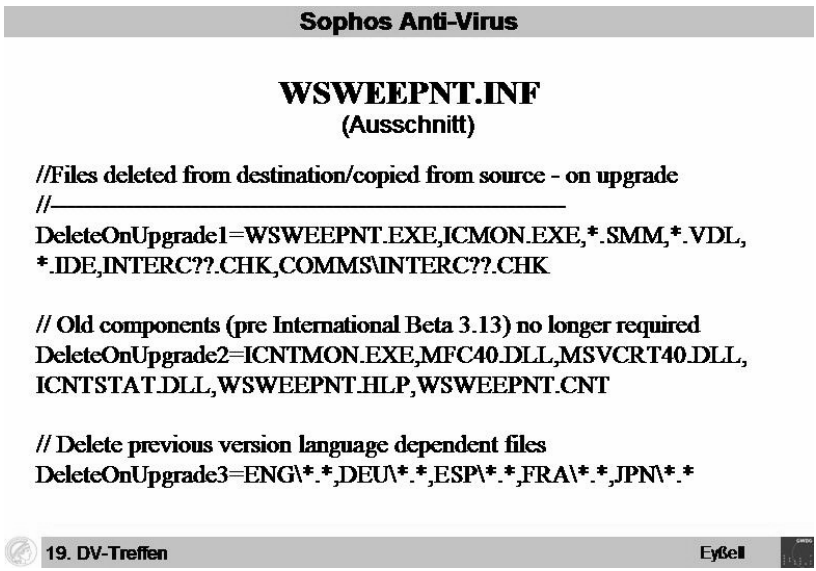


Um zu zeigen, dass eine vollständige einwandfreie Aktualisierung der Sophos-Programme nicht gelingt, wenn diese mit Kommandotateien automatisch geholt werden und auf das nur im Dialog durchzuführende Kommando „Setup“ verzichtet wird, folgende Folie:



In den Versionsangaben im Bedienungs-Fenster von Sophos wird zwar angezeigt, dass eine neue Version installiert ist, aber ein Blick auf die Dateien im Sophos-Verzeichnis zeigt, dass dies nicht wirklich geschehen ist.

Die Dateiübertragungen bei der Aktualisierung werden mit dem Inhalt der Datei „WSSWEEPNT.CFG“ gesteuert. Hier ein Ausschnitt:



Diese Datei kann auch ediert werden, um z. B. Einstellungen, die beim Einrichten des Programms zentral vorgenommen wurden, zu korrigieren. Die letzte Folie zeigt beispielhaft den Ausschnitt, in dem festgelegt wird, in welchen Zeitabständen sich ein Arbeitsplatzrechner aktualisieren soll:

WSWEEPNT.CFG

(Ausschnitt)

```
[%APPNAME\Current Version\RunTimeInfo\SweepNT Specific]
Show Uninstall Info=1
Immediate Sweep On Startup=0
Service As System=1
Upgrade SweepNT=1
Upgrade DOSSweep=1
Upgrade InterCheck=1
Install InterCheck Server=0
Install InterCheck Client=1
InteractiveUpgrade=0
AllowUserToPostponeUpgardes=0
AllowUserToPostponeAttempts=1
AllowUserToPostponeLifeDays=0
UpgradeMinuteFreqency=1
UpgradeDailyFrequency=0
UpgradeWeeklyFrequency=0
UpgradeMinuteFrequencyNumber=10
UpgradePostponeLifeDaysNumber=14
UpgradePostponeNumber=5
HardShutDownAfter=9000
ShutDownWarnUserAfter=5000
ShutDownAfterWarnUser=8000
```

Dienste für die MPG

Wilfried Grieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Einleitung

Grundsätzlich bietet die GWDG alle Dienste, die sie anbietet, selbstverständlich auch den Instituten der Max-Planck-Gesellschaft an. Der komplette Dienstleistungskatalog „Rechner, Netze, Spezialisten“ ist im WWW unter dem URL

`http://www.gwdg.de/service/nutzung/katalog`

abrufbar. Ein regelmäßig angebotener Kurs, nämlich die „Einführung in die Nutzung des Leistungsangebots der GWDG“ erläutert detailliert die einzelnen Dienste und die Voraussetzungen zu deren Nutzung.

Laut Votum einer Unterkommission des Beratenden Ausschusses für EDV-Anlagen in der Max-Planck-Gesellschaft (BAR) aus dem Jahr 2001 hat die GWDG darüber hinaus vornehmlich die folgenden zentralen Dienste für die Max-Planck-Institute außerhalb Göttingens anzubieten:

- IT-Sicherheit
- Betrieb von Mail- und Web-Servern

- Backup und Langzeitarchivierung
- Bibliothekssysteme und Informationsdatenbanken
- Netzplanung
- Schulungsprogramm

Diese Dienste werden deshalb auch verstärkt in den Instituten bekannt gegeben, damit die GWDG ihrer zentralen Rolle gerecht wird. Informationen zu diesen Diensten lassen sich montags bis freitags von 7.10 bis 23.00 Uhr und samstags von 10.00 bis 18.00 Uhr über die Zentrale Auftragsannahme der GWDG unter der Telefonnummer

```
0551 201-1523
```

anfordern. Diesbezügliche Anfragen werden an die entsprechenden Mitarbeiter weiter geleitet, um eine fachkundige Auskunft sicher zu stellen.

In den folgenden Abschnitten werden die zentralen Dienste näher beschrieben.

1. IT-Sicherheit

Der zentrale Dienst „IT-Sicherheit“ beinhaltet die Beratung und Hilfestellung zu allen sicherheitsrelevanten Problemen in der elektronischen Datenverarbeitung. Zur effizienten Unterstützung des Dienstes wurde ein Security-Team in der GWDG eingesetzt. Es besteht aus den Mitarbeitern Dr. H. Beck, B. Gelbe, A. Ißleiber, M. Reimann und H. Sheikhikhou. Bei Bedarf werden noch weitere Mitarbeiterinnen oder Mitarbeiter in das Team integriert.

Das Security-Team ist zusätzlich zur obigen Telefonnummer auch unter der E-Mail-Adresse

```
itsz@gwdg.de
```

erreichbar. Eingehende Anfragen werden schnellstmöglich von einem Team-Mitglied beantwortet.

Im Vortrag „IT-Sicherheitszentrale der GWDG“ geht Herr Beck genauer auf die Aufgaben des Teams ein.

2. Mail-Server

Mail-Server werden von den Mitarbeitern B. Gelbe, M. Reimann und Dr. E. Handke betrieben. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail über die folgenden Adressen erreichbar:

bgelbe@gwdg.de
mreiman1@gwdg.de
ehandke@gwdg.de

In diesem Dienst bietet die GWDG den Betrieb von virtuellen Mailern an. Er wird u. a. bereits von der Generalverwaltung, dem Max-Planck-Institut für biophysikalische Chemie und dem Max-Planck-Institut für experimentelle Medizin genutzt.

Weiter kann der Mailer der GWDG eine Prüfung auf Viren und SPAM-Mails des eingehenden Mail-Verkehrs übernehmen. Entsprechende Informationen werden im Mail-Header vermerkt. Dieser Teil des Dienstes wird bereits vom Max-Planck-Institut für Hirnforschung und vom Max-Planck-Institut für Limnologie in Anspruch genommen.

3. Web-Server

Auch virtuelle Web-Server werden von der GWDG betrieben. Zuständig für diesen Dienst sind die Mitarbeiter G. Koch und M. Reimann, die zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

gkoch@gwdg.de
mreiman1@gwdg.de

erreichbar sind. Zur Zeit betreibt die GWDG für die Max-Planck-Gesellschaft 46 virtuelle WWW-Server unter dem Betriebssystem SUN-Solaris, demnächst unter Linux. Dabei wird auch die Programmiersprache PHP und das Datenbanksystem mySQL zur Verfügung gestellt.

4. Backup und Langzeitarchivierung

Ansprechpartner für den zentralen Dienst „Backup und Langzeitarchivierung“ sind die Mitarbeiter Dr. W. Möller, M. Röhrig und Dr. E. Handke, die zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail über die Adressen

wmoelle@gwdg.de
mroehri@gwdg.de
ehandke@gwdg.de

erreichbar sind. Zur Zeit wird der Dienst bereits vom Max-Planck-Institut für Biogeochemie, vom Max-Planck-Institut für biophysikalische Chemie, vom Max-Planck-Institut für Chemie, vom Max-Planck-Institut für chemische Ökologie, vom Max-Planck-Institut für chemische Physik fester Stoffe, vom Max-Planck-Institut für Geschichte, vom Max-Planck-Institut für Hirn-

forschung, vom Max-Planck-Institut für Meteorologie und vom Max-Planck-Institut für Strömungsforschung genutzt.

5. Bibliothekssysteme Aleph - VLib - SFX

Die Bibliothekssysteme Aleph, VLib und SFX werden vom Aleph-Team betreut. Es besteht aus den Mitarbeiterinnen und Mitarbeitern R. Maaß, A. Bruns, R. Bost und O. Lachkova. Bei Bedarf werden noch weitere Mitarbeiterinnen und Mitarbeiter hinzugezogen. Das Aleph-Team ist zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

rmaass@gwdg.de
abruns1@gwdg.de
rbost@gwdg.de
olachko@gwdg.de

erreichbar. Zusätzlich sind zur Informationsverbreitung über die verschiedenen Systeme noch die drei Diskussionslisten

aleph-projekt@gwdg.de
aleph-support@gwdg.de
mpg-vlib@gwdg.de

eingerichtet. Zur Zeit werden vom Aleph-Team Einzelprojekte von etwa 30 Max-Planck-Instituten bearbeitet.

6. Informationsdatenbanken Ovid

Für die Informationsdatenbanken unter Ovid sind die Mitarbeiter J. Hattenbach und M. Röhrig zuständig. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

jhatten@gwdg.de
mroehri@gwdg.de

erreichbar. Das Ovid-System wird von nahezu allen Max-Planck-Instituten genutzt.

7. Informationsdatenbanken Beilstein - Gmelin

Die Informationsdatenbanken Beilstein und Gmelin werden von den Mitarbeitern Dr. B. Heise und Dr. R. Baier betreut. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

bheise@gwdg.de
rbaier@gwdg.de

erreichbar. Zur Zeit werden diesbezüglich Einzelprojekte des Max-Planck-Instituts für Biochemie, des Max-Planck-Instituts für biophysikalische Chemie, des Max-Planck-Instituts für Dynamik komplexer technischer Systeme, des Max-Planck-Instituts für Festkörperforschung, des Max-Planck-Instituts für Kohlenforschung des Max-Planck-Instituts für Kolloid- und Grenzflächenforschung, des Max-Planck-Instituts für molekulare Physiologie, des Max-Planck-Instituts für chemische Ökologie, des Max-Planck-Instituts für Polymerforschung und des Max-Planck-Instituts für Strahlenchemie bearbeitet.

8. Informationsdatenbanken Oracle

Für Informationsdatenbanken unter Oracle sind die Mitarbeiter Dr. B. Heise und Dr. R. Baier zuständig. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

bheise@gwdg.de
rbaier@gwdg.de

erreichbar. Zur Zeit werden Einzelprojekte der Generalverwaltung, des Max-Planck-Instituts für biophysikalische Chemie, des Max-Planck-Instituts für Geschichte und des Max-Planck-Instituts für marine Mikrobiologie bearbeitet.

9. Informationsdatenbanken Wisconsin Package (GCG)

Die Informationsdatenbanken des Wisconsin Packages, besser bekannt als GCG-Paket, werden von den Mitarbeitern Dr. R. Bohrer und Prof. Dr. O. Haan betreut. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

rbohrer@gwdg.de
ohaan@gwdg.de

erreichbar. Das GCG-Paket der GWDG wird zur Zeit vom Max-Planck-Institut für biophysikalische Chemie, vom Max-Planck-Institut für experimentelle Medizin, vom Max-Planck-Institut für Neurobiologie und vom Max-Planck-Institut für physiologische und klinische Forschung genutzt. Darüber hinaus werden die GCG-Systeme im Max-Planck-Institut für Biochemie, auf dem Campus in Tübingen und im Max-Planck-Institut für Plasmaphysik von der GWDG ferngewartet.

10. Informationsdatenbanken Lotus Notes

Für die Erstellung und Pflege von Informationsdatenbanken unter Lotus Notes sind Frau S. Greber und Dr. W. Grieger zuständig. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail unter den Adressen

sgreber@gwdg.de
wgriege@gwdg.de

erreichbar. Informationsdatenbanken unter Lotus Notes dienen der Veranstaltungsorganisation, als Wiedervorlagesystem, als Adressdatenbank und zur Kalenderverwaltung, beinhalten also ein komplettes Groupware-System. Genutzt wird es zur Zeit von der Generalverwaltung und vom Max-Planck-Institut für biophysikalische Chemie.

11. Netzplanung

Die Planung von Datenübertragungsnetzen innerhalb von Instituten obliegt den Mitarbeitern H. Witt und Dr. H. Beck. Sie sind zusätzlich zur oben angegebenen Telefonnummer auch per E-Mail über die Adressen

hwitt@gwdg.de
hbeck@gwdg.de

erreichbar. Bisher wurde von ihnen die Netzplanung für etwa 35 Max-Planck-Institute durchgeführt.

12. Schulungsprogramm

Informationen zum umfangreichen Schulungsprogramm der GWDG sind im WWW unter dem URL

http://www.gwdg.de/service/kurse

abrufbar. Selbstverständlich lassen sich bei Bedarf auch weitere Termine vereinbaren. Das Abhalten von Spezialkursen durch Mitarbeiterinnen und Mitarbeiter der GWDG ist auch in den Instituten möglich.

Teil 2: Beiträge vom 20. DV-Treffen

Alternative Sicherungskonzepte: LiveBackup

Bernd Gliss

Max-Planck-Institut für Metallforschung, Stuttgart

Dieser Beitrag schildert eine Alternative zu herkömmlichen Verfahren der Datensicherung. Er beruht auf Erfahrungen mit dem Produkt LiveBackup (LB) der Firma Storactive und seinem Einsatz im Institut während der letzten beiden Jahre.

LiveBackup wird hier konventionellen Verfahren der Datensicherung gegenübergestellt. Unter konventionellen Verfahren verstehe ich Vorgehensweisen, die auf einer periodischen Regelsicherung innerhalb eines bestimmten Zeitfensters beruhen und eine Verbindung zwischen Klienten und Server während des Sicherungszeitfensters voraussetzen.

Konzepte, Softwarearchitektur und Implementierungserfahrungen mit dem Produkt werden dargestellt.

1. Konzepte

LiveBackup sichert Benutzerdaten auf Windows-PCs zeitnah, permanent, autonom und - falls verlangt - vollständig. Die Gültigkeit dieser Aussage kann man am besten anhand von folgenden Anwendungsbeispielen verstehen:

1. Rücksichern einer versehentlich gelöschten Datei,
2. Sichern von mobilen Rechnern, die zeitweise nicht mit dem Institutsnetz verbunden sind und
3. Systemwiederherstellung nach Totalausfall eines Rechners.

Hauptanwendungsfall für die Datensicherung ist das **Zurückspielen von versehentlich gelöschten Dateien**. Bei intensiver Arbeit mit einer Datei wird es immer wieder vorkommen, daß nach dem letzten Sicherungstermin eines konventionellen Verfahrens mit wesentlichen Änderungen begonnen und vor dem nächsten Sicherungstermin die Datei gelöscht wurde. Dies bedeutet im allgemeinen, daß der letzte Änderungszustand nicht wiederhergestellt werden kann.

LiveBackup sichert Dateien hingegen beim Entstehen und während der Veränderung; damit kann man auch in dem genannten Fall den Dateizustand zeitnah restaurieren. Deshalb ist die in Abb. 1 angedeutete, zunächst überraschende Alternative (I know I saved the file..., d.h. Betrachten aller Dateien, mit denen in einem Zeitintervall gearbeitet wurde) durchaus sinnvoll. LiveBackup bietet die entsprechenden Versionen zum Rückschreiben an.

Betrachten wir das **Sichern mobiler Rechner**. Hier bieten konventionelle Verfahren nur sehr eingeschränkte Möglichkeiten:

Der PC wird nach Rückkehr in das Institut mit dem Hausnetz verbunden und dann bei der nächsten Regelsicherung miterfaßt oder er wird nach Anschluß ins Hausnetz auf Benutzerinitiative hin gesichert (ad-hoc-Sicherung).

LiveBackup arbeitet grundsätzlich anders: Wird die Verbindung des Klienten zum Sicherungsserver unterbrochen, so schreibt der Klient Sicherungsinformationen in einen lokalen Plattenbereich, den sogenannten Plattencache. Dessen Größe richtet sich nach dem verfügbaren, nicht anderweitig belegten

Plattenspeicherplatz. Die Cachegröße kann vom Benutzer über die Schnittstelle „Control Center“ beeinflußt werden.

Abb. 1

Nach Rückkehr ins Institut und Wiederherstellen der Verbindung zum Hausnetz meldet sich der Klient automatisch beim LiveBackup-Server und überträgt die „unterwegs“ gesicherten Dateifragmente zu ihm.

Nun zur **Totalrestaurierung**: LiveBackup legt entweder automatisch bei Systemstart oder auf Benutzerinitiative einen sogenannten „**System Checkpoint“** (SC) an, in dem der Gesamtzustand des Systems zu einem bestimmten Zeitpunkt festgehalten wird. Fehlt dieser „System Checkpoint“, so kann man zwar Benutzerdaten zurückspielen, nicht aber den Gesamtzustand des Klienten restaurieren. Ich setze voraus, daß ein SC vorhanden ist und daß der zeitlich nächstgelegene SC zum Restaurieren ausgewählt wurde (s. Abb. 2).

Man wählt hier den Typ der Rücksicherung aus. Hat man beim Erstellen des Sicherungsprofils **Gesamtsicherung** vereinbart, so kann man nun die Restaurierung aller Dateien, egal ob System- oder Benutzerdatei, verlangen. Sonst sind nur die gemäß Sicherungsprofil vereinbarten Dateien und Verzeichnisse restaurierbar.

Welche Möglichkeiten zur Datenwiederherstellung gibt es für ein **total korrumpiertes System**? Auch hier hängen die Möglichkeiten davon ab, ob ein Systemstand (SC) gesichert wurde oder nicht. Ist ein SC vorhanden, so kann der LiveBackup-Administrator sogar dann tätig werden, wenn der Inhalt der Festplatten des Klienten völlig korrumpiert ist. Er kann aus dem Inhalt der LB-Datenbank **bootbare CDs** erstellen, mit deren Hilfe zunächst ein Notsys tem inklusive LB-Klient installiert wird. Dieses wird dann um die restlichen System- und Benutzerdaten - wie oben geschildert - ergänzt.

Abb. 2

2. Architektur

Die geschilderten Möglichkeiten scheinen zunächst hohen Aufwand nach sich zu ziehen. Selbst wenn LiveBackup die üblichen Verfahren der Delta- und Differenzsicherung sowie der Datenkompression anwendet, erwartet man eine hohe Belastung des LiveBackup-Servers und der Netzverbindungen zwischen Klient und Server. Daß dem nicht so ist, ist in erster Linie Folge der gewählten Architektur des Systems.

LiveBackup ist im Gegensatz zu den üblichen Verfahren ein stark klientenorientiertes System. Die Serverseite besteht lediglich aus einer Internet-Information-Server-Anwendung, die sich einer SQL-Datenbank für die Metadaten und eines Nutzdatenbereichs bedient. Klientenseitig sitzt die LB-

Komponente „Deltafilter" zwischen dem Ein/Ausgabe-Subsystem und dem Plattentreiber und analysiert den Datenstrom zur Platte (s. Abb. 3). „Deltas", d.h. Differenzen der aktuellen zur bereits gesicherten Datei werden in den lokalen Datencache bzw. zum LB-Server übertragen. Der Transfer geschieht über HTTP. Dabei wird über Signaturen und eine Zerlegung großer Dateien in einzelne „Zonen" dafür gesorgt, daß der Vergleich durch Austausch weniger Informationen vorgenommen werden kann (s. Abb. 4).

LiveBackup-Signaturen sind 32-Bit-Prüfsummen über den Dateiinhalt. Für Dateien von mehr als 1 MB Umfang werden mehrere 32-Bit-Prüfsummen angelegt; somit wird die Datei in kleinere Teilbereiche zerlegt und der Aufwand für die Prüfsummenberechnung wird reduziert.

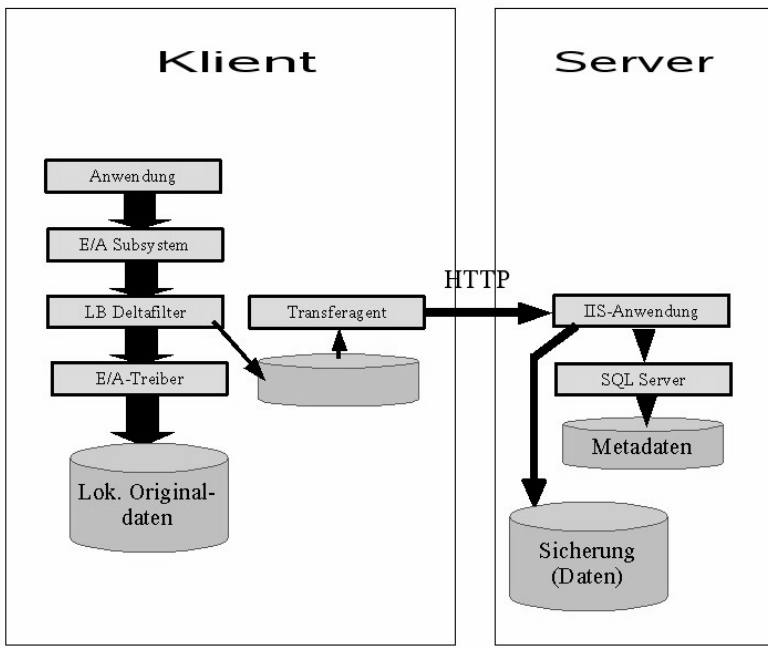


Abb. 3

Darüber hinaus realisiert LiveBackup das Prinzip der kontenübergreifenden Einmalsicherung von Dateien. Wird eine Datei in mehreren Benutzerkonten identisch abgspeichert, so wird sie einmal gesichert. Über Verweise und „Benutzt-Zähler" in den Metadaten wird dafür gesorgt, daß die gesicherte Version erst dann gelöscht wird, wenn der letzte Verweis auf die Datei nicht

mehr benötigt wird. Dies reduziert das Sicherungsvolumen insbesondere für mehrfach installierte PC-Anwendungen wie Microsoft-Office.

3. Implementierung

Als Hardware für LiveBackup ist ein PC-basierter Server und ein SCSI-IDE-RAID ausreichend. Für die Archivierungskomponente, über die hier nicht berichtet wird, ist ein Bandlaufwerk oder eine Bandbibliothek notwendig. Ohne Archivierungskomponente ermöglicht LiveBackup dem Administrator, die Meta- und die Benutzerdaten - falls notwendig auch bei laufendem Betrieb - als Block zu sichern. Die so gesicherten Daten können dazu verwendet werden, den Gesamtzustand des LiveBackup-Systems nach dessen Totalausfall zu restaurieren; sie sind nicht geeignet, um einzelne Dateien zurückzuschreiben.

Die Softwarekonfiguration setzt eine 100-prozentige Microsoftumgebung voraus. Basis des Systems ist in unserem Fall ein Windows-2000-Server. Daneben müssen der Internet-Informationserver und der Microsoft-SQL-Server aktiviert sein.

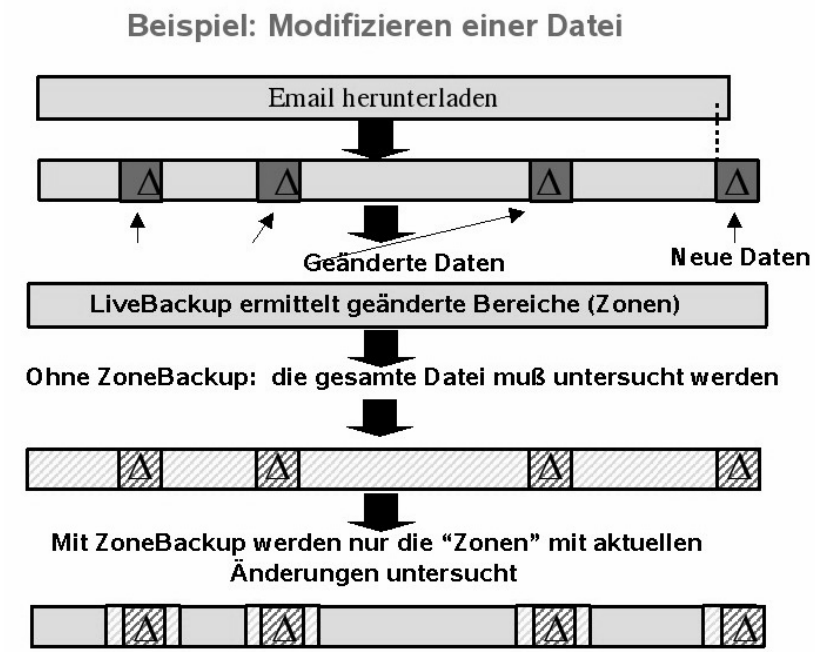


Abb. 4

4. Erfahrungen

LiveBackup bietet gegenüber herkömmlichen Systemen folgende **Vorteile:**

1. Es ist unabhängig von Benutzeraktivitäten. Dies ist in der Praxis äußerst wichtig; man kann nie sicher sein, daß der Benutzer notwendige Maßnahmen (z.B. eine adhoc-Sicherung nach Wiederaufnahme der Verbindung eines Notebooks mit dem Institutsnetz) auch durchführt. Hier ist die Automatik von LB von Vorteil.
2. LiveBackup ist leicht administrierbar. So lassen sich Klienten zu Gruppen mit definierten Merkmalen und Sicherungsprofilen zusammenfassen. Neue Klienten sind dann per Mausklick anlegbar. Abweichungen vom Gruppenprofil können jederzeit zugelassen werden. Dem Benutzer können Rechte nach einem dreistufigen System zugewiesen werden; insbesondere kann man verhindern, daß ein Benutzer die Sicherungsmechanismen außer Kraft setzt.
3. Die Aktualisierung der Serversoftware erfolgt automatisch durch Einspielen der Folge-CD. Klientensoftware wird über Netz automatisch verteilt und aktiviert, falls der Benutzer einwilligt.

LiveBackup hat aber auch eine Reihe von **Nachteilen**, die in unserem Fall allerdings nicht gravierend sind:

1. Die zentralen Möglichkeiten zur Rücksicherung sind beschränkt. Insbesondere gibt es keine Auswahlmöglichkeit für den Administrator zum Restaurieren bestimmter Dateien.
2. Das Anlegen von Systemzuständen könnte robuster sein; es gibt Hardware-Konfigurationen, bei denen ein Systemzustand nur durch Benutzerinitiative angelegt werden kann. Dieser Mangel soll in der zur Auslieferung ansteheden Version des Produkts (2.72) behoben sein.
3. Die Einbindung der Archivierungskomponente ist rudimentär. Insbesondere unterstützt sie keine Bandpoolverwaltung, wie sie für den Einsatz von Bandbibliotheken notwendig ist.

Insgesamt hat sich LiveBackup im Praxiseinsatz bewährt. Der administrative Aufwand hält sich in Grenzen. Bisher hatten wir - aufgrund eines Mißverständnisses bei der Installation einer neuen Version - erst einen Totalausfall. Auch ein Wechsel der zugrundegelegten Hardware mit „Umzug“ der gesicherten Daten auf sie wurde bewältigt.

Sobald die angekündigte Komponente zum Sichern von Windows-Servern verfügbar ist, werden wir LiveBackup auch auf diese Systeme anwenden.

Digitale Langzeitarchivierung in Bibliotheken, Rechenzentren und der Max-Planck-Gesellschaft

Dagmar Ullrich

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Abstract

Übliche Archivsysteme dienen der sicheren Speicherung von Daten ohne besondere Berücksichtigung des schnellen Technologiewandels außerhalb der Systeme. Wird dieser Wandel nicht beobachtet und rechtzeitig auf ihn reagiert, laufen bestehende Systeme Gefahr, Daten zu sichern, die nicht mehr lesbar und damit wertlos sind. Institutionen wie Bibliotheken und wissenschaftliche Institute arbeiten gemeinsam mit Rechenzentren an Lösungen, um der Gefahr langfristigen Datenverlustes zu entgehen. Die wachsende Archivierungsdauer wirft Fragen nach der Haltbarkeit verwendeter Speichermedien, der Aktualität der Speichertechnologie sowie der Verfügbarkeit erforderlicher Software auf. Erste Lösungen liegen in der regelmäßigen Erneuerung von Datenträgern, der Emulation von Interpretationsplattformen oder der Migration veralteter Formate. Es werden konkrete Projekte vorgestellt, die solche Lösungsansätze realisieren sollen.

1. Zunehmende Bedeutung Digitaler Langzeitarchivierung

Digitale Langzeitarchivierung ist zurzeit ein Thema wachsenden Interesses. Worauf beruht dieses Interesse und warum nimmt es stetig zu?

Die Antwort auf diese Frage liegt, ähnlich wie bei analogen Daten, in der Bedeutung digitaler Daten. Bis vor wenigen Jahren lagen nachhaltig wichtige Daten kaum in digitaler Form vor. Das hat sich radikal geändert. Die Menge rechtlich oder kulturell bedeutungsvoller digitaler Daten wächst stetig. Bei vielen dieser Daten besteht eine gesetzliche oder sonstige Verpflichtung zur Langzeitarchivierung. So hat Die Deutsche Bibliothek den gesetzlichen Auftrag, alle deutschen und deutschsprachigen, gedruckten oder elektronischen Publikationen zu sammeln und zu archivieren. Innerhalb der Max-Planck-Gesellschaft besteht für die einzelnen Institute auf der Basis der vom Senat der MPG beschlossenen „Regeln zur Sicherung guter wissenschaftlicher Praxis“ die Verpflichtung, Daten, die für Publikationszwecke genutzt wurden, über mindestens zehn Jahre zu sichern. Das gilt auch für digitale Daten. Neben einer solchen direkten Verpflichtung zur Archivierung kann auch der besondere kulturelle Wert von Daten Anlass ihrer Archivierung sein. Die langfristige Archivierung dient dann dem Erhalt des kulturellen Erbes und des kollektiven Gedächtnisses. Digitale Daten von solchem Wert finden sich z.B. im Bereich wissenschaftlicher Primärdaten, wie Sprachaufzeichnungen, Fotographien oder Messdaten, die kein zweites Mal erhoben werden können. Zwar gibt es für den Erhalt solcher Datenbestände möglicherweise keine gesetzliche Verpflichtung, aber dennoch können es gerade solche Bestände sein, deren Verlust besonders schwer wiegen würde.

2. Vier zentrale Aspekte Digitaler Langzeitarchivierung

Ein Hauptfaktor für die zunehmende Bedeutung Digitaler Langzeitarchivierung ist **der schnelle Technologiewandel** im Bereich der elektronischen Datenverarbeitung. Im Gegensatz zu beispielsweise gedruckten Texten können digitale Daten schon nach wenigen Jahren nicht mehr lesbar sein. Sowohl die verwendeten Speichermedien als auch die Software zur Darstellung der Daten veraltern in vergleichsweise kurzer Zeit.

Auf der anderen Seite nimmt **die Menge digitaler Daten**, für die eine zuverlässige langfristige Speicherung erforderlich ist, rasant zu. Hierzu trägt zunehmend auch die EDV-gestützte Forschung mit ihren digitalen Messtechniken bei. Eine weitere Ursache liegt in den vereinfachten Produktions- und Publikationsmöglichkeiten digitaler Daten, die auch deren leichte Wieder- und Weiterverwendung in neuen Kontexten einschließt.

Neben Zeitdruck und Menge spielt **die große Heterogenität** der Daten eine wichtige Rolle. So kann es sich bei den zu archivierenden Daten um wissenschaftliche Primärdaten, wie Bilddateien, digitale Tonaufnahmen, Messergebnisse und komplexe Datenbanken handeln. Ähnlich vielfältig, jedoch in der Regel textuellen Inhalts, sind digitale Publikationen inklusive spezieller Netzpublikationen. Letztere sind teilweise sehr kurzlebig und liegen nicht notwendig auf einem direkt archivierbaren Trägermedium vor. Weiter können hier Retrodigitalisate ursprünglich analoger Bestände genannt werden. Hierbei handelt es sich vorwiegend um Bilddateien. Auch im Umfeld von E-Learnig-Systemen entstehen zum Teil hoch komplexe, proprietäre Formate. Ähnlich wie Verwaltungsdaten sind sie häufig besonders eng an das Programm gebunden, in dem sie erstellt und bearbeitet werden. Diese Proprietät stellt für die langfristige Archivierung eine besondere Schwierigkeit dar.

Die breite Palette digitaler Daten lässt auch **die Archivierungsanforderungen** sehr unterschiedlich ausfallen. Wo bei einigen Daten lediglich einer gesetzlichen Auflage über wenige Jahre genügt werden muss und die Wahrscheinlichkeit, dass die Daten tatsächlich noch mal gelesen werden, eher gering ist, können andere Bestände von großem allgemeinen Interesse und auf unabsehbare Zeit als kulturelles Erbe von Bedeutung sein.

3. Mehr als „nur speichern“

Um digitale Daten langfristig verfügbar zu halten, muss an zwei Stellen angesetzt werden. Zum einen muss der Erhalt des gespeicherten Bitstreams auf einem entsprechenden Speichermedium gesichert sein. Zum anderen muss dafür Sorge getragen werden, dass dieser Bitstream auch interpretierbar bleibt, d.h. dass eine entsprechende Hard- und Software-Umgebung verfügbar ist, in der die Daten für einen menschlichen Betrachter lesbar gemacht werden können.

Um die Sicherheit von Speichermedien zu gewährleisten, kann anhand der geschätzten Lebensdauer eine entsprechende Erneuerungspolitik entwickelt und umgesetzt werden. Dabei muss auch die Möglichkeit berücksichtigt werden, dass noch vor Ablauf der erwarteten Lebensdauer des Mediums die verwendete Speichertechnologie veraltet und daher nicht nur ein Wechsel des Trägermediums, sondern deutlich weitreichendere Neuerungen erforderlich werden. Das ist derzeit sogar häufiger der Fall, als die tatsächliche physische Unbrauchbarkeit des Speichermediums. Ebenso wie bei üblichen Archivierungs- und Backupverfahren sollten zusätzlich zu den bei Kopiervorgängen impliziten Kontrollallgorithmen, je nach Sicherheitsbedarf, zusätzliche Prüfungen, z.B. anhand von Checksummen vorgenommen werden. Gängige Vorgehensweisen wie redundante Datenhaltung ggf. auf unter-

schiedlicher Hardware und räumlich getrennte Aufbewahrung gewinnen besonders für die Langzeitarchivierung an Bedeutung.

Die sichere Archivierung der gespeicherten Bits ist jedoch „nur“ die Voraussetzung für die Lösung einer wesentlich umfassenderen Problemstellung. Die archivierten Daten müssen langfristig verfügbar gehalten werden. D.h. sie müssen anhand inhaltlicher Aspekte suchbar, zuverlässig zitierbar und in für Menschen lesbarer Form darstellbar sein. Letzteres kann nur gewährleistet werden, wenn systematisch sichergestellt wird, dass für alle archivierten Datenobjekte auch in ferner Zukunft mindestens eine Interpretationsplattform verfügbar ist.

Ein Digitales Langzeitarchiv muss also neben dem zuverlässigen Speichern von Bitstreams die drei Funktionen Suchbarkeit, Identifizierbarkeit und Interpretierbarkeit bieten. Um ein archiviertes Datenobjekt anhand bestimmter Kriterien suchen zu können, werden in der Regel zusätzliche, das Datenobjekt beschreibende Daten erfasst. Solche inhaltsbeschreibenden Metadaten, wie sie beispielsweise in Bibliothekskatalogen zu finden sind, bilden, insbesondere bei nicht textuellen Daten, oft die einzige Möglichkeit, ein Archiv effizient zu durchsuchen. Neben den inhaltlichen Metadaten gibt es noch eine Reihe anderer, z. T. speziell für die Archivierung relevanter technischer oder administrativer Metadaten. Die oben angeführte Heterogenität zu archivierender Daten erschwert eine Festlegung einheitlicher Metadatenstandards für Archivsysteme erheblich. Weiter unten wird daher auch ein Archivsystem vorgestellt werden, das die inhaltlichen Metadaten extern verwaltet und die zugehörigen Informationsobjekte über eine eindeutige Referenz mit diesem externen System verbindet. Die langfristige Gültigkeit solcher Identifikatoren ist von entscheidender Bedeutung, um den wissenschaftlichen und kulturellen Wert von Archivinhalten zu bewahren. Denn nur mittels langfristig gültiger Identifikatoren bleiben die Datenobjekte ggf. auch systemübergreifend auffindbar und zuverlässig zitierbar. Die Identifikatoren müssen daher den gleichen langfristigen Bestand haben wie die archivierten Datenobjekte selbst[1].

Der wichtigste Punkt hinsichtlich der Verfügbarkeit von archivierten Daten liegt jedoch darin, dass der gesicherte Bitstream interpretierbar bleiben muss. Im Gegensatz zu analogen Daten, z.B. Druckerzeugnissen, reicht es bei digitalen Daten nicht aus, lediglich das Trägermedium zu sichern. Ein Buch ist in der Regel menschenlesbar, solange es physisch ausreichend

1. Weiterführende Informationen zu dem Themenbereich „persistent identifier“ finden sich unter: www.persistent-identifier.de [2004, 21. März]

erhalten bleibt. Eine gesicherte Datei dagegen kann aufgrund ihres veralteten Formats, auch wenn die Diskette, das Magnetband oder die CD-ROM völlig unbeschädigt sind, wertlos sein, da sie nicht mehr interpretierbar ist. An dieser Stelle liegt die größte Herausforderung der Langzeitarchivierung. Der technologische Wandel muss systematisch beobachtet werden, um zu reagieren, bevor Informationen unzugänglich werden.

4. Emulation oder Migration?

Zur Sicherung der Interpretierbarkeit eines archivierten Bitstreams werden zwei Grundstrategien verfolgt. Hinter beiden steht das Ziel, stets eine EDV-Umgebung verfügbar zu haben, mittels derer die enthaltenen Daten wieder lesbar gemacht werden können.

Ein Ansatz besteht darin, eine veraltete EDV-Umgebung nachzubilden. Dabei kann es sich sowohl um eine Hardware- als auch um eine Softwareemulation handeln. In einer so emulierten Umgebung kann das archivierte Datenobjekt dann interpretiert und menschenlesbar dargestellt werden. Der Vorteil eines solchen Vorgehens liegt darin, dass keine Veränderungen am Datenobjekt erforderlich sind. Der Nachteil ist, dass es sich in der Regel um eine sehr aufwendige Technik handelt.

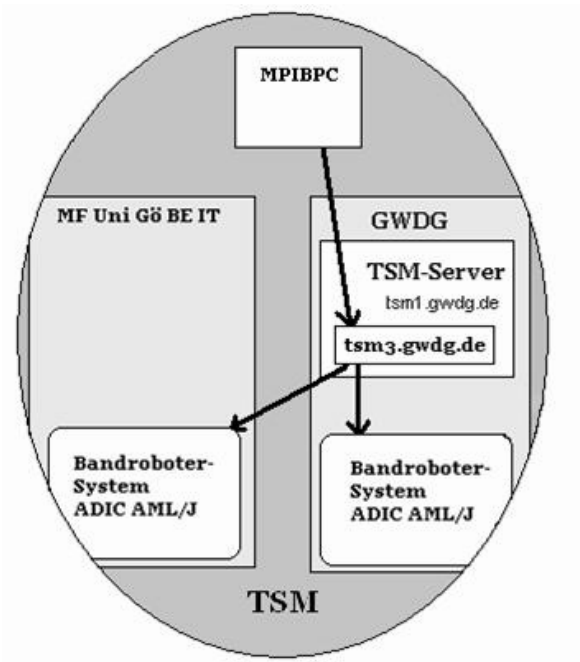
Demgegenüber steht die Migration von Datenobjekten in ein aktuelles Format. Diese Lösungsmöglichkeit ist die derzeit häufigste. Der Vorteil der Migration liegt auf kurze Sicht in ihrer Einfachheit. In der Praxis ist es in der Regel leichter, eine einzelne Datei einer neuen Umgebung anzupassen als die ganze Umgebung an die Datei. Langfristig jedoch hat diese Einfachheit einen nicht unbeträchtlichen Preis. Jede Änderung des ursprünglichen Datenobjekts birgt die Gefahren seiner möglichen Beschädigung oder sogar seines Verlusts. Mit Blick darauf, dass die Migration das Original verändert, ergibt sich zwangsläufig auch die Frage, was als Original zu verstehen ist. So kann z.B. bei einer Keilschrifttafel für den Archäologen auch die Textur der Tonoberfläche wichtige Informationen enthalten und digitale Fotos einer solchen Tafel sind für ihn ggf. nur in sehr hoher Auflösung eine geeignete Arbeitsgrundlage. Ein Literaturwissenschaftler dagegen wird hauptsächlich an dem textuellen Inhalt Interesse haben und möglicherweise sogar mit einer guten Abschrift arbeiten können. Auf welche Darstellungsaspekte bei der Migration einer entsprechenden Bilddatei am ehesten verzichtet werden kann, ist oft eine schwierige Frage, die nur mit Blick auf die Nutzergruppe des Archivsystems sinnvoll beantwortet werden kann.

5. Beispiele

Im Folgenden sollen einige Beispiele bestehender Archivierungsverfahren erste Lösungsansätze zu den aufgezeigten Problemen vorstellen.

5.1 Langzeitarchivierung GWDG / Max-Planck-Institut für biophysikalische Chemie (MPI BPC)

Das MPI BPC hat auf Grund der vom Senat der Max-Planck-Gesellschaft am 24. November 2000 veröffentlichten „Regeln zu Sicherung guter wissenschaftlicher Praxis“ die Verpflichtung, Daten von Wissenschaftlern, die für Veröffentlichungen genutzt wurden, über zehn Jahre aufzubewahren. Der Focus des Interesses liegt auf einer zuverlässigen, unkomplizierten Speicherung von Datenbeständen zur Erfüllung dieser Aufbewahrungspflicht und nicht so sehr auf Aspekten einer späteren Nutzung der Daten. Daher ist dieses Beispiel gut geeignet, um besonders die Seite der Bitstream-Preservation zu beleuchten. Im vorliegenden Fall wird die Sicherung der Daten durch Nutzung des Archivsystems der GWDG mit seiner redundanten räumlich verteilten Datenhaltung realisiert.



In Göttingen stehen an räumlich getrennten Standorten zwei Magnetband-Roboter des Typs ADIC AML/J mit je einer Kapazität von 200 TByte und 270 TByte zur Verfügung. Als Standorte dienen die Betriebseinheit IT im Universitäts-Klinikum und die GWDG selbst. Zwischen beiden Gebäuden liegt eine ungefähre Distanz von drei Kilometern. Die Daten des MPI BPC werden an beiden Standorten gehalten. Das Einstellen der Daten erfolgt über ein einfaches HTML-Eingabe-Interface. Aus den dort gemachten Angaben wird eine Informationsdatei erstellt. Über die eingestellten Daten wird eine MD5-Checksumme generiert. Alle Daten werden anschließend über den vereinbarten Zeitraum von 10 Jahren aufbewahrt und nach Ablauf dieser Zeitspanne gelöscht. Das Verfahren ist unkompliziert und erfüllt seinen vorgegebenen Zweck, einer Aufbewahrungspflicht von zehn Jahren nachzukommen.

5.2 DoBeS: Dokumentation Bedrohter Sprachen[2]

DoBeS ist ein Projekt des Max-Planck-Institutes für Psycholinguistik (MPI PL) in Nijmegen, Niederlande. Es handelt sich um digitale Sprachaufzeichnungen aussterbender Sprachen. Diese Aufzeichnungen umfassen Video-, Audio- und auch Textdateien. Der kulturelle Wert dieser Daten und die sehr lange Archivierungsdauer geben diesem Projekt seine besondere Bedeutung. Die betroffenen Daten wären im Verlustfall nicht wieder herstellbar, da niemand die betroffenen Sprachen mehr beherrscht. Ihr Verlust würde bedeuten, dass die Menschheit einen wesentlichen Teil ihres Sprachschatzes für immer verliert. Gleichzeitig ist die Dauer der Aufbewahrung nicht absehbar. Zwar wird aktuell ein Zeitraum von 50 Jahren betrachtet, doch ist der tatsächlich erforderliche Archivierungszeitraum unbegrenzt, solange das Interesse am sprachlichen Erbe anhält.

Um dieser besonderen Aufgabe gerecht zu werden, haben sich die Projektbeteiligten für ein Vorgehen entschieden, dass auf eine Vielzahl von Kopien an unterschiedlichen Standorten setzt. Im Gegensatz zum zuvor vorgestellten Projekt, bei dem eine redundante Datenhaltung bei räumlicher Trennung genutzt wird, setzt DoBeS auf die Sicherung der Daten über Institutionsgrenzen hinaus. Zu diesem Zweck wurde mit verschiedenen Rechenzentren Kontakt aufgenommen. Derzeit werden die Daten in zwei Rechenzentren der Max-Planck-Gesellschaft in Garching (RZG) und Göttingen (GWDG) sowie am MPI PL selbst gehalten. Auf diesem Wege wird eine Vielfalt

2. http://www.mpi.nl/DOBES/ [2004, 21. März]

sowohl hinsichtlich der eingesetzten Technik als auch der institutionellen und organisatorischen Strukturen erreicht.

Das hohe Maß an langfristiger Sicherheit der Daten dieses Projektes zeigt exemplarisch einen besonderen Aspekt der Langzeitarchivierung, der leicht übersehen werden kann. Langfristige Sicherheit und Zugänglichkeit von Daten wirft nicht nur technische Fragen auf, sondern auch organisatorische, institutionelle und, im Falle vergleichbar langer Zeiträume, sogar politische.

5.3 Das Archivsystem der Koninklijke Bibliotheek in Den Haag (KB)

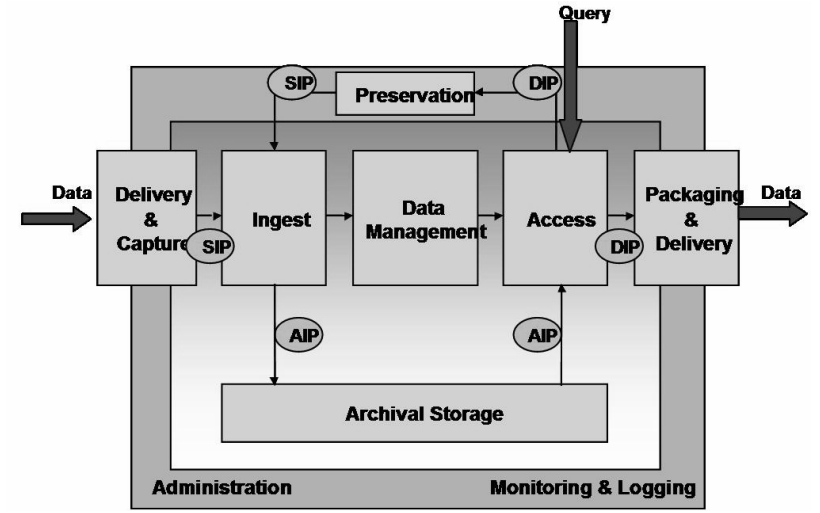
Bevor das Archivsystem der Königlichen Bibliothek in Den Haag im folgenden Kapitel vorgestellt wird, soll noch kurz auf ein für Digitale Archive wichtiges Referenz-Modell eingegangen werden.

Das OAIS-Referenz-Modell[3]

Das „Reference Model for an Open Archival Information System“, kurz OAIS-Referenz-Modell, bildet die unterschiedlichen Funktionseinheiten in einem Digitalen Archiv ab. Hierzu gehören die Funktionseinheiten „Delivery & Capture“ sowie „Ingest“, die den Eingabevorgang in das Archivsystem umfassen. Die Funktionseinheit „Datamanagement“ bildet die Metadatenverarbeitung ab. „Access“ und „Packaging & Delivery“ beschreiben den Ausgabevorgang. In der Funktionseinheit „Archival Storage“ erfolgt die eigentliche Speicherung der Daten. Die Funktionseinheit „Preservation“ dient der Sicherstellung der Langzeitverfügbarkeit, also der langfristigen

3. Consultative Committee for Space Data Systems (CCSDS), *Reference Model for an Open Archival Information System (OAIS)*, Washington, DC 20546, Januar 2002. Verfügbar: http://ssdoo.gsfc.nasa.gov/nost/isoas/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf [2004, 21. März]

Interpretierbarkeit der Datenobjekte. Dieses Modell[4] erlaubt eine differenzierte Sicht auf die verschiedenen Prozesse in einem Archiv.



Das im folgenden Abschnitt vorgestellte Archivsystem der Königlichen Bibliothek der Niederlande in Den Haag entspricht weitgehend diesem Modell.

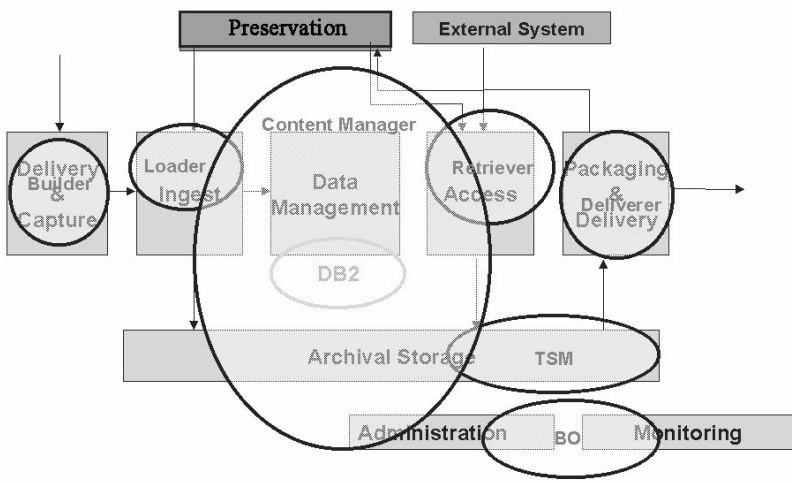
Digital Information Archiving System (DIAS[5]):
Das Archivsystem der Koninklijke Bibliotheek in Den Haag (KB)

Gemeinsam mit IBM wurde an der Königlichen Bibliothek in Den Haag ein System entwickelt, das auf den IBM-Produkten DB2, Content Manager und

4. Grafik entnommen aus: Van Diessen, Raymond J, *Preservation Requirements in a Deposit System*, Amsterdam, IBM Niederlande, Dezember 2002, IBM/KB Long-Term Preservation Study Report Series Number 3, Seite 4. Verfügbar: http://www-5.ibm.com/nl/dias/resource/preservation.pdf [2004, 21. März]

5. http://www-5.ibm.com/nl/dias/ [2004, 21. März]

Tivoli Storage Manager basiert. Die untenstehende Grafik[6] zeigt den Aufbau des Systems.



Die zentralen Komponenten des OAIS-Referenz-Modells sind leicht wiederzuerkennen. Der Bereich „Archival Storage“ umfasst die Aufgaben der „Bitstream Preservation“, der Bereich „Preservation“ beinhaltet die Funktionen zur Gewährleistung der Langzeitverfügbarkeit. Bei diesem Beispiel soll der Focus auf das „External System“, von dem aus ein Informationsobjekt angefordert wird, und auf die Funktionseinheit „Preservation“ gelenkt werden.

Bei dem „External System“ handelt es sich um den Bibliothekskatalog der KB, in dem alle bibliografischen Metadaten der Archivobjekte verwaltet werden. Die Verwaltung inhaltsbeschreibender Metadaten findet hier also nicht innerhalb des eigentlichen Archivsystems statt, sondern verbleibt im Bibliothekskatalog. Die Verbindung von Katalog und Archivsystem wird durch eindeutige Referenzen auf die Archivobjekte gesichert. Die langfri-

6. Grafik entnommen aus: Van Diessen, Raymond J. und Steenbergen, Johan, *The Long-Term Preservation Study of the DNEP Project - an Overview of the Results,* Amsterdam, IBM Niederlande, Dezember 2002, IBM/KB Long-Term Preservation Study Report Series Number 1, Seite 6. Verfügbar: http://www-5.ibm.com/nl/dias/resource/overview.pdf [2004, 21. März].

stige Eindeutigkeit solcher Referenzen im Sinne eines „Persistent Identifier“ zu gewährleisten, ist ein Entwicklungziel von DIAS.

Die Funktionseinheit „Preservation“ beinhaltet diejenigen Funktionen des Systems, die die Langzeitverfügbarkeit der Datenobjekte sicherstellen sollen.

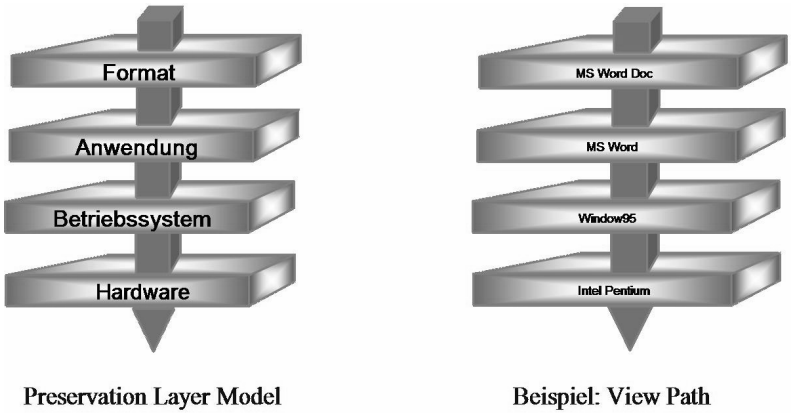
Arbeiten an der KB im Bereich Langzeitverfügbarkeit (Funktionseinheit „Preservation“)

Im Rahmen der Entwicklung von DIAS wurden bereits erste Konzepte entwickelt, um die langfristige Verfügbarkeit der archivierten Daten zu sichern.

„Preservation Layer Model“ und „View Path“

Um ein digitales Datenobjekt lesbar zu halten, muss eine entsprechende Plattform verfügbar sein. Diese umfasst Hardware, Betriebssystem und Anwendungssoftware. Eine funktionsfähige Kombination dieser Ebenen wird als gültiger „View Path“ eines digitalen Datenobjektes angesehen und dem entsprechenden Objekt zugeordnet. Um rechtzeitig zu erkennen, wann ein Datenobjekt Gefahr läuft, dass kein gültiger View Path mehr erhalten ist, wurde an der KB ein Modell entwickelt, dass die möglichen View Paths in ihre Komponenten zerlegt, das „Preservation Layer Model“. Wird eine Komponente obsolet, lässt sich automatisch feststellen, welche View Paths davon betroffen sind und somit welche Datenobjekte. Auf der Grundlage dieser Erkenntnis kann dann entweder eine Emulationsstrategie entwickelt oder eine Migration betroffener Datenobjekte angegangen werden.

Die nachstehende Grafik[7] zeigt die Beziehungen von View Path und Preservation Layer Model.

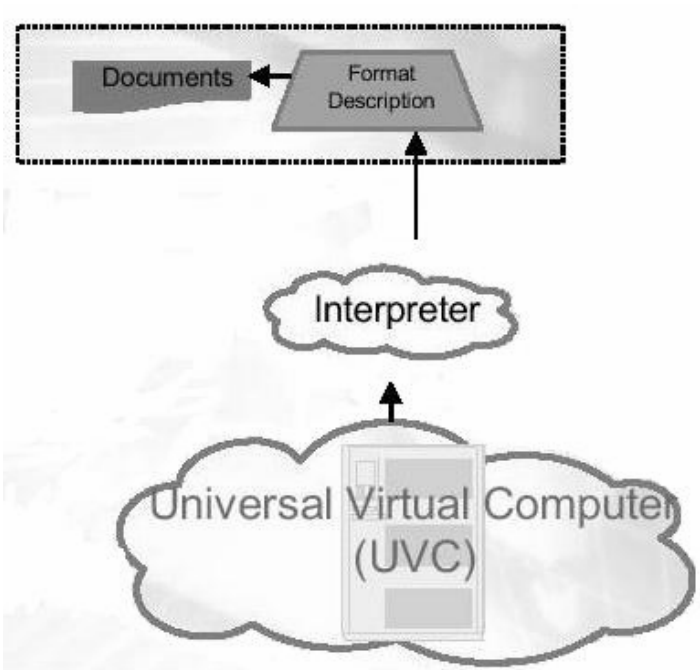


Preservation Layer Model | Beispiel: View Path

7. Die Grafiken wurden einer Präsentationsfolie von Dr. Raymond van Diessen, IBM, entnommen. Die Präsentation fand im Rahmen eines Content Manager User Workshops am 09. Mai 2001 in Amersfoort statt. Die Grafiken wurden geringfügig verändert.

Universal Virtual Computer (UVC)

Einen interessanten Lösungsansatz im Bereich Emulations- und Migrationsstrategien hat IBM mit dem Konzept[8] des „Universal Virtual Computer“ entwickelt.



Dieses Konzept stellt eine Kombination aus Emulation und Migration dar. Auf der einen Seite wird ein sehr einfaches Modell einer Interpretationsplattform entworfen. Die Spezifikation ist so einfach gehalten, dass sie leicht auf jeder beliebigen realen Hardware emuliert werden kann. Das zu interpretierende reale Dateiformat bleibt erhalten, jedoch nicht, um selbst interpretiert zu werden, sondern, um im Bedarfsfall auf der Basis einer Formatanalyse von einer auf der UVC-Plattform laufenden Interpretationssoftware dargestellt zu werden. Wenn die Emulation des UVC auf aktueller Hardware gesi-

8. Die Grafik wurde einer Präsentationsfolie von Joost Hubregtse, IBM Global Services, entnommen. Die Präsentation fand im Rahmen eines Content Manager User Workshops am 05.-06. September 2002 in Essen statt.

chert ist und für das jeweilige Dokument eine entsprechende Formatanalyse erstellt wurde, kann die langfristige Interpretierbarkeit des digitalen Dokuments als gewährleistet angesehen werden[9].

Übergangslösung „Reference Workstation"

Eine für die Archivierung besonders schwierige Aufgabe stellen installierbare Datenobjekte dar. Das sind Datenobjekte, die auf einem Rechner installiert werden müssen, um ihre Informationsgehalt zugänglich zu machen. Solche „installables" können z.B. Datenbanken oder multimediale Lexika sein. Für diese Sorte Datenobjekte hat die KB eine Interimslösung entwikkelt. Vor Ort wurden genau spezifizierte PCs aufgestellt, die eine kontrollierte Hard- und Software-Umgebung darstellen. Sie können auch als eine konkrete Repräsentation eines der oben beschriebenen möglichen View Paths angesehen werden. Auf diesen Rechnern werden die betroffenen Datenobjekte installiert und anschließend wird ein komplettes Disk-Image archiviert. Im zukünftigen Bedarfsfall kann dieses Disk-Image auf der ursprünglichen Hardware an der KB wieder zugänglich und nutzbar gemacht werden.

Dieser Ansatz zeigt zum einen, wie unbefriedigend derzeitige Lösungen oft noch sein müssen, aber auch, dass ein einfacher pragmatischer Ansatz oft die einzige reale Lösung darstellt. Solche Ansätze gewährleisten, dass ein Informationsverlust verhindert wird bis umfassendere Lösungen vorliegen.

9. Eine ausführliche Beschreibung der Funktionsweise des UVC findet sich in: Lorie, Raymond, *The UVC: a Method of Preserving Digital Documents – Proof of Concept,* Amsterdam, IBM Niederlande, Dezember 2002, IBM/KB Long-Term Preservation Study Report Series Number 4. Verfügbar: http://www-5.ibm.com/nl/dias/resource/uvc.pdf [2004, 21. März]

Nutzung des CMS der Fa. Infopark durch die GWDG

Wilfried Grieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Einleitung

Auf dem ersten DV-Treffen der Max-Planck-Institute, das in Göttingen stattfand und von der GWDG organisiert wurde, nämlich 1993, wurde von der GWDG das gerade neue World Wide Web vorgestellt. Damals wurde es allgemein bestaunt und vielleicht sogar als elitäre Spielwiese abgetan. Mittlerweile hat es sich vehement durchgesetzt. Das WWW ist aus unserer Alltagswelt kaum noch wegzudenken.

Vergessen sind Parallelentwicklungen, die es natürlich auch gegeben hat, beispielsweise das Hyper-G der Universität Graz aus dem Jahr 1994, das später noch Hyperwave genannt wurde, um etwas mehr an das Surfen zu erinnern. Wenn sich Hyper-G anstelle des WWW durchgesetzt hätte, müssten heute Browser mit Namen Harmony (unter Unix) oder Amadeus (unter Windows) bedient werden. Die Software wurde eben in Österreich entwikkelt.

Die Vorteile von Hyper-G gegenüber dem WWW waren:

1. Das Informationsangebot war hierarchisch strukturiert, die Navigation erfolgte sowohl entlang der Links als auch innerhalb der Struktur.
2. Alle Dokumente wurden automatisch beim Einfügen indiziert. Die Suche konnte nach Titeln, Stichwörtern oder auch im Volltext erfolgen.
3. Die Hyperlinks wurden auf Konsistenz überwacht und nötigenfalls automatisch aktualisiert.
4. Die Browser waren zu allen wichtigen Informationssystemen offen: zum WWW, Gopher usw.

„Sicherlich ist die Anfangshürde beim Aufbau eines Informationsangebotes bei Hyper-G höher als in anderen Informationssystemen, weil die Dokumente nicht wie z. B. im WWW-Server über das Dateisystem verwaltet werden, sondern nur über systemeigene Schnittstellen mit neuen, zunächst unbekannten Funktionen. Aber nur dadurch, dass der Benutzer nicht direkt auf Betriebssystemebene die Dokuemnte manipuliert, kann sichergestellt werden, dass das Informationsangebot jederzeit konstistent und damit professionell erstellt ist.“[1]

Wenn damals Hyper-G den Wettlauf um das komfortabelste Informationssystem gewonnen hätte, wäre heute ein Vortrag über das Content Management System (CMS) der Firma Infopark überflüssig.

1. Das Content Management System NPS

Die Max-Planck-Gesellschaft hat zur Verwaltung ihrer WWW-Seiten und für weitere Anwendungen das Content Management System NPS der Firma Infopark beschafft. Dieses System steht auch allen angeschlossenen Instituten zur Nutzung zur Verfügung. Für die Max-Planck-Institute steht ein „Baukasten“ bereit, mit dem die einzelnen Institute ihre WWW-Seiten gestalten können. Alle Daten werden in einer Datenbank, nämlich Oracle, gespeichert und verwaltet.

Um jedoch das CMS in seiner inneren Struktur besser zu verstehen, hat die GWDG ein Projekt begründet, das die Migration des Inhalts des bestehenden WWW-Servers der GWDG in das CMS vorsieht und nicht den Baukasten der Max-Planck-Gesellschaft verwendet. Die GWDG ist dazu zunächst ein eigenständiger Mandant des CMS geworden.

---

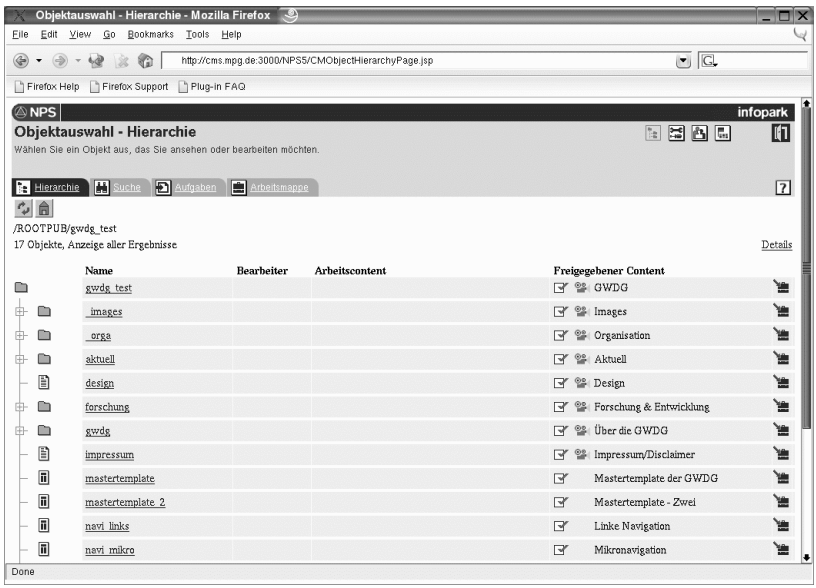
1. W. Dalitz, G. Heyer: Hyper-G - Das Internet-Informationssystem der 2. Generation, Heidelberg 1995

2. Struktur des WWW-Servers im CMS

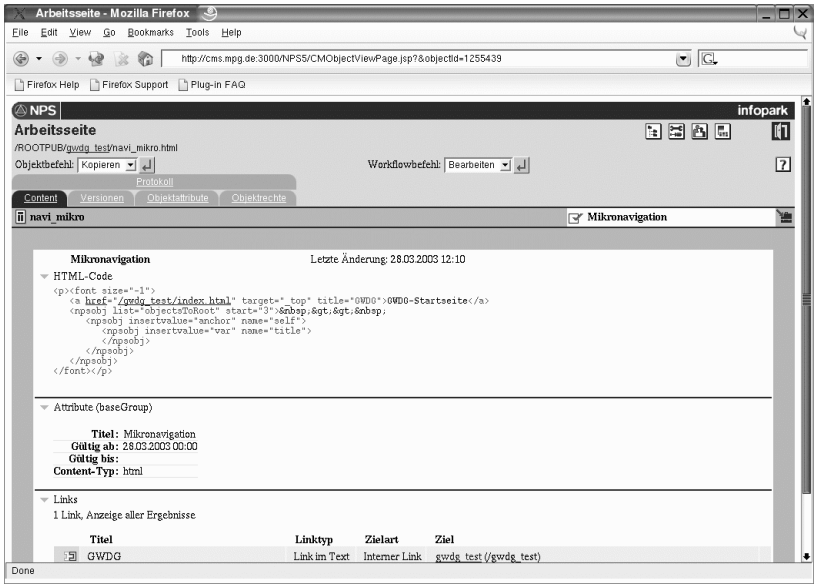
Als erstes wurde die Struktur des Inhalts des aktuellen WWW-Servers unter dem URL

`http://www.gwdg.de`

im CMS nachgebildet:



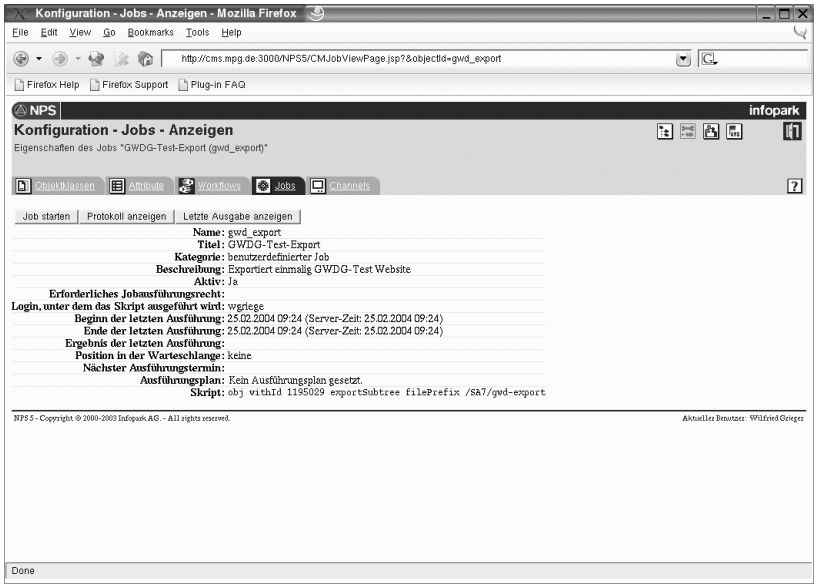
Der Aufbau der einzelnen Seiten erfolgt dabei durch die Templates. Insbesondere wird die Mikronavigation durch das Template *navi_mikro* gesteuert:



Zu beachten ist dabei die Sprache *npsobj*, die eigens für das CMS entwickelt wurde und Abläufe automatisiert. Die Syntax ist HTML-ähnlich.

In der Vorschau lassen sich dann die Seiten anzeigen:

Damit liegen die Seiten jedoch noch nicht auf dem aktuellen WWW-Server. Sie müssen noch exportiert werden, was mit Hilfe eines Jobs erfolgen kann:



Nach dem Ausführen des Jobs werden die Seiten aus dem CMS auf den aktuellen WWW-Server kopiert, so dass sie im WWW öffentlich verfügbar sind.

Der Einfluss des GÖ*-Projektes auf die MPG

Hartmut Koke

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

1. Ausgangslage

Das GÖ*-Projekt entstand aus einem von der DFG initierten Innovationswettbewerb an deutschen Hochschulstandorten mit dem Ziel, Leistungszentren durch Schaffung eines integrierten Informationsmanagement im Verbund von Rechenzentrum, Bibliothek, Medienzentrum sowie den Informationseinrichtungen der Fachbereiche bzw. Institute und anderer Forschungseinrichtungen aufzubauen

GÖ* ist ein gemeinsamer Antrag der Universität Göttingen und ihres Bereichs Humanmedizin, der in Abstimmung mit der Max-Planck-Gesellschaft eine höchst leistungsfähige IT/ID-Dienstleistungsumgebung für alle Forschenden, Lehrenden und Lernenden bereitstellen will.

GWDG

1

Der Einfluss des GÖ*-Projektes auf die MPG

21. November 2003

Hartmut Kolle

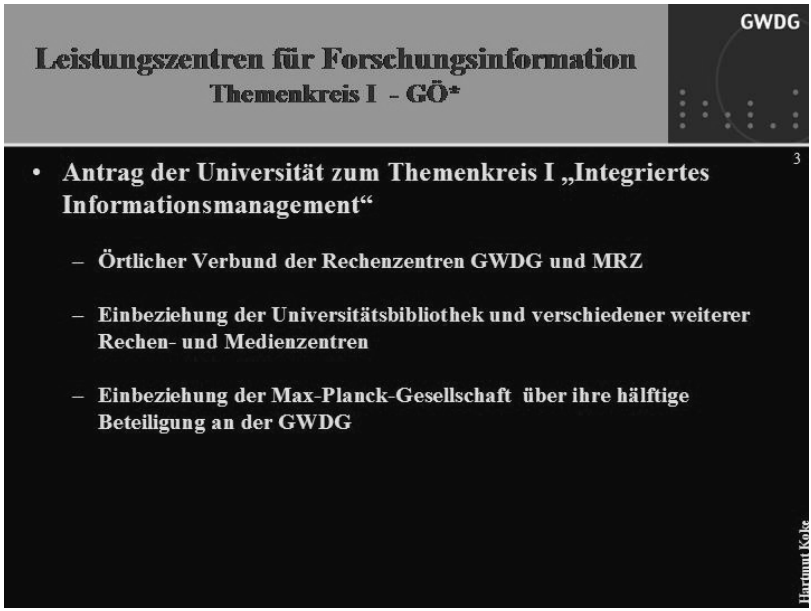
GWDG

Leistungszentren für Forschungsinformation
Förderinitiative der DFG

2

- **Innovationswettbewerb an einzelnen Hochschulstandorten durch Aufbau von Leistungszentren**
  - **Themenkreis I**
    - **Integriertes Informationsmanagement an Hochschulen durch neuartige Organisationsmodelle im Verbund von Rechenzentrum, Bibliothek, Medienzentrum sowie den Informationseinrichtungen der Fachbereiche bzw. Institute.**
  - **Themenkreis II**
    - **Digitale Text- und Datenzentren zur Sammlung, Sicherung und Bereitstellung von digitalen Quellenbeständen und Datengrundlagen für Forschung und Lehre.**

Hartmut Kolle



2. Globale Ziele

Zur Verbesserung der Informationsversorgung und -leistungen für die Nutzer der Universität Göttingen, des Bereichs Humanmedizin und der Max-Planck-Institute soll die Leistungsfähigkeit der IT- und der Informationsdienstleister am Standort durch Kooperation und konsequente Nutzung von Synergieeffekten gesteigert werden.

Hauptziele sind dabei:

2.1 Wirtschaftlichkeitssteigerung

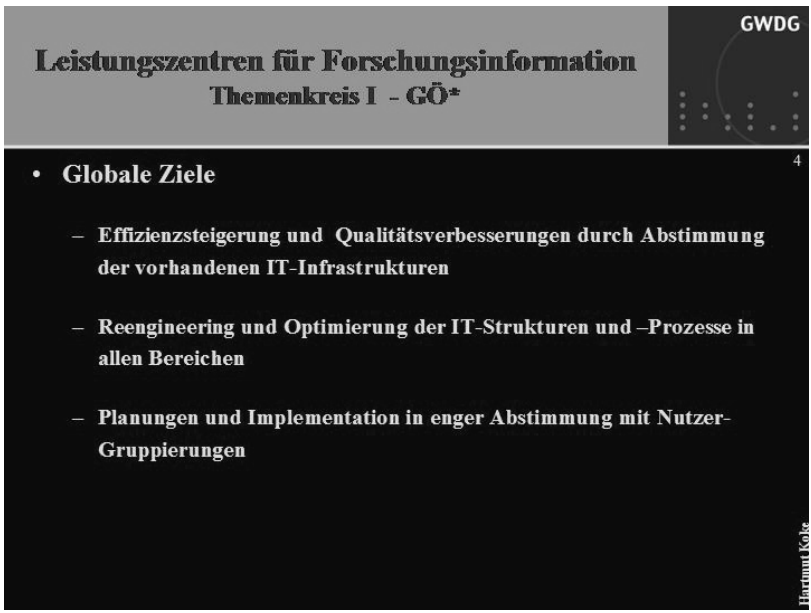
Durch die systematische Bündelung von gemeinsamen Funktionen und Bildung von Kernkompetenzen der einzelnen Dienstleister können auch bei begrenzten Budgets hohe bzw. steigende Anforderungen der Nutzer erfüllt werden. Die Steigerung der Leistungsfähigkeit wird zum einen durch die Optimierung der Abläufe, d.h. durch Produktivitätssteigerung von Geschäftsprozessen, zum anderen durch Ausrichtung auf Elemente einer maßgeschneiderten IT/ID-Infrastruktur durch Kosten sparende Ansätze wie „Capacity on Demand“ und „Ressourcen-Sharing“ erreicht.

2.2 Gestaltung und Optimierung von gemeinsamen Geschäftsprozessen

Für eine Kooperation der Dienstleister sind gemeinsame Geschäftsprozesse notwendig. Diese müssen exakt definiert werden. Ihre Leistung muss anhand von Kennzahlen mess- und vergleichbar gemacht sowie überwacht werden.

2.3 Bereitstellung und Virtualisierung von kundenindividuellen Informationsservices

Der Zugriff auf die komplexen im GÖ*-Umfeld gebotenen Vorgänge und Leistungen muss für den Anwender virtualisiert werden, um die Benutzerfreundlichkeit zu erhöhen. Der Nutzer muss auch auf komplexe Leistungen einfach zugreifen und sie nach seinen Vorstellungen anpassen können. Dazu ist eine enge Abstimmung mit den einzelnen Nutzergruppierungen erforderlich.



3. Technische Kernziele

Zu den Kernaufgaben, die durch schnelle Innovationen geprägt sind und zugleich erhebliches Know-how in der organisatorischen und technischen Umsetzung erfordern, gehören folgende Themenkreise:

3.1 Ubiquitärer Informationszugriff sowie Erzeugung, Speicherung und Archivierung von Informationen in einer für den Nutzer transparenten Form, die die Komplexität von Netzwerk-Strukturen und -Technologien sowie der zugrunde liegenden verteilten Ressourcen verbirgt. Dazu müssen bereitgestellt werden:

- Single SignOn, Authentifizierung und Verzeichnisdienste, Sicherheit (Verschlüsselungsverfahren usw.)

  Um verteilte Daten und Ressourcen gesichert im Netzwerk, auch über verschiedene Betriebssysteme hinweg, zur Verfügung zu stellen, ist eine plattformübergreifende Authentifizierung notwendig. Dies ist eine Voraussetzung für „Single SignOn"-Lösungen, die es dem Benutzer ermöglichen, sich mit seinem Benutzernamen und Kennwort in der Gesamtstruktur anzumelden und danach die Daten zu referieren beziehungsweise Ressourcen und Dienste zu benutzen, für die ihm die Berechtigung eingeräumt wurde.

- Abgestuftes System von Netzwerkverbindungen, das durchgehend vom aktuellen Arbeitsplatz zu lokalen und externen Informationsquellen adäquate Übertragungsleistungen, -medien und Qualitätsmerkmale bereitstellt.

- Bereitstellung von Rechen- und E/A-Leistung

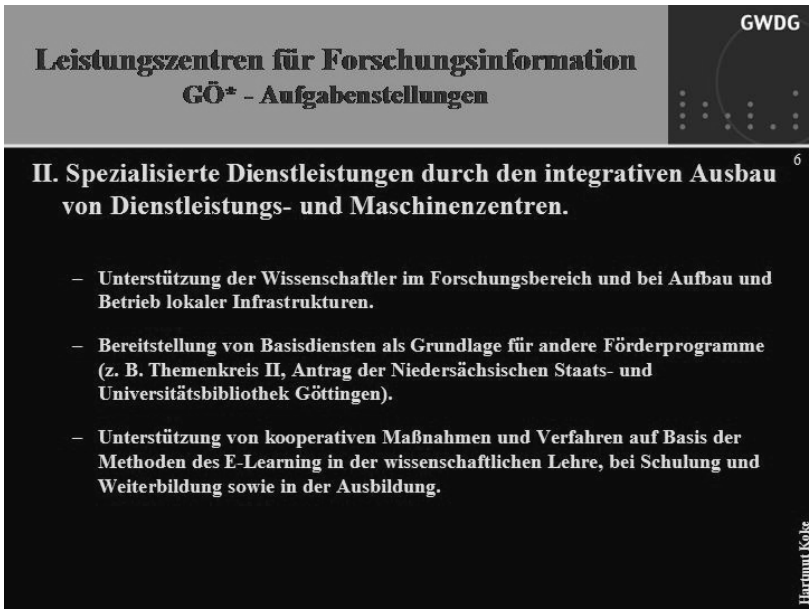
- Der wachsende Bedarf an Parallelrechnerleistung macht eine Erweiterung der Parallelrechnerkapazität notwendig. Es liegt nahe, neben den vorhandenen Parallelrechnersystemen von IBM ein Parallelrechner-Cluster auf der Basis von PC-Hardware und dem Linux-Betriebssystem aufzubauen; mit einem System von ca. 200 Prozessoren kann ein großer Teil des zusätzlichen Bedarfs gedeckt werden. Ein solches Linux-Cluster bietet die Rechenleistung zu einem sehr viel günstigeren Preis, allerdings ohne die hohe Interprozessor-Kommunikationsleistung der IBM-Multiprozessorsysteme. Die breite Streuung der Anforderungen der verschiedenen Nutzergruppen garantiert die Auslastung beider Systeme, wenn die Anwendungen anforderungsbezogen auf die unterschiedlichen Rechnersysteme verteilt werden.

- Leistungsfähige Speicher-, Backup-, und Archivierungs-Systeme, die, unter Nutzung von SAN-Technologien, auch in einem verteilten Umfeld, flexibel administriert werden können.

- Allgemeine Web-Services, Portale, Hilfsdienste (Mediendienste, CMS, FM usw.)

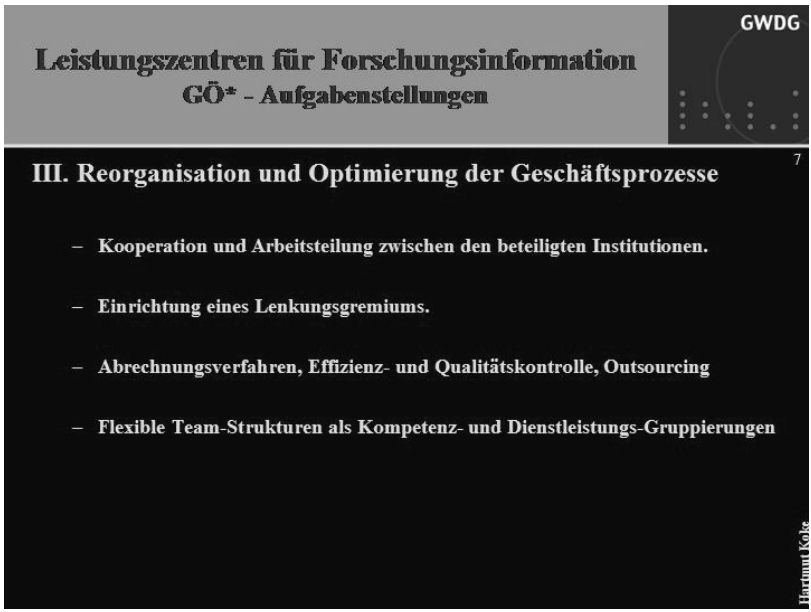
3.2 Spezialisierte Dienstleistungen durch den integrativen Ausbau von Dienstleistungs- und Maschinenzentren

- Unterstützung der Wissenschaftler im Forschungsbereich und bei Aufbau und Betrieb lokaler Infrastrukturen
- Bereitstellung von Basisdiensten als Grundlage für andere Förderprogramme (z.B. Themenkreis II, Antrag der Niedersächsischen Staats- und Universitätsbibliothek in Göttingen)
- Unterstützung von kooperativen Maßnahmen und Verfahren auf Basis der Methoden des E-Learning in der wissenschaftlichen Lehre, bei Schulung und Weiterbildung sowie in der Ausbildung



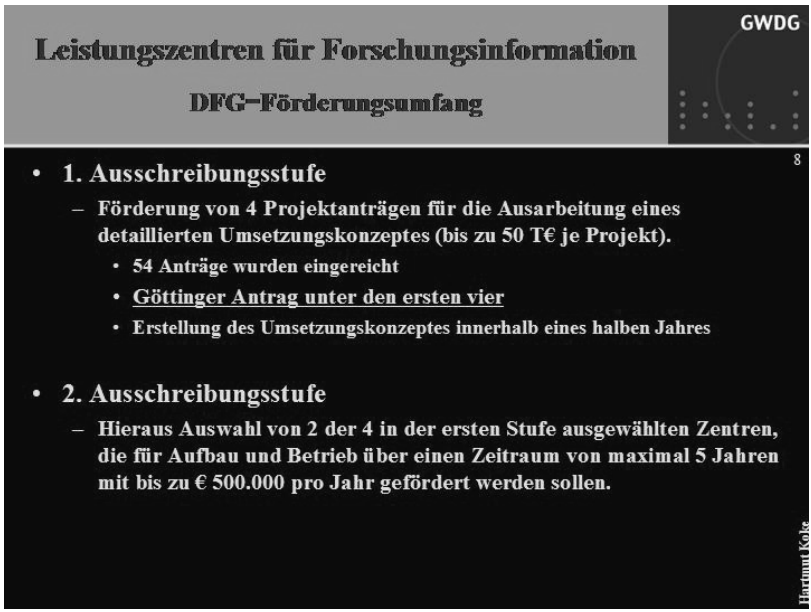
3.3 Reorganisation und Optimierung der Geschäftsprozesse

- Kooperation und Arbeitsteilung zwischen den beteiligten Institutionen
- Einrichtung eines Lenkungsgremiums
- Abrechnungsverfahren, Effizienz- und Qualitätskontrolle, Outsourcing
- Flexible Team-Strukturen als Kompetenz- und Dienstleistungs-Gruppierungen



Zur Zeit erfolgt die Ausarbeitung des Antrages für die Teilnahme in der 2. Stufe. Die Konzeptionsphase ist bereits weitgehend abgeschlossen:

- Schwerpunktsetzung im Bereich „Nutzerorientierung“
- Definition und Optimierung des Dienstleistungsangebotes
- Steuerung der Investitionsvorhaben nach GÖ*-Zielvorgaben
- Organisationsstrukturen



Die Förderung dieses Antrags wird die Integration bisher getrennter Abläufe und die Bündelung von personellen und maschinellen Ressourcen am Göttinger Wissenschaftsstandort in erheblichem Ausmaß ermöglichen.

Durch Einbeziehung der Max-Planck-Gesellschaft und durch überregionale Kooperationen werden über den örtlichen Zusammenhang hinaus wichtige Impulse für die Lösung der auch im internationalen Kontext relevanten Problemstellungen erwartet.

Die folgenden Folien 10-18 sind selbsterklärend und beschreiben eine Reihe von Projekten, die im Zusammenhang mit GÖ* stehen und im Vorgriff auf die geplanten Zielsetzungen unmittelbare Relevanz für die Institute der MPG aufweisen.

Dazu zählen das Content-Management-System, das eDOC-Server-Projekt im Zusammenhang mit den Vorhaben zur Langzeitarchivierung, verschiedene Einzelprojekte zur Stärkung der IT-Sicherheit und die Einrichtung von Verzeichnisdiensten, die Umsetzung von Konzepten zur einheitlichen Authentifizierung einschließlich einer umfassenden PKI-Infrastruktur.

Applikationsserver für die MPG

GWDG

10

- Content Management Projekt der MPG (+ GWDG)
  - Einführung eines Content Management-Systems durch die Pressestelle
    - CMS NPS5 von Infopark ausgewählt
    - 2-tägiger Workshop im Juli in Göttingen mit Vertretern aus allen Instituten
    - Mehrtägiger Administrator Kurs in Göttingen
    - Aufbau der zentralen NPS- und DatenbankServer in der GWDG im November 02 abgeschlossen
    - Software-Installation durch von der MPG beauftragte Firma
      - Betriebsfertige Übergabe noch im Februar 2003
  - Eigene Content Projekte der GWDG
    - WWW-Server der GWDG als Pilotprojekt
    - Dienstleistungen für Institute

Hartmut Kolle

Applikationsserver für die MPG

GWDG

Metadata Initiative am 29.2.

11

- E-Document Server für die MPG
  - Angebot der GWDG für die Bereitstellung eines professionellen E-Document Systems
    - Basis für das eDocument-Server Projekt der MPG
      - System zum Verwalten und Veröffentlichen von wissenschaftlichen Dokumenten
  - Realisierung des Angebotes
    - 2 Server mit je 1,6 TB Plattenspeicher, Spiegelbetrieb
    - Systembetreuung durch GWDG, Arbeitsteilung GWDG/ZIM
    - Backup auf Bandroboter der GWDG

Max Planck Society eDoc-Server

Hartmut Kolle

GWDG

IT-Sicherheit

..... Sicherheit (Verschlüsselungsverfahren usw.)

12

- **Wachsendes Bedrohungspotential**
  - **Gefährliche Symbiose von Hackern und Virenschreibern**
- **Zunehmend komplexe IT-Security-Landschaft**
  - **Antiviren-Software auf Servern, Nutzer-PC´s und Gateways**
  - **Netz und Anwendungs-Firewalls**
  - **Intrusion-Detection-Systeme und Schwachstellenscanner**

Hartmut Kolke

GWDG

IT-Sicherheit

..... Sicherheit (Verschlüsselungsverfahren usw.)

13

- **Einrichtung eines IT-SEC Teams**
  - **Aufklärung, Musterlösungen, Workshops**
  - **Erkennung und Beseitigung von Schwachstellen in Netzen und Anwendungen**
- **Entwurf und Einführung von Sicherheitsleitlinien**
  - **Schwachstelle „Mensch“**
- **Security Workshop der GWDG vom 24. bis 26. September**
  - **Der Workshop richtet sich an die EDV-Betreuer der von der GWDG betreuten Institute.**

Hartmut Kolke

GWDG

Active Directory

Active Directory im GÖNET

Single SignOn, Authentifizierung und Verzeichnisdienste, Sicherheit (Verschlüsselungsverfahren usw.)

14

- **Weiterer Ausbau des zentralenVerzeichnisdienstes A/D**
  - **Zugriff auf verteilte Daten und Ressourcen (Drucker, etc.) entsprechend den zugewiesenen Berechtigungen**
  - **Anmeldung mit Benutzername und einem Passwort im gesamten Netz (Single SignOn)**
  - **Zentrale Administration und Software-Verteilung**
  - **Delegierbar auf Instituts- oder andere Organisations-Ebenen**

Hartmut Kolle

GWDG

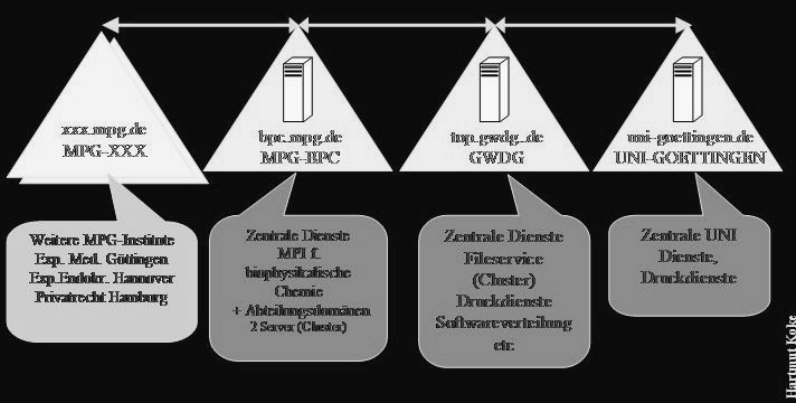
Active Directory

Active Directory im GÖNET

Single SignOn, Authentifizierung und Verzeichnisdienste, Sicherheit (Verschlüsselungsverfahren usw.)

15

- **Verzeichnis-Struktur**



Hartmut Kolle

Strategische Aufgaben

GWDG

16

- Übergang von „Archivierung“ zu „Langzeit-Archivierung“
  - Basis-technische Aspekte
    - Mengen-Problem
    - Überwindung der technischen Obsolenz (Daueraufgabe !)
    - Verfügbarkeit, Redundanz
  - Standardisierte Beschreibung der für die Archivierung erforderlichen Funktionen (Metadaten, etc.)
  - Ökonomische Aspekte
  - u.v.a.

Relevanz:

Max-Planck- und Universitäts-Einrichtungen

International

Hartmut Kölz

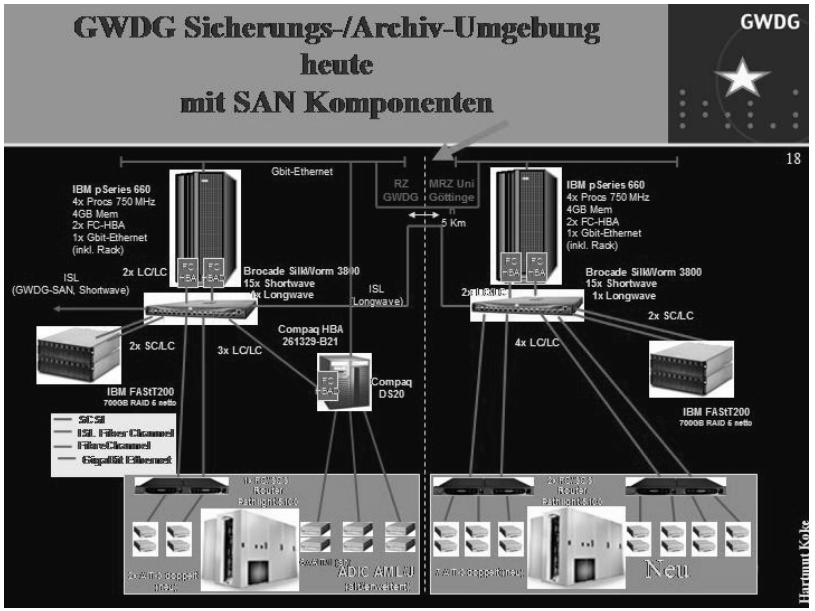
Relevante Projekte zum Thema Langzeit-Archivierung im Göttinger Kontext

GWDG

17

- DFG-Förderinitiative
  - Themenkreis 1 (Integriertes Informationsmanagement)
    - GÖ* Antrag
      - GWDG, MRZ, (SUB)
- MPG Konzept-Papier „Virtual Wisdom“ WISDOM.doc
  - Gemeinsames Treffen GWDG/MPG/SUB in Göttingen am 20. Februar
- SUB
  - Aufbau eines Zentrums für digitales Wissensmanagement am Wissenschaftsstandort Göttingen

Hartmut Kölz


GWDG Sicherungs-/Archiv-Umgebung
heute
mit SAN Komponenten
GWDG
18
Gbit-Ethernet
RZ GWDG
MRZ Uni Göttinge n
5 Km
IBM pSeries 660
4x Procs 750 MHz
4GB Mem
2x FC-HBA
1x Gbit-Ethernet
(inkl. Rack)
2x LC/LC
ISL
(GWDG-SAN, Shortwave)
Brocade SilkWorm 3800
15x Shortwave
1x Longwave
ISL
Longwave)
2x SC/LC
3x LC/LC
Compaq HBA
261329-B21
Compaq
DS20
IBM FAStT200
7000B RAID 6 netto
SCSI
ISL Fiber Channel
FibreChannel
Gigabit Ethernet
4x LC/LC
ADIC AML-J
Neu
Hartmut Kolle

Verteilung von Windows-XP-Klonen

Ulrich Schwardmann

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Einleitung

Eine einfache Methode zur Ausstattung vieler Rechner mit einer gleichgestalteten Benutzeroberfläche ist die Erstellung vollständiger Kopien einer einmal erstellten Installation. Diese Methode wird üblicherweise als Klonen bezeichnet. Es ist nun ein in der Windows-Welt zur Gewohnheit gewordenes Problem, dass sich Klone eines Rechners im Netzwerk nicht vertragen. Diese Gewohnheit ist natürlich eine schlechte, es muss keineswegs notwendigerweise so sein: Linux-Rechner mit DHCP-Konfiguration kennen die Schwierigkeiten nicht.

Aber es gibt eben bei Windows-Rechnern eine starke Kraft, die dafür sorgt, dass das einfache Kopieren eines lizenzpflichtigen Betriebssystems mit Schwierigkeiten gekoppelt wird.

Was trotzdem möglich ist, und welche Klimmzüge notwendig sind, um auch hier zu einer Lösung zu kommen, die dem einfachen Klonen möglichst ähnlich ist, ist Gegenstand dieses Beitrages. Die wesentlichen Prinzipien sind im Rahmen eines Schülerpraktikums entstanden, an dem Phillip Jaquet und

Johannes Lier (beide 11. Jg.), Max-Planck-Gymnasium, Göttingen, teilgenommen haben.

1. Ziel

Das Ziel ist die Ferninstallation von Windows XP bei vielen gleichartigen Rechnern. Die hier entwickelten Verfahrensweisen sollten ebenfalls bei anderen Windows-2000-Derivaten funktionieren.

Wichtigstes Prinzip dabei soll sein, dass nach entsprechenden Vorarbeiten die Ferninstallation vollkommen automatisch abläuft, also insbesondere keine Anwesenheit eines Administrators oder einer sonstigen Person am Rechner notwendig ist.

Allenfalls das physikalische Einschalten eines Rechners könnte als Auslöser der Ferninstallation in Frage kommen, wobei die Installation zum Beispiel bei Einschalten durch WakeOnLAN und PXE-Boot nach entsprechenden Vorarbeiten im PXE-Server ebenfalls automatisch durchgeführt werden kann.

Einfacher wäre allerdings eine Installation, die bei vorhandenem Betriebssystem (z.B. Linux) durch Remote Shell durchgeführt wird. Dieses Verfahren lässt sich zum Beispiel bei VMware-Installationen durchhalten, kann aber auch bei realer Hardware zum Zuge kommen.

Eine weitere wichtige Eigenschaft sollte zudem die einfache Handhabung der Installationsinstanzen sein. Damit ist insbesondere die Beschränkung der Anzahl der vorzuhaltenden Instanzen auf im wesentlichen eine Masterkopie pro Softwareinstanz gemeint.

2. Software zum Klonen von NTFS-Partitionen

Es gibt bereits Erfahrungen mit verschiedenen Softwaresystemen, die in der c't 23, 2003 in einem Test von Imaging-Programmen zusammengefasst wurden. Hierbei handelt es sich zuallererst um Software, die für Backup-Zwecke ganzer Installationen eingesetzt wird, bei der also der Aspekt der Individualisierung im Netzwerk keine Rolle spielt.

Dabei geschieht das Lesen im allgemeinen durch eine komprimierte Low-Level-Kopie von nicht leeren Blocks. Beim Schreiben wird meist eine vorhandene Partitionierung, oft auch eine entsprechende Formatierung des NTFS vorausgesetzt.

Das Ergebnis des c't-Tests lässt sich in Kürze wie folgt zusammenfassen:

- Knoppix mit Partimage bekam gute Noten.

- NTFS ist hier im Schreibmodus noch experimentell; doch wenn es Fehler gab, dann beim Lesen.
- Der Befehl diskdump (dd), also das Schreiben des kompletten Raw-Device unter Linux/Knoppix in genügend große Zielpartitionen geht auch.
- Drive Image (PowerQuest) gibt es nur auf Windows 2000/XP und kostet 70,- €. Das Urteil von c't: „Hier paart sich hervorragende Technik mit diversen Macken und Schikanen.“
- Norton Ghost hat eher schlecht abgeschnitten: „Fast nichts klappt auf Anhieb.“ (c't)

3. Remote Installation Service (RIS)

Warum hier nicht das Microsoft-Werkzeug der Wahl, RIS, verwendet wurde, liegt vor allem an seiner Unverträglichkeit mit VMware: Unter VMware mit bridged networking war keine PXE-Anmeldung am RIS-Server gelungen. Für VMware müssen sowieso (kleine) Plattendateien für die RIS-Installation verteilt werden, dann kann man auch gleich die Klone verteilen. Aber es gibt mit RIS ein weiteres Problem, das über den Rahmen der VMware-Klones hinausweist:

- RIS-Images sind genau wie Windows-XP-Klones nur auf identische Hardware übertragbar, wobei RIS geradezu für VMware geschaffen wäre, wenn es denn ginge.
- Außerdem muss eine zusätzlich Infrastruktur aufgebaut werden. RIS braucht einen eigenen Softwareserver und den PXE-Bootserver.

4. Klonen von NTFS-Partitionen

Es sind verschiedene zusätzliche Voraussetzungen beim Klonen von Windows-Systemen zu erfüllen, die hier kurz angesprochen werden sollen.

Windows-Installationen sind sehr stark mit der Hardware verwoben: Hardware-Änderungen erzwingen üblicherweise den Versuch der automatischen Installation neuer Treiber. Dies wiederum ist fast immer mit irgendeinem Eingriff des Administrators verbunden, der eine CD einlegen muss, einen Installationspfad bestätigen muss oder einfach nur auf OK klicken muss. Dies widerspricht dem oben genannten wichtigsten Prinzip. Daher wird im folgenden von Systemen mit (nahezu) identischer Hardware ausgegangen.

Es muss auf irgendeine Weise die Lizenzierung des Klones erfolgen. Hier kann unter Umständen einfach die Existenz einer entsprechenden Sammelli-

zenz, die sich über die verwendete Hardware erstreckt, als ausreichend angesehen werden. Vorzugsweise aber sollte dies nach den Vorgaben von Microsoft geschehen.

Als weitere Voraussetzung muss zur Verträglichkeit der Klone im Netz eine Individualisierung der sogenannten Security Identifier (SID) durchgeführt werden. Da zudem eine Domänenanmeldung möglich sein soll, und der indivduelle Computername daher der Domäne bekannt zu sein hat, muss auch der Computername geändert werden.

5. Sysprep

Microsoft bietet selbst ein Werkzeug zur Individualisierung von Klones an, ohne später eventuelle SID-Konflikte zu erleiden. Es befindet sich als sogenanntes MS-Supporttool auf der Windows-XP-Professional-CD im Ordner

`Support/Tools/Deploy.cab`

und besteht aus den folgenden Komponenten:

- **`Sysprep.exe`** ist jene Datei, die den Computer „versiegelt“, d.h. den SID-Wechsel initialisiert und bei erneutem Systemstart das Setupprogramm aufruft.
- Sie greift auf die **`Setupcl.exe`** zu, die nach Neustart das Setup steuert.
- Die **`Setupmgr.exe`** hilft bei der Erstellung einer so genannten Antwortdatei „**`sysprep.inf`**“, in der die jeweiligen Angaben, die beim Setup gemacht werden müssten, bereits vordefiniert werden können. So läuft das Setup nach Systemstart komplett automatisch und verlangt keine Eingabe des Users.

Das Supporttool setzt den gleichen HAL (hardware abstraction layer) voraus, was bedeutet, dass die Hardware sehr ähnlich sein muss, aber dass es durchaus kleinere Unterschiede geben darf. Zum Beispiel erlaubt es zusätzlich verschiedene Massenspeicher-Controller.

Zum einen diese Eigenschaft, die für allgemeine Klones interessant sein dürfte, sowie die Tatsache, dass es sich um ein von Microsoft selbst vorgeschlagenes Verfahren handelt, haben den Ausschlag für die Auswahl dieses Verfahren gegeben.

Ein Nachteil dieses Programms besteht jedoch darin, dass Sysprep automatisch auch den Computernamen auf zufällige Weise ohne Einflussmöglich-

keit ändert. Daher muss hinterher ein neuer determinierbarer Computername festgelegt werden und mit diesem der Domäne beigetreten werden.

Sysprep „versiegelt“ das System in der Terminologie von Microsoft, d.h. es wird bei Neustart ein neuer Setup des Systems inklusive Lizenzierung (es wird vorher ein entsprechender Lizenzschlüssel übergeben) und Hardwareanpassung durchgeführt.

6. Der Setupmanager von Sysprep

Mit Hilfe des Setupmanagers, einem interaktiven Assistenten, wird die Antwortdatei erstellt. Nach dem Aufruf und einem Klick auf „Weiter“ wählt man „Neue Antwortdatei erstellen“ aus und klickt noch einmal auf „Weiter“. Im nun folgenden Fenster wählt man „Systemvorbereitungsinstallation“ aus.

Die anderen beiden Funktionen erstellen eine jeweils andere Antwortdatei für unterschiedliche Optionen, beides ist allerdings für das Klonen von Installationen nicht von Nutzen.

Nachdem man im nächsten Fenster die richtige Windows-Version ausgewählt hat (Windows XP Professional), wird im darauffolgenden Fenster „Ja,

vollautomatisierte Installation“ ausgewählt. Nach einem erneuten Klick auf „Weiter“ beginnt die eigentliche Erstellung der Antwortdatei.

In einer Liste links sieht man die Einstellungen, die zu bearbeiten sind, und auf der rechten Seite erscheinen die Eingabefelder.

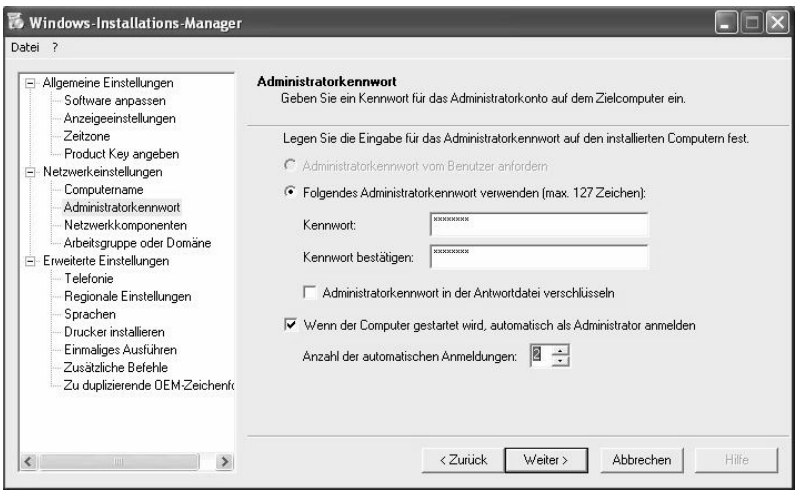
Zunächst muss man den Namen und die Organisation eingeben. Nach einem Klick auf „Weiter“ erscheinen die Einstellungen der Anzeige, die jedoch allesamt auf „Windows Standard“ verbleiben können.

Nach einem erneuten „Weiter“-Klick stellt man die richtige Zeitzone ein, damit die Systemuhr im neuen Windows richtig eingestellt ist.

Im nächsten Fenster wird ein gültiger Lizenz-Key abgefragt. Achtung: Die Standardlizenzen von Windows sehen Disk-Cloning mit ein und demselben Produktschlüssel nicht vor! Man benötigt schon eine entsprechende Lizenz, um auf diesem Weg das Disk-Cloning legal durchzuführen. Eine Möglichkeit, mehrere Keys für mehrere Rechner einzugeben, gibt es nicht.

Im nun folgenden Fenster ist es möglich, den Computernamen festzulegen. Hier ist es allerdings nicht ratsam, einen Computernamen einzugeben, da sonst jede neue Maschine den gleichen Computernamen hat und somit nicht im Netzwerk vertreten sein kann! Somit sollte hier auf „Neuen Computernamen generieren“ geklickt werden, damit Windows einen zufälligen Namen auswählt. Leider fehlt, wie bereits erwähnt, an dieser Stelle ein Verfahren, aus der vorhandenen MAC-Adresse des Rechners einen individuellen, aber bekannten Rechnernamen zu generieren.

Das nächste Feld erbittet das neue Passwort des Administrators. Dieses sollte nicht verschlüsselt werden, da es sonst nach dem Versiegeln zu einer Fehlermeldung kommt. Achtung: Das neue Passwort muss identisch mit dem alten sein, da es sonst zu Fehlern nach dem Systemstart kommt! Die Anzahl der automatischen Anmeldungen sollte auf „2“ festgelegt werden, da es weitere zwei Zyklen des Restarts gibt durch Festlegung des Rechnernamens und Domänenanmeldung.

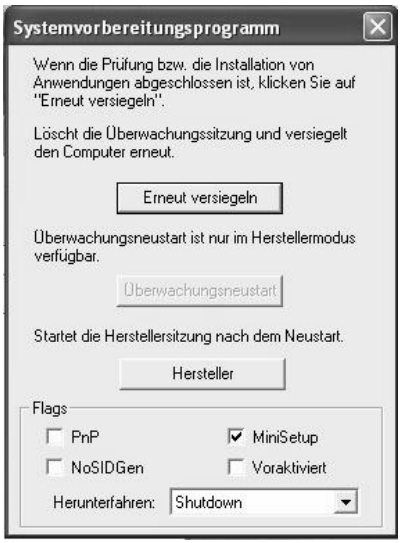


Im nun folgenden Fenster „Netzwerkkomponenten“ kann das Netzwerk für den neuen Computer festgelegt werden. Bei unserem Beispiel reicht die Vorgabe.

Das nächste Fenster gibt die Möglichkeit, sich in einer Arbeitsgruppe bzw. in einer Domäne anzumelden. Die automatische Anmeldung an einer Domäne ist zum Zeitpunkt des Sysprep-Aufrufs allerding sehr problematisch. Erstens ist der Name des Rechners durch Sysprep zufällig vorgegeben, was nicht in jeder Domäne akzeptiert werden kann. Zweitens klappt die Anmeldung an einer Samba-Domäne, z.B. der Domäne GWDG-SAMBA, via Sysprep nicht automatisch, da durch Sysprep die Eintragung **`requiresignorseal`** in der Registrierungsdatenbank wieder auf „1“ gesetzt wird (siehe dazu auch das Kapitel „Beitreten des Computers in eine Domäne“). Es sollte daher hier zunächst „Arbeitsgruppe“ angewählt werden.

Beinahe alle Einträge der Gruppe „Erweiterte Einstellungen“ können auf Standard belassen oder je nach Bedarf geändert werden, lediglich in „Einma-

liges Ausführen“ wird ein Skriptname eingetragen. Nach dem Klick auf „Fertig Stellen“ kann die nun fertige Antwortdatei gespeichert werden.



Hiernach kann **`sysprep.exe`** selber ausgeführt werden. Es erscheint ein Eingabefeld, in welchem lediglich die Option „Minisetup“ angeklickt wird und im Dropdownfeld „Shutdown“ angewählt wird. Drückt man nun auf den Button „erneut versiegeln“, wird das System heruntergefahren. Nach erneutem Hochfahren von Windows (evtl. auf einer anderen Maschine) werden die Einstellungen der Antwortdatei ausgeführt und die SIDs geändert.

7. NewSID ist keine brauchbare Alternative

Weitaus unkomplizierter als die beschriebene Methode mit „sysprep“ erscheint die Möglichkeit, mittels eines simplen Programms direkt die SID zu ändern und danach zu rebooten. Im Internet stößt man dabei eigentlich nur auf ein Programm: NewSID von SysInternals. Dieses Programm kann man sich kostenlos unter

`http://www.sysInternals.com/ntw2k/source/newsid.shtml`

herunterladen.

Das Programm wird in einer **`ZIP`**-Datei geliefert und bringt, einmal entpackt, eine ausführbare Datei mit sich, die mittels „**`newsid.exe /a`**“

auch automatisch aus der Kommandozeile ausführbar ist. Egal auf welche Art und Weise es bei unseren Tests eingesetzt wurde, verbrauchte das Programm schlagartig annähernd 100 % der CPU-Auslastung und vergrößerte die Auslagerungsdatei. Stieß diese an ihre Grenzen, gab das Programm eine Fehlermeldung aus und beendete sich. Berichte aus dem Internet legen nahe, dass NewSID offenbar nur auf wenigen Systemen funktioniert.

8. WSname: Die automatische Vergabe eines neuen Computernamens

Die Verwendung eines zusätzlichen Programmes zur neuerlichen Festlegung des Computernamens wäre nicht nötig, wenn **`sysprep`** MAC-Adressen zur Namenswahl nutzen könnte.

Das Programm Workstation Name Changer (**`WSname.exe`**) als ZIP-Datei kann von dem URL

`http://mytoolsandstuff.tripod.com/wsname266.zip`

heruntergeladen werden. Entpackt man die Datei, hat man das Executable direkt vorliegen. Führt man dieses ohne weitere Optionen aus, erscheint die Aufforderung, den neuen Computernamen einzugeben. Danach startet sich der Computer nach einer Sicherheitsabfrage neu und der Computername ist geändert. Das Programm ermöglicht es durch Einbindung in ein einfaches Script, diesen Vorgang zu automatisieren und bestimmte weitere Features zu nutzen. All diese werden auf

`http://mytoolsandstuff.tripod.com/wsname.html`

erläutert.

Die wichtigsten Optionen sind:

`/N:Neuername`

Das Programm benennt den Computer in **`Neuername`** um. Nach erfolgreicher Umbenennung wird der User gefragt, ob er den Computer neu starten möchte.

`/Reboot`

Diese Flag sollte immer gesetzt werden, um die Maschine neu zu starten, damit die Änderungen wirksam werden und um die Abfrage auf Neustart zu umgehen.

Der PC startet sich nicht neu, wenn keine Umbenennung stattgefunden hat. Soll der PC nicht rebootet werden und keine Aufforderung erscheinen, sollte die Flag **/Noreboot** gesetzt werden.

/RDF:"Pfad/zur/Datei.txt"

und

/DFK:"Suchwort1 Suchwort2"

Diese beiden Befehle weisen WSname an, in einer bestimmten Datei nach dem neuen Computernamen zu suchen. Befinden sich im Pfad zur Datei oder in den Suchwörtern Leerzeichen, so müssen Anführungszeichen gesetzt werden.

Achtung: In diesem Beispiel sucht WSName nach der Zeichenfolge "**Suchwort1 Suchwort2**" (Ohne die Anführungszeichen), und nicht etwa nach den einzelnen Wörtern.

Besonders hilfreich für die gezielte automatische Individualisierung ist die DFK:!Mac-Option (**/dfk:!Mac**), der ein Dateiname mit MAC-Adressen und zugehörigen Rechnernamen mitgegeben wird. WSName sucht hierbei automatisch in der Datei nach der MAC-Adresse der primären Netzwerkkarte (Achtung: Bei der MAC-Adressen-Bestimmung werden normalerweise Striche mit angegeben; diese werden von WSname nicht erkannt!)

Die Datei ist so aufgebaut, dass pro Zeile zunächst die Suchbezeichnung steht, dann ein Gleichheitszeichen und dann die neue Computerbezeichnung, demnach also in einer Zeile

Suchwort = Computername

wobei die Suchwort-Zeichenfolge unikat bleiben muss, da das Programm sonst durcheinander kommt.

Als Beispiel also

```
00508B052AE8 = gwdg-vxpi1
```

```
Suchwort1 Suchwort2 = gwdg-vxpi2
```

usw.

Beispiele für die Verwendung dieser Syntax:

- Einen Computer zu **Neuername** umbenennen

  ```
  wsname.exe /N:Neuername /reboot
  ```

- Einen Computer anhand des Suchbegriffes **GWDG0203** in der Datei **c:\windows\scomp02.txt** umbenennen:

  ```
  wsname.exe /rdf:"C:\Windows\SComp 02.txt"
  /dfk:GWDG0203 /reboot
  ```

- Einen Computer anhand der MAC-Adresse als Suchbegriff in der Datei **D:\rename\ren.txt** umbenennen

  ```
  wsname.exe /rdf:D:\rename\ren.txt /dfk:!MAC
  /reboot
  ```

Insbesondere diese Variante der Namenszuordnung bietet sich für die Verwendung von virtuellen Maschinen an, da hier die MAC-Adresse in der Konfigurationsdatei für die VM festgelegt werden kann.

Bei jedem der hier angegebenen Beispiele ist die Option **/reboot** optional, jedoch wird der User beim Weglassen der Flag aufgefordert, die Maschine neu zu starten. Mit der Option **/noreboot** statt **/reboot** wird der Computer nach erfolgreicher Umbenennung nicht neu gestartet und der Administrator wird auch nicht aufgefordert dies zu tun.

Der Programmierer dieses hilfreichen Werkzeuges erbittet bei Gebrauch des Programms eine kleine Information darüber, wo und in welcher Weise man das Programm nutzt. Seine Mailadresse ist **wsname@clarke.co.nz**.

9. Domänen-Anmeldung via NETDOM

Um einen Rechner per Shell-Kommando einer Domäne hinzuzufügen, kann das Programm **netdom.exe** verwendet werden. Es ist im Lieferumfang von Windows XP Professional ebenfalls in den sogenannten „Supporttools“ enthalten.

Um diese Windows-XP-Supporttools zu installieren, muss daher zunächst auf der Windows-CD im Ordner **/Support/Tools** das Programm **Setup.exe** ausgeführt werden.

Das Programm NETDOM ist ein reines Kommandozeilenprogramm. Die Befehlssyntax lautet wie folgt (alles in eine Zeile geschrieben):

```
Netdom.exe JOIN Computername /Domain:domain
/UserD:Domainuser /PasswordD:Domainuserpass
/UserO:Lokaleruser /PasswordO:Lokalespass
/reboot:Zeitinsekunden
```

Die folgenden Einträge müssen angepasst werden:

Computername

Hier muss der Netzwerkname der Maschine eingegeben werden, die einer Domäne beitreten soll. Es kann an dieser Stelle auch die Umgebungsvariable **%COMPUTERNAME%** eingesetzt werden, die den lokalen Rechnernamen enthält.

Domain

Der Name der Domäne, der beigetreten werden soll.

Domainuser

Der Username auf der Domäne, der berechtigt ist, der Domäne beizutreten.

Domainuserpass

Das Passwort, welches den Domänen-User identifiziert. Wird an dieser Stelle statt des Passwortes ein * eingetragen, erscheint bei Ausführung des Befehls eine Eingabeaufforderung, um das Passwort einzugeben.

Lokaleruser

Der lokale User mit Administrationsrechten, unter Windows XP standardmäßig „Administrator“.

Lokalespass

Das Passwort des lokalen Users. Auch hier kann ein Stern gesetzt werden, um nachträglich eine Eingabeaufforderung anzuzeigen

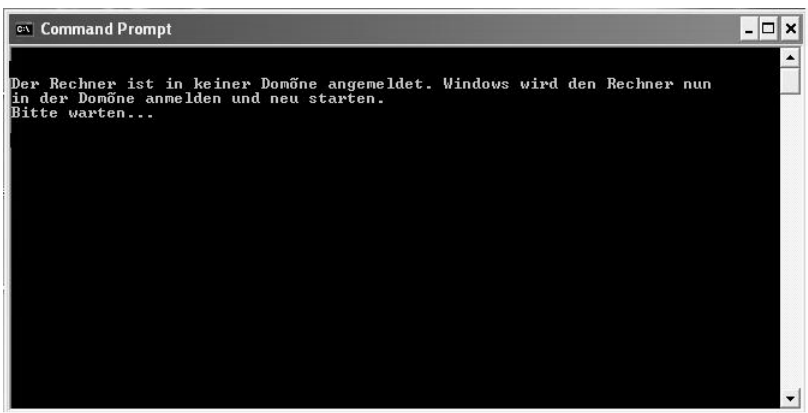
Zeitinsekunden

Eine Angabe, nach wievielen Sekunden der Rechner automatisch neu gestartet wird, um die Domänenanmeldung zu vollenden.

Das folgende Beispiel bewirkt den Eintritt des Computers **GWDG-Winxp05** in die Domäne **GWDG-Windomain** mit dem Domänenuser **winxp**, dem Domänenpasswort **7761e8** und den lokalen Administratorrechten. Das Administratorkennwort wird abgefragt, nach fünf Sekunden startet sich der Rechner dann neu.

```
Netdom.exe join GWDG-Winxp05 /domain:GWDG-Windomain
/userd:winxp /passwordd:7761e8 /usero:administrator
/passwordo:* /reboot:5
```

Die Reboot-Option nach Zeitintervall hat sich für die Zwecke der Individualisierung von VMware-Maschinen als unbrauchbar erwiesen, da hier schlussendlich eine Abschaltung der Maschine nötig ist, damit die verwendete virtuelle Platte anschließend wieder in den nicht bechreibbaren Modus gebracht werden kann. Hier muss ein explizites „**shutdown -s**“ vereinbart werden.



Die Verwendung von netdom im Skript verlangt die explizite Angabe des Passwortes der Domäne im Klartext. Daher darf die entsprechende Skriptdatei den Benutzern der Installation nicht zugänglich werden. Am einfachsten geschieht dies durch eine vollständige Löschung der Datei nach Benutzung.

10. Domänen-Anmeldung an Samba-Domäne

Mit Windows XP ist Microsoft dazu übergegangen, die Domänen-Anmeldung standardmäßig über eine durch ein spezielles Microsoft-Protokoll gesi-

cherte Verbindung abzuwickeln. Diese Einstellung wird durch die Versiegelung und anschließende Individualisierung wieder voreingestellt.

Sofern der Domänenkontroller mit einem Samba-Server betrieben wird, kann es deshalb zu Problemen bei der Domänenanmeldung kommen. Daher muss man in diesem Fall den entsprechenden Registry-Eintrag anpassen. Der Wert des Schlüssels **`requiresignorseal`** in

`Hkey_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\`

muss dann auf Null gesetzt werden.

11. Ablauf des Klonens für VMware-Installationen

Die Verwendung dieses Verfahrens bei der Verteilung von VMware-Maschinen lässt sich durch verschiedene Eigenschaften von VMware zusätzlich einfach steuern.

Die Einrichtung und Update der Master-Installation, die dann auf die gewünschten anderen Rechner verteilt wird, kann durch Fremdpersonen, z.B. durch Kurshalter, geschehen. Notwendig hierfür ist im allgemeinen nur das Administrator-Passwort im Windows XP der verwendeten virtuellen Maschine.

Die für die Versiegelung notwendigen Dateien befinden sich auf einer (virtuellen) Diskette auf einem speziellen Rechner, auf die lediglich der Administrator Zugriff hat, der auch die entsprechenden Domänen-Rechte besitzt. Typischerweise wird von ihm auch die Update-Kontrolle für Sicherheitspatches und das Einspielen weiterer Service-SW durchgeführt.

Anschließend geschieht durch ihn die Versiegelung des Systems. Damit die Installation auch später, zum Beispiel beim nächsten Kurs zu dem Thema, noch zur Verfügung steht, empfiehlt sich eine vollständige Archivierung der virtuellen Platte des Systems.

Aus diesem Archiv heraus lässt sich dann die Installation durch Kopieren der virtuellen Platten auf die gewünschten Rechner verteilen.

Anschließend ist ein initialer Neustart des versiegelten Systems mit persistenter Platte nötig. Im Anschluss der dadurch erreichten Initialisierung fährt das System automatisch herunter. Für den normalen Betrieb wird dann auf den Einsatz nicht persistenter Platten umgeschaltet.

12. Problem der Domänen-Anmeldung bei nicht persistenter VMware-Platte

Nach einer gewissen Zeit (ca. 3-4 Wochen) erneuert Windows 2000/XP automatisch die Domänen-Anmeldung mit der Vergabe neuer Schlüssel auf beiden Seiten. Daher ist spätestens nach dieser Periode eine erzwungene Domänen-Neuanmeldung mit dann wieder persistenter Platte notwendig.

Dies geschieht automatisch, indem bei jedem Start des Systems nach einem geeigneten Skript im Floppy-Laufwerk B: geschaut wird. Ist es da, wird es ausgeführt und damit eine Domänen-Ab- und -Anmeldung erreicht. Üblicherweise ist dieses Skript nicht vorhanden, lediglich in einem speziellen Servicemodus mit persistenter Platte wird das zweite Diskettenlaufwerk in der VMware-Konfigurationsdatei als virtuelles Laufwerk (Image) eingebunden. Auf diese Diskette kann in eine Log-Datei der Returncode der Ab- und Anmeldung geschrieben werden. Dies kann dann auch zur Erfolgskontrolle verwendet werden (Loopback-Device).

In der Reihe GWDG-Berichte sind zuletzt erschienen:

Nähere Informationen finden Sie im Internet unter
`http://www.gwdg.de/forschung/publikationen/gwdg-berichte`

Nr. 40 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1994
1995

Nr. 41 *Brinkmeier, Fritz* (Hrsg.):
Rechner, Netze, Spezialisten. Vom Maschinenzentrum zum Kompetenzzentrum - Vorträge des Kolloquiums zum 25jährigen Bestehen der GWDG
1996

Nr. 42 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1995
1996

Nr. 43 *Wall, Dieter* (Hrsg.):
Kostenrechnung im wissenschaftlichen Rechenzentrum - Das Göttinger Modell
1996

Nr. 44 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1996
1997

Nr. 45 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
13. DV-Treffen der Max-Planck-Institute - 21.-22. November 1996 in Göttingen
1997

Nr. 46 **Jahresberichte 1994 bis 1996**
1997

Nr. 47 *Heuer, Konrad, Eberhard Mönkeberg und Ulrich Schwardmann*:
Server-Betrieb mit Standard-PC-Hardware unter freien UNIX-Betriebssystemen
1998

Nr. 48 *Haan, Oswald* (Hrsg.):
Göttinger Informatik Kolloquium - Vorträge aus den Jahren 1996/97
1998

Nr. 49 *Koke, Hartmut und Engelbert Ziegler* (Hrsg.):
IT-Infrastruktur im wissenschaftlichen Umfeld - 14. DV-Treffen der Max-Planck-Institute, 20. - 21. November 1997 in Göttingen
1998

Nr. 50 *Gerling, Rainer W.* (Hrsg.):
Datenschutz und neue Medien - Datenschutzschulung am 25./26. Mai 1998
1998

Nr. 51 *Plesser, Theo und Peter Wittenburg* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1997
1998

Nr. 52 *Heinzel, Stefan und Theo Plesser* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1998
1999

Nr. 53 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Internet- und Intranet-Technologien in der wissenschaftlichen Datenverarbeitung - 15. DV-Treffen der Max-Planck-Institute, 18. - 20. November 1998 in Göttingen
1999

Nr. 54 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 1999
2000

Nr. 55 *Kaspar, Friedbert und Hans-Ulrich Zimmermann* (Hrsg.):
Neue Technologien zur Nutzung von Netzdiensten - 16. DV-Treffen der Max-Planck-Institute, 17. - 19. November 1999 in Göttingen
2000

Nr. 56 *Plesser, Theo und Helmut Hayd* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2000
2001

Nr. 57 *Hayd, Helmut und Rainer Kleinrensing* (Hrsg.):
17. und 18. DV-Treffen der Max-Planck-Institute
22. - 24. November 2000 in Göttingen
21. - 23. November 2001 in Göttingen
2002

Nr. 58 *Plesser, Theo und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2001
2003

Nr. 59 *Suchodoletz, Dirk von*:
Effizienter Betrieb großer Rechnerpools - Implementierung am Beispiel des Studierendennetzes an der Universität Göttingen
2003

Nr. 60 *Haan, Oswald* (Hrsg.):
Erfahrungen mit den IBM-Parallelrechnersystemen RS/6000 SP und pSeries690
2003

Nr. 61 *Rieger, Sebastian:*
Streaming-Media und Multicasting in drahtlosen Netzwerken - Untersuchung von Realisierungs- und Anwendungsmöglichkeiten
2003

Nr. 62 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2002
2003

Nr. 63 *Kremer, Kurt und Volker Macho* (Hrsg.):
Forschung und wissenschaftliches Rechnen - Beiträge zum Heinz-Billing-Preis 2003
2004

Nr. 64 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Vorantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 65 *Koke, Hartmut* (Hrsg.):
GÖ* – Integriertes Informationsmanagement im heterogenen eScience-Umfeld: GÖ*-Hauptantrag für die DFG-Förderinitiative „Leistungszentren für Forschungsinformation“
2004

Nr. 66 *Bussmann, Dietmar und Andreas Oberreuter* (Hrsg.):
19. und 20. DV-Treffen der Max-Planck-Institute
20. - 22. November 2002 in Göttingen
19. - 21. November 2003 in Göttingen
2004