

infoforum

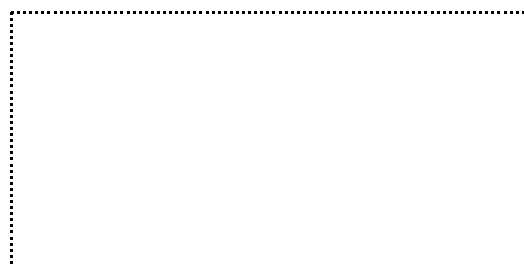
Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 27, Nr. 3 – Dezember 2003

ISSN 0931-4008

Inhalt

| | |
|--|-----------|
| Editorial | 2 |
| ZIV-Aktuell | 3 |
| Sicherheit in der Informationsverarbeitung | 3 |
| Bluetooth und Funknetze der Universität | 4 |
| ZIV-Pools in der Einsteinstraße 60 nachts und am Wochenende nutzbar | 5 |
| Kleines Jubiläum auf dem Linux-Parallelrechner | 6 |
| Systemüberwachung mit MOM (Microsoft Operations Manager) | 8 |
| Systemüberwachung mit Tivoli | 9 |
| Meinberg Lantime: NTP über IPv6 | 11 |
| Neues von SPSS | 13 |
| Neues von McAfee VirusScan | 13 |
| Neues von der ZIV-Bibliothek | 14 |
| Neues von NIC_online | 15 |
| Neue Pakete auf dem JOIN-FTP-Server | 16 |
| Neues von ZIVprint | 17 |
| Landeslizenz für StarOffice 7 | 18 |
| Neues von Deleatur | 19 |
| Bildgewinnung und Bilddarstellung – Ein Praktikum | 20 |
| perMail – E-Mail-Retter, Spam-Vernichter und noch viel mehr | 21 |
| Vom Rechner- zum Ressourcen-Verbund in NRW | 25 |
| Neue Netzstrukturen für den Internet/G-WiN-Anschluss der Universität und der Fachhochschule Münster | 26 |
| Über 500 Teleport-ADSL-Anschlüsse geschaltet | 28 |
| Die K-Säule – Ein Lösungsansatz zur Versorgung mobiler Nutzer | 29 |
| ZIV-Lehre | 31 |
| Veranstaltungen in der Vorlesungszeit (Wintersemester 2003/2004) | 31 |
| Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2004) | 32 |
| ZIV-Regularia | 33 |
| Fingerprints | 33 |



Impressum

info

ISSN 0931-4008

Westfälische Wilhelms-Universität
 Zentrum für Informationsverarbeitung (Universitätsrechenzentrum)
 Röntgenstr. 9 – 13
 48149 Münster

E-Mail: ziv@uni-muenster.de

WWW: <http://www.uni-muenster.de/ZIV/>

Redaktion: H. Pudlatz (G 83-31672, J pudlatz@uni-muenster.de)

E. Sturm (G 83-31679, J sturm@uni-muenster.de)

Satz: K. Hovestadt (G 83-31562, J hovestadt@uni-muenster.de)

Satzsystem: Corel WordPerfect 11 für Windows XP

Druck: Drucktechnische Zentralstelle der WWU
 (Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Editorial

E. Sturm



Als die ersten Artikel für dieses i eintrudelten, dachte ich, schon wieder ein i, in dem es nur um PC-Sicherheit geht. Glücklicherweise kam es dann doch ganz anders! Das am häufigsten vorkommende Wort in Artikel-Titeln ist dieses Mal „neu“. Von vielerlei Hard- und Software gibt es Neues zu berichten.

Neue Software-Versionen gibt es von McAfee VirusScan (oh, doch PC-Sicherheit), ZIVprint, StarOffice, perMail und Deleatur. (Na ja, in gewisser Weise kann ein Spamfilter auch zur Sicherheit beitragen: Manchmal wird eine Virus-Mail schon als Spam entfernt, bevor ihre Virus-Eigenschaft bekannt ist.)

An neuer Hardware werden beschrieben: der Linux-Parallelrechner, neue Netzinfrastrukturen, ADSL-Anschlüsse sowie die K-Säule, deren futuristisches Design Sie auch im Bild bewundern können.

Aus der Personalnot geboren wurde die Möglichkeit, die Pools des Zentrums für Informationsverarbeitung auch außerhalb der Geschäftszeiten benutzen zu können. Hierzu wurde im ZIV in der Einsteinstr. 60 entsprechende „Hardware“ installiert: eine Vereinzelungsanlage mit Videokameras und Kartenlesern. Wer also interessiert ist, kann sich im ZIV eine Kennkarte besorgen. Vorher muss man sich auf der entsprechenden Webseite mit Nutzerkennung und Passwort legitimieren. Das System ist so ausgelegt, dass auch andere Institutionen Zugangsberechtigungen für ihre Gebäude hinzufügen können – natürlich unter Benutzung derselben Karte.

Trotz dieser vielen Artikel über Neuigkeiten in Hard- und Software gilt auch für dieses i: Der wichtigste Artikel ist der direkt hinter diesem Editorial!

ZIV-Aktuell

Sicherheit in der Informationsverarbeitung

W. Held, G. Richter

**So geht es nicht weiter!
Die Belästigungen durch
Spam-Mail werden
immer unerträglicher.**

Viren, Würmer und viele andere Angriffe gegen diejenigen IV-Systeme, die bisher nicht durch besondere Maßnahmen geschützt sind, verursachen immer längere Ausfallzeiten für eine wachsende Zahl betroffener Nutzer und immer höhere Kosten in den Instituten und Lehrstühlen, aber auch in den IV-Versorgungseinheiten und im ZIV. IV-Sicherheitsteam, IV-Versorgungseinheiten und ZIV wollen dies nun ändern. Und IV-Kommission, IV-Lenkungsausschuss und Rektorat unterstützen das.

Die Zahl der Angriffe vervierfachte sich in den beiden letzten Jahren. Die Spam-Mails machen oft mehr als 80 % aller E-Mails aus. In der 2. Oktoberhälfte und in der 1. Novemberhälfte haben wir allein im ZIV 107.500 bzw. 85.000 E-Mails abgefangen, die Viren enthielten. Auf Umwegen über nicht gesicherte Server oder häusliche Arbeitsplätze sind aber sicher immer noch mehr als 500 in die Universität gekommen. Wir haben es überwiegend mit vorsätzlichen Hackerangriffen auf das Netzwerk, auf die Arbeitsfähigkeit der Server und der Arbeitsplatzrechner zu tun. Die Angriffe kommen u. U. auch von Insidern. Immer wieder werden „ungepflegte“ Systeme in Besitz genommen und zu weiteren Angriffswellen missbraucht. Schlecht gewählte, zu selten geänderte Nutzer-Passwörter werden ausgespäht oder sogar bewusst, aber ohne Kenntnis der Folgen unbedacht weitergegeben. Daten werden manchmal erfolgreich ausgespäht. Zum Glück hat es bisher noch keine Angriffe gegeben, die bereits ernsthafte Folgen für Leib und Leben gehabt hätten.

Leider sind die Abwehrmaßnahmen nicht in einem großen Schritt zu bewältigen. Vielmehr sind vielfältige Einzelheiten zu bedenken und zu regeln.

Diese beginnen damit, bei allen Mitgliedern der Universität das Bewusstsein für die notwendigen Schritte zur IV-Sicherheit zu schaffen. Es geht weiter über die Festlegung der erforderlichen organisatorischen Rahmenbedingungen. Hier ist unsere Universität sicher vorbildlich. Das Rektorat hat z. B. schon vor fast zwei Jahren „Regelungen zur IV-Sicherheit in der Universität Münster“ erlassen. Ein Sicherheitsteam wurde eingesetzt. Schon vor vier Jahren wurden „Einzelne Vorschläge zur Sicherung der Informationsverarbeitung in heterogenen Umgebungen“ veröffentlicht. Aufgaben und Verantwortung eines „Technisch Verantwortlichen“ sind neulich von der IV-Kommission und dem IV-Lenkungsausschuss beschrieben worden.

Die bisher schon eingerichteten Sicherungen in den Rechnernetzen müssen in Absprache mit den IV-Versorgungseinheiten vervollständigt werden. Die Server in der Universität müssen auf vorhandene Lücken untersucht und gegebenenfalls in einen besseren Stand versetzt werden.

Sehr viele Angriffe (weit mehr als 1.000 angegriffene und mehrere 1.000 gefährdete Systeme), mit denen wir in den letzten Monaten zu kämpfen hatten, sind durch „ungepflegte“ Arbeitsplatzrechner verursacht worden, die in der Universität oder von zu Haus zum Zugang zur Universität genutzt wurden. Vielfach ist dies auf die Unwissenheit der Nutzer zurückzuführen, seltener auf Bequemlichkeit. Hier soll und muss jetzt Abhilfe geschaffen werden. IV-Kommission, IV-Lenkungsausschuss und Rektorat haben dazu beschlossen:

„Zur deutlichen Verbesserung der IV-Sicherheit und damit zur möglichst weitreichenden Vermeidung von Schäden in der Universität soll die Nutzung von IV-Arbeitsplatzsystemen im/am Netz der Universität durch Regelungen und Verpflichtungen verbunden mit Durchsetzungsrechten und Reglementierungen – abgesichert werden. Notwendige Maßnahmen werden den technischen Entwicklungen folgend durch das IV-Sicherheitsteam in Abstimmung mit IVVen und ZIV festgelegt und der IVK zur Kenntnis gebracht. Wer diesen Regelungen und Verpflichtungen nicht nachkommt, wird nur eingeschränkte Zugänge zum Netz und begrenzte Handlungs- und Nutzungsmöglichkeiten der Ressourcen der Universität erhalten.“

Wer also zukünftig von seinem Arbeitsplatz aus wie bisher im Rechnernetz der Universität flexibel bleiben und die notwendigen Ressourcen in Anspruch nehmen will, muss sowohl für seinen Dienst-Rechner als auch für seinen Privat-Rechner einige Spielregeln beachten. Wer diese Spielregeln nicht einhalten kann, wird nur eingeschränkte Zugänge zum Rechnernetz der Universität nutzen können. Wir bitten dafür um Verständnis, aber die Kosten zur Beseitigung von Schäden können nicht mehr hingegenommen werden. Und Angriffe können schließlich auch zu Datenverlusten und Datenmanipulationen, also zu schwer reparablen Schäden führen.

Die für die dienstlichen und privaten Arbeitsplatzrechner einzuführenden Software-Lösungen werden von den IV-Versorgungseinheiten gemeinsam mit dem ZIV erarbeitet und – das ist die Absicht – möglichst leicht umzusetzen sein. Die Überlegungen konzentrieren sich zzt. darauf, die Betriebssysteme ständig up-to-date zu halten, stets aktuelle Virens Scanner einzusetzen und eine *Personal Firewall* zu nutzen. Die Durchführung dieser Maßnahmen ist außerordentlich arbeitsaufwändig und nicht kurzfristig zu erreichen. Viele Varianten sind vor ihrer Umsetzung noch zu erproben. Dazu werden zwei Sicherheits-Arbeitsgruppen aus ZIV- und IVV-Mitarbeitern für Windows- und Unix/Linux-Systeme eingerichtet. Das ZIV bemüht sich darüber hinaus um eine Kooperation im Rahmen des RV-NRW (Rechner- oder Ressourcen-Verbund), da alle Universitäten vergleichbare Probleme zu lösen haben.

Wir wissen aus vielen Gesprächen, dass viele Mitglieder der Universität froh wären, wenn die Sicherheit der Rechner an den Arbeitsplätzen endlich verbessert werden würde.

Bluetooth und Funknetze der Universität

W. Held

Bluetooth und Funk-LAN vertragen sich nicht miteinander.

Mit Bluetooth wird eine Schnittstelle beschrieben, über die z. B. Geräte an Rechner angeschlossen oder Rechner miteinander verbunden werden können. Dabei erfolgt der Datentransfer über Funk. Über Funk arbeiten aber auch entsprechende Netzkomponenten der Universität, mit denen der Rechnereinsatz mobiler, also ortsunabhängiger werden soll.

Beides sind also erfreuliche Weiterentwicklungen zum Rechnereinsatz. Leider arbeiten beide Technologien in denselben unregulierten, relativ frei nutzbaren Frequenzbändern, so dass wechselseitige Störungen und andere unerwünschte Effekte nicht ausgeschlossen werden können. Deshalb hatte die IV-Kommission am 30.04.2002 beschlossen:

„Bluetooth-Geräte sollen bis auf Weiteres nicht im Gelände der Universität eingesetzt werden, um die Investitionen in Funk-LAN-Infrastrukturen nicht zu gefährden. Sofern Universitätseinrichtungen unbedingt Bluetooth-Geräte einsetzen müssen, sind diese verpflichtet, sich vorher durch das ZIV beraten zu lassen. Im Falle von Funktionsstörungen im Funk-LAN sind die verursachenden Bluetooth-Geräte außer Betrieb zu setzen. Diese Regelung soll spätestens Ende 2003 überprüft werden.“

Da keine neuen Erkenntnisse über diese Störproblematik bekannt sind, also auch keine Entwarnung gegeben werden kann, hat die IV-Kommission ihren alten Beschluss um ein Jahr bis zum 31.12.2004 verlängert.

Der Beschluss ist auch deshalb vermeintlich „hart“ formuliert worden, weil bei Störungen im Funk-Netz der Aufwand für eine detaillierte Untersuchung über evtl. vorhandene Bluetooth-Ursachen zu groß werden würde.

ZIV-Pools in der Einsteinstraße 60 nachts und am Wochenende nutzbar

W. Held, W. Lange, E. Sturm

Nachdem die Bauarbeiten im ZIV-Gebäude Einsteinstraße 60 viel zu lange gedauert haben und oft von sehr umfangreichen Belästigungen und Störungen begleitet waren, kommen sie nun doch langsam zu einem Ende. Damit sind u. a. endlich neue Zugangsregelungen möglich geworden.

Die ZIV-Pools im Erdgeschoss der Einsteinstraße werden zukünftig auch nachts und am Wochenende nutzbar sein. Dazu sind jedoch die folgenden Spielregeln zu beachten:

1. Wer von den neuen Möglichkeiten Gebrauch machen will, muss eine gültige Nutzerkennung im ZIV besitzen und auf der ZIVintro-Webseite unter Eingabe von Uni-Nutzerkennung und Passwort eine Kennkarte beantragen.
2. Im Sekretariat des ZIV, Einsteinstr. 60, bekommt man diese Kennkarte dann gegen eine Gebühr von 5 € ausgehändigt.
3. Die Kennkarte muss nach der Aushändigung zur Initiierung an die Lesegeräte am Eingang des Gebäudes gehalten werden, dabei ist eine persönliche Identifikationsnummer (PIN) einzugeben. Die Karte ist danach sofort nutzbar.
4. Nachts und am Wochenende muss man sich mit dieser Kennkarte, die ein elektronischer Hausschlüssel ist, die Zugangs- und auch die Ausgangstür öffnen.
5. Karte und PIN dürfen nicht an andere Personen weitergegeben werden. Jeder Missbrauch führt zur dauerhaften Sperrung der Karte.
6. Wenn eine Karte verloren gegangen ist, muss diese umgehend gesperrt werden. Dazu kann man wiederum die oben erwähnte ZIVintro-Webseite benutzen. Hier kann man auch die Sperrung aufheben, wenn man die Karte wiedergefunden hat. Natürlich ist auch hierzu jeweils die Eingabe von Kennung und Passwort erforderlich.
7. Mitglieder der Universität, die keinen elektronischen Hausschlüssel haben, können die ZIV-Pools nur während der regulären Öffnungszeiten nutzen. Am Ende dieser Zeiten werden diese Nutzer aufgefordert, das ZIV zu verlassen, weil die Ausgangstüren später ohne elektronischen Hausschlüssel nicht mehr geöffnet werden können. Die Rechner dieser Nutzer werden dann zwangsweise ausgeschaltet. Die Nutzer, die mit der Karte das Gebäude betreten haben, können über das reguläre Dienstende hinaus aktiv bleiben. Nachts und am Wochenende werden zur ergänzenden Sicherung Videokameras eingeschaltet sein.
8. Datenschutzrechtliche Hinweise und Regelungen:
 - Die elektronischen Hausschlüssel enthalten im Chip lediglich eine Kartenummer und die nicht auslesbare PIN. Die Kartenummer wird in einer Datenbank auf einem Server der Technischen Dienste der Universität aufbewahrt.
 - In dieser Datenbank der Technischen Dienste werden Zugangs- und Abgangszeiten registriert. Diese Daten und die Aufzeichnungen der Videokameras werden innerhalb von 24 Stunden (beginnend mit Arbeitsbeginn am nächsten Arbeitstag im ZIV) gelöscht.
 - In einer Datenbank im ZIV wird festgehalten, wer welchen Hausschlüssel erhalten hat. Diese Daten werden bei Rückgabe des Schlüssels gelöscht.
 - In einer weiteren Datenbank wird festgehalten, wer sich zur jeweiligen Zeit ausgewiesenermaßen in den Räumen des ZIV aufhält. Außerdem, wer Aushändigung oder Rückgabe der Kennkarte beantragt hat. Die Lebensdauer dieser Daten ist naturgemäß zeitlich begrenzt: Sie werden gelöscht nach Verlassen des Gebäudes bzw. nach der Aktion des Operateurs im ZIV.
 - Der Datenaustausch zwischen der Datenbank des Schließsystems in den Technischen Diensten und denen des ZIV erfolgt nur indirekt. Es werden nur die zuvor beschriebenen Daten bereitgestellt.
 - Wer einen elektronischen Hausschlüssel erhalten will, muss sich mit diesen datenschutzrechtlichen Hinweisen und Regelungen schriftlich einverstanden erklären.
9. Damit dieser Dienst dauerhaft erhalten werden kann, sind alle aufgefordert, besondere Vorkommnisse an das ZIV zu melden.

Kleines Jubiläum auf dem Linux-Parallelrechner

M. Leweling

ZIVCLUSTER bringt die ersten 10.000 Rechentage hinter sich.

Seit Ende Februar 2003 ist nun – mit mehr oder weniger kurzen Unterbrechungen – der Linux-Parallelrechner ZIVCLUSTER in Betrieb. Anfängliche thermische Probleme führten im Mai/Juni noch zu einer zweiwöchigen Umbauphase, in der die Komponenten des Clusters in eine Anordnung gebracht wurden, die einen stabilen Betrieb ohne vorzeitigen Hitzetod der Hardware ermöglicht. Probleme bereiteten auch die Module des Myrinet-Switches (Rücklaufquote 33 Prozent), die aber spätestens mit Drucklegung dieser i -Ausgabe dank eines präventiven Austausches mit zuverlässigeren Modulen durch den Hersteller behoben werden. In den letzten Monaten lief der Produktionsbetrieb dennoch bereits auf Hochtouren, daher ist es an der Zeit, ein kleines Zwischenfazit zu ziehen.

Zur Erinnerung: Der Cluster besteht aus 2 Kopfstationen (*head nodes*), die mit 2.2 GHz Intel Xeon Prozessoren und 1.5 GB Hauptspeicher ausgerüstet sind, und 94 Rechenknoten (*compute nodes*), die jeweils 2.4 GHz Intel Xeon CPUs und 1 GB Hauptspeicher ihr Eigen nennen. Als Dateisystem für die Benutzer kommt das *General Parallel Filesystem* von IBM mit insgesamt 587 GB Speicherplatz zum Einsatz (kleine Anmerkung am Rande: diese Kapazität ist nicht als Langzeit-Deponie für die produzierten Datenmassen gedacht; es dürfte sich wohl um den teuersten Plattenplatz der gesamten Universität handeln ...).

Die theoretische Gesamtleistung des Clusters beträgt 460 Gflops (Milliarden Gleitkomma-Operationen pro Sekunde). In der Realität sind auf dem Cluster unter Einsatz aller Rechenknoten etwa 300 Gflops erreichbar, ein Wert, der ZIVCLUSTER Mitte des Jahres noch einen respektablen Platz in der Liste der 500 schnellsten Supercomputer der Welt (www.top500.org) eingebracht hätte – wenn wir denn hinreichend eitel gewesen wären.

In der Praxis kann ZIVCLUSTER im Oktober auf ein kleines Jubiläum verweisen: Die ersten 10.000 Rechentage (oder anders ausgedrückt, etwas über 27 Jahre CPU-Zeit) sind vollbracht. Dabei wurde im August trotz der Sommerferien mit etwa 80 Prozent der bisher größte Auslastungsgrad erreicht (siehe Abbildung 1), während sich in der Anfangs- und Testphase noch relativ wenige Nutzer an den Cluster heran trauten. Zur Zeit sind die Bedingungen für die Benutzer immer noch recht günstig: Die durchschnittliche Wartezeit eines Rechenjobs betrug im Oktober trotz Langzeit-Rechenqueues nur etwa zweieinhalb Stunden.

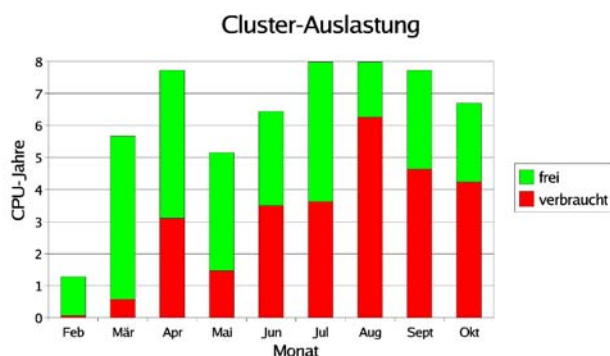


Abbildung 1

Die bisherige Nutzung des Clusters zeigt erfreulicherweise ein breites Anwendungs- und Anwenderspektrum (Abbildung 2). Auffällig ist die überwiegende Auslastung durch

Anwender aus der Geophysik, allerdings kommt das aufgrund der langjährigen Erfahrung dieser Nutzergruppe im Umgang mit Parallelrechnern auch nicht unerwartet. Im Lauf der Zeit werden andere Arbeitsgruppen sicher aufholen. In diesem Zusammenhang sei auch noch einmal auf die Lehrveranstaltungen des ZIV verwiesen: Der Besuch von Programmierkursen und Linux-Einführungsveranstaltungen kann sicher nicht schaden, wenn man den Cluster effektiv nutzen möchte. Allmählich gesellen sich zu den Angehörigen der Uni Münster auch Clusterbenutzer mit Kennungen des Rechnerverbundes NRW hinzu, so dass der Auslastungsgrad mit Sicherheit noch steigen wird, zumal mittlerweile die Anmeldung von den Nutzern selbst einfach über ein Web-Interface vorgenommen werden kann.

Clusternutzung nach Instituten/Arbeitsgruppen

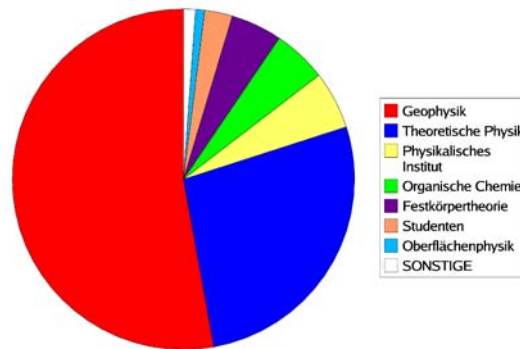


Abbildung 2

Weitere Informationen zur Anmeldung, Benutzung und zu installierter Software finden Sie unter der URL <http://zivcluster.uni-muenster.de>. Zusätzlich zu den dort erhältlichen Informationen befindet sich ein Benutzerhandbuch im Planungsstadium, das in etwas ausführlicherer und übersichtlicherer Form das Arbeiten auf dem Cluster erleichtern soll.

Systemüberwachung mit MOM (Microsoft Operations Manager)

O. Winkelmann

MOM ist ein Werkzeug zur Überwachung von Windows-Servern. Es basiert auf Regelsätzen, welche für verschiedene Servertypen definiert werden können.

Auch am ZIV beobachtet man den Trend, dass für die verschiedenen angebotenen Dienstleistungen die Anzahl der dafür notwendigen Server immer weiter zunimmt. Lösungen für diese Problematik bieten Servermanagement-Produkte, mit denen größere Serverumgebungen von Rechenzentren überwacht werden können. Am ZIV kommen zur Zeit zwei Produkte zum Einsatz: MOM [1] für den Einsatz in reinen Windowsumgebungen und Tivoli von IBM, welches sowohl für die UNIX- als auch für die Windows-Plattform geeignet ist (siehe den folgenden Artikel: „Systemüberwachung mit Tivoli“). Beide Produkte sind sich in ihrer Funktionsweise ähnlich. Sie arbeiten mit Agenten bzw. Endpoints, welche auf den zu überwachenden Servern installiert werden.

Zur Funktionsweise des Microsoft Operations Manager

Die MOM-Agenten werten nach der Installation auf dem Server unermüdlich Logfiles und andere Datenquellen anhand von Regelsätzen aus. Übereinstimmungen mit den Regelsätzen melden die Agenten an einen MOM-Server zurück, welcher das Herzstück der verteilten Umgebung darstellt. Zusätzlich leiten sie automatisch Gegenmaßnahmen auf Servern mit Fehlfunktionen ein, falls entsprechende Regelsätze definiert sind. Ferner besteht die Möglichkeit beteiligte Administratoren über kritische Situationen per E-Mail zu benachrichtigen. Die gesammelten Informationen der Agenten werden nach der Auswertung in einer SQL-Datenbank gespeichert und stehen für einen längeren Zeitraum zur Verfügung. Eine Management-Konsole liefert ein aktuelles Bild der überwachten Serverumgebung. Die Konsole ist das Hauptarbeitswerkzeug eines MOM-Administrators. Mit dieser werden Regelsätze neu erstellt bzw. geändert oder weitere Server in die MOM-Überwachung aufgenommen.

Die Einsatzmöglichkeiten eines MOM-Systems sind vielfältig. Microsoft liefert vordefinierte Regelsätze (*Management Packs*) für verschiedene Server-Dienste mit, die sofort nach der Installation des MOM-Servers zur Verfügung stehen. Management Packs stellen Regelsätze für das Active Directory, den Internet Information Server, den Terminalserver, die Windows-Server-Basisfunktionalitäten und weitere Server-Dienste bereit. Die Erfahrung zeigt allerdings, dass diese Regelsätze im allgemeinen noch an die jeweilige Umgebung angepasst werden müssen. Regelsätze für fremde Produkte können mit genügend Detailkenntnissen eigenhändig konstruiert bzw. von Drittanbietern erworben werden. Interessant ist MOM auch für den Bereich „Server-Sicherheit“. Zwar wird von Microsoft kein Management Pack zu diesem wichtigen Punkt angeboten, aber selbstgeschriebene Regeln, wie sie am ZIV zum Einsatz kommen, erlauben die Überwachung von sensiblen Systemdiensten und -daten.

Zur Zeit werden am ZIV ca. 30 Windows-Server mit MOM überwacht, welche sich in unterschiedlichen Domänen innerhalb der Active-Directory-Struktur der WWU befinden. Der Einsatz von MOM muss sich also nicht auf Server innerhalb einer Windows-Domäne beschränken. Administratoren anderer Versorgungseinheiten haben innerhalb eines Pilotprojektes die Möglichkeit Windows-Server in das MOM-System des ZIV zu integrieren und anhand von Standard-Regelsätzen überwachen zu lassen. Die Alarmierung über Fehlfunktionen erfolgt via E-Mail. Ein administrativer Zugang zur MOM-Konsole ist nicht vorgesehen, da die Delegation von administrativen Rechten innerhalb eines MOM-Systems stark eingeschränkt ist. Versorgungseinheiten, die selber Regelsätze entwickeln wollen, haben die Möglichkeit ein eigenständiges MOM-System zu betreiben, welches mit dem System am ZIV verbunden werden kann.

(J winkeol@uni-muenster.de, G 3 16 18)

Literatur:

[1] <http://www.microsoft.com/mom>

Systemüberwachung mit Tivoli

M. Grote

Seit dem Frühjahr 2003 setzt das ZIV zur Überwachung seiner Server Software der Firma Tivoli ein, die im Rahmen eines landesweiten Projekts beschafft und installiert wurde.

Diese Software besteht aus auf den überwachten Systemen (den Endpoints) installierten Programmen und zwei zentralen Komponenten:

- dem *Tivoli Management Framework Server* und
- dem *Event Server*.

Die beiden zentralen Komponenten sind mit ihren zugehörigen Daten jeweils auf einem AIX-Server installiert.

Das **Tivoli Management Framework** besteht aus den beiden oben genannten Servern und sämtlichen Endpoints. Seine Aufgaben sind u. a.:

- Zugangskontrolle und Abbildung von administrativen Rollen. Hierbei ist es möglich, den Zugriff eines Administrators auf die von ihm betreuten Endpoints oder bestimmte Teilfunktionen zu beschränken.
- Verwaltung und Verteilung von Anwendungsprofilen.

Das Framework wird durch *Policy Regions* und *Profile Manager* strukturiert.

Aufgabe des **Event Servers** ist es, die von den Endpoints erzeugten Meldungen (Events) zu bearbeiten und darzustellen. Einige Möglichkeiten zur Event-Verarbeitung sind:

- Event löschen,
- Event anzeigen,
- Event mit anderen Events korrelieren, z. B. ein vorher angezeigtes Event löschen,
- E-Mail verschicken.

Zur Darstellung von Events dient die **Event Console**.

| Time Received | Class | Hostname | Severity | Rep. | Status | Admin. | Message |
|---------------------|-------------------------|--------------------|----------|------|--------------|--------|---|
| 28.10.2003 14:30:52 | Sentry2_0_daemonct | BATCH11 | Warning | 0 | Open | | Process instances smtp -t unix on BATCH11 Greater than 358 |
| 28.10.2003 14:33:26 | OV_Node_Down | FMXWMA.UNI... | Fatal | 0 | Open | | Node Down. |
| 28.10.2003 08:23:47 | Sentry2_0_daemon | comix3 | Critical | 17 | Acknowledged | grate | Daemon status dtsd on comix3 Equal to down |
| 28.10.2003 08:23:47 | Sentry2_0_daemon | comix3 | Critical | 17 | Acknowledged | grate | Daemon status cdsadv on comix3 Equal to down |
| 28.10.2003 08:13:52 | Sentry2_0_daemon | comix3 | Critical | 18 | Acknowledged | grate | Daemon status dced on comix3 Equal to down |
| 28.10.2003 04:08:50 | Sentry2_0_zombies | ganzfiz.uni-mue... | Minor | 36 | Open | | Lingering terminated processes on ganzfiz.uni-muenster.de Greater than 11 |
| 28.10.2003 11:53:54 | Logfile_Ptd | miami02 | Warning | 0 | Open | | Failed dereferencing clean_func call |
| 28.10.2003 09:40:53 | Sentry2_0_waitforio | obelix7 | Warning | 41 | Open | | Percent of waiting for I/O on obelix7 Greater than 89(percentage) |
| 28.10.2003 14:29:23 | NT_Base | openuss02 | Warning | 0 | Open | | Replication of license information failed because the License Logging Service on serv |
| 28.10.2003 14:31:48 | universal_ncustom | pap5.uni-muens... | Warning | 0 | Open | | Numeric script \$LDRROOT/Monitore/chk_dceuxd on pap5.uni-muenster.de Greater |
| 28.10.2003 13:28:09 | universal_filesystempct | psyswap15 | Warning | 3 | Open | | /programs on psyswap15 Greater than 81 |
| 26.10.2003 02:36:22 | AIX_Errorlog_SSA | tsm01 | Critical | 0 | Open | | Msg SSA_DISK_ERR3 88DD5B42 |
| 28.10.2003 11:06:12 | w2k_LogDiskPrfFreeSpace | wuucsv | Warning | 3 | Open | | Percent Free Space C: on wuucsv Greater than 93.6246(percent) |

Für jeden Operator kann eine eigene Konsole definiert werden, so dass er nur die für ihn relevanten Events bearbeiten kann. Die Bearbeitungsmöglichkeiten beinhalten u. a.:

- Event akzeptieren,
- Event schliessen,
- Event als E-Mail weiterleiten,
- Eventpriorität ändern.

Auf den **Endpoints** werden vom Management Server nur die jeweils benötigten Überwachungs-routinen installiert. Unterstützt werden hier die folgenden Betriebssysteme:

- Windows NT, XP, 2000, 2003,
- AIX 4.33 und AIX 5.1,
- Solaris 2.x,
- Linux (SuSE und RedHat).

Logfile Adapter filtern aus den auf den Endpoints vorhandenen Logfiles Informationen heraus und leiten diese an den Event Server weiter. Solche Logfiles sind beispielsweise:

- das Windows Eventlog,
- das UNIX Syslog,
- und das AIX Errlog.

Monitore überwachen bestimmte Funktionen oder Parameter auf einem Endpoint, z. B.:

- CPU-Last,
- Speicherauslastung,
- Netzlast,
- Dateisysteme,
- Länge von Mail- und Print-Queues,
- Vorhandensein von Prozessen.

Darüber hinaus ist es möglich, eigene Monitore einzubinden. Im ZIV geschieht dies zur Überwachung:

- der Bandroboter,
- des Parallelrechners,
- der Temperatur im Maschinensaal, d. h. indirekt der Klimaanlage,
- der Funktionalität der DCE- und DFS-Server.

Ein noch weitergehender Schritt ist die direkte Einbindung der Systemüberwachung in Applikationen. Dies ist bei den im ZIV eingesetzten Tivoli-Produkten **Netview** und **Tivoli Storage Manager**, aber auch beim WWW-Mailprogramm **perMail** der Fall.

Neben der Erzeugung von Events sind vor allem folgende Reaktionsmöglichkeiten innerhalb eines Monitors von Bedeutung:

- das Versenden von E-Mail,
- das Ausführen eines Programms, z. B. zum Neustart eines Dämons.

Zur Zeit werden 90 Server des ZIV überwacht. Mit der Einbeziehung erster Fachbereiche und der ULB wurde begonnen.

Abschließend ist anzumerken, dass die Tivoli-Systemüberwachung bereits in etlichen Fällen dabei geholfen hat, Fehlersituationen frühzeitig zu erkennen und zu beseitigen, so dass schwerwiegende Störungen des Betriebs vermieden werden konnten.

Für weitere Informationen wenden Sie sich bitte an Mathias Grote, G 31675.

Meinberg Lantime: NTP über IPv6

C. Strauf

NTP ist ein Protokoll zur Übermittlung einer genauen Uhrzeit innerhalb eines Netzes. Dieses Protokoll ist mittlerweile auch für Netze verfügbar, die das neue Internet Protokoll Version 6 (IPv6) verwenden. Die Aufgabe des JOIN-Forschungsprojektes am ZIV der Uni Münster bestand darin, Produkte für NTP über IPv6 auszusuchen. Daraus entwickelte sich eine produktive Kooperation zwischen JOIN und der Firma Meinberg zur Portierung ihres NTP-Servers „Lantime“ nach IPv6.

Was ist NTP?

NTP steht für „Network Time Protocol“ und ist ein Verfahren, um möglichst genau und ohne Schwankungen eine aktuelle Uhrzeit zwischen Time-Servern und -Clients zu übertragen. Dazu werden sehr genaue Zeitquellen wie GPS-Satelliten, aber auch Zentren mit Atomuhren, deren Zeitsignale per Funk übertragen werden, verwendet.

Die Stärke eines NTP-Netzwerkes liegt darin, dass sich alle beteiligten NTP-Server untereinander synchronisieren. Auf diese Weise ist gewährleistet, dass selbst beim Ausfall einer Außenanbindung die lokale Zeit innerhalb des Netzes möglichst lange genau bleibt. Dieses wird dadurch erreicht, dass die NTP-Server untereinander Zeitschwankungen registrieren, vergleichen und dann auch ausgleichen.

Wofür wird eine hochgenaue Zeit benötigt?

NTP ist ein sehr wichtiges Werkzeug vor allen Dingen für die Sicherheit in einem großen Netzwerk. Eine Vielzahl von verwendeten Mechanismen zur Authentifizierung, wie z. B. Kerberos, sind anfällig für so genannte „Replay-Attacks“. Diese Form von Angriffen beruht darauf, dass der Verkehr zwischen einem Client und einem Server von einem feindlichen Rechner abgehört und aufgezeichnet wird. Teile dieses Verkehrs werden dann erneut „abgespielt“ und es können so u. U. Daten erschlichen bzw. Authentifizierungen gefälscht werden. Um dies zu verhindern, werden häufig Zeitstempel in die anfälligen Protokolle eingebaut, anhand derer ein Server bzw. ein Client feststellen kann, ob zeitliche Abfolgen im Austausch von Daten plausibel sind, oder nicht. Die Verwendung von Zeitstempeln ist aber nur dann sinnvoll, wenn die Zeit auf Clients und Servern möglichst synchron ist.

Ein weiteres Gebiet, auf dem genaue Zeitstempel benötigt werden, ist das Logging. Viele Komponenten eines Netzwerkes verwenden Zeitstempel beim Schreiben von Logfiles. Um die Ursachen von Störungen einzukreisen, müssen Logfiles von Netzwerkkomponenten verglichen werden. Dieser Vergleich ist aber nur dann sinnvoll, wenn die dort angegebenen Zeitstempel von möglichst synchron laufenden Uhren stammen. Auch dies ist mit Hilfe von NTP kein Problem. Netzwerkkomponenten namhafter Hersteller unterstützen meist die Verwendung von NTP-Servern.

Wo kommt das neue Internet Protokoll Version 6 (IPv6) ins Spiel?

NTPv3 sah bislang nur vor, über das alte, derzeit verwendete Internet Protokoll Version 4 (IPv4) transportiert zu werden. Mittlerweile gibt es NTPv4, welches auch für den Transport über IPv6 ausgelegt ist.

Das JOIN-Team hat sich im Mai 2003 näher mit NTP beschäftigt. Alle bisherigen Lösungen für NTP über IPv6 basieren bislang auf Linux-Rechnern. Aus administrativer Sicht ist die Verwendung von Linux-Rechnern ein Nachteil, da für die Wartung solcher Server im Normalfall nicht genügend Zeit zur Verfügung steht. Vielmehr ist es wünschenswert, eine so genannte „Appliance“ zu betreiben, im Wesentlichen eine Black-Box, an die eine Antenne zum Empfang eines Zeitsignals angeschlossen wird und die dann auf NTP-Anfragen antwortet. Leider konnte trotz intensiver Suche eine solche NTP-Appliance im Mai 2003 nicht aufgetan werden.

Meinbergs Lantime

Das JOIN-Team hat sich Ende Mai 2003 an die Firma Meinberg Funkuhren gewendet, einem mittelständischen deutschen Unternehmen mit ca. 30 Mitarbeitern, das sich auf die Herstellung von Funkuhren spezialisiert hat und einen eigenen NTP-Server produziert (nach ISO 9001). In Gesprächen mit Mitarbeitern von Meinberg stellte sich heraus, dass Interesse daran besteht, den Markt für IPv6-fähige NTP-Appliances zu erschließen. Die von Meinberg hergestellte NTP-Appliance mit dem Namen Lantime ist eine auf Linux aufbauende Eigenentwicklung. Der Einsatz von Standard-Software erleichtert deutlich die Portierung des Lantime zu IPv6. JOIN berät Meinberg bei IPv6-relevanten Fragen und gibt des Weiteren Anregungen für wünschenswerte Features, die ein NTP-Gerät besitzen sollte. Im Oktober 2003 stellten die Ingenieure von Meinberg eine erste Version des Lantime-Betriebssystems vor, die IPv6 beherrschte. Die Hoffnung ist, dass die vorhandenen Kinderkrankheiten einer solchen Neuentwicklung möglichst schnell beseitigt werden können, damit dem Einsatz des Lantime in einem produktiven Netzwerk nichts mehr im Wege steht. Zur Unterstützung der Portierungsarbeiten hat JOIN einen Lantime im Servernetz des ZIV installiert.

Alle Interessierten können diesen NTP-Server unter dem Namen `tmpntpsrv.uni-muenster.de` erreichen (über IPv4 und IPv6). Es ist dabei allerdings zu beachten, dass es sich um ein experimentelles System handelt, an dem Portierungsarbeiten durchgeführt werden. Die Benutzung des Servers ist also nur zu Testzwecken empfehlenswert, für den produktiven Betriebs ist der NTP-Server bisher nicht geeignet. Der im ZIV installierte Meinberg Lantime ist weltweit eine der ersten IPv6-fähigen NTP-Appliances, die im Einsatz ist.

Wie sieht die Kooperation mit Meinberg in Zukunft aus?

Das JOIN-Team handelt derzeit ein Abkommen mit Meinberg für Feldtests des Lantime im Rahmen des europäischen 6NET-Projektes und des 6WiN, dem IPv6-Netz des DFN aus. Dazu werden günstige Konditionen für die Beschaffung von Geräten und das Beziehen der neuesten Software für das Gerät abgemacht. Im Gegenzug sollen die Feldtests und der Feedback der Ergebnisse Meinberg helfen, die IPv6-Unterstützung im Lantime zu verbessern und zu optimieren.

Der Bedarf an IPv6-fähigen NTP-Geräten wird mit der zunehmenden Anzahl an IPv6-Netzwerken steigen. Die Zusammenarbeit zwischen JOIN und Meinberg ist ein erster Schritt, die dort vorhandene Lücke an Geräten zu schließen und gleichzeitig den Fortschritt auf dem Gebiet von NTP über IPv6 voran zu treiben.

Links

<http://www.join.uni-muenster.de/Join/Kooperationen.php>

<http://www.ntp.org>

<http://www.meinberg.de/german/products/lantime.htm>

Neues von SPSS

S. Zörkendörfer

**Für das statistische
Programmsystem SPSS
beginnt am 1. Dezember
ein neues Lizenz-
jahr.**

Einzelheiten dieses Vertrag sowie Neuigkeiten werden auf der Webseite <http://www.uni-muenster.de/ZIV/Organisation/SoftwareVerteilungSPSS.html> angekündigt. Der Lizenzvertrag sieht vor, dass Nutzungslizenzen nicht nur für dienstliche Rechner, sondern auch für häusliche Arbeitsplätze der Mitarbeiter/Studierenden erworben werden können.

Wesentliches Programmprodukt dieses Hochschullandeslizenzvertrages ist das SPSS selbst mit den Komponenten *Base, Regression Models, Advanced Models, Tables, Trends, Categories, Exact Test, Missing Value Analysis, Conjoint* und *Custom Tables*. Aktuell ausgeliefert ist die (deutschsprachige) Version 11.5. Im einem Artikel der letzten Ausgabe Nr. 2/2003 des i haben wir die Neuerungen beschrieben. Ein Termin zur Auslieferung der 12er-Version kann noch nicht genannt werden.

Es seien die aktuellen Versionen der weiterer Produkte des Vertrags aufgezählt:

- AMOS 5.0 (*structural equation modeling SEM*, ersetzt LISREL im Vertrag)
- SPSS AnswerTree 3.1 (*decision trees*)
- SPSS DATA ENTRY Builder 3.0
- AXUM7 (*technical graphics and data analysis*)

Neues von McAfee VirusScan

S. Zörkendörfer

**In der vorangegangenen
Ausgabe des i
haben wir das Programm
McAfee VirusScan Enter-
prise angekündigt. Mit
dem hier vorliegenden
Artikel sei auf die aktuelle
Version 7.1.0 dieses
Produkts hingewiesen.**

Die WWU hat einen Lizenzvertrag zu McAfee-Virenschutzprogrammen abgeschlossen, die laufende Lizenzperiode gilt zunächst bis einschließlich März 2004. Der Umfang der Nutzung auf dienstlichen Rechnern ist über die IVVen geregelt, darüber hinaus dürfen Mitarbeiter und Studierende die Produkte gemäß der Bedingungen des Lizenzvertrages am häuslichen Rechner nutzen. Über den Winkiosk <http://winkiosk.uni-muenster.de/> bekommen berechtigte Nutzer Zugang zu den Installationsmaterialien <https://winkiosk.uni-muenster.de/VirScan/VirusScan/Windows/Enterprise/VSE710DE.zip>, ich nenne in diesem Zusammenhang ferner die Produktliste <https://winkiosk.uni-muenster.de/VirScan/produkte.txt> zu der Lizenzvereinbarung. McAfee VirusScan Enterprise 7.1.0 ist u. a. in englischer und in deutscher Sprachversion ausgeliefert. Die Systemvoraussetzungen sind derzeit nicht explizit im README genannt, auch der Verweis auf die Produktdokumentation mag ins Leere führen. Deshalb zähle ich hier die im Installationshandbuch genannten Betriebssysteme auf, *und zwar für Arbeitsplatzrechner:*

Windows NT Workstation 4.0 mit Service Pack 6 oder 6a,
Windows 2000 Professional mit Service Pack 1, 2 oder 3,
Windows XP Home, Professional und Tablet PC Edition mit Service Pack 1,

und für Server:

Windows NT Server 4.0 mit Service Pack 6 oder 6a,
Windows NT Enterprise Server 4.0 mit Service Pack 6 oder 6a,
Windows NT Terminal Server Edition mit Service Pack 6,
Windows 2000 Server mit Service Pack 1, 2 oder 3,
Windows 2000 Advanced Server mit Service Pack 1, 2 oder 3,
Windows 2000 DataCenter Server mit Service Pack 1, 2 oder 3,
Windows Server 2003 Standard (früher Windows .NET Server 2003, Standard Edition),
Windows Server 2003 Enterprise (früher Windows .NET Server 2003, Enterprise Edition),

Windows Server 2003 Web (früher Windows .NET Server 2003, Web Edition),
Windows Server 2003 DataCenter.

Für die Betriebssysteme Windows 95, 98, ME bietet die Lizenzvereinbarung weiterhin das Produkt VirusScan Version 4.5.1 an.

Insbesondere bezüglich der Aktualisierung der Virendefinitionen sei auf die Anleitung https://winkiosk.uni-muenster.de/VirScan/VirusScan/Windows/Enterprise/VSE710_Anleitung.html hingewiesen. Wir bemühen uns, die Virendefinitionen möglichst aktuell zu spiegeln – das heißt mindestens einmal täglich, wobei vom Hersteller in der Regel nur einmal wöchentlich neue Virendefinitionen herausgegeben werden. Aber bei Attacken mögen es auch zwei Ausgaben an einem Tag sein – auch das Einstellen von EXTRA-DATs (zuletzt anlässlich W32Sober@MM) in die Repository wird vom Autoupdate beachtet. Je nach Art der Anbindung des Rechners gilt also die Empfehlung für Einzelplatzrechner: Täglich ein „AutoUpdate“ als geplante Task konfigurieren oder von Hand anstoßen. In der Regel werden dabei Datenmengen für ein inkrementelles Update übertragen, eine upd-Datei hat einen Umfang in der Größenordnung 100 KiloByte.

Probieren geht über Studieren? Vergewissern Sie sich, ob bzw. dass eine Task zum Zeitpunkt „Bei der Anmeldung“ oder „Bei Systemstart“ wirklich aktiviert wird. Auch ist ganz schnell erprobt, von welcher Quelle ein Update der Virendefinitionen zügig gelingt – im Laufe der Zeit mögen Sie diesbezüglich zu neuen Erkenntnis gelangen. Mit unserem Vorschlag `sitelistZIV.xml` (nämlich ftp zum Winkiosk und als *Fallback* ebenfalls ftp zu `ftp.nai.com`) haben wir auch weitere deaktivierte Quellen zum Erproben genannt. Sie gewinnen schnell einen Überblick, indem Sie die VirusScan Konsole aufrufen und über den Menüeintrag „Extras“ die AutoUpdate-Repository-Liste importieren und/oder bearbeiten. Voraussichtlich bei Lizenzverlängerung zum 1. April 2004 werden wir unsere Empfehlungen neu fassen.

Administratoren, die in Ihrer Umgebung gespiegelte Virendefinitionen bereitstellen, seien auf die aktuelle Version 1.1.1 des McAfee AutoUpdate Architect hingewiesen. (VirusScan Enterprise 7.0 und AutoUpdate Architect 1.0 behindern sich gegenseitig im gleichem System.)

Neues von der ZIV-Bibliothek

R. Nienhaus

Leider mußte der Bestand der Bibliothek des ZIV wegen Platzmangels in die Universitäts- und Landesbibliothek verlegt werden.

In diesem Bestand befinden sich über 2700 Bände der Reihe „Lecture Notes Computer“ sowie zahlreiche Bände der Reihe „Informatik aktuell“ des Springer-Verlages Heidelberg. Der Grundstock dieser Bibliothek wurde bereits in den 60er-Jahren gelegt und bot einen kompletten Überblick über die Entwicklung der EDV, deren Wurzeln in der numerischen Mathematik und mathematischen Logik liegen.

Neues von NIC_online

M. Kamp

Der Web-Zugang zur Netz-Datenbank des ZIV erfreut sich großer Beliebtheit.

Bereits in i Nr. 1/2001 haben wir unter dem Titel „NIC_online – Endgeräteverwaltung über das WWW“ den Web-Zugang zur Netz-Datenbank des ZIV vorgestellt. Inzwischen ist aus NIC_online mehr als eine reine „Endgeräteverwaltung“ geworden. Reger Zuspruch durch die Benutzer¹ hat dazu geführt, dass zahlreiche Funktionen hinzugefügt wurden. Bereits sehr früh wurde von den Nutzern der Wunsch geäußert, die Online-Administration, die zunächst nur den leitend und technisch Verantwortlichen möglich war, an weitere Personen delegieren zu können. Dazu wurden Administrationsgruppen eingeführt, die Verantwortliche selbst einrichten können. Innerhalb solch einer Gruppe kann weiteren Personen das Recht erteilt werden, Informationen über die Endgeräte abzufragen oder zu ändern, die ebenfalls zu dieser Gruppe gehören.

Neu ist auch die Verwaltung von so genannten Anwendungsumgebungen. Durch Anwendungsumgebungen lassen sich Dienstleistungen, die mit dem ZIV vereinbart wurden, einer Gruppe von Endgeräten zuordnen. Hierzu gehören beispielsweise Netzbasisdienste wie DHCP oder WINS, besondere Dienste wie RIS (siehe i Nr. 3/2002: „ZIV bietet RIS-Support“), aber auch Schutzmaßnahmen für Rechner durch Access-Control-Listen² und vieles andere. Spezielle Anwendungsumgebungen können auf Anforderung durch das ZIV eingerichtet werden, dabei wird jeweils festgelegt, welche Nutzer diese Umgebung verwalten dürfen.

Darüber hinaus wurden verschiedene Erleichterungen im Umgang mit NIC_online hinzugefügt. So ist es jetzt möglich neue Endgeräte online für den direkten Zugang zum Rechnernetz anzumelden. Sehr bequem geschieht dies, indem ein schon vorhandenes Gerät als Vorlage genommen und kopiert wird. Es brauchen dann meist nur noch wenige Attribute (Ethernet-Adresse, Rechnername, Netz-Anschlussdose) geändert werden; viele Eigenschaften wie Verantwortung, Aufstellungsort u. a. werden von der Vorlage kopiert. Da für eine Endgeräte-Anmeldung weiterhin die Unterschrift des Betreibers notwendig ist, muss ein LAN-Antrag in Papierform nachgereicht werden. Dieser kann vom Nutzer direkt nach der Neuanmeldung ausgedruckt werden und muss unterschrieben an das ZIV gesendet werden.

Es besteht inzwischen auch die Möglichkeit DNS-Subdomänen zu verwalten. Dies wurde insbesondere durch die Einführung des Active-Directory (i Nr. 3/2001: „Windows 2000 Active Directory“) notwendig. Betreiber von Subdomänen können jetzt selbst definieren welche Namen aus der Domäne „uni-muenster.de“ zusätzlich auch in einer Subdomäne „domaene.uni-muenster.de“ gelten sollen. Subdomänen unterhalb von „uni-muenster.de“ können auf Anfrage durch das NIC (nic@uni-muenster.de, G 83-31598) eingerichtet werden. Für das UKM wurde zusätzlich die Möglichkeit programmiert, Alias-Namen auch in der UKM-eigenen Domäne „ukmuenster.de“ zu verwalten. Um weiterhin einen möglichst störungsfreien Betrieb des Datennetzes zu gewährleisten, wird auch hier darauf geachtet, dass Namen netzweit eindeutig bleiben³. Namen für „ukmuenster.de“ werden daher immer auch in „uni-muenster.de“ eingetragen.

Zur Suche von Endgeräten wurden zusätzliche Suchkriterien eingefügt. So ist es jetzt möglich, Endgeräte zu Räumen, Gebäuden, Einrichtungen u. v. a. zu suchen und aufzulisten.

¹ Von etwa 1000 Personen, die für Verwaltung und Betrieb von Rechnern im LAN der Universität und des UKM verantwortlich sind, haben sich bereits mehr als 400 für die Nutzung von NIC_online angemeldet. Täglich wird NIC_online von ca. 60 Nutzern verwendet.

² Paketfilter in den Routern, die nur bestimmte Kommunikationstypen zulassen (IP-Adressräume, TCP-Ports, etc.).

³ Dies betrifft insbesondere das WINS- bzw. Netbios-Problem, der Name muss auch ohne Domänen-Suffix eindeutig sein.

Speziell für Leiter von IV-Versorgungseinheiten sowie für die jeweiligen Ansprechpartner von LAN-Bauprojekten wurde eine Übersicht der aktuell vom ZIV durchgeführten Bauprojekte geschaffen. In einer Rangliste kann eingesehen werden, auf welchem Listenplatz sich ein Bauprojekt für Netzanschlüsse jeweils befindet.

Insgesamt sehen wir die Entwicklung von NIC_online aber noch lange nicht als abgeschlossen an. Ein wichtiger Schritt wird sein, die Verknüpfung von Endgeräten und Netz-Anschlussdosen zu verbessern. Hier sollen auch netztechnische Parameter einer Anschlussdose angezeigt werden, also Parameter wie Anschlussgeschwindigkeit (10/100/1000 Mbit/s); Duplex-Modus (full/half); Port-Status (enabled/disabled) angezeigt werden.

Ein leidiges Thema hierbei ist die Diskrepanz zwischen Dokumentation und der Realität. Leider bewirken Änderungen am Datenbestand derzeit noch keine Umkonfiguration der jeweiligen Netzwerkkomponenten.

Neue Pakete auf dem JOIN-FTP-Server

C. Schild

Wie schon im i Nr. 3/2002 berichtet, stellt der JOIN-FTP-Server im Universitätsnetz diverse Softwarepakete zur Verfügung, wodurch der Download für lokale Benutzer beschleunigt und zudem der G-WiN-Zugang ins Internet entlastet wird.

Im Laufe des Jahres sind einige neue gespiegelte Pakete hinzugekommen. Mittlerweile sind auf dem FTP-Server folgende Mirrors verfügbar (neuere Pakete sind mit einem * gekennzeichnet):

Linux-Distributionen:

*Gentoo und Gentoo-portage
Mandrake
RedHat
*Fedora
Debian
*Debian-non-US
SuSE

Weitere Software:

*OpenOffice
*Comprehensive Perl Archive Network (CPAN)
*Sun Public Patches
Linux-Kernels
Mozilla
USAGI-Projekt
Bieringer IPv6 Stuff

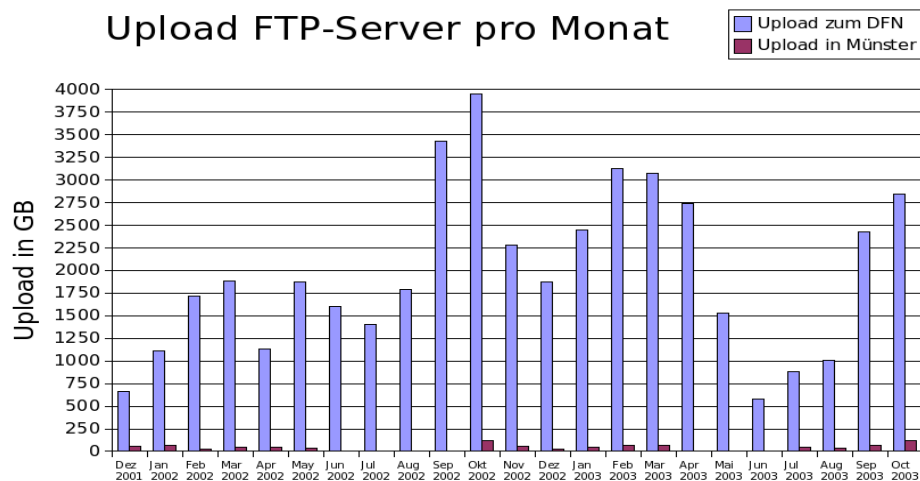
BSD-Distributionen:

FreeBSD
NetBSD

Dokumentation:

RFCs und Drafts

Neben den normalen FTP-Zugang über `ftp://ftp.join.uni-muenster.de` kann auf alle Pakete auch mit „rsync“ zugegriffen werden. Das folgende Diagramm zeigt das vom FTP-Server zu Nutzern im DFN bzw. der Universität Münster übertragene Datenvolumen.



Neues von ZIVprint

E. Sturm

Nur 5 Poster pro Benutzer werden in der Warteschlange geduldet. Außerdem wird ein neuer PostScript-Druckertreiber empfohlen.

Seriendrucke

An dieser Stelle soll noch einmal darauf hingewiesen werden, dass das ZIV keine Druckerei ist. Möchte also jemand ganze Serien von Postern drucken, so können wir dies nur dann ermöglichen, wenn die anderen Nutzer nicht behindert werden.

Um die Operateure bei der Kontrolle zu entlasten, haben wir einen Automatismus eingebaut, der in gewissen Abständen nachschaut, ob sich von einem Benutzer mehr als fünf Druckaufträge in der Posterwarteschlange befinden. Ist dies der Fall, so werden die überzähligen gelöscht und der Benutzer per E-Mail davon unterrichtet.

Sollte jemand Bedarf an einer größeren Posterserie haben, so möge er sich an mich wenden. Wir können dann eine eigene Warteschlange definieren, so dass dann ein Drucker die Serie bearbeitet und der andere die normalen Aufträge. (Für die Hochglanzposter ist sowieso ein dritter Drucker zuständig.)

Gerade bei Serien sollte man darauf achten, Papier sparend zu drucken. Zum Beispiel sollte man bei einem DIN-A1-Bild möglichst festlegen, dass es quer gedruckt wird (unabhängig davon, wie es später aufgehängt wird). DIN A1 quer ist nämlich gerade so breit wie DIN A0 hochkant. Damit wird die A0-Rolle des Druckers optimal ausgenutzt. Zur Not kann ich die Drehung (und ggf. Skalierung) des Bildes auch nach der Erstellung der PostScript-Datei vornehmen.

Druckertreiber

Damit wären wir schon beim Thema Druckertreiber.

Druckertreiber sind Programme, die entweder vom Betriebssystem mitgeliefert oder von einem Druckerhersteller auf CD zur Verfügung gestellt werden. Sie sorgen dafür, dass ein Anwendungsprogramm ein Dokument zum Drucker schicken kann, ohne zu „wissen“, welche Drucker-„Sprache“ dieser denn „versteht“. Das geht sogar so weit, dass man einen Drucker gar nicht real zu besitzen braucht, sondern die Ausgabe des Druckertreibers in einer Datei abspeichern kann. Dieser Weg ist ja bekanntlich für ZIVprint zu wählen.

Nachdem unser Farblaserdrucker HP Color LaserJet 8550 unverständlicherweise begonnen hatte, Druckaufträge, die mit dem von uns empfohlenen Druckertreiber Xerox MajestiK Fiery XJ erstellt waren, auf orange statt auf weißem Papier auszugeben, mussten wir uns etwas Neues einfallen lassen.

Gefunden habe wir den Windows-Druckertreiber AdobePS Akrobat Destiller, der sowohl für die Laserdrucker als auch für die Posterdrucker geeignet ist – sofern man keine Sonderwünsche hat. Das Bild wird in DIN A4 (einstellbar auch A3) erstellt, kann auf dem Farblaserdrucker getestet und danach auch auf den Posterdrucker (mit automatischer Vergrößerung auf DIN A0) geleitet werden.

Man bekommt diesen Druckertreiber bei Adobe oder auf unserer ZIVsoft-Webseite. Dort kann man auch nachlesen, wie die Installation bei Windows zu erfolgen hat:

1. Kopieren Sie die Dateien `winstger.exe` und `ADIST5.PPD` in ein Verzeichnis, dessen Namen Sie sich merken, und starten Sie `winstger.exe` (Doppelklick).
2. Druckerverbindungstyp: Lassen Sie die Einstellung „Lokaler Drucker“ unverändert.
3. Auswahl des lokalen Anschlusses: „FILE:“ auswählen.
4. Druckermodell auswählen: Klicken Sie auf „Durchsuchen...“ und wählen Sie die obige Datei `ADIST5.PPD` aus (nicht den angebotenen Generic PostScript Printer!).
5. Druckerinformationen: Entfernen Sie den Haken bei „Testseite drucken“.
6. Fertigstellen und Rechner neu starten.

Die Zukunft

Wie wird ZIVprint weiter entwickelt werden? Wie man an den chaotischen Sonderwünschen sehen kann, ist das Programm, das wir zur Abwicklung derselben verwenden, unwartbar. Wir werden es also demnächst streichen und damit alle Sonderwünsche ebenfalls – mit Ausnahme der erwähnten Vergrößerung beim Posterdrucker (etwa von A4 nach A0) und der Angabe der Exemplaranzahl bei allen Druckern.

Sollten Sie andere Sonderwünsche haben, etwa einseitigen oder doppelseitigen Druck, so sollten Sie diese Einstellung ab sofort beim Druckertreiber vornehmen. Unser empfohlener Druckertreiber „AdobePS Akrobat Destiller“ ist hierfür geeignet und kann sogar mehrere Dokumentseiten auf eine Papierseite drucken.

Wenn Sie spezielle Eigenschaften eines Druckers ausnutzen wollen, können Sie den modellspezifischen Druckertreiber benutzen, haben dann aber z. B. nicht die Möglichkeit, ein Posterbild vorher mit dem Farblaserdrucker zu testen. Außerdem müssen Sie dann wissen, welche Drucker wir gerade installiert haben. Zur Zeit sind dies:

- Schwarzweißlaserdrucker HP LaserJet 8000/8100,
- Farblaserdrucker HP Color LaserJet 9500hdn,
- Posterdrucker HP DesignJet 2500 CP.

Landeslizenz für StarOffice 7

E. Sturm

Auch StarOffice 7 dürfen wir kostenlos an Universitätsangehörige abgeben.

Entsprechend den Vorgaben der Fa. Sun kann das Zentrum für Informationsverarbeitung auch die Software StarOffice 7 an Universitätsangehörige verteilen. Eine einfache Kontrollmöglichkeit dieser Eigenschaft ergibt sich aus der Gruppenzugehörigkeit jeder Nutzerkennung am ZIV. Die neue Version von StarOffice kann wieder über die ZIVsoft-Webseite heruntergeladen werden.

Folgende Versionen gehören zur CD, die uns zugeschickt wurde:

- Linux
- Solaris (Sparc)
- Windows 98/ME/NT/2000/XP

Weiterhin kann man noch die Datenbank ADABAS und zusätzliche Wörterbücher herunterladen.

Die Größe der Dateien kann für Nutzer, die nur eine Modem-Verbindung zum Internet besitzen, zum Problem werden. Sie müssen mit einer Download-Zeit von 7 Stunden, wahrscheinlicher aber mit einem Leitungszusammenbruch rechnen. Einfacher ist es da, einen CIP-Pool zu verwenden und z. B. eine ZIP-Diskette (250 MB) oder eine CD zu beschreiben. Bei DSL oder im Universitäts-LAN sollte es keine Probleme geben. Für Informationsversorgungseinheiten (IVVen) stellen wir die CD auch auf dem bekannten CDROM-Server zur Verfügung.

Es sei hier noch einmal darauf hingewiesen, dass Sie StarOffice 7 nur selbst nutzen oder allenfalls an jemanden weitergeben dürfen, der ebenfalls Angehöriger unserer Universität ist und sich nur das Herunterladen sparen möchte. Der Beweis der Universitätszugehörigkeit ist z. B. durch unsere ZIVsoft-Webseite möglich. Gasthörer etwa sind keine Universitätsangehörigen.

Neues von Deleatur

E. Sturm

Eine neue Deleatur-Version steht an: 1.9; eigene und Benutzerwünsche sind eingeflossen.

Eine neue Version des Spamfilters Deleatur ist fertig. An Äußerlichkeiten wird man zunächst eine Mitteilung bemerken, dass die Wortbasis von `spam.basis` in `deleatur.bas` umbenannt worden sei. Dies ist nur für jemanden wichtig, der seine Wortbasis von Windows nach AIX oder umgekehrt mitnehmen will.

Als Nächstes fällt eine blau hinterlegte Zeile auf, die fragt, ob es weitergehen soll. Standardmäßig wird nach 24 Zeilen angehalten, so dass man die Wertungen von Deleatur kontrollieren und dann einfach die Eingabetaste drücken kann. Beim heutigen Ansturm von Spam wird man diesen Wert bald hochsetzen wollen, z. B. durch die Angabe `z=1000` in der Parameterdatei `deleatur.prm`.

Hat man doch eine mögliche Fehlbeurteilung entdeckt, so sollte man sich die Nummer der Mail notieren, denn am Ende hat man jetzt die Möglichkeit, sich einzelne Mails noch einmal vorlegen zu lassen – einfach durch Eingabe einer Nummernliste. Mir ist dabei noch nie eine Mail aufgefallen, die fälschlicherweise als Spam bezeichnet wurde. Gegen Mail, die fälschlicherweise als ordentlich gewertet wird, schütze ich mich durch Festlegung der Akzeptanzgrenze auf 0 (`a=0`). Deutsche Mail mit einer neuen „Geschäftsidee“ flucht sonst schon mal durch. Es kommt ja zunächst kein „verräterisches“ Wort vor!

Wer mehr Sicherheit wünscht, kann jetzt eine Bonus- und eine Malusdatei anlegen (`deleatur.bon` bzw. `deleatur.mal`). In diesen Dateien kann man Text angeben, der, wenn er in den Headerzeilen der Mail auftaucht, zu einer besonderen Reaktion führt: Wird ein Text der Bonusdatei gefunden, so wird die Mail nicht automatisch gelöscht. Wird ein Text der Malus-Datei gefunden, so wird sie nicht automatisch akzeptiert. Wer also Post von seinem Professor in jedem Fall benötigt, würde z. B. in der Bonusdatei schreiben:

```
from:prof.meier@uni-muenster.de
```

Noch einmal, dies bedeutet: Kommt in der Headerzeile, die mit `from:` anfängt, irgendwo der Text `prof.meier@uni-muenster.de` vor, so wird die Post, je nach Bewertung, entweder automatisch akzeptiert oder es wird eine Beurteilung erfragt. Nie wird eine solche Mail automatisch gelöscht. Andere Header können ebenso berücksichtigt werden.

Nun möchte ich auch zugeben, dass Deleatur noch Fehler enthalten hat. Vor der Reduzierung der Wortbasis unter AIX hatte ich ja in den Hot News gewarnt. Andere Fehler waren im Wesentlichen auf Mail zurückzuführen, die nicht der Norm entsprachen. Die neue Deleatur-Version ist hier nicht so gutgläubig, sondern reagiert auf fehlerhafte Mail nicht mehr empfindlich.

Inhaltlich habe ich noch die Reduzierung der Wortbasis geändert. Es wird weiterhin garantiert, dass die Untergrenze nach der Reduzierung nicht überschritten wird. Außerdem wird jedes Wort entfernt, das nur einmal vorgekommen ist. Zumindest beim ersten Mail wird man feststellen, dass so ungefähr zwei Drittel aller Wörter wegfallen.

Einen genauen Zeitplan für Deleatur 1.9 möchte ich nicht aufstellen. Bisher habe ich nur allein getestet, als Nächstes müssen meine Kollegen „dran glauben“, die Deleatur vom Netz nutzen. Dann kommt die AIX-Version an die Reihe und zum Schluss die Windows-Version auf ZIVsoft (www.uni-muenster.de/zivsoft).

Bildgewinnung und Bilddarstellung – Ein Praktikum

H.-W. Kisker

Zu Beginn des Wintersemesters 2003/2004 wurde vom ZIV zum zweiten Mal ein Multimedia-Praktikum angeboten.

Das Praktikum bot in einem einwöchigem Intensivkurs eine Einführung in die breite Palette der Bildgewinnung und der Bilddarstellung. Die Teilnehmer arbeiteten in Gruppen von zwei bis drei Personen zusammen. An jedem Tag wurde ein anderes Thema behandelt. Dabei wurde der Umgang mit verschiedenen Arten von Scannern und Kameras geübt und praktisch erprobt. Auch die



Bildgewinnung aus dem und die Bereitstellung im Internet wurde behandelt. Die geleistete Arbeit und das dabei gesammelte Bildmaterial wurde abhängig vom Thema in unterschiedlichen Formen dokumentiert, Foto-CDs und Video-DVDs wurden ebenso erzeugt wie Dokumente im PDF- oder Word-Format.

Als Anmerkung sei hinzugefügt, dass im Vorfeld eine das Praktikum vorbereitende Vorlesung ins Web gestellt wurde. Sie ist unter

<http://winkiosk.uni-muenster.de/MMR1/Inhalt.htm>

für jedermann zu erreichen. Eine zum Druck geeignete PDF-Version ist über das Miami-System der ULB unter

<http://miami.uni-muenster.de/servlets/DerivateServlet/Derivate-1105/MMR1.pdf>

erhältlich.

Für den Dozenten entwickelte sich das Praktikum zu einer rundum erfreulichen Veranstaltung – auch eine so positive Bemerkung muss erlaubt sein. Die Teilnehmer waren hochgradig motiviert, investierten bereitwillig Zeit und Arbeit und entwickelten viel Eigeninitiative bei der Umsetzung von eigenen Ideen. Rein quantitativ ist der Fleiß der Teilnehmer beachtlich. Die 13 Teilnehmer des Praktikums vom September 2003 erzeugten auf dem zur Verfügung stehenden Server

- ein Datenvolumen von 40 Gbyte mit
- 3.280 Directories und
- 27.192 Fotos und Filmen.

Die Ergebnisse wurden neben der Realisierung in Filmen und Fotos auf dem Server zusätzlich in einem persönlichen Praktikumsbuch dokumentiert. Die teilweise sehr aufwändig gestaltete Form dieser Dokumentation hat mich veranlasst, einige der Ergebnisse auf der Seite

<http://winkioskr/Artikel/MM-Praktikum/MM-Praktikum.htm>

auszugsweise zu veröffentlichen.

perMail – E-Mail-Retter, Spam-Vernichter und noch viel mehr

R. Perske

Unser WWW-Mail-Programm perMail wurde in den letzten Monaten um einige wichtige Möglichkeiten erweitert.

Seit Erscheinen des letzten Artikels zu perMail sind unzählbar viele Kleinigkeiten verbessert, geändert und erweitert worden, häufig auch auf Ihre Anregung hin, und hat es auch etliche bedeutendere Erweiterungen gegeben, die ich hier noch einmal vorstellen möchte.

Beachten Sie bitte, dass die meisten der hier beschriebenen Einstellungsmöglichkeiten und Schaltflächen erst dann dargestellt werden, wenn Sie von der Oberfläche „Start – für Einsteiger“ unter Benutzung des Auswahlfeldes „Bedienung – perMail kann viel mehr“ mindestens auf die Oberfläche „Text – für gelegentliche Nutzer“ umgestellt haben.

E-Mails verloren?

Natürlich legen wir *keine* Kopien aller durchlaufenden E-Mails an. In aller Regel werden also entsorgt oder anderweitig vernichtete E-Mails endgültig verloren sein.

Jedoch erfolgt jede Nacht eine Datensicherung (Backup), welche auch Ihr zentrales Postfach (von perMail als Posteingang bezeichnet) und Ihre perMail-Ordner umfasst. Falls sich eine verloren gegangene E-Mail also zum Zeitpunkt einer Datensicherung in ihrem Postfach befand, existiert möglicherweise noch eine Kopie in unserem Datensicherungssystem.

Früher bedeutete der Wunsch verlorene E-Mails wiederherzustellen, dass ein Mitarbeiter des ZIV von Hand entsprechende Restaurierungsarbeiten durchführen musste.

Jetzt ist dieser Vorgang automatisiert und in perMail integriert. Nach der Anmeldung finden Sie in perMail unten auf der Index-Seite eine Schaltfläche „Aus Sicherungskopie zurückholen“.

Durch einen Klick auf diesen Knopf veranlassen Sie, dass nacheinander alle Sicherungskopien des aktuellen Ordners (im Regelfall also Ihres Postfachs) durchsucht werden und alle darin vorhandenen E-Mails, sofern sie nicht noch im Ordner vorhanden sind, dorthin zurückkopiert werden.

Ältere Sicherungskopien sind üblicherweise auf Magnetbänder in unser Robotersystem ausgelagert, können also nicht innerhalb weniger Sekunden erreicht werden. Daher wird für diese Sicherungskopien nur ein Rückruf abgesetzt. perMail wird Sie darüber entsprechend informieren.

Falls Sie auch die in diesen Sicherungskopien enthaltenen E-Mails benötigen, benutzen Sie bitte nach etwa ein bis zwei Stunden (bitte nicht früher!) noch einmal die Schaltfläche „Aus Sicherungskopie zurückholen“, dann sollten auch diese E-Mails zurückgeholt werden können.

Wenn das immer noch nicht ausreicht, um eine vermisste E-Mail wiederherzustellen, dann haben Sie Pech gehabt: Dann können auch die ZIV-Mitarbeiter nichts mehr für Sie tun.

Übergroße E-Mails

Wer größere Dokumente und Dateien per E-Mail versenden möchte, stößt angesichts des Platzhungers heutiger Anwendungsprogramme immer öfter gegen Grenzen: Die E-Mail-Transport- und -Zustellserver leiten nur solche E-Mails weiter, die eine bestimmte Größe nicht überschreiten. Dadurch schützen die E-Mail-Server sich selbst und die Mailboxen der Empfänger vor Verstopfung.

Schon lange bieten wir für diese Fälle unter der Adresse <https://user.uni-muenster.de/exec/bigmail> den Bigmail-Dienst an, bei dem Dateien auf einem WWW-Server hinterlegt werden und der Empfänger nur noch eine Benachrichtigung erhält, von wo er sich die Daten innerhalb einer Woche herunter laden kann. Bei vielen Mailprogrammen braucht der Empfänger dafür nur einen einzigen Mausclick vorzunehmen.

Die obige WWW-Adresse wird nur noch benötigt, wenn Sie sich von Auswärtigen über große E-Mails zusenden lassen möchten, denn Bigmail ist seit vielen Monaten schon nahtlos in perMail integriert: Falls Sie mit perMail eine E-Mail mit so großen Anlagen versenden, dass die Gefahr besteht, dass der Transport oder die Zustellung der E-Mail beim Empfänger deshalb verweigert wird, dann schaltet perMail automatisch auf Hinterlegen um: Die Anlage wird auf dem perMail-Server hinterlegt und in die E-Mail nur ein Hinweis auf die Download-Adresse aufgenommen.

Ab der Bedienoberfläche „Text“ haben Sie auch die Möglichkeit, das Beifügen oder Hinterlegen der Anlage selbst zu steuern.

Natürlich gibt es auch beim Bigmail-Dienst und bei der Hinterlegung mit perMail noch Größenbeschränkungen: Bedingt durch die Technik der WWW-Server können zur Hinterlegung vorgesehene Dateien nicht größer als etwa 90 bis 95 MB sein. Das ist aber fast das Dreißigfache dessen, was Sie per herkömmlicher E-Mail versenden können; selbst mit einem DSL-Anschluss benötigen sie gut anderthalb Stunden zum Hochladen einer so großen Datei.

Unabhängig von allen Größenbeschränkungen empfehle ich Ihnen schon wegen der Ladezeiten, größere Dokumente und Dateien vor dem Versenden in eine Archivdatei zu kopieren und dann diese Archivdatei zu versenden. Die Archivdateien sind komprimiert und benötigen viel weniger Platz. Üblicherweise benötigt man zum Erzeugen oder Auspacken solcher Archivdateien ein ZIP-Programm; bei Windows XP heißen diese Archivdateien einfach „komprimierte Ordner“ und sind im Betriebssystem integriert. Daher werden nur noch wenige Empfänger Probleme haben, solche Archivdateien auszupacken.

Mehrere Anlagen gleichzeitig

Schon länger ermöglicht perMail auch das Versenden mehrerer Anlagen in einer einzigen E-Mail. Dazu müssen Sie einfach in dem Dateiauswahlfeld „Anlagen“ mehrere Dateien angeben – wenn Ihr WWW-Programm mitspielt.

Leider wird diese Möglichkeit selbst von den aktuellen Versionen einiger weit verbreiteter WWW-Programme (Internet Explorer, Mozilla, Netscape) nicht unterstützt. Als Alternative empfiehlt sich der abgesehen von Werbeeinblendungen kostenlose WWW-Browser von Opera: <http://www.opera.com>.

Natürlich können Sie auch einfach meiner obigen Empfehlung folgen, die zu versendenden Dateien in eine Archivdatei zusammenzufassen und dann nur diese Archivdatei zu versenden.

Rückfragen – sinnvoll oder nervend?

Solange Sie nichts anderes eingestellt haben, verhält sich perMail sehr geschwätzig und fragt bei jeder Aktion, mit der Sie wichtige Daten verändern könnten, lieber einmal mit einer Dialogbox nach, ob Sie das denn wirklich tun möchten. Sobald Sie etwas mehr Sicherheit im Umgang mit perMail gewonnen haben, können Sie mit dem Auswahlfeld „Rückfragen“ einstellen, wie viele Rückfragen gestellt werden sollen.

Bei der Einstellung „keine“ erfolgt keinerlei Rückfrage. Bei „wenige“ wird nur vor drohendem Datenverlust und Ähnlichem rückgefragt. Bei „normal“ erfolgen Rückfragen auch vor Ablegen, Kopieren, Absenden und anderen Datenveränderungen. Die Voreinstellung „viele“ schützt Sie zusätzlich vor dem Verändern von Markierungen, und die Auswahl „alle“ fragt Sie sogar beim Blättern.

Die Rückfragen und das Auswahlfeld erscheinen nur dann, wenn Sie in Ihrem WWW-Programm JavaScript aktiviert haben. Bei modernen WWW-Programmen ist das trotz der Risiken (man kann mehr mit JavaScript anfangen als nur Dialogboxen öffnen) standardmäßig der Fall.

Platz sparen

Falls Sie eine E-Mail mit Anlagen empfangen haben und diese Anlagen auf Ihren eigenen Rechner geholt haben (beispielsweise mit der Schaltfläche „Speichern nach Viruskontrolle“), dann könnten Sie natürlich die E-Mail auf dem perMail-Server in die Abfalltonne

„wegwerfen“ oder gar im Reißwolf „entsorgen“. Vielleicht möchten Sie die E-Mail aber auch ohne die Anlage aufbewahren. Dann können Sie mit der Schaltfläche „Teil entsorgen“ die Anlage aus der E-Mail ausschneiden und entsorgen; danach belegt die E-Mail nur noch einen Bruchteil des vorher benötigten Platzes. Achten Sie aber darauf, den richtigen Teil der E-Mail zu entsorgen.

HTML-Mails

Leider verwenden nicht nur Versender unerwünschter Werbe-E-Mails, sondern auch zunehmend seriöse E-Mail-Nutzer immer häufiger statt des einfachen Textformats das HTML-Format. Jedoch birgt dieses Format für den Empfänger große Gefahren, da man im HTML-Code sehr leicht Anweisungen unterbringen kann, mit denen man die Tätigkeiten des Empfängers überwachen oder noch schlimmere Dinge anstellen kann (Stichwort „Webbugs“ usw.).

Um Ihnen die Möglichkeit zu bieten, auch HTML-Mails lesen zu können, ohne sich diesen Gefahren auszusetzen, wurde in perMail ein HTML-zu-HTML-Konverter eingebaut, welcher nur garantiert ungefährliche HTML-Elemente durchlässt.

Mit dem Auswahlfeld „Alternativtexte“ können Sie jetzt einstellen, welche Alternative Sie sehen möchten, falls eine E-Mail sowohl einfachen Text als auch HTML-Text enthält.

Internationalität

Falls Sie E-Mails in fremden Zeichensätzen erhalten (perMail versteht jetzt sogar Chinesisch), können Sie den Text auch dann mit perMail lesen, falls Ihr WWW-Programm die fremden Schriftzeichen nicht kennt: Wenn Sie das Auswahlfeld „Textsatz“ auf „Bild“ oder „Bild+Umbruch“ einstellen, werden die Inhalte als Grafik dargestellt. Dabei können dank der frei verfügbaren UCS-Fonts über 30.000 verschiedene Schriftzeichen dargestellt werden.

In einigen Wochen werden Sie hoffentlich fremde Schriftzeichen auch in Betreff- und sonstigen Kopfzeilen lesen können, in einigen Monaten wird hoffentlich das gesamte System Unicode beherrschen, inklusive der Möglichkeit, mit entsprechenden WWW-Programmen E-Mails auch in asiatischen Schriften zu versenden.

Tipps und Tricks

Wie man es von vielen anderen Programmen her kennt, zeigt auch perMail jetzt nach jeder Anmeldung einen neuen Tipp an. Natürlich können Sie auch durch die verschiedenen Tipps blättern.

Spam, Spam, Spam

Fühlen auch Sie sich durch die vielen unerwünschten Werbe-E-Mails belästigt? Das kann ich gut verstehen: Ich selbst bekomme fast 200 Stück pro Tag.

Wir dürfen solche Mails nicht herausfiltern, genauso wie auch die Deutsche Post alle an Sie adressierten Sendungen zustellen muss. Aber wir können Ihnen Möglichkeiten an die Hand geben, um diese Flut auszusortieren. Über die Software „Deleatur“ meines Kollegen E. Sturm ist schon wiederholt hier im i berichtet worden.

In Kürze werden wir unsere Mailserver ausbauen und mit einer Software versehen, welche alle E-Mails anhand bestimmter Regelsätze überprüft und solche E-Mails, die offensichtlich oder wahrscheinlich als Spam anzusehen ist, durch Einfügen zusätzlicher Kopfzeilen markiert. Das von Ihnen verwendete E-Mail-Programm kann dann diese Markierungen auswerten und die E-Mail entsorgen oder was sonst Sie immer damit machen möchten.

Auch perMail versteht bereits diese Markierungen und zeigt offensichtliche Spam-Mails mit einem auffälligen schwarzen Warndreieck an. Außerdem sind für alle Nutzer „Wegsor-

tierregeln“ voreingestellt, welche auf Mausklick alle offensichtlichen Spam-Mails in die Abfalltonne befördert und alle wahrscheinlichen Spam-Mails in den Ordner „spam-messages“.

Sobald der Ausbau der Mailserver abgeschlossen ist, brauchen Sie also nach dem Anmelden in perMail nur noch die Schaltfläche „Alle E-Mails wegsortieren“ zu drücken, um den größten Teil der Spam-Mails loszuwerden. Sie können auch auf der Anmeldeseite schon „Beginne mit ... Weggordieren“ einstellen.

Während die sicher erkannten Spam-Mails dann endgültig vernichtet werden, sobald Sie die Abfalltonne leeren, sollten sich doch regelmäßig einen Blick in den Ordner „spam-messages“ werfen. Kein Spam-Filter arbeitet perfekt: Es ist durchaus möglich, dass eine „echte“ E-Mail versehentlich im Ordner „spam-messages“ landet. Sichern Sie diese E-Mails, bevor Sie den Rest des Ordnerinhalts entsorgen.

Die Spam-Markier-Maßnahmen werden bewusst konservativ eingestellt, daher wird es immer wieder einigen Spam-Mails gelingen, unentdeckt und unmarkiert in Ihr Postfach zu rutschen.

Es steht Ihnen natürlich frei, durch Ändern und Erweitern der voreingestellten Weggordierregeln die Weggordiertrate zu verbessern: Beispielsweise werden sicherlich alle an Sie adressierten E-Mails mit chinesischen Schriftzeichen Spam sein – es sei denn, Sie haben Kontakte in den chinesischen Sprachraum oder zum sinologischen Institut. Die an die neuen Möglichkeiten angepassten Beispiel-Weggordierregeln in der Online-Hilfe geben entsprechende Hilfestellung.

perMail im WWW

Als Einstiegsseite für alle Informationen zu perMail wurde die Adresse <http://www.permail.uni-muenster.de> eingerichtet. Dort finden Sie Links auf alle i -Artikel, Online-Hilfe-Seiten, Tipp-Seiten und sonstigen Informationsquellen sowie natürlich zum perMail-System selbst. In der Online-Hilfe finden Sie auch eine Liste aller für den Nutzer sichtbaren Änderungen an perMail.

Etwa zeitgleich mit dem Erscheinen dieses i wird die Anzahl der perMail-Server von vier auf sechs erhöht werden, um weiterhin möglichst gute Antwortzeiten bieten zu können. Immerhin haben in den letzten 12 Monaten über 17.100 verschiedene Nutzer perMail an der Universität Münster benutzt, das sind über 50 % aller Nutzer.

Auch die anderen Hochschulen, an denen perMail eingesetzt wird, melden jeweils Nutzungsquoten von über 50 %, so dass perMail jetzt von über 35.000 Nutzern verwendet wird.

Sicherheit geht vor

Natürlich sollte man zum Schutz seines Passworts und seiner Daten diese niemals unverschlüsselt über das Internet verschicken. Schon immer hat Ihnen perMail daher unter <https://permail.uni-muenster.de> einen abhörsicheren Zugang geboten und Sie dazu gedrängt, diesen Zugang zu benutzen.

Mittlerweile sollte jeder ein WWW-Programm benutzen, welches mit den hochsicheren Verschlüsselungen umgehen kann, die von den WWW- und perMail-Servern des ZIV verwendet werden. Daher wird jetzt auch bei Benutzung der Einstiegsseite <http://permail.uni-muenster.de> automatisch auf den abhörsicheren Zugang umgeschaltet.

perMail wird auch weiterhin ständig verbessert und ergänzt werden. Bei vielen Nutzern darf ich mich für die zahlreiche Anregungen und Hinweise bedanken.

Vom Rechner- zum Ressourcen-Verbund in NRW

St. Ost

Der Rechnerverbund NRW ist längst mehr als eine Einrichtung, den Zugang zu den Hochleistungsrechnern des Landes zu erleichtern.

Angefangen hat alles schon vor mehr als 6 Jahren mit landesweit abgestimmten IV-Versorgungskonzepten der Universitätsrechenzentren, mit dem DV-Infrastruktur-Ausschuss und mit dem wissenschaftlichen Ausschuss im Lande. Dabei wurden z. B. die Hoch- und Höchststreckerausstattung, die lokalen Rechnernetze, der Zugang zum Wissenschaftsnetz, die Perspektive zur Weiterentwicklung der DV und Themen zur Verbesserung der Sicherheit in der IV behandelt.

Verstärkt wurde dieser Verbund im Jahr 2000 im Vorfeld der Beschaffung des SUN-Hochleistungsrechners in Aachen. Mit der Idee einer NRW-weiten Nutzerverwaltung und eines landesweit verteilten Dateisystems wurde die Landes-DCE-Zelle `rv-nrw.de` mit DFS als verteiltem Dateisystem aufgebaut. Nicht zuletzt die guten Erfahrungen, die wir in Münster mit dem DCE/DFS gemacht haben, führte zu dieser Entscheidung. Folgerichtig ist die Universität Münster für die Landes-DCE-Zelle technisch verantwortlich.

Die Nutzer des Rechnerverbundes haben prinzipiell Zugang zu den Hochleistungsrechnern in Aachen, Dortmund, Münster, Köln und Bochum. Sie können außerdem die „Beilstein Reaktions- und Stoffdatenbank“ in Aachen und Dortmund aufsuchen.

Die DCE-Zelle hat sich in den folgenden Jahren als Kristallisationspunkt für eine sehr viel weitere Zusammenarbeit der Rechenzentren erwiesen. So wurden landesweit eine ganze Reihe von gemeinsamen Projekten begonnen, die nicht unbedingt viel mit der ursprünglichen Idee des Rechnerverbundes zu tun hatten, aber bewiesen haben, wie sinnvoll es ist, gemeinsame Probleme der Rechenzentren auch gemeinsam zu lösen. Beispiele wichtiger Projekte sind:

- Backup der Archiv-Dateien im Dreieck Aachen-Essen-Münster
- Gegenseitige Vertretungsregelung im Bereich Backup und Archiv
- Gemeinsame Beschaffungen
 - < System-Management mit „Tivoli“ und „BMC“
 - < Auswahl und Beschaffung des Content Management Systems „Imperia“
 - < Anwendungs-Software
 - ProEngineer
 - Ideas
 - Windchill
- Arbeitskreis Speichersysteme zur Gewinnung von Kompetenz im SAN-Umfeld
- Identity Management zur umfassenden Verwaltung von Nutzer-Identitäten und den damit verbundenen Zugriffsrechten

Die Vielfachheit der gemeinsamen Aktivitäten hat zu einer Namensänderung geführt: Der „Rechnerverbund NRW“ heißt nunmehr „Ressourcen-Verbund NRW“. Über die Aktivitäten des Ressourcen-Verbundes können Sie sich auf den Web-Seiten (<http://www.rv-nrw.de>) informieren.

Neue Netzstrukturen für den Internet/G-WiN-Anschluss der Universität und der Fachhochschule Münster

M. Speer

Seit einigen Monaten betreibt die Universität Münster zusammen mit der Fachhochschule Münster aus Kostengründen einen gemeinsamen Anschluss an das Internet/ G-WiN, einen sog. G-WiN-Cluster-Anschluss. Die technische Realisierung erfolgte im Juli 2003. Die zur Erhöhung der Verfügbarkeit der Internet/G-WiN-Anbindung schon seit Juni 2001 realisierte Backup-Funktionalität wurde dabei beibehalten. Gleichzeitig wurde ein neues Konzept zur Anbindung von Fremdnetzen an das Universitätsnetz realisiert.

Im Juli 2003 wurde der G-WiN-Cluster-Anschluss von Universität und Fachhochschule Münster technisch realisiert. Hatte zuvor jede der beiden Hochschulen einen eigenen G-WiN-Anschluss, so nutzen nun beide Hochschulen gemeinsam einen Anschluss. Dabei wurde der bisherige Anschluss der Universität (155 Mbps) zum neuen Primäranschluss für beide Einrichtungen. In der Summe steht nun beiden Hochschulen letztlich eine geringere Bandbreite als zuvor zur Verfügung. Dem gegenüber steht nun allerdings für beide Hochschulen eine Einsparung bei den Entgelten für die Nutzung des Anschlusses.

Um die zur Erhöhung der Verfügbarkeit der Internet/G-WiN-Anbindung schon seit Juli 2001 realisierte Backup-Funktionalität (vgl. entsprechende Artikel im i Nr. 2/2001) beizubehalten, fungiert der bisherige Fachhochschulanschluss (34 Mbps) nun als reiner Backup-Anschluss, d. h. der 34-Mbps-Anschluss wird nur bei Ausfall des 155-Mbps-Primäranschlusses benutzt. Außerdem existiert eine Hardware-Umschaltmöglichkeit für den Fall, dass nicht der 155-Mbps-Primäranschluss ausfällt, sondern der mit dem Anschluss verbundene Primär-Router. Die Umschaltung ermöglicht die Nutzung des 155-Mbps-Primäranschlusses über den Sekundär-Router (vgl. Abb. 1).

Uni und FH Münster: G-WiN-Cluster / Backup

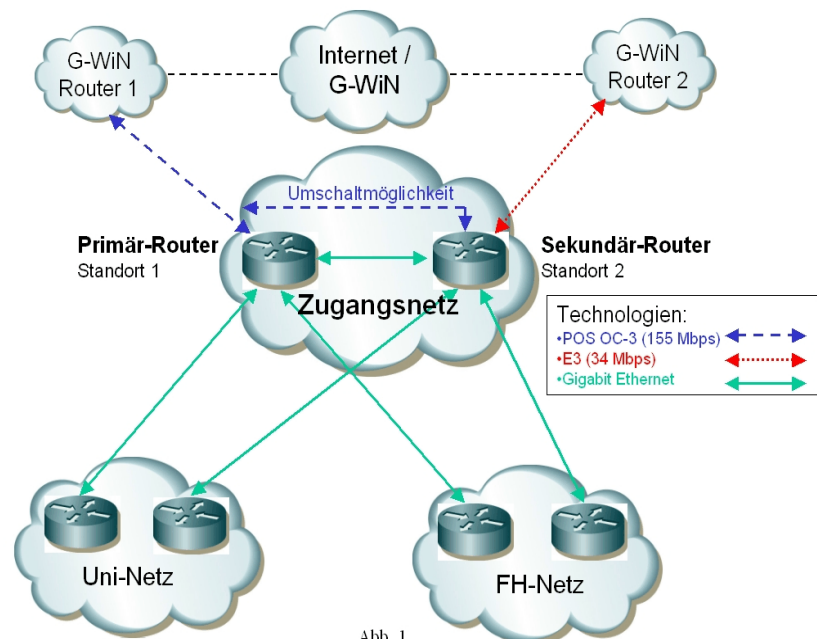


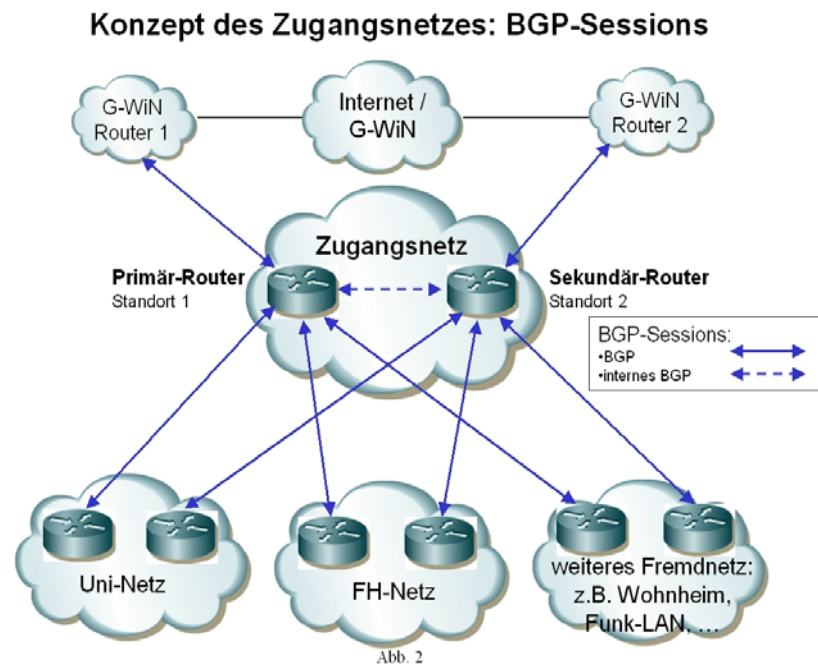
Abb. 1

Im Zuge der Realisierung des Cluster-Anchlusses wurde gleichzeitig ein neues Konzept für die Verbindung von Fremdnetzen mit dem Universitätsrechnernetz in einem ersten Schritt umgesetzt. Fremdnetze sind dabei ganz allgemein Netze, die nicht unter der Verantwortung bzw. nicht vollständig unter der Kontrolle der Universität betrieben werden. Beispiele für Fremdnetze sind z. B. das Gigabit-Wissenschaftsnetz (G-WiN), das Fachhochschulnetz, Wohnheimnetze oder auch öffentliche Netzbereiche (z. B. Funk-LAN-Zellen oder pLANet-Anschlussdosen). Hauptprinzip des neuen Konzeptes ist dabei, dass Fremdnetze niemals direkt mit dem Universitätsnetz verbunden werden, sondern dass die Kommunikation zunächst immer über ein sog. Zugangsnetz erfolgt. Die Abb. 1 zeigt, wie das Konzept des Zugangsnetzes für die Realisierung des G-WiN-Cluster-Anchlusses umgesetzt wurde. Aus Sicht des Zugangsnetzes wird dabei das Universitätsnetz auch zu

einem Fremdnetz. Im Zugangsnetz ist dabei die Möglichkeit vorgesehen, Fremdnetze redundant an einen sog. Primär- und einen Sekundär-Router anzubinden. Primär- und Sekundär-Router befinden sich dabei ebenso wie die beiden G-WiN-Anschlüsse an unterschiedlichen Standorten.

Der zunächst scheinbar höhere Aufwand für die Einrichtung und den Betrieb des Zugangsnetzes ermöglicht eine stärkere technische Trennung zwischen den einzelnen angeschlossenen Netzen. Das bedeutet zum einen eine geringere gegenseitige Beeinflussung der angebundenen Netze. Außerdem konzentriert sich die Zahl der Netzkomponenten (Router), auf denen die Verbindungen zu den verschiedenen Fremdnetzen berücksichtigt werden muss, auf einige wenige Systeme. Jedes der angeschlossenen Fremdnetze kann von der G-WiN-Backup-Konfiguration profitieren. Auch findet nur im Zugangsnetz sog. Transit (Durchleiten von Daten fremder Netze) statt. In der Konsequenz führt die Konzeption letztlich zu einer höheren Betriebssicherheit für alle beteiligten Netze. Auch lassen sich Sicherheitsfunktionen (Router-ACLs, Firewall-Funktionen, Security-Policies, ...) in den einzelnen Netzen auf Grund der starken Entkopplung leichter realisieren.

Besonderheit des Konzeptes ist neben den eingesetzten Netztechnologien (Gigabit Ethernet, 155 Mbps Packet over SONET, 34 Mbps E3), den Hardware-Redundanzen (Primär- und Sekundär-Router im Zugangsnetz und den angebundenen Fremdnetzen) und den Standort-Redundanzen der Einsatz des IP-Routing-Protokolls BGP (Border Gateway Protocol). BGP ist speziell dafür vorgesehen, Routing-Information (Erreichbarkeitsinformation) zwischen Fremdnetzen auszutauschen (vgl. Abb. 2). Außerdem unterstützt BGP eine Vielzahl von Möglichkeiten zur Steuerung der ausgetauschten Routing-Information, um bestimmte sog. Routing Policies zu realisieren. In der Konsequenz bedeutet das, dass für die Anbindung von Netzen an das Zugangsnetz zwingend BGP-Routerfunktionen erforderlich sind. Die Netze, zwischen denen BGP-Routing-Information ausgetauscht wird, werden dabei als sog. Autonome Systeme (kurz AS) bezeichnet.



Zum derzeitigen Realisierungsstand des Zugangsnetzkonzeptes ist folgendes zu sagen: Das Zugangsnetz wird vom ZIV der Universität betrieben. Die Fachhochschule ist derzeit nur mit einer einzigen Verbindung an das Zugangsnetz angebunden. Die redundante Anbindung der Fachhochschule soll baldmöglichst erfolgen. Wegen einer noch durch den Hersteller zu behebenden Fehlfunktion bei dem im Zugangsnetz eingesetzten Router-Typ ist zurzeit für die Anbindung des 155-Mbps-Primäranschlusses als Übergangslösung ein weiterer Router im Zugangsnetz in Betrieb. Die Anbindung weiterer derzeit noch direkt an

das Universitätsnetz angebotenen Fremdnetze (z. B. Wohnheimnetze) an das Zugangnetz wird in absehbarer Zeit umgesetzt werden.

Ein Schwachpunkt der jetzigen Konstruktion liegt leider noch außerhalb des unmittelbaren Implementierungsbereiches der Universität: Die beiden Zugänge zum G-WiN-Netz führen zu einer einzigen Lokation in Bielefeld (zum sog. G-WiN-Access-Router). Auch die Verbindung von dort zum G-WiN-Kernnetz und der entsprechende Kernnetz-Router in Essen bilden so genannte *Single Points of Failure*, die durchaus schon zu entsprechenden Totalausfällen der Internet-Konnektivität in Münster geführt haben. Das ZIV versucht eine weitere Verbesserung der Redundanzsituation an dieser Stelle zu erreichen, indem eben unabhängige Wege zum Internet oder mindestens zum G-WiN (also nicht über Essen) möglichst kostengünstig gesucht werden. Gespräche mit einigen Internet-Service-Providern einschließlich des G-WiN-Betreibers (DFN e. V.) lassen die Hoffnung gerechtfertigt erscheinen, dass spätestens nach Ablauf des jetzigen Vertrages 2004 eine Verbesserung erreicht werden kann.

Über 500 Teleport-ADSL-Anschlüsse geschaltet

M. Speer

Bei dem in Zusammenarbeit mit der Fachhochschule Münster und der Deutschen Telekom AG realisierten Angebot „Telearbeitsplatz Student“ im Rahmen des Teleport wurde im September 2003 in den Wohnheimen des Studentenwerkes der 500. ADSL-Anschluss für den Zugang zum Netz der Universität oder der Fachhochschule und zum weltweiten Internet geschaltet. Die technische Realisierung der ADSL-Einwahl wird in ihren Grundzügen beschrieben.

Seit Beginn des Pilotbetriebs im März 2001 betreibt das ZIV in Zusammenarbeit mit der Fachhochschule und der Deutschen Telekom im Rahmen des Teleport-Angebotes „Telearbeitsplatz Student“ ADSL-Einwahlmöglichkeiten für die Bewohner von Studentenwohnheimen des Studentenwerkes Münster in Münster und in Steinfurt. Im September 2003 wurde der 500. Teleport-ADSL-Anschluss geschaltet. Inzwischen (Stand November 2003) sind sogar bereits 590 Anschlüsse eingerichtet. Im Gegensatz zur konventionellen Einwahl (analoges Modem, ISDN), wo einer Teilnehmergruppe ein gemeinsamer Pool von Anschlüssen zur Verfügung steht, muss bei der ADSL-Technologie für jeden Teilnehmer eigens dauerhaft eine Verbindung (ein sog. ATM PVC) konfiguriert werden.

Insgesamt ist die Realisierung der direkten ADSL-Einwahl aus dem Teleport-Netz der Telekom in die Netze der beiden Hochschulen durch die Vielzahl der letztlich eingesetzten Technologien und die Komplexität der Konfiguration des Gesamtsystems ein anspruchsvolles Projekt. Folgende Technologien kommen u. a. zum Einsatz (vgl. Abb. 1):

Teleport ADSL – Konfiguration Nov. 2003

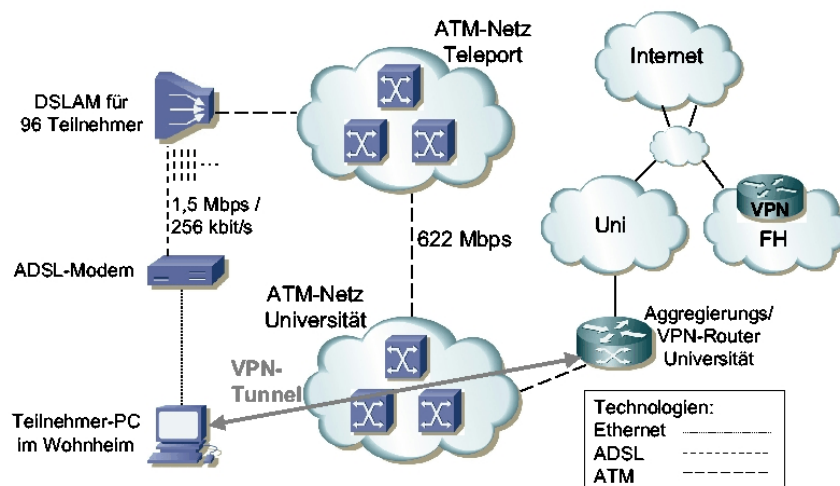


Abb. 1

- Ethernet: vom Teilnehmer-PC zum ADSL-Modem
- ADSL: vom ADSL-Modem bis zum sog. DSLAM (*Digital Subscriber Line Access Multiplexer* für typischerweise 96 Teilnehmer): 1500 kbit/s Downstream, 256 kbit/s Upstream. Die Ethernet-Pakete des Teilnehmers werden in ATM-Zellen verpackt und per ADSL zum DSLAM übertragen.
- ATM: Konfiguration eines PVCs für jeden Teilnehmer im Telekom-Netz und im Universitätsnetz. Über einen PVC werden dabei die Etherpakete eines Teilnehmers durch das ATM-Netz der Telekom und das ATM-Netz der Universität zu einem Router übertragen, auf dem die PVCs sämtlicher Teilnehmer aggregiert werden.
- VPN: Virtuelle Private Netze für die Nutzerauthentifizierung zum Übergang aus dem Teleport-Netz in die Universitätsnetze und das Internet. Die VPN-Funktion ist derzeit für die Universität auf dem Aggregierungs-Router realisiert. Für die Fachhochschule ist die VPN-Funktion auf einem eigenen Router realisiert. Als VPN-Verfahren wird derzeit das PPTP (Point-to-Point Tunneling Protocol) eingesetzt. Vom Teilnehmer-PC wird zum VPN-Router eine Verbindung (sog. VPN-Tunnel) aufgebaut. Über den VPN-Tunnel ist eine authentifizierte Kommunikation aus dem Teleport-Netz heraus möglich.

Die K-Säule – Ein Lösungsansatz zur Versorgung mobiler Nutzer

J. Chakoh

Wir haben einen Weg gefunden, beim Einsatz mobiler Rechner den lästigen Kabelverhau zu bändigen.

Der *nomadic user* ist in der jüngeren Vergangenheit zu einem fest gefügten Begriff geworden, der einen Nutzer von Ressourcen der Informationsverarbeitung beschreibt, der an häufig wechselnden Arbeitsplätzen, typischerweise mit seinem Notebook-Rechner, im Internet über verschiedenste Zugänge agiert. Wichtige Zugangsmethode wird immer mehr natürlich das Wireless LAN (WLAN). Entsprechend hat die Universität in den letzten drei Jahren in erheblichem Umfang in Netzausstattung investiert, so dass unsere nomadischen Nutzer inzwischen an mehr als 50 Standorten mit ihren Notebooks einen recht leistungsfähigen Zugang zu den IV-Diensten der Universität vorfinden. Auch die neue WLAN-Technologie IEEE 802.11g mit 54 MBit/s kommt den Bedürfnissen der Nutzer noch stärker entgegen; in Neuinstallationen wird diese Technologie bereits an der Universität eingesetzt, alle anderen Installationen (bisher 11 MBit/s, IEEE 802.11b) werden Zug um Zug abwärtskompatibel umgerüstet werden.

Trotz der vergleichsweise hohen Leistungsfähigkeit im Funk-LAN mit 11 bzw. 54 MBit/s ist dies nicht immer ausreichend. Zum einen handelt es sich bei WLANs um ein *shared medium*, d. h. dass die Bandbreite unter allen Nutzern in einer Funk-Zelle aufgeteilt wird. Bei Lehrveranstaltungen mit 10 Teilnehmern und mehr stehen so unter Umständen weniger als 1 MBit/s pro Teilnehmer zur Verfügung. Das ist manchmal für Standardanwendungen schon wenig (z. B. beim Zugriff auf Disk-Server), kann aber bei anspruchsvolleren Anwendungen sogar zum Versagen führen. Dies trifft zum Beispiel für einige Multimedia-Anwendungen zu. Aus diesem Grunde sind Alternativen zur Standardversorgung des Notebook-Nutzers mit WLAN sehr wünschenswert, und das ZIV hat eine Anfrage des Fachbereichs Erziehungswissenschaften gern zum Anlass genommen, eine entsprechende Lösung zu entwickeln.

Anfang 2003 sollten zwei Seminarräume in der Georgskommende 33 für Lehrveranstaltungen für den Einsatz von Multimediawerkzeugen in Erziehung, Bildung und Unterricht (MIEBU) ausgestattet werden; besonderes Merkmal der Teilnehmer war die Verwendung eigener Notebook-Rechner. Entsprechend dem Einsatzbereich sollte eine relativ hohe Leistungsfähigkeit des Netzes bereitgestellt werden. Auch musste berücksichtigt werden, dass keinesfalls feste Anschlüsse inmitten der Räume an den Tischen erwünscht waren, vielmehr sollte der Zugang zum Netz immer möglichst kurzfristig und variabel entsprechend der flexiblen Bildung von Arbeitsgruppen gestaltet werden können.

Da auf dem Markt derzeit keine Lösungen angeboten werden, die diesen Anforderungen entsprechen, wurde durch das Zentrum für Informationsverarbeitung (ZIV) eine Kommunikationssäule (K-Säule) entworfen und in Zusammenarbeit mit dem Institut für Kernphysik für den Fachbereich Erziehungswissenschaften in entsprechender Anzahl gefertigt. Die K-Säule ist ein mobiles Anschluss-Terminal mit LAN- und Stromnetzanschlüssen für bis zu vier Nutzer gleichzeitig. Als LAN-Anschlusstechnologie steht Fast-Ethernet (FE, 100 MBit/s) zur Verfügung, das auch über schon integrierte FE-USB-2.0-Adapter notebookgerecht (d. h. über den USB-Anschluss) genutzt werden kann. Das Bild unten zeigt aus der Vogelperspektive eine typische Anwendungssituation. Man kann erkennen, dass die Versorgungskabel in Form von Spiralkabeln aus Rohren herausgezogen werden können – Stolperfallen werden damit vermieden, gleichzeitig ist die Verstauung der Kabel bei Nichtgebrauch ohne Durcheinander gelöst. Dies ermöglicht auch einen einfachen Auf- und Abbau der K-Säule in kurzer Zeit.

Der Anschluss der K-Säule selbst an Daten- und Stromnetz kann über an der Decke oder im Wandbereich befindliche Anschlussdosen erfolgen und zwar ebenfalls mit Spiralkabeln, die sich in den Rohren befinden. Im Regelfall soll die K-Säule dabei an das im Aufbau befindliche pLANet-Zugangssystem der Universität erfolgen, das ausschließlich einen Zugang erlaubt, wenn der Nutzer sich authentifiziert (vgl. <http://www.uni-muenster.de/ZIV/Rechennetz/planet>).

Die K-Säule hat sich bereits in der Praxis bewährt, obwohl wir die Erprobungsphase als noch nicht ganz abgeschlossen betrachten. Die Nutzer sind von der Mobilität und Einsatzfähigkeit der Säule begeistert. Interessenten für weitere K-Säulen wenden sich bitte an das Geschäftszimmer des ZIV.



Die K-Säule

ZIV-Lehre

Veranstaltungen in der Vorlesungszeit (Wintersemester 2003/2004) für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse Hier seien noch einmal zur Dokumentation die laufenden Veranstaltungen des Wintersemesters 2003/2004 genannt. Für die Veranstaltungen in den Semesterferien sei auf die jeweils Di, Do 11-12, nachfolgende Aufstellung verwiesen.
G 83-31561

| | | |
|---------------|---|--|
| 260109 | cms@uni – Werkzeuge für den Webauftritt Mittwoch 15-17 Uhr Hörsaal: M4, Einsteinstr. 64 | Neukäter, B. |
| 260113 | Programmieren in C++ Mittwoch 13-15 Uhr Hörsaal: M4, Einsteinstr. 64 | Mersch, R. |
| 260128 | Programmieren in Java Dienstag 13-15 Uhr Hörsaal: M4, Einsteinstr. 64 | Pudlatz, H. |
| 260132 | Statistische Datenanalyse mit dem Programmsystem SPSS Mittwoch 11-13 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60 | Nienhaus, R. |
| 260147 | Windows-Betriebssysteme: Einführung und Grundlagen Mittwoch 9-11 Uhr Hörsaal: M4, Einsteinstr. 64 | Sturm, E. |
| 260151 | Windows-Systemadministration: Ausgewählte Themen Mittwoch 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13 | Lange, W./ Winkelmann, O. |
| 260166 | Rechnernetze und Internet: Technische Grundlagen Donnerstag 10-12 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13 | Richter, G./ Forsmann, A./ Kamp, M./ Speer, M./ Wessendorf, G. |
| 260170 | Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 9-13 | Held, W. |

Veranstaltungen in der vorlesungsfreien Zeit (Frühjahr 2004) für Hörer aller Fachbereiche

| | | |
|---|---|-----------------------------|
| Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, G 83-31561 | Für alle Veranstaltungen ist eine frühzeitige Online-Anmeldung erforderlich, die ausgehend von der Webadresse http://www.uni-muenster.de/ZIV/Content-Lehre.html unter „Anmelden zu den Veranstaltungen“ erfolgen kann. Für den Dialog sollte dabei vorzugsweise auf die dort angebotene verschlüsselte (abhörsichere) Datenübertragung umgeschaltet werden. Anmeldungen zu den Veranstaltungen sind 5. Januar 2004 möglich. | |
| 260016 | Publizieren im Internet mit XML Blockveranstaltung vom 22.3. bis 2.4.2004 Mo-Fr 10-12, 14-16 Hörsaal: ZIV-Pool 3, Einsteinstr. 60 | Neukäter, B. |
| 260020 | Publizieren mit LaTeX Blockveranstaltung vom 1.3. bis 12.3.2004 Mo-Fr 9-11, 15-17 Hörsaal: M4, Einsteinstr. 64 (vormittags), ZIV-Pool 3, Einsteinstr. 60 (nachmittags) | Kaspar, W. |
| 260150 | Programmieren in Fortran Blockveranstaltung vom 15.3. bis 26.3.2004 Mo-Fr 8-10 Hörsaal: ZIV-Pool 2, Einsteinstr. 60 | Reichel, K. |
| 260035 | Programmieren in Java Blockveranstaltung vom 15.3. bis 26.3.2004 Mo-Fr 9-11 Hörsaal: M4, Einsteinstr. 64 | Süselbeck, B. |
| 260040 | Statistische Datenanalyse mit dem Programmsystem SPSS Blockveranstaltung vom 9.2. bis 20.2.2004 Mo-Fr 9-11 Hörsaal: ZIV-Pool 3, Einsteinstr. 60 | Zörkendörfer, S. |
| 260054 | Betriebssystem Linux/Unix: Einführung und Grundlagen Blockveranstaltung vom 24.2. bis 5.3.2004 Mo-Fr 10-16 (Beginn dienstags!) Hörsaal: ZIV-Pool 3, Einsteinstr. 60 | Grote, M. |
| 260069 | Einführung in die Benutzung des Parallelrechners Blockveranstaltung vom 13.4. bis 16.4.2004 Di-Fr 9-12 Hörsaal: Raum 206, Röntgenstr. 9-13 | Leweling, M. |
| 260073 | Systemadministration für Linux-Systeme Blockveranstaltung vom 15.3. bis 19.3.2004 Mo-Fr 9-16 Hörsaal: ZIV-Pool 3, Einsteinstr. 60 | Hölters, J. |
| 260088 | Systemadministration für Windows-Systeme Blockveranstaltung vom 22.3. bis 26.3.2004 Mo-Fr 9-16 Hörsaal: Raum 206, Röntgenstr. 9-13 | Lange, W. Winkelmann, O. |

ZIV-Regularia

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptographischen Prüfsummen der öffentlichen Schlüssel, die von der WWUCA und vom ZIV verwendet werden.

Bei E-Mails, WWW-Servern und an vielen anderen Stellen wird zunehmend mit Verschlüsselung und elektronischen Unterschriften gearbeitet. Dabei besitzt mindestens einer der Kommunikationspartner (beispielsweise der WWW-Server) einen öffentlichen Schlüssel, der vom anderen Partner (beispielsweise Ihrem WWW-Browser) zum Verschlüsseln oder zum Überprüfen einer elektronischen Unterschrift benutzt wird.

Um zu verhindern, dass Ihnen falsche öffentliche Schlüssel untergeschoben werden, sollten Sie überprüfen, ob der jeweilige Schlüssel tatsächlich zur angegebenen Person bzw. zum angegebenen Server gehört. Zu diesem Zweck sind die Schlüssel häufig mit Zertifikaten versehen, das sind elektronische Beglaubigungen, ausgestellt von sog. Zertifizierungsstellen, in denen die Eigentümerschaft bestätigt wird.

Im Bereich des deutschen Wissenschaftsnetzes erstellen die DFN-PCA als übergeordnete Zertifizierungsinstanz und die WWUCA als Zertifizierungsstelle der Universität Münster solche Zertifikate, siehe <http://www.dfn-pca.de> und <http://www.uni-muenster.de/WWUCA/>.

DFN-PCA und WWUCA unterstützen zwei verschiedene Verschlüsselungs- und Zertifizierungssysteme: Die PGP-Familie (Pretty Good Privacy), zu der auch GnuPG (Gnu Privacy Guard) gehört, wird meistens bei E-Mail eingesetzt. Die X.509-Familie wird beispielsweise bei abhörsicheren WWW-Servern, bei S/MIME und bei Object Signing verwendet.

Zum Überprüfen der von DFN-PCA und WWUCA ausgestellten Zertifikate benötigen Sie deren öffentliche Schlüssel. Diese finden Sie auf <http://www.uni-muenster.de/WWUCA/zertifikate.html> (X.509 und PGP) oder auch an anderen Stellen wie beispielsweise der perMail-Titelseite <http://permail.uni-muenster.de> (nur X.509), der ZIVprint-Einstiegsseite <http://www.uni-muenster.de/ZIV/zivprint.html> (nur X.509) oder der ZIV-Mitarbeiterliste <http://www.uni-muenster.de/ZIV/Mitarbeiter/> (nur PGP).

Die Fingerabdrücke (Fingerprints) dieser Schlüssel sind nachfolgend abgedruckt, damit Sie beim Aktivieren der Schlüssel auf Ihrem Rechner kontrollieren können, dass Sie tatsächlich die echten Zertifizierungsschlüssel erhalten haben.

PGP-Kommunikationsschlüssel

Da die Zertifizierungsschlüssel ausschließlich zum Zertifizieren verwendet werden, gibt es gesonderte Kommunikationsschlüssel, die Sie bitte verwenden, wenn Sie eine verschlüsselte E-Mail an die jeweilige Zertifizierungsstelle schreiben möchten:

KeyID 4CB7658D: Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
2048 Bits, Fingerprint: 383D 0F16 CEFC 1F9E B7C3 04B1 2020 FCE6
KeyID 94E799B5: DFN-PCA (2004), ENCRYPTION Key <dfnpca@dfn-pca.de>
2048 Bits, Fingerprint: A9F8 2DC4 09CC DA7F DC67 8FE5 28DE AAAC (ab 01.01.2004)
KeyID E77ADB85: DFN-PCA, ENCRYPTION KEY <dfnpca@pca.dfn.de>
2048 Bits, Fingerprint: 48BE 7479 7F5D BD4C 652B 9853 DD5A 0305 (bis 31.12.2003)

PGP-Zertifizierungsschlüssel der WWUCA

KeyID 38B7A481: Zertifizierungsstelle Universitaet Muenster 2004-2005
2048 Bits, Fingerprint: 973E 0725 040B 1745 F272 180D 08C2 C15A

KeyID BC811EB1: Zertifizierungsstelle Universitaet Muenster 2002-2003
2048 Bits, Fingerprint: 2864 01BC F0EF D5BA D9A0 866C 4379 4C1D

KeyID 313C02F5: Zertifizierungsstelle Universitaet Muenster 2000-2001
2048 Bits, Fingerprint: 3762 F5E0 C278 7697 530F 2DF2 F3B3 27F5

KeyID EF750F1D: Rainer Perske +49(251)83-31582 Certification Key
2048 Bits, Fingerprint: 2F38 6EF8 DC2E D85E 5B35 DB49 8AE4 52AF

PGP-Zertifizierungsschlüssel der DFN-PCA

KeyID FDCB1C33: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2004-2005)
<<http://www.dfn-pca.de/>>
2048 Bits, Fingerprint: 96B0 AD7F B8DC 0018 DCA0 7053 1C3B 4DA5

KeyID F2D58DB1: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2002-2003)
<<http://www.dfn-pca.de/>>
2048 Bits, Fingerprint: DE31 690D BC6A E779 4DCD A1B5 8180 FE7B

KeyID 63EB5391: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 2001)
<not-for-mail>
2048 Bits, Fingerprint: CFAF 6C29 4E57 4E0E E81C BDB4 54FD 2AAB

KeyID F7E87B9D: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1999-2000)
<not-for-mail>
2048 Bits, Fingerprint: 6570 7274 B5E0 3FF0 EA7C ABE4 465F B8B2

KeyID 35DBF565: DFN-PCA, CERTIFICATION ONLY KEY (Low-Level: 1997-1998)
<not-for-mail>
2048 Bits, Fingerprint: 097C 0919 D3C3 86DC 7A30 1511 1295 8DE3

X.509-Zertifikate der WWUCA

Inhaber: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2004-2005/Email=ca@uni-muenster.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 64774066 (0x3dc5fb2)
MD5-Fingerprint: 2619 6BEF 66B2 7044 52CC BE11 4C5F 3CB8
SHA1-Fingerprint: 1765 AE6D 57C7 7914 D2AF BAF3 439C E139 66E1 A0AE

Inhaber: C=DE, O=Universitaet Muenster,
CN=Zertifizierungsstelle 2002-2003/Email=ca@uni-muenster.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 1774668 (0x1b144c)
MD5-Fingerprint: A431 AD41 D8F2 1856 4E31 CC69 71E6 174F
SHA1-Fingerprint: 6945 20CA 1AFE 5CFA 6C37 52EB B772 B054 90EC D979

X.509-Wurzelzertifikat der DFN-PCA

Inhaber: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Aussteller: C=DE, O=Deutsches Forschungsnetz, OU=DFN-CERT GmbH, OU=DFN-PCA,
CN=DFN Toplevel Certification Authority/Email=certify@pca.dfn.de
Seriennummer: 1429501 (0x15cffd)
MD5-Fingerprint: 3E1F 9EE6 4C6E F022 0825 DA91 2308 0503
SHA1-Fingerprint: 8E24 22C6 7E6C 86C8 90DD F69D F5A1 DD11 C4C5 EA81

Alle Angaben zur DFN-PCA ohne Gewähr.

Liebe Leserin, lieber Leser,

wenn Sie i regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von i nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

Bitte haben Sie Verständnis dafür, dass ein Versand außerhalb der Universität nur in begründeten Einzelfällen erfolgen kann.

Vielen Dank!

Redaktion i

.....



- ~ Ich bitte um Aufnahme in den Verteiler.
- ~ Bitte streichen Sie mich/den nachfolgenden Bezieher aus dem Verteiler.
- ~ Mir reicht ein Hinweis per E-Mail nach dem Erscheinen einer neuen WWW-Ausgabe.
Meine E-Mail-Adresse:

+

- ~ Meine Anschrift hat sich geändert.
Alte Anschrift:

An die
Redaktion i
Zentrum für Informationsverarbeitung
Röntgenstr. 9-13
48149 Münster

| |
|---|
| Absender: Name: _____ FB: _____ Institut: _____ Straße: _____ Außerhalb der Universität: _____ |
|---|

(Bitte deutlich lesbar in Druckschrift ausfüllen!)

Ich bin damit einverstanden, dass diese Angaben in der i -Leserdatei gespeichert werden (§ 4 DSGVO).

Ort, Datum

Unterschrift

