inforum

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 25, Nr. 2 – Juli 2001 ISSN 0931-4008

Inhalt

Editorial 2

ZIV-Aktuell **3**
Laptops und Funk-LAN – Neues im ZIV 3
Modernisierung und Erneuerung der ZIV-Pools 3
Backup, Redundanzen und Single Points of Failure des G-WiN-Anschlusses 4
Unsere Antwort: *perMail* 6
Neue TUSTEP-Version 2001 16
IV-Sicherheitslösungen durch Funktionen des Rechnernetzes 17
ZIVprint – der Nachfolger von WWWplot 18
McAfee VirusScan 4.5.1 23
Zugang zum Rechnernetz der Universität über das Internet 24
Virtuelle Private Netze an der WWU im Test 25
Teleport-ADSL-Zugänge zum Netz der Universität 26
ADSL: Status der Möglichkeiten des Zugangs zum Netz der Universität 27
Uni@home II – eine Nachfolge für *uni@home* ? 28
Fingerprints 30

ZIV-Tutorial **31**
Einführung in Virtuelle Private Netze (VPN) 31

ZIV-Lehre **35**
Veranstaltungen in der vorlesungsfreien Zeit (August/September 2001) 35
Veranstaltungen in der Vorlesungszeit (Wintersemester 2001/2002) 35
Kommentare zu den Lehrveranstaltungen 36

Impressum

infoRUM

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: W. Bosse (✆ 83-31561, ✉ bosse@uni-muenster.de)
R. Perske (✆ 83-31582, ✉ perske@uni-muenster.de)
H. Pudlatz (✆ 83-31672, ✉ pudlatz@uni-muenster.de)
E. Sturm (✆ 83-31679, ✉ sturm@uni-muenster.de)

Satzsystem: Corel WordPerfect 8.0 für Windows 98/NT

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

Auflage dieser Ausgabe: 1500

Editorial

E. Sturm

In dieser Ausgabe des infoRUM schwirrt es nur so von neuen Namen und Begriffen. Einige wurden im ZIV selbst erfunden, andere findet man auch in aktuellen anderen Publikationen. Wenden wir uns zunächst den hauseigenen neuen Namen zu:

perMail heißt die endlich geschaffene Möglichkeit, E-Mail über ein Web-Interface abholen und verschicken zu können. Man braucht also nicht mehr über die Klippen der Mailprogramm-Konfiguration zu springen, sondern nur noch Nutzerkennung und Passwort auswendig zu lernen. Ein weiterer wichtiger Vorteil ist die Datenhaltung auf dem Server: Von wo man sich auch anmeldet, immer kann man auf dieselben Mail-Ordner zugreifen.

ZIVprint hieß vorher *WWWplot*. Die Namensänderung zeigt die Funktionserweiterung: Nicht nur Bilddateien, sondern beliebige PostScript-Dateien kann man jetzt auf jeden der zentralen Drucker schicken. Bei Postern kann man jetzt wünschen, Hochglanzpapier zu bekommen, also erhöhten UV- und Feuchtigkeitsschutz. Auch die Druckstraße in der Drucktechnischen Zentralstelle gehört zur Palette der ansprechbaren Drucker.

ZIVpool heißt der CIP-Pool des ZIV im Gegensatz zu den (ähnlich klingenden) CIP-Pools anderer Institute. Über 70 neue PCs in drei Räumen stehen zur Verfügung.

Kommen wir zu den Begriffen, von denen man nicht nur bei uns etwas hört:

Das *Funk-LAN* ist eine neue Errungenschaft, die Benutzer von Laptops unabhängig von einer LAN-Steckdose macht.

Uni@home II ist ein neues Projekt, das es wieder attraktiv macht, die Universität als Internet-Provider zu benutzen.

VPN ist eine trickreiche Möglichkeit, die Vorteile eines LAN auch über das Internet zu genießen.

ADSL kennt man aus der Werbung nur mit einem T für das A. Was ADSL mit unseren Einwahlsystemen zu tun hat, war schon oft Gegenstand von Anfragen an uns. Auch hierzu finden Sie Erläuterungen in diesem Heft.

Das *G-WiN* ist das Rückgrat des Internets für die Universitäten und wissenschaftlichen Einrichtungen in Deutschland. Von seiner Existenz haben manche erst etwas bemerkt, als es auf einmal bei uns nicht mehr funktionierte. In diesem Heft ist beschrieben, was sich seitdem zur Verbesserung getan hat. Hier kann man auch erfahren, was ein *single point of failure* ist, nämlich die Stelle, die ein Bagger treffen muss, um uns vom Internet abzukoppeln.

ZIV-Aktuell

Laptops und Funk-LAN – Neues im ZIV

W. Held

Das ZIV ermöglicht eine neue Qualität des Rechnerzugangs.

Laptop-Sammelbestellungen für Mitglieder der Universität

Mehrere Studierende haben den Wunsch geäußert, die Universität Münster möge Sammelbestellungen für Laptops organisieren. Wir, d. h. ZIV und Dez. 5.3 der Universitätsverwaltung, greifen diesen Wunsch auf, nicht zuletzt, um durch die Verbreitung der Laptops die Nutzung der bereits installierten Funk-LANs zu fördern. Über Laptops und Funk-LANs wird dabei nicht nur ein hohes Maß an Mobilität bei Anbietern und Nutzern von Informationen erreicht, vielmehr werden dadurch neue Lehr- und Lernformen entstehen.

ZIV und Dez. 5.3 haben inzwischen die Preisermittlung für Laptops abgeschlossen. Die Ergebnisse zusammen mit der Möglichkeit zu einer ersten Bestellung finden Sie auf den WWW-Seiten des ZIV unter

```
http://www.uni-muenster.de/ZIV/wwuonly/
SammelbestellungLaptop.html
```

Die erste Lieferung soll noch vor Beginn der vorlesungsfreien Zeit erfolgen.

Wichtig: An der Sammelbestellung können sich nur Mitglieder (Ordentliche Studierende, Beschäftigte) der Universität und des UKM beteiligen.

Funk-LAN

Über das Funk-LAN an der Universität, seine Technik und den derzeitigen Ausbaustand findet man Informationen unter

```
http://www.uni-muenster.de/ZIV/Rechnernetz/funklan/ .
```

Sicherheit der IV

Zur Steigerung der Sicherheit sind vielfältige Maßnahmen erforderlich. Mehr dazu findet man unter

```
http://www.uni-muenster.de/ZIV/Content--HinweiseSicherheit.html
```

und dort insbesondere unter

```
http://www.uni-muenster.de/ZIV/Papers/SicherheitIV.html .
```

Dieser Bericht ist durch zahlreiche Hinweise für Personalcomputer ergänzt worden.

Modernisierung und Erneuerung der ZIV-Pools

H.-W. Kisker

Im Zentrum für Informationsverarbeitung wurden die beiden vorhandenen ZIV-Pools modernisiert und um einen weiteren ZIV-Pool erweitert.

Insgesamt stehen jetzt für die Arbeit der Studierenden 74 neue PCs und 11 teilweise erneuerte AIX-Systeme, verteilt auf drei Räume, zur Verfügung.

Die PCs sind einheitlich als Pentium-III-Rechner ausgelegt. Sie verfügen alle neben einem CD-Laufwerk auch über ein 250-MB-Iomega-Zip-Laufwerk zum Datenaustausch. Als Besonderheit sind sie mit zwei Platten ausgestattet, die die Betriebssysteme Windows und Linux bereitstellen. Von den beiden Platten ist, um die Betriebssysteme zuverlässig voneinander zu isolieren, jeweils nur eine physisch verfügbar. Die Umschaltung erfolgt über einen besonderen Schaltmechanismus, der nur wirkt, wenn der Rechner ausgeschaltet

ist. Um auch eine Fernwartung, wie sie im ZIV üblich ist, zu ermöglichen, wird für administrative Zwecke auch ein Umschalten über das Netz vorgesehen. Die Umschaltelektronik wurde von uns konzipiert und in Zusammenarbeit mit der Werkstatt der Kernphysik gebaut. Zzt. ist ein erster Raum hiermit ausgestattet.

Die jetzt erfolgte Modernisierung ist als erster Schritt zu sehen. Es galt, die beschaffte Hardware einer Nutzung durch die Studierenden zuzuführen. Die Arbeitsumgebung wurde dabei nicht geändert – auch nicht modernisiert. Im Laufe der nächsten Wochen werden zwei weitere Umstellungsschritte folgen.

1. Alle PCs werden mit einer Umschaltelektronik ausgestattet. Auch die Fernumschaltung muss noch verfeinert werden. Bei endgültiger Verfügbarkeit werde ich im Web darüber berichten.
2. Die Rechner werden in Zukunft unter Windows 2000 laufen. Die Software soll vorrangig über Terminal-Server-Mechanismen zur Verfügung gestellt werden.

Der neu eingerichtete, klimatisierte ZIV-Pool 3 ist besonders für das Abhalten von Lehrveranstaltungen ausgelegt. Neben einer Tafel besteht die Möglichkeit zwei Quellen gleichzeitig zu projizieren, z. B. Beamer und Overhead-Folie. Für den Dozenten steht ein besonderer Dozentenplatz zur Verfügung. Von diesem können Rechner und Overheadprojektor auch sitzend bedient werden.

Backup, Redundanzen und Single Points of Failure des G-WiN-Anschlusses

G. Richter

Darf man sich auf das Internet verlassen?

Der Anschluss des Rechnernetzes der Universität an das Wissenschaftsnetz G-WiN wird als Selbstverständlichkeit von vielen sicherlich gar nicht mehr bewusst wahrgenommen, man nutzt ihn eben. Das ändert sich für viele schlagartig, wenn eine Störung des Anschlusses vorliegt, weil Ressourcen und Dienste des Internet nicht mehr zugänglich sind. Selbst im ZIV als Betreiber des Anschlusses sind wir verblüfft, wenn uns dann z. B. Anfragen von anderen Hochschulen erreichen, die sich über die Störung einer Prüfungsklausur dort beklagen, weil die Universität Münster als Partner einer Kooperation nicht mehr erreichbar ist.

Ein längerer Ausfall des Anschlusses im Januar 2001 als auch wenige kleinere Störungen haben in der Universität besonders deutlich gemacht, wie groß inzwischen die persönlichen und institutionellen Abhängigkeiten von dem Medium Internet mit seinen Kommunikations- und Informationsmöglichkeiten sind – von der E-Mail über das Web-Angebot bis hin zu Datenbank-basierten Informations- und Transaktionssystemen. Es wird deshalb bereits seit längerem gefordert, dass durch Organisation, Gerätequalität und Netzdesign Verfügbarkeiten vergleichbar mit den Standards von Telekommunikationsanlagen hergestellt werden müssen, die mit bis zu 99,999% angegeben werden – dies entspricht einer Ausfalldauer von maximal 5 Minuten pro Jahr für jeden Teilnehmer. Auch im Hinblick auf die viel beschworene uns früher oder später erreichende Konvergenz der Netze (Telefon-, Sprach-, Video- und Datennetze werden in wenigen Jahren unter einem technologischen Dach vollständig zusammenwachsen) wird die so geforderte Verfügbarkeit des Netzes unabdingbar. Für das lokale Rechnernetz kann die Universität selbst Einfluss auf die Qualität nehmen. Für den Anschluss an das Wissenschaftsnetz sind die Verhältnisse viel komplexer; hier bestehen Abhängigkeiten von direkten und indirekten Dienstleistern (DFN-Verein als Vertragspartner, verschiedene Einrichtungen der Deutschen Telekom AG als Kern- und Zubringernetzbetreiber, DFN-Netz-Operating-Center und Wartungsfirmen für die netztechnischen Geräte/Router) sowie von den Hochschulen, welche bestimmte Router beherbergen und für Strom, Klima und Zugang zu den Räumen sorgen.

Das ZIV hat deshalb einen Arbeitskreis im Rahmen des DFN-Vereins initiiert, der sich zum Ziel gesetzt hat, Anforderungen an die Verfügbarkeit der G-WiN-Anschlüsse zu erörtern sowie praktische Konsequenzen jeglicher Art (organisatorisch-betrieblich, tech-

nisch, vertraglich) daraus abzuleiten. Gemeinsam mit der Fachhochschule führt die Universität Münster in einem Pilotprojekt als erste Teilnehmereinrichtung des G-WiN Maßnahmen durch, die zur Erhöhung der Verfügbarkeit des G-WiN-Zugangs für beide Hochschulen führen sollen. Dabei wird im Störungsfall wechselseitig auf den jeweils nicht betroffenen Anschluss als Backup-Anschluss zugegriffen (s. Abbildung auf Seite 27). Zwar besitzt der Anschluss der Fachhochschule eine vergleichsweise geringe Kapazität (34 MBit/s gegenüber 155 MBit/s), jedoch kann mit wenig Aufwand so für eine Erhaltung der Funktionalität bei reduziertem, aber noch zeitweise erduldbarem Durchsatz gesorgt werden – die Fachhochschule freilich kann sich im Störungsfall wahrscheinlich über erhöhten Durchsatz freuen. Die Umschaltung erfolgt im Fehlerfall automatisch auf der Basis weltweit im Einsatz befindlicher und damit ausreichend erprobter Mechanismen (BGP-Routing-Protokoll), ohne dass Nutzer oder das Netz-Operating-Center im ZIV etwas tun müssten; wie erste Tests zeigen, kann allerdings eine Unterbrechung im Fehlerfall von ca. 3 Minuten auftreten, während die Rückschaltung praktisch unterbrechungsfrei abläuft. Der jetzige Status ist so, dass die erste Forderung nach Redundanz der Anschaltung erfüllt und in ersten Tests erprobt ist; angekündigte kurzzeitige Betriebsunterbrechungen im Mai und Juni 2001 für Installation und Tests haben einigen Nutzern sicher schon den Hinweis auf unsere Aktivitäten gegeben. Die durch diese Schaltung zwischen FH und WWU erreichte Redundanz hätte uns zumindest die oben genannten Ausfälle erspart. Der Backup-Schaltung vorausgegangen waren weitgehend unbemerkt umfangreiche Umstrukturierungen im Netz, insbesondere erkennbar an der Umstellung von einigen IP-Adressräumen. Abgeschlossen sind die Aktivitäten noch nicht. Insbesondere sind noch lokale Optimierungen notwendig.

Lokal ist weitergehend zu klären, ob in der Trassierung der G-WiN-Zugangsleitungen auf dem Hochschulgelände noch *Single Points of Failure*, d. h. topologische Elemente, die zwangsweise durchlaufen werden müssen, zu beseitigen sind.

Aber wirkliche Redundanz muss über das zuvor Gesagte hinausgehen. Dabei sind die Redundanzverhältnisse im engeren Bereich des G-WiN erheblich schwieriger zu klären:

- Für die Wege- und Leitungsnutzung im Bereich des Zubringernetzes zwischen Münster und dem Zugangs-Router-Standort Bielefeld ist bisher z. B. nicht bekannt (weil Betriebsgeheimnis der Telekom), inwieweit diese für Fachhochschule und Universität unabhängig voneinander sind – die berühmt berüchtigte Baggerschaufel ist keine Chimäre aus der Vorstellungswelt übervorsichtiger Netzbetreiber, sondern aus den Medien wohlbekannt für Zusammenbrüche größten Ausmaßes in ausgedehnten Telefon- und Datennetzen, weil eben durch sie oft genug ganz banal Kabel zerstört werden können.
- Der Router-Standort Bielefeld mit seinem einzigen Zugangs-Router für mehrere Hochschulen bildet *Single Points of Failure* par excellence. Wünschenswert ist hier sicherlich, dass zumindest zwei unabhängige Router-Systeme für die beiden Zugangsleitungen vorhanden wären. Zur Zeit ist eine derartige Unabhängigkeit lediglich auf Modul-Basis vorhanden. Optimal wäre im Übrigen für jede Zuleitung ein eigener Standort des Zugangs-Routers, um auch Infrastrukturausfälle wie Klimaanlagendefekte und Zusammenbrüche der so genannten „unterbrechungsfreien“ Stromversorgungen (USV) kompensieren zu können.

Natürlich darf man bei all diesen grundsätzlichen Überlegungen das Augenmaß nicht verlieren und muss an die Finanzierung der unweigerlich mit der höheren Sicherheit verbundenen Zusatzkosten und auch an die personellen Zusatzaufwendungen denken. Wenn man Sicherheit der Datenverarbeitung aber ernst nimmt (Verfügbarkeit ist ein wichtiges Sicherheitskriterium), dann darf die Sicherheit nicht immer aufgrund von Finanzierungsfragen hinten anstehen. Insofern ist es erfreulich, dass die IV-Kommission der WWU empfohlen hat, der G-WiN-Redundanz Vorrang vor bestimmten Einsparungsmöglichkeiten zu geben.

Unsere Antwort: *perMail*

R. Perske

Als neuer Service des ZIV können E-Mails jetzt auch über das WWW bearbeitet werden.

Seit vielen Jahren bieten wir zwei grundsätzliche Wege an, auf eingegangene und im eigenen Postfach abgelegte E-Mails zuzugreifen.

Dialogserver – nicht immer bequem, aber schnell und mächtig

Der ältere Weg ist der direkte Zugriff auf das Postfach von verschiedenen Dialogservern aus, hier ist insbesondere das auf dem Dialogserver `asterix.uni-muenster.de` laufende E-Mail-Programm *Pine* zu nennen. Jeder Nutzer kann von überall aus der Welt ein `slogin`- oder `telnet`-Programm starten, sich mit dem angegebenen Server verbinden und nach erfolgreicher Anmeldung dieses Programm aufrufen. Aber auch andere E-Mail-Programme und andere Dialogserver im Zentrum für Informationsverarbeitung und in verschiedenen Fachbereichen nutzen diesen Weg.

Trotz der umfangreichen Möglichkeiten und der hohen Geschwindigkeit, die dieser Weg bietet, sind gerade Einsteiger von ihm nicht besonders begeistert. Die Bedienung ohne Maus und grafische Unterstützung ist für Windows-gewohnte Nutzer gewöhnungsbedürftig und erfordert eine Bereitschaft zur Einarbeitung, die häufig nicht mehr gegeben ist.

POP3 – komfortabler, aber doch sehr beschränkt

Etwas neuer, aber auch seit Jahren bewährt, sind unsere POP3-Server, auf die geeignete E-Mail-Programme von überall aus dem Internet mit Hilfe des *Post Office Protocol version 3* zugreifen können. Praktisch jeder unserer Nutzer, der mit *Netscape Communicator, Microsoft Outlook Express, Eudora, Pegasus Mail* usw. seine E-Mail liest, nutzt diesen Weg.

Jedoch bietet das POP3-System nur recht eingeschränkte Möglichkeiten: Es ermöglicht nur, E-Mails aus dem Briefkasten auf den eigenen Rechner zu kopieren und E-Mails aus dem Briefkasten zu löschen. Viele E-Mail-Programme bieten sogar nicht einmal die Möglichkeit, diese beiden Funktionen getrennt zu nutzen. Auch die Erkennung, welche E-Mails neu sind, gerät durcheinander, sobald man auf verschiedenen Wegen auf den Briefkasten zugreift. Häufig vermisst wird auch die Möglichkeit, erst einmal anhand von Absender-, Betreff- oder Größenangaben auszuwählen, welche E-Mails man über die häufig langsame Modem-Leitung herunterladen will.

Vor allem diejenigen Nutzer, die von verschiedenen Rechnern aus oder gar mit Pool-Rechnern ihre E-Mails bearbeiten möchten, stehen vor zwei großen Problemen:

- E-Mails, die man von einem Rechner aus abgerufen hat, sind von anderen Rechnern aus nicht mehr zugreifbar.
- E-Mails, die man von einem Pool-Rechner aus abgerufen hat, liegen, falls der Pool-Betreuer nicht aufwändige Vorkehrungen getroffen hat, anschließend auf der Festplatte herum und können von jedem nachfolgenden Nutzer dieses Rechners gelesen werden. **PC**-Programme sind halt für **P**ersönliche **C**omputer und nicht für Pool-Rechner gedacht.

Man kann sich zwar bemühen, vor dem Verlassen eines Rechners immer sorgfältig aufzuräumen, und auch mit der von einigen E-Mail-Programmen angebotenen Option, E-Mails nach dem Abruf auf dem Server zu belassen, etwas herumtricksen, doch handelt man sich gerade damit sehr schnell andere Probleme ein.

Außerdem ist es mit dem POP3-System überhaupt nicht möglich, E-Mails in zentral

gespeicherten Ordnern zu verwalten, auf die von überall her zugegriffen werden kann.

Von vielen Nutzern gewünscht wird also ein System, welches sowohl den Komfort heutiger Maus-orientierter E-Mail-Programme bietet als auch die Möglichkeiten, von überall aus seine E-Mails zu bearbeiten und in zentral gelagerten Ordnern zu verwalten.

IMAP – viel versprechend, aber böse überraschend

Alle diese Wünsche und etliche weitere zu erfüllen verspricht IMAP, das *Internet Mail Access Protocol*. IMAP-fähige E-Mail-Programme sollen mit Hilfe von IMAP-Servern auf zentrale Briefkästen und Ordner zugreifen und so mit der gewohnten Oberfläche alle Möglichkeiten bieten, ohne den Einschränkungen des POP-Systems unterworfen zu sein.

Wir hatten solche Server für längere Zeit im Testbetrieb. Leider mussten wir feststellen, dass etliche E-Mail-Programme, insbesondere einige Versionen des *Netscape Communicators*, den IMAP-Server auf eine derart unmögliche Art und Weise benutzen, dass schon wenige Nutzer selbst leistungsstärkste IMAP-Server regelmäßig überlasten. Um Ihnen einen stabilen Betrieb auf IMAP-Basis anbieten zu können, hätten wir also bei täglich über zehntausend Nutzern eine untragbare Anzahl von IMAP-Servern kaufen und einrichten müssen.

In Anbetracht dieser Umstände haben wir uns dann dafür entschieden, den Gedanken, IMAP-Server anzubieten, zu verwerfen und einen ganz anderen Ansatz zu verfolgen.

WWW – die Eier legende Wollmilchsau

Wie schon viele kommerzielle Internet Service Provider haben auch wir uns entschlossen, das erst zehn Jahre junge World Wide Web als Transportmedium zum Abrufen und Bearbeiten von E-Mails anzubieten.

Das daraufhin in den letzten Monaten entwickelte *perMail* steht ab sofort allen unseren Nutzern zur Verfügung. Sie finden die Login-Seite von *perMail* unter folgender WWW-Adresse:

```
http://permail.uni-muenster.de
```

perMail steht sowohl über diesen ungeschützten als auch über einen abhörsicheren Zugang zur Verfügung. Wenn Sie den abhörsicheren Zugang benutzen, kann anders als bei POP3, IMAP, Telnet oder dem ungeschützten Zugang niemand Ihr Passwort oder Ihre E-Mails mitlesen. Daher bietet die Login-Seite von *perMail*, wenn Sie obige ungeschützte Adresse verwenden, Ihnen eine Schritt-für-Schritt-Anleitung zum Installieren der notwendigen CA-Zertifikate und zum Umschalten auf den abhörsicheren WWW-Zugang. Die dabei zu kontrollierenden Fingerprints finden Sie in jedem infoWWW.

Allerdings benötigen Sie für den abhörsicheren Zugang ein WWW-Programm, welches starke Verschlüsselung beherrscht. Dies trifft zu für alle Versionen von *Opera*, für den *Netscape Communicator* ab Version 4.74 (oder eine mit *Fortify* aufgerüstete Version), für den *Internet Explorer* ab Version 5.5 (oder eine mit dem *Internet Explorer High Encryption Pack* aufgerüstete Version), für den *Konquerer* und für jedes andere auf OpenSSL-Basis arbeitende WWW-Programm.

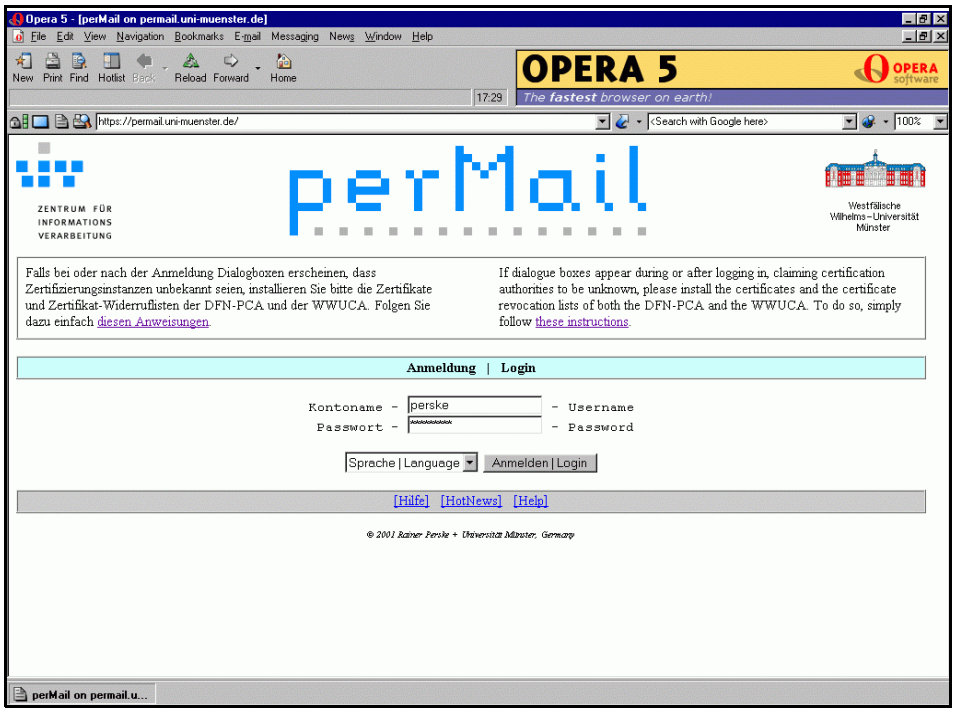
Wenn Sie ein solches Programm benutzen, sollten Sie jetzt den angegebenen Schritten folgen. Das müssen Sie nur dieses eine Mal machen, später können Sie dann direkt die WWW-Adresse für den abhörsicheren Zugang verwenden:

```
https://permail.uni-muenster.de
```

perMail in der Praxis

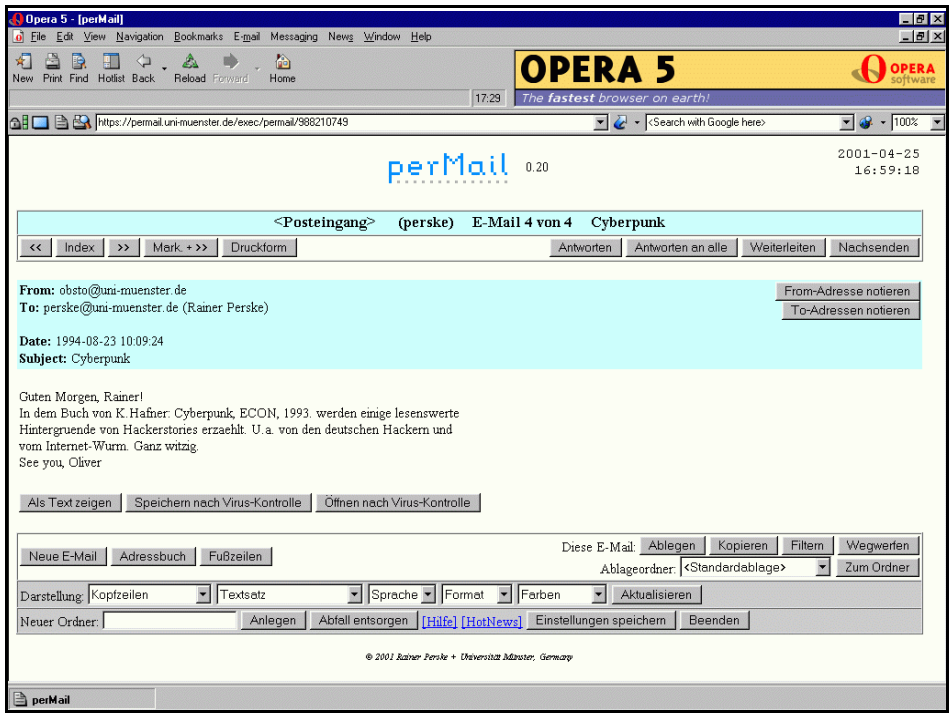
Beim ersten Anmelden präsentiert *perMail* sich im Startformat, hier stehen Ihnen nur die notwendigsten Funktionen zur Verfügung, um Einsteiger durch die Vielfalt der Möglichkeiten nicht zu sehr zu verwirren. Sobald Sie die ersten Schritte hinter sich gebracht haben, sollten Sie auf das in den nachfolgenden Abbildungen gezeigte Textformat umschalten. Mit wachsender Erfahrung werden Sie dann in das Symbolformat umschalten, denn bei identischer Bedienung ermöglichen die platzsparenden Symbolschaltflächen einen aufgeräumteren Bildschirmaufbau. Erfahrene E-Mail-Nutzer werden die weiteren Modi bevorzugen, die weiter reichende Funktionen und einige Abkürzungen zur Verfügung stellen.

Unabhängig vom Anzeigeformat setzt sich die Oberfläche von perMail aus einem Satz von WWW-Seiten zusammen, auf denen Sie alle grundlegenden Funktionen von E-Mail-Programmen wieder finden:

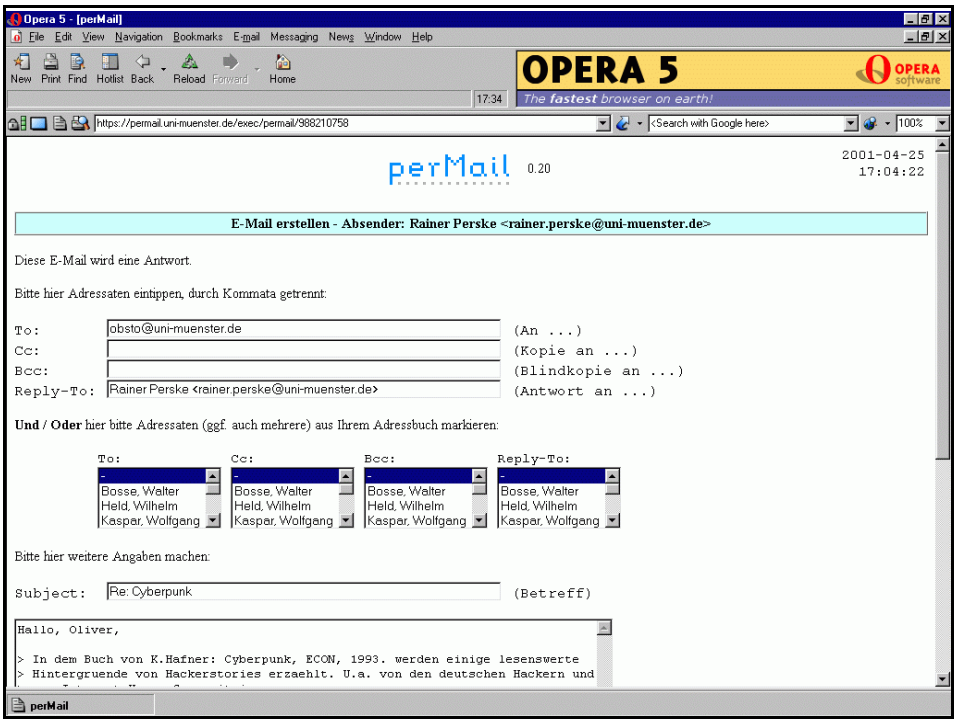


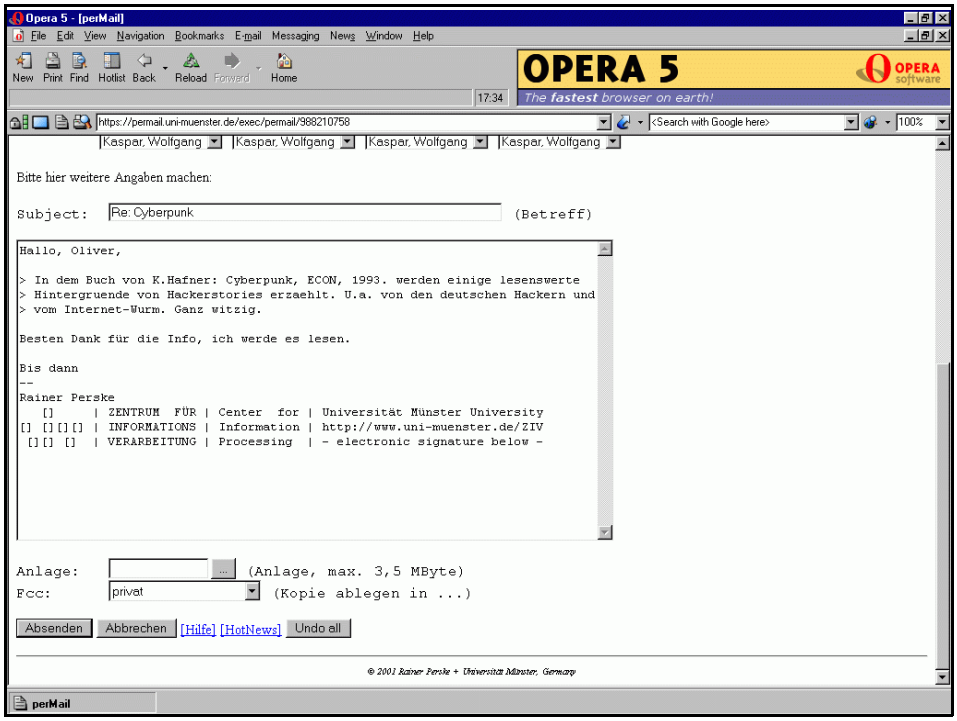
Wenn Sie auf der Login-Seite (egal ob abhörsicher oder ungeschützt) Ihre Nutzerkennung und Ihr Passwort in die entsprechenden Felder eintragen und dann die Schaltfläche „Anmelden | Login“ bedienen, werden Sie mit einem der aktuell laufenden *perMail*-Server verbunden. (Da jeder dieser Server sein eigenes Zertifikat besitzt, sollten Sie vor der Nutzung des abhörsicheren Zugangs wirklich die oben genannten CA-Zertifikate einbauen, um die sonst sehr lästigen Dialogboxen Ihres WWW-Programms für jeden neuen Server zu vermeiden.) Sie können hier auch vorab die Sprache der nachfolgenden Seiten auswählen. Wenn Sie keine Auswahl treffen, wird eine eventuell früher abgespeicherte Einstellung oder sonst Deutsch verwendet.

Die nachfolgend dargestellte Index-Seite zeigt Ihnen eine Liste der vorhandenen E-Mails im aktuell eingestellten Ordner, anfangs ist dies der Posteingang. Schaltflächen zum Blättern befinden sich links oberhalb und unterhalb der laufenden Nummern. Mit den Schaltflächen in der Aktionsspalte können Sie die jeweilige E-Mail anzeigen und bearbeiten. Unmittelbar unter der Liste finden Sie die Schaltflächen zum Erstellen neuer E-Mails und zum Bearbeiten von Fußzeilen und Adressbucheinträgen. Einstellungen über das Aussehen der Seite können Sie am unteren Tabellenrand vornehmen.



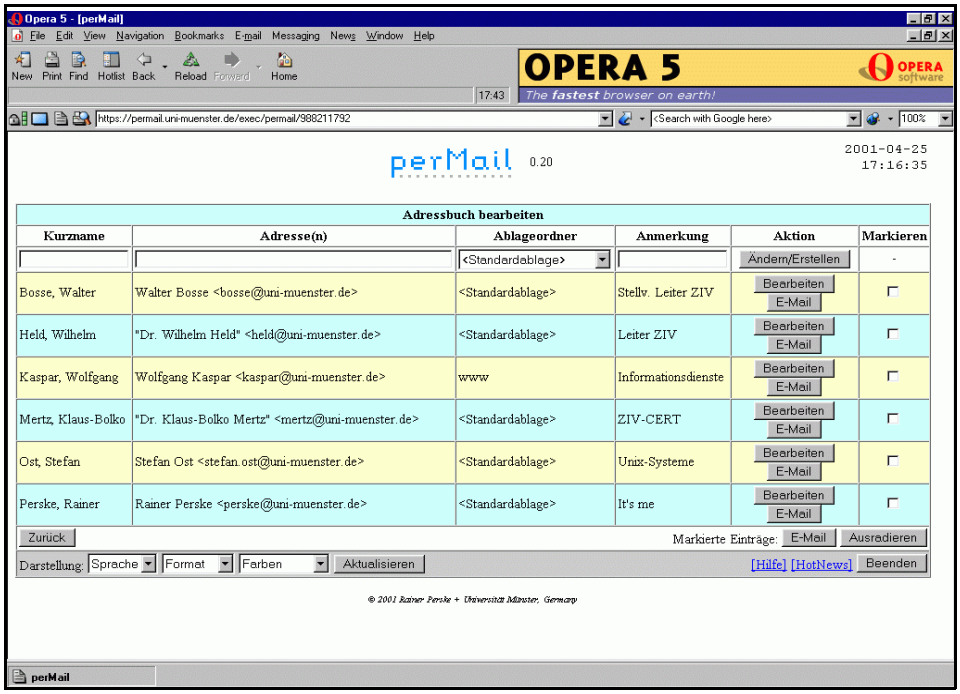
Die Ansicht-Seite zeigt Ihnen eine einzelne E-Mail mit eventuell vorhandenen Anlagen. Alle Teile einer E-Mail können als Text angezeigt, heruntergeladen oder auch direkt mit dem entsprechenden Anwendungsprogramm auf Ihrem Rechner geöffnet werden. Vor dem Herunterladen oder Öffnen werden die entsprechenden Teile auf bekannte Viren und Schadfunktionen untersucht. Natürlich finden Sie hier auch Schaltflächen zum Weiterblättern, Antworten, Ablegen, Wegwerfen usw.



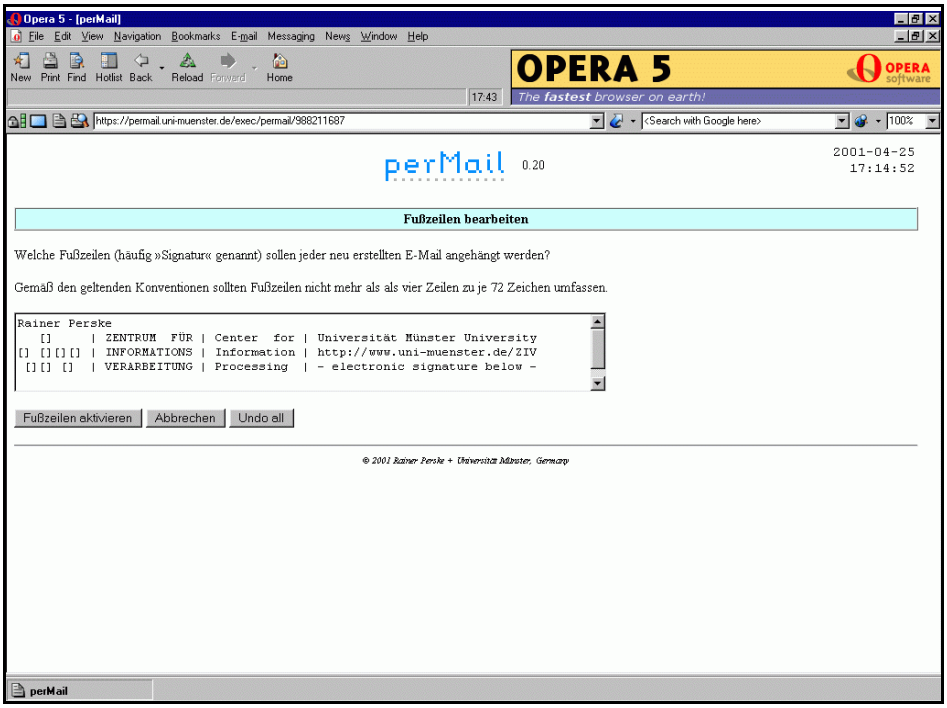


Die Neue-E-Mail-Seite erscheint, wenn Sie E-Mails erstellen, beantworten, weiterleiten oder nachsenden. Beim Eintippen mehrerer Adressaten müssen Sie darauf achten, zwischen den Adressaten ein Komma einzufügen. Falls vorhanden, können Sie Adressaten auch aus einem Adressbuch auswählen.

Welche Bearbeitungsmöglichkeiten Ihnen das Texteingabefenster bietet, hängt ganz alleine vom WWW-Programm ab. In aller Regel werden diese nicht besonders umfangreich sein, darauf hat *perMail* jedoch keinen Einfluss.



Die Adressbuch-Seite benutzen Sie zum Verwalten Ihrer Adressbucheinträge, welche durch Kurznamen identifiziert werden. Ein Adressbucheintrag kann durchaus mehrere E-Mail-Adressen enthalten. Von dieser Seite aus können Sie unmittelbar mit dem Erstellen einer neuen E-Mail an die Adressen eines Eintrags beginnen.



Die Fußzeilen-Seite ermöglicht Ihnen das Verändern Ihrer Fußzeilen (Signatur). Diese werden bei jeder neuen E-Mail automatisch in das Texteingabefeld eingefügt.

Eine Filterregeln-Seite zum Bearbeiten der Regeln, nach denen der Inhalt eines Ordners automatisch in andere Ordner wegsortiert wird, ist für die Zukunft geplant.

Auf der hier nicht dargestellten PGP-Schlüssel-Seite können Sie einstellen, welchen Schlüsselinhabern Sie vertrauen, falls Sie die PGP-Installation auf `asterix` benutzen.

Zu jeder Seite gibt es eine Hilfe-Seite, auf der alle Möglichkeiten, die Ihnen zur Verfügung stehen, aufgeführt und erklärt werden.

Auf fast allen Seiten finden Sie unten rechts eine Schaltfläche „Beenden“. Bitte benutzen Sie diese Schaltfläche, bevor Sie Ihren Rechner verlassen. Dies gilt insbesondere, wenn Sie Pool-Rechner oder Internet-Cafés benutzen. Die Schaltfläche markiert auf dem WWW-Server das in den WWW-Seiten versteckt enthaltene Ticket als ungültig. Wenn Sie dies nicht tun, kann es nachfolgenden Nutzern Ihres Rechners noch einige Stunden lang möglich sein, auf Ihre E-Mails zuzugreifen.

Eigenschaften von *perMail*

Zum Ausprobieren einladen möchte ich Sie mit der Aufzählung einiger Eigenschaften von *perMail* und mit einigen Tipps zum geschickten Umgang mit diesem System.

Systemvoraussetzungen

- Sie können ein beliebiges WWW-Programm benutzen, ohne dass Sie irgendwelche Einstellungen an Ihrem Rechner vornehmen müssen. (Zwar muss das Programm das Hochladen von Dateien beherrschen, doch das ist bei allen neueren Programmen der Fall.) Sogar tabellenfähige Nur-Text-Programme wie `w3m` lassen sich problemlos verwenden.
- *perMail* kann über jeden vollwertigen Internet Service Provider und natürlich mit Pool-Rechnern ohne jede Einschränkung benutzt werden.
- Da *perMail* die Passwortverwaltung der zentralen Systeme des Zentrums für Informationsverarbeitung benutzt, sind keine spezielle Anmeldung und kein neues Passwort erforderlich.

Darstellung

- Bei *perMail* können Sie zwischen unterschiedlichen Anzeigeformaten wählen, passend für Einsteiger, erfahrenere Nutzer und Experten. Jedes dieser Formate können Sie durch Wahl einer Farbkombination und weitere Layouteinstellungen Ihrem persönlichen Geschmack anpassen.
- Keinerlei Vorschriften macht Ihnen *perMail* bei der Auswahl von Schriftart und Schriftgröße, es verwendet einfach die Schriften, die Sie in Ihrem WWW-Programm eingestellt haben.
- Sie können sich Ihre E-Mails in einer einstellbaren Reihenfolge anzeigen lassen. *perMail* vermag sogar, Antworten und Weiterleitungen anhand der Betreffzeilen den entsprechenden Ursprungs-E-Mails zuzuordnen.
- Die von Ihnen vorgenommenen Einstellungen können Sie fast jederzeit abspeichern. Beim nächsten Anmelden finden Sie dann gleich Ihre gewohnte Umgebung vor.

Hilfen

- Eine umfangreiche Online-Hilfe in der jeweils eingestellten Sprache erklärt Ihnen die Benutzung der verschiedenen Schaltflächen. (Die englischen Hilfetexte sind zzt. noch nicht ganz fertig gestellt.)

- Sofern Ihr WWW-Programm dies unterstützt, wird Ihnen die Bedeutung einer Schaltfläche angezeigt, sobald Sie den Mauszeiger auf diese Schaltfläche bewegen. (Der von einigen Programmen zusätzlich angezeigte Zeichensalat enthält Kenndaten der jeweiligen E-Mail und lässt sich leider nicht unterdrücken.)
- *perMail* integriert auf unaufdringliche Weise die HotNews des Zentrums für Informationsverarbeitung, das sind wichtige betriebliche Hinweise über Störungen, geplante Ausfallzeiten usw.

E-Mail-Ordner

- *perMail* verwaltet alle Ordner auf dem zentralen Server und verwendet die gleichen Briefkasten- und Ordnerdateien wie das Programm *Pine*, kann dieses also in den meisten Fällen ersetzen.
- Selbstverständlich können Sie neue Ordner erstellen und leere Ordner löschen.
- *perMail* bietet die Möglichkeit, Ordner in Verzeichnissen zusammenzufassen.
- *perMail* beachtet *Symbolic Links*, die Sie vielleicht von Hand eingerichtet haben, um an anderen Stellen gelegene Ordner und Ordnerverzeichnisse einzubinden.
- Weggeworfene E-Mails werden in einer Abfalltonne gesammelt, aus der sie wieder hervorgeholt werden können. Erst wenn sie von dort einzeln oder zusammen in den Reißwolf gesteckt werden, sind sie wirklich weg.
- Wie auch bei der Verwendung von *Pine* gilt: E-Mails, die im Posteingang belassen werden, können weiterhin über die POP3-Server abgerufen werden; *perMail* kann also auch zum Vorsortieren bzw. Vorfiltern für andere E-Mail-Programme verwendet werden.

Adressbuch und Fußzeilen

- *perMail* enthält ein eigenes Adressbuch. Adressbücher des Programms Pine können übernommen werden, indem auf `asterix` der Befehl `pine2permail` eingetippt wird.
- *perMail* erlaubt Ihnen, Adressen aus angezeigten E-Mails direkt in das Adressbuch zu übernehmen.
- In einem entsprechenden Fenster können Sie die Fußzeilen bearbeiten, die jeder neuen E-Mail hinter der von der Netiquette angeratenen Trennmarkierung (*Sig-dashes*) angehängt werden. Sie können die Fußzeilen jeder einzelnen E-Mail vor dem Absenden noch bearbeiten. (Verwechseln Sie diese Fußzeilen bitte nicht mit elektronischen Unterschriften, auch wenn beide als *Signatur* bezeichnet werden.)
- *perMail* entfernt beim Antworten automatisch die Fußzeilen des Absenders und hilft auch an anderen Stellen beim Einhalten der Netiquette. (Selbstverständlich müssen Sie weiter selbst darauf achten, vor dem Absenden einer Antwort auch alle anderen irrelevanten Zitatzeilen zu löschen und Ihre Antworten *unter* statt über der Frage einzufügen.)

Anlagen (Attachments)

- *perMail* beherrscht den Umgang mit E-Mails im MIME-Format (*Multimedia Internet Mail Enhancement*), das heißt mit E-Mails mit kompliziert verschachtelten Anlagen. (Falls Sie nacheinander mehrere Anlagen einer E-Mail abrufen, kann es bei etlichen WWW-Programmen erforderlich sein, den Aktualisieren-Knopf

(*Reload*) zu benutzen, um die richtige Anzeige hervorzubringen.[1])

- Sie haben die Möglichkeit, als Anlagen beigefügte E-Mails herauszulösen und als eigenständige E-Mails in Ordnern abzulegen.
- Sie können jeder neuen E-Mail eine Datei direkt von Ihrem Rechner anhängen. (Um mehrere Dateien zu versenden, benutzen Sie bitte getrennte E-Mails oder fassen Sie sie vorher mit einem ZIP-Programm zu einer komprimierten Archivdatei zusammen; dann haben Sie auch weniger Schwierigkeiten mit den Größenbeschränkungen der E-Mail-Server.)
- *perMail* achtet bereits beim Anhängen der Datei auf die von unseren SMTP-Servern zugelassene Maximalgröße. (Für später ist eine Integration des Bigmail-Mechanismus für übergroße E-Mails geplant, vgl. `http://user.uni-muenster.de/exec/bigmail`.)

Besondere Fähigkeiten

- *perMail* vermag die E-Mails eines Ordners nach von Ihnen vorgegebenen Regeln in verschiedene Ordner wegzusortieren. (Allerdings müssen Sie diese Filter-Regeln wie in der Online-Hilfe beschrieben noch manuell erstellen.)
- *perMail* verwendet für die eigene E-Mail-Adresse den aktuell eingestellten Aliasnamen, und erkennt in der Liste der E-Mails eines Ordners, welche man selbst geschrieben hat.
- Sie können E-Mails nicht nur weiterleiten (mit neuem Absender), sondern auch nachsenden (*Bounce/Resend*, mit Original-Absender).
- *perMail* beherrscht das gemeinsame Weiterleiten mehrerer E-Mails.
- Beim Antworten auf E-Mails können Sie wählen, ob Sie nur an den Absender oder an alle Adressaten einer E-Mail antworten möchten und ob dabei die Kopfzeilen mitzitiert werden oder nicht.
- Mit Hilfe einer Vorschau können Sie kontrollieren, wie eine neu erstellte E-Mail aussähe, wenn Sie sie jetzt absenden würden. (Nach Benutzen der Vorschau müssen Anlagen und PGP-Einstellungen jedoch erneut angegeben werden.)

Sicherheitsmaßnahmen

- *perMail* kontrolliert E-Mail-Inhalte beim Öffnen mit einem meist mehrmals wöchentlich aktualisierten Virenschutzprogramm. (Das heißt natürlich nicht, dass Sie eigene Vorsichtsmaßnahmen außer Acht lassen dürfen!)
- Sie können sich alle Inhalte erst einmal als unschädlichen reinen Text anzeigen lassen. Selbst den Text vieler Microsoft-Word-DOC-Dateien kann man so vor dem Herunterladen bereits erkennen.
- *perMail* wurde so entwickelt, dass Angreifern möglichst wenig Angriffspunkte geboten werden, und benötigt weder Frames noch Cookies noch JavaScript noch Java noch ActiveX, auch werden keine sensitiven Informationen in der URL aufbewahrt. Sie können Ihr WWW-Programm also in der höchsten Sicherheitsstufe betreiben.

---

[1] In manchen Fällen hilft es, wenn Sie in Ihrem WWW-Programm einstellen, dass *jedesmal* beim Server nachgefragt wird, ob eine Seite neu geladen werden soll, und nicht nur *einmal pro Sitzung*. Leider verhalten sich einige WWW-Programme besonders bei Bilddateien derart fehlerhaft, dass *perMail* selbst dann keine Chance mehr hat, das Problem vor Ihnen zu verbergen. Die fortlaufende Zahl in der URL hat keinen anderen Zweck, als diesen Fehler soweit wie möglich zu umgehen.

- *perMail* arbeitet intern mit einem hochsicher verschlüsselten Sitzungs-Ticket beschränkter Lebensdauer. Selbst wenn Sie den Rechner verlassen, ohne die Sitzung zu beenden, verliert das Ticket nach einigen Stunden seine Gültigkeit.

Verschlüsselung und elektronische Unterschriften

- *perMail* arbeitet gut mit *Pretty Good Privacy (PGP)* zusammen, einem Programm zum Verschlüsseln und zum elektronischen Unterschreiben, und zwar sowohl (über Schaltflächen) mit dem auch von *Pine* verwendeten PGP auf dem Dialogserver `asterix` als auch (über HotKeys) mit einer PGP-Installation auf Ihrem eigenen Windows-PC. (Für Windows-Nutzer empfehlen wir PGP 6.5.8 mit RSA-Schlüsseln.)
- *perMail* erlaubt Ihnen, per E-Mail empfangene PGP-Schlüssel Ihrem PGP-Schlüsselring auf `asterix` hinzuzufügen, und bietet eine weitreichende (jedoch noch nicht vollständige) eingebaute Schlüsselverwaltung, mit der Sie viel bequemer als mit PGP selbst Vertrauensparameter einstellen und Schlüssel aktivieren und deaktivieren können.

Störfestigkeit

- *perMail* erkennt und umgeht einige Programmierfehler in den WWW-Programmen von Microsoft, Netscape und Opera Software.
- *perMail* kommt auch mit etlichen defekten Ordnerdateien zurecht und repariert diese auf Anforderung oder spätestens sobald der Ordner das erste Mal neu geschrieben wird.
- Da die E-Mails eines Ordners nicht an der Reihenfolge im Ordner, sondern an internen Kenndaten und Quersummen identifiziert werden, kann *perMail* problemlos gleichzeitig mit anderen E-Mail-Programmen eingesetzt werden. (Sie sollten dies aber trotzdem nicht probieren, denn andere Programme wie *Pine*, *Netscape Messenger* oder *Outlook Express* sind nicht so robust.)
- *perMail* verwendet größte Sorgfalt (noch mehr als *Pine*) darauf, dass keine Ordner durch Erreichen der Plattenplatzquote oder andere Probleme beschädigt werden. (Dies erfordert jedoch einen höheren Plattenplatzbedarf, denn E-Mails können aus einem Ordner nur dann entfernt werden, wenn kurzzeitig sowohl der alte Zustand als auch der neue Zustand des Ordners gleichzeitig auf der Platte Platz finden.)
- Der Autor von *perMail* ist Mitarbeiter des Zentrums für Informationsverarbeitung. Eventuell auftretende Probleme können daher in aller Regel zügig beseitigt werden.

Geschwindigkeit

- Da das Programm *perMail* in C geschrieben wurde und unmittelbar auf die Briefkasten- und Ordnerdateien zugreift, ist es erheblich schneller als die meisten anderen WWW-Mail-Programme. (Da es bei jedem Mausklick den aktuellen Ordner neu lesen muss, kann es natürlich nicht die Geschwindigkeit von *Pine* erreichen.)
- Sie können E-Mails eines Ordners markieren und später gesammelt wegwerfen oder ablegen. Diese Markierungen werden nicht abgespeichert, sondern in den WWW-Seiten versteckt aufbewahrt; daher können Sie in verschiedenen Fenstern verschiedene E-Mails markieren und durch geschickte Bedienung die Antwortzeit weiter verbessern.

- *perMail* kann auf beliebig vielen Servern gleichzeitig laufen und sorgt selbständig für eine Lastverteilung, indem Sie bei der Anmeldung auf einen zufällig ausgewählten Server weitergeschaltet werden, wobei ausgefallene Server (anders als bei POP3) übersprungen werden.
- Zeit fressende Veränderungen an den Ordnerdateien werden vermieden, wo immer dies möglich ist. (Das heißt allerdings, dass keine Markierung in die Ordnerdatei geschrieben wird, ob eine E-Mail gelesen oder beantwortet wurde. Vorhandene Gelesen- und Beantwortet-Markierungen anderer E-Mail-Programme bleiben unverändert.)

Ecken und Kanten, Tipps und Tricks

Ganz ohne Kanten ist *perMail* natürlich nicht. Die beschränkten Möglichkeiten der WWW-Oberfläche und die getroffenen Sicherheitsmaßnahmen erzwingen kleine Unbequemlichkeiten. (Einige wurden oben bereits in Klammern erwähnt.)

Beispielsweise ist es beim Anzeigen von Anlagen nicht möglich, diese automatisch in einem eigenen Fenster darzustellen. Sie werden also bisweilen den Zurück-Knopf Ihres WWW-Programms benutzen müssen, um zur normalen Anzeige von *perMail* zurückzukehren.

Mit etlichen WWW-Programmen können Sie gerade hier aber einen netten Trick verwenden, den ich Ihnen auch für andere WWW-Seiten nur ans Herz legen kann: Wenn Sie nicht mit der linken, sondern mit der mittleren Maustaste (ersatzweise mit der rechten Maustaste und dem Punkt „in neuem Fenster öffnen“) auf eine Schaltfläche oder einen Querverweis klicken, wird die nächste Seite in einem neuen Fenster dargestellt. Anschließend können Sie in beiden Fenstern parallel weiterarbeiten und sich auf die gleiche Weise sogar weitere Fenster erzeugen. Sie brauchen bei *perMail* hinterher auch nur in einem der Fenster die Schaltfläche „Beenden“ zu benutzen, um sich abzumelden.

Neue TUSTEP-Version 2001

W. Kaspar

In regelmäßigen Abständen erfahren Sie hier etwas über das „Tübinger System von Textbearbeitungs-Programmen“.

Ab sofort steht bei uns die neue TUSTEP-Version 2001 für die Betriebssysteme Solaris, AIX, Linux und Windows 95/98/ME/NT/2000 zur Verfügung. Die Autoren schreiben hierzu auf Ihren WWW-Seiten (`http://www.uni-tuebingen.de/zdv/tustep/`):

> Die Version 2001 enthält keine „spektakulären“ Neuerungen gegenüber der Vorgängerversion. Der Schwerpunkt der Arbeiten an TUSTEP lag in der Abrundung und Konsolidierung der Neuerungen, die in den letzten beiden Jahren hinzugekommen sind, sowie in der Überarbeitung der Dokumentation.
>
> Zu den wichtigsten Neuerungen in TUSTEP 2001 zählen
>
> - Verbesserungen im Editor und Viewer,
> - Neuregelung der Behandlung von TUSTEP-Steuerzeichen bei der Umwandlung von TUSTEP nach Unicode und umgekehrt,
> - Nutzung der Windows-Zwischenablage in Kommandomakros,
> - Vereinfachung der Decodierung von CGI-Querystrings in Kommandomakros,
> - Einrichten von CGI-Scripts über Standardmakro,
> - Verbesserte Silbentrennung in FORMATIERE und SATZ,
> - Steueranweisung zum Ändern der Standard-Spatienbreite innerhalb eines Abschnitts in SATZ,
> - Möglichkeit zur Ausgabe einer Hintergrundgrafik auf jeder Seite der Satzausgabe.

Außerdem wird mit der Version 2001 von TUSTEP ein Werkzeug mit ausgeliefert, das beim Export von Word-Dateien Formatvorlagen expliziert und wohlgeformte XML-Dateien erzeugt. Dies sollte die Übernahme von Word-Dateien nach TUSTEP wesentlich erleichtern.

Die Unix-Varianten befinden sich wie üblich auf unserem zentralen Server und können von dort direkt aufgerufen werden. Die Windows-Variante ist wie auch die Linux-Variante auf CD erhältlich. Außerdem steht auch noch für MS-DOS die etwas ältere Version 10/95 zur Verfügung.

Die TUSTEP-CD kann direkt über mich (W. Kaspar, ✆ kaspar@uni-muenster.de, ✆ 83-3 16 73) bezogen werden.

IV-Sicherheitslösungen durch Funktionen des Rechnernetzes

C. Ossendorf

Mehr Sicherheit im Rechnernetz ist möglich. Fragen Sie uns!

Im lokalen Datennetz der Universität Münster gibt es heute auf Grund des stark ausgeweiteten Rechnernetzes immer mehr Bereiche mit klarem Sicherheitsbedürfnis für ihre Daten, zum Teil sogar extrem hohem Schutzbedürfnis; andererseits gibt es aber auch „natürlich“ den Zwang zur Öffnung zum Internet. Nur *eine* zentrale Sicherheitsinstanz am Übergang zum Wissenschaftsnetz wäre sicher völlig unzureichend, denn nach verlässlichen Untersuchungen erfolgen ca. 70% aller Angriffe von innen.

Um diesen Ansprüchen und Gefahren gerecht zu werden, bietet das ZIV Möglichkeiten, verteilt im *Transportsystem* Sicherheitsfunktionen auf Anfrage einzurichten. Transportsystem steht hier für das Rechnernetz, welches mittels aktiver Komponenten (Router etc.) so genannte *packet screens* ermöglicht, die im Wesentlichen nicht in das *Anwendungssystem* eingreifen, aber sehr wohl für ein hohes Maß an Sicherheit sorgen können. Ihre Funktionen beschränken sich weitestgehend auf transportspezifische Aspekte („wer zu wem mit welchen Kommunikationsprotokollen“). Sicherheitsfunktionen des Anwendungssystems werden dagegen dort realisiert, wo auch die Anwendungsadministration (für Inhalte, Nutzer, Rechte) geschieht: in den Endgeräten (Server und auch Arbeitsstationen) und zwar auch durch die Anwendungsverantwortlichen (Nutzer, Systemadministratoren) selbst. Das Rechnernetz als Transportmedium beschreibt die Schnittstelle für Sicherheitslösungen, die in sinnvoller Arbeitsteilung zwischen Netzbetreiber/ZIV und Endsystembetreiber installiert werden können. Die Verantwortung für Endgeräte und deren Sicherheit liegt somit weiterhin vor allem dort, wo Sie Ihrer Natur nach vor allem hingehört: bei den Systembetreibern und -anwendern.

Eine Kombination von Sicherheitsfunktionen im Transportsystem und den Anwendungssystemen (bzw. Endgeräten) verspricht Lösungen, die dauerhaft, wirtschaftlich, in wachsenden Netzen skalierbar (da ohne hohe Leistungseinbußen verteilt realisierbar), arbeitsteilig umgesetzt werden können. In enger Zusammenarbeit von Anwendern und ZIV wurden in dieser Art und Weise bereits mehrere Pilotprojekte umgesetzt. Herausragendes Merkmal dieser Projekte war eine auf die Anwender bezogene maßgeschneiderte Lösung. Wie solche Lösungen realisiert werden können, wird in größerer Tiefe unter

```
http://www.uni-muenster.de/ZIV/Rechnernetz/Sicherheit/Daten/
     Sicherheitslösungen_I.html
```

auf den WWW-Seiten des ZIV beschrieben.

ZIVprint – der Nachfolger von WWWplot

E. Sturm

War WWWplot dafür gedacht, einzig und allein Bilder auf einen zentralen Drucker zu schicken, so ermöglicht es der Nachfolger *ZIVprint*, beliebige PostScript-Dateien auf allen zentralen Druckern der Universität auszugeben.

Bei Rechnern, die Zugriff auf die Windows-Domäne WWU haben, kann man direkt aus dem Anwendungsprogramm heraus auf einen zentralen Drucker ausgeben. Für alle die, die diese Möglichkeit nicht haben oder die Sonderwünsche äußern wollen, die auf diese Weise nicht erfüllt werden können, ist *ZIVprint* gedacht. Im Prinzip geht es darum, eine auf Ihrem Rechner vorliegende PostScript-Datei zu einem von Ihnen ausgewählten zentralen Drucker zu schicken.

Ausdruck in Datei

Wie kommt man nun als Windows-Benutzer an eine PostScript-Datei? Dazu ist es erforderlich, lokal einen PostScript-Drucker „installiert“ zu haben. Dies heißt nicht, dass bei Ihnen tatsächlich einer angeschlossen sein müsste, sondern nur, dass ein so genannter Druckertreiber für einen PostScript-Drucker in Ihr System integriert sein muss. Welcher Treiber es ist, ist relativ egal – nur PostScript muss es sein. Die verschiedenen Treiber unterscheiden sich vor allem in der Größe des Randes, den sie freihalten. Wir empfehlen aus diesem Grunde den Druckertreiber „Xerox MajestiK Fiery XJ“, den Sie z. B. von `www.xerox.com` (Punkt „Drivers“, dann „Fiery XJ“) herunterladen können.

Zur Erzeugung einer PostScript-Datei brauchen Sie jetzt nur noch in Ihrem Anwendungsprogramm auf „Drucken“ zu klicken, diesen – real nicht existierenden – Drucker auszuwählen, ein Häkchen bei „Ausdruck in Datei“ zu machen und einen Namen für die neue Datei einzugeben.

ZIVprint-Anmeldung

Auf der WWW-Startseite des ZIV findet man einen Punkt „Drucken im ZIV“, der bisher WWWplot aufrief, ab sofort aber das allgemeinere *ZIVprint*. Auf der ersten Seite von *ZIVprint* werden Sie gebeten, Kennung und Passwort einzugeben (siehe Abb. 1). Hier handelt es sich um die üblichen Unix-Dinge, die auch z. B. beim Abholen von E-Mail benötigt werden. Es soll ja kein anderer auf Ihre Kosten (bzw. die Ihres Instituts) Papier, Farbe und Rechenzeit verbrauchen können.

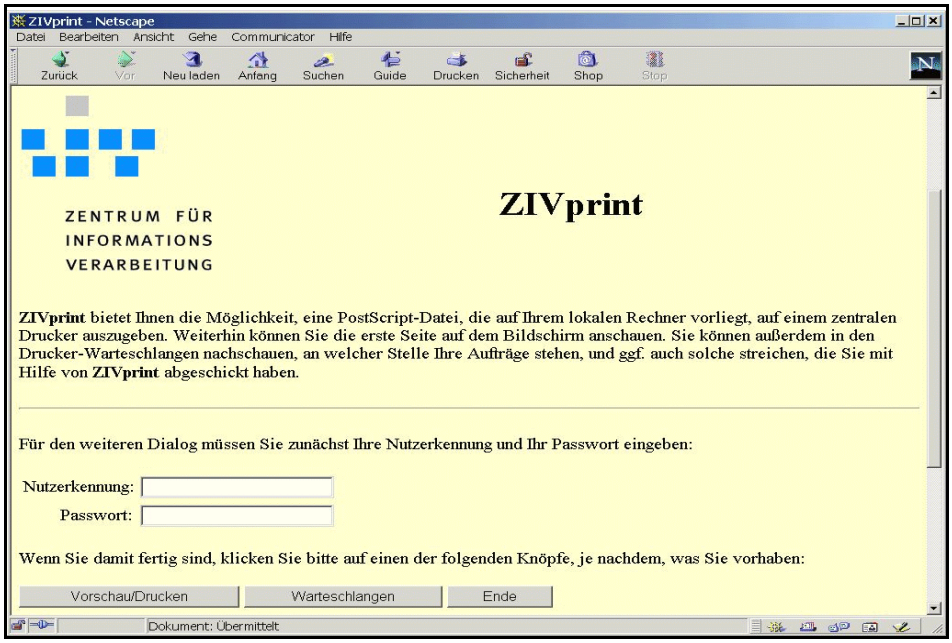


Abb. 1. Eingabe von Kennung und Passwort

Dann entscheiden Sie, ob sie einen Druckauftrag abschicken oder nach dem Stand schon abgeschickter Aufträge sehen wollen. Die Beschriftung „Vorschau/Drucken“ deutet schon an, dass man nicht nur einen Druckauftrag abschicken, sondern auch das Bild bzw. die erste Seite der Datei im Vorhinein anschauen kann.

Vorschau und Druckauftrag

Haben Sie sich für Drucken bzw. Vorschau entschieden, so geben Sie auf der zweiten WWW-Seite (siehe Abb. 2) an, um welche lokal auf Ihrem Rechner vorliegende Datei es sich handelt. Meistens wird es ja die eben erzeugte PostScript-Datei (bei Windows mit der Endung `.prn`) sein.

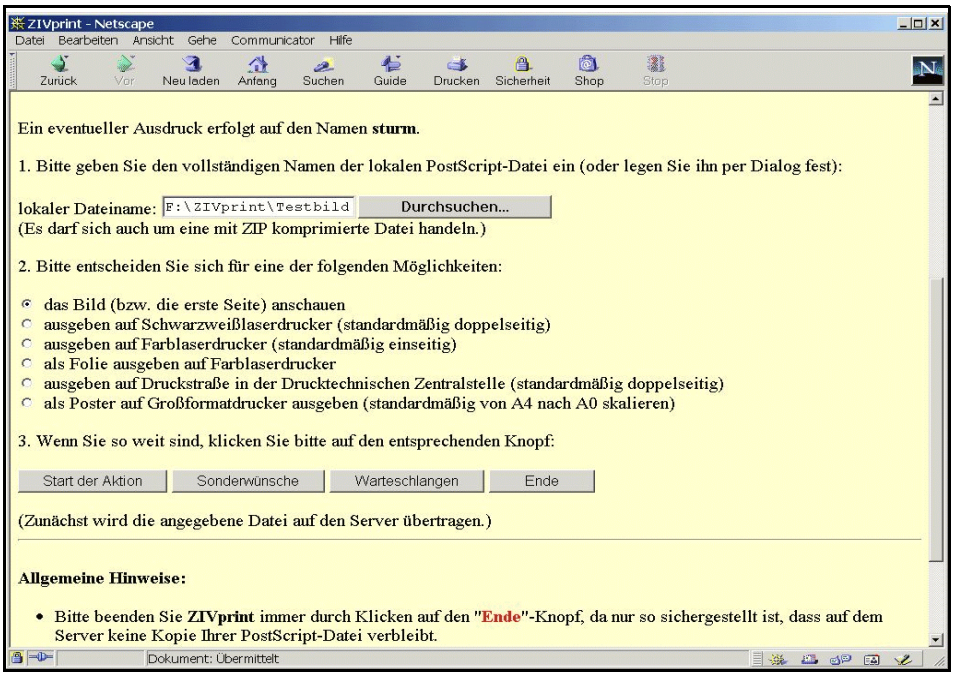


Abb. 2. Eingabe des Dateinamens

Wenn Sie den exakten Pfad der Datei nicht auswendig wissen oder nicht so viel tippen wollen, gibt es einen Weg, der sich je nach Betriebssystem und Browser unterschiedlich darstellt: Drücken Sie den Knopf „Durchsuchen...“ (engl. „Browse...“) rechts neben dem Eingabefeld für den Dateinamen. Daraufhin erscheint der betriebssystemtypische Dateidialog. Leider hat z. B. Netscape voreingestellt, dass nach HTML-Dateien gesucht werden soll. *ZIVprint* verarbeitet aber nur PostScriptDateien. Auch diese werden sichtbar, wenn Sie „Alle Dateien (*.*)“ anklicken. Der schließlich ausgewählte Dateiname erscheint dann im Eingabefeld der *ZIVprint*-Seite.

Besonders für die Benutzung vom heimischen PC aus empfiehlt es sich, eine große PostScript-Datei vorher mit einem Zip-Programm zu komprimieren und den Namen der komprimierten Datei bei *ZIVprint* einzutragen. Dies wird natürlich nach der Übertragung erkannt und per `unzip` rückgängig gemacht.

Nachdem Sie so festgelegt haben, um welche Datei es im Weiteren gehen soll, können Sie sich zwischen folgenden Möglichkeiten entscheiden:

- das Bild (bzw. die erste Seite) anschauen,
- ausgeben auf Schwarzweißlaserdrucker (standardmäßig doppelseitig),
- ausgeben auf Farblaserdrucker (standardmäßig einseitig),

- als Folie ausgeben auf Farblaserdrucker,
- ausgeben auf Druckstraße in der Drucktechnischen Zentralstelle (standardmäßig doppelseitig),
- als Poster auf Großformatdrucker ausgeben (standardmäßig von A4 nach A0 skalieren).

Studenten mit DaWIN-Kennung sehen allerdings nur die folgenden Punkte:

- das Bild (bzw. die erste Seite) anschauen,
- ausgeben auf Endlosdrucker IBM 3835,
- ausgeben auf Schwarzweißlaserdrucker (standardmäßig doppelseitig),

können also insbesondere nicht auf Farbdruckern ausgeben.

Nutzen sollten Sie auf jeden Fall den (voreingestellten) ersten Punkt – Vorschau: Wenn Sie auf „Start der Aktion“ klicken, wird Ihre lokale Bilddatei (bzw. die erste Seite) auf einen zentralen Server übertragen, dieselbe in das GIF-Format übersetzt, zurück übertragen und in Ihrem Browser dargestellt (siehe Abb. 3.). Zzt. sehen Sie bei Bildern, die größer als DIN A4 sind, nur die linke untere Ecke. Sind in der Vorschau Teile der Seite abgeschnitten, so können Sie davon ausgehen, dass dies auch beim Druck der Fall sein wird, Sie also erst einmal dieses Problem lösen sollten.

Wünschen Sie keine Vorschau, so können sie einen Drucker auswählen und dann auf „Start der Aktion“ klicken. In jedem Fall beginnt jetzt die Übertragung der angegebenen Datei, was über eine Modemstrecke entsprechend lange dauert. („In jedem Fall“ heißt, dass, wenn Sie einen Dateinamen eingetragen haben, auch dann die Datei übertragen wird, wenn Sie nur den „Ende“-Knopf angeklickt haben. Das Übertragungsprotokoll HTTP schreibt es so vor.)

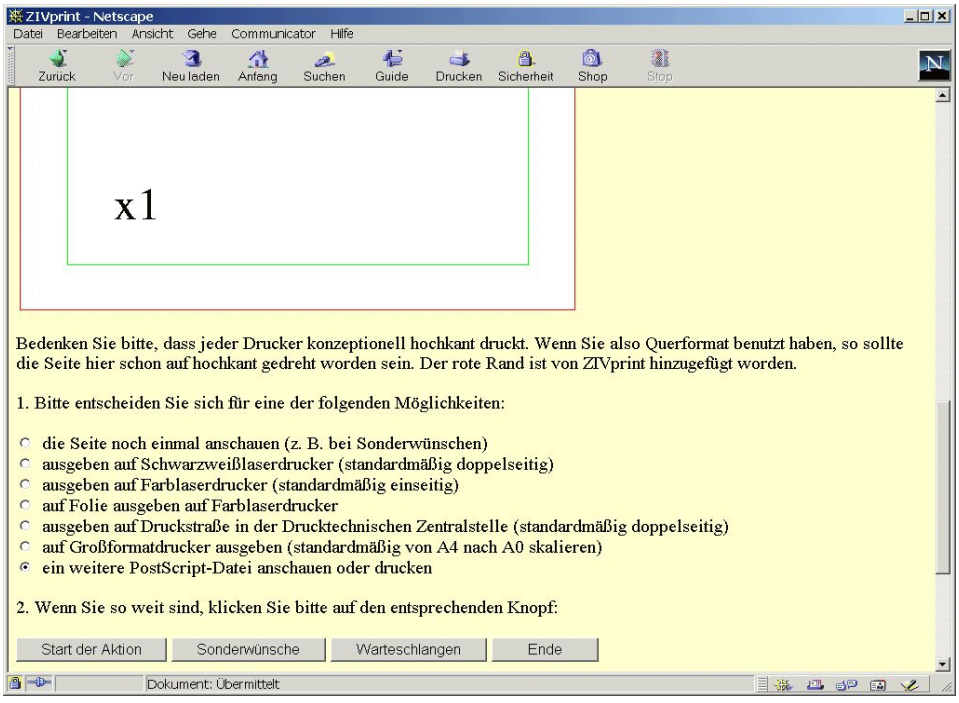


Abb. 3. Vorschau

Sonderwünsche

Sind Sie mit den Voreinstellungen nicht einverstanden, so sollten Sie nicht den Knopf „Start der Aktion“ anklicken, sondern den Knopf „Sonderwünsche“. Die dann angezeigten Sonderwünsche sind vom ausgewählten Drucker abhängig: Je nach Auswahlpunkt können

Sie unterschiedliche Sonderwünsche äußern. Beim Anschauen etwa können Sie verlangen, dass das Bild um 90° gedreht wird. Dies sollte aber nur in Ausnahmefällen notwendig sein. Im Normalfall wird ein Querbild vom Druckertreiber auf hochkant gedreht. Wenn Sie also ein Querbild erstellt haben, so ist alles in Ordnung, wenn Sie es hier als Hochkantbild sehen. Sollte allerdings etwas abgeschnitten sein, so würde ich *ZIVprint* drehen lassen und schauen, wie es dann aussieht. Hilft auch das nicht weiter, so wende man sich bitte an mich (s. u.).

Die Sonderwunschseiten sind im Prinzip selbsterklärend. Ich möchte hier nur noch auf den Großformatdrucker eingehen. Standardmäßig, wenn man also keine Sonderwünsche äußert, wird das Bild von DIN A4 auf DIN A0 vergrößert. Liegt das Bild etwa schon im A0-Format vor oder will man nur ein A1-Bild, so klickt man also nicht auf „Start der Aktion“, sondern auf „Sonderwünsche“. Auf der nächsten Seite sieht man dann Auswahlpunkte für das Originalformat und solche für das Wunschformat und kann dann entsprechend spezifizieren (siehe Abb. 4.).

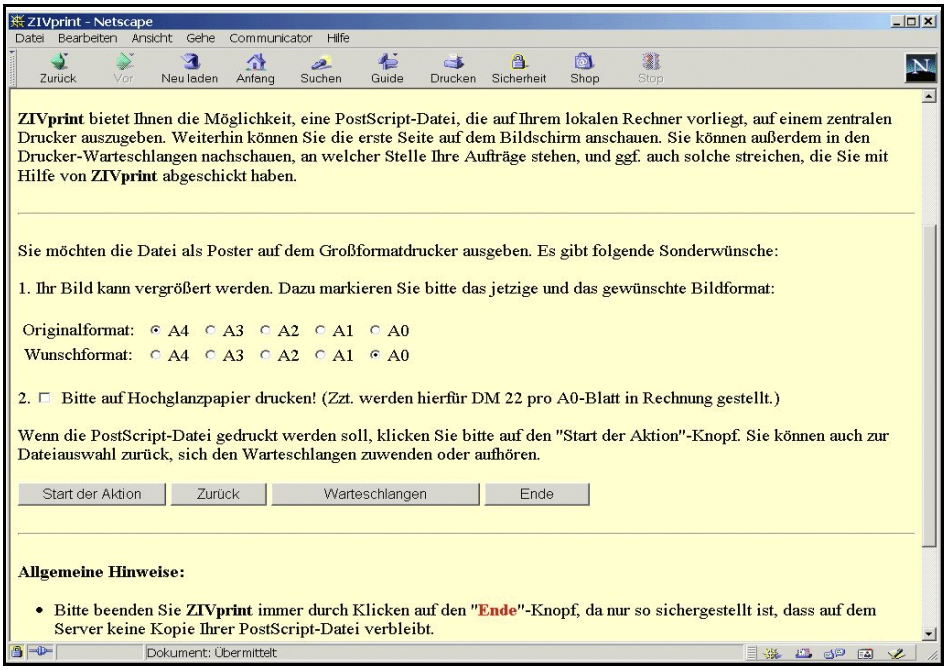


Abb. 4. Sonderwünsche

Hinzugekommen ist jetzt die Möglichkeit auf Hochglanzpapier zu drucken. Die Farben sind UV-resistent, das Papier nicht so feuchtigkeitsempfindlich. Allerdings wird für eine A0-Seite ein Betrag von DM 22,– in Rechnung gestellt. Hochglanzposter sind übrigens nicht zum Laminieren (Einschweißen) geeignet. Wer sich daran stört, dass das Hochglanzbild dunkler als das auf Normalpapier ist, kann den Windows-Druckertreiber HP 2500 CP benutzen und unter „Farbanpassung für Rasterbilder“ den Punkt „Dunkles Bild“ ankreuzen.

Klicken Sie an dieser Stelle auf „Start der Aktion“, so wird die (ja schon auf den Server übertragene) Datei an den Drucker geschickt. Klicken Sie hingegen auf „Zurück“, so wird die schon übertragene Datei auf dem Server gelöscht, man kehrt zur vorigen Seite zurück und kann einen anderen Dateinamen eingeben.

Warteschlangen

Wenn Sie statt auf „Vorschau/Drucken“ auf den Knopf „Warteschlangen“ klicken, wird in allen zentralen Warteschlangen nachgeschaut und es werden die Aufträge aufgelistet, die Sie abgeschickt haben (siehe Abb. 5). Als zusätzliche Angabe findet man die aktuelle Position in der Schlange sowie den Status, damit man absehen kann, wann es sich lohnt,

vor Ort nach dem Druck-Erzeugnis zu schauen.

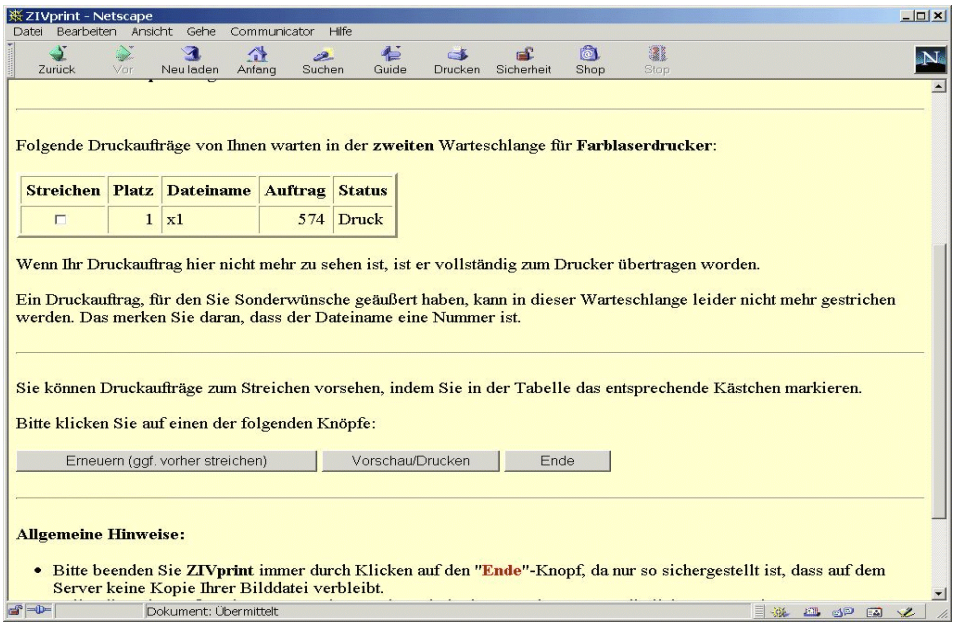


Abb. 5. Warteschlangen

Links von jedem Eintrag findet man ein Kästchen, das man ankreuzen kann. Tut man dieses und drückt dann den Knopf „Erneuern (ggf. vorher streichen)“, so wird der entsprechende Auftrag aus der Warteschlange gestrichen und die Anzeige aktualisiert. Außerdem bekommen Sie dann eine E-Mail, die Ihnen die Streichung bestätigt. Wir wissen noch nicht, ob und wie man Letzteres unterbinden kann.

Leider spiegelt nicht jede Warteschlange die ganze Realität wider. Beim Endlosdrucker und der Druckstraße in der Drucktechnischen Zentralstelle landen die Aufträge in Warteschlangen, die für einen Benutzer nicht einsehbar sind.

Außerdem kommen Druckaufträge an den Farblaserdrucker, für die Sonderwünsche geäußert wurden, zuerst in eine erste Warteschlange, aus der sie in kurzer Zeit in eine zweite übertragen werden. Letztere befindet sich immerhin unmittelbar vor dem eigentlichen Drucker. Leider ändert sich hier der Name in eine Nummer, Löschen ist dann auch nicht mehr möglich.

Ausgabefächer

Ausgaben des Großformatdruckers werden in unregelmäßigen Abständen in die Ständer neben dem Eingang Einsteinstr. 60 gestellt. Die Ausgabe der Hochglanzposter und der Folien erfolgt am Service-Schalter, da in Anbetracht des höheren Preises kein Exemplar verloren gehen sollte. Blätter, die der Schwarzweiß- bzw. der Farblaserdrucker erzeugt hat, findet man in seinem Ausgabefach, zzt. im „Glaskasten“ links, wenn man das oben genannte Gebäude betritt.

Haben Sie vergessen, welches Fach Ihnen zugeordnet wurde, so gibt es folgende Möglichkeiten, es in Erfahrung zu bringen: Zum einen können sie auf `asterix` das folgende Unix-Kommando eingeben:

```
dcecp -c acc show Benutzerkennung
```

natürlich mit der eigenen Benutzerkennung. (Unter Windows müssten Sie also vorher eine `telnet`-Sitzung starten.) Wenn Sie „Hilfe, es tut nicht“ auf der WWW-Startseite des ZIV anklicken, erfahren Sie u. a. auch Ihr Ausgabefach.

ZIVprint-Abmeldung

Theoretisch können Sie bei einem Browser jederzeit Schluss machen oder sich eine andere WWW-Seite anschauen. Bei *ZIVprint* sollten Sie aber bitte immer auf den „Ende“-Knopf klicken, da sonst die Kopien Ihrer Bilddateien auf dem zentralen Server irgendwann für Verstopfung sorgen würden.

Bei Problemen mit *ZIVprint* oder weiteren Wünschen wende man sich bitte an mich (@ sturm@uni-muenster.de, ✆ 31679).

McAfee VirusScan 4.5.1

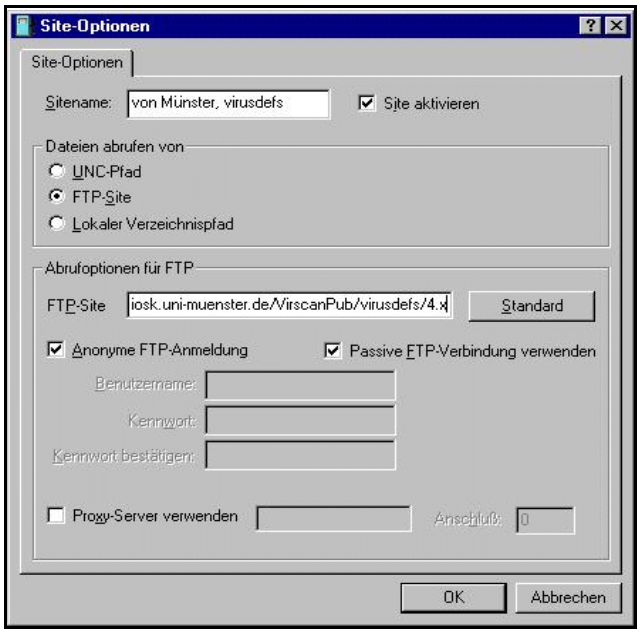
S. Zörkendörfer

Im Rahmen unserer Campuslizenz zum Virenschutz ist die Version 4.5.1 des McAfee VirusScan (Windows-Multiplattform) ausgeliefert. Insbesondere wegen der einfacheren Handhabung zur Aktualisierung empfehlen wir die Nutzung dieser neuen Version.

Zur Nutzungsberechtigung und zum Zugang zu den Installationsmaterialien verweise ich auf den diesbezüglichen Artikel im infoWWW Nr. 1/2000 (auch auf die gleichlautende Web-Seite `http://www.uni-muenster.de/ZIV/inforum/2000-1/a03.html` und auf die Web-Seite `http://www.uni-muenster.de/ZIV/Organisation/Software-VerteilungMcAfeeVirusScan.html`. Diese neue Version ist unter dem Dateinamen `VSC451L.zip` im Unterverzeichnis `VirusScan v4.5 (deutsch)` abgelegt. Unter gleichem Dateinamen finden Sie im Unterverzeichnis `Zuwachs` die englische Version 4.5.1.

Nach meinen Erfahrungen mit diesem Produkt sollte eine Installation problemlos gelingen. Bei der Installation wird ein erkanntes bestehendes Virenschutzprogramm aus dem System entfernt – eine Deinstallation des Vorgängers ist also nicht notwendig.

Wir empfehlen weiterhin, ein (z. B. wöchentliches) *AutoUpdate* zu konfigurieren. Diesbezüglich sind einige Hinweise angebracht. Zunächst ist nun bei diesem *AutoUpdate* die Option „Scan-Modul aktualisieren, falls aktuellere Version verfügbar ist“ möglich und voreingestellt. Damit entfällt die Notwendigkeit zum *AutoUpgrade*. Sodann ist offensichtlich erreicht, dass mit dem AutoUpdate auch eine allerneuste Virendefinition, ein so genanntes `EXTRA.DAT` eingespielt werden kann. Voreingestellt ist, dass nicht alle Dateien, sondern nur *Standarddateien* nach Viren gescannt werden, wobei diese *Standarddateien* durch ihre Erweiterung im Dateinamen (z. B. `.DOC` oder `.VBS`) erkannt werden. Die Liste dieser Dateinamenerweiterungen mag sich ändern und wird von McAfee auch auf dem Weg des *AutoUpdate* gepflegt werden.



Schließlich sei erwähnt, dass in der Regel ein inkrementelles Update angestoßen wird. Für diese Neuerungen wurde notwendig, die Struktur der bereitgestellten Dateien abzuändern und zu erweitern. Derzeit (und hoffentlich auch für lange Zukunft) empfehle ich, diese Dateien aus einem neu

benannten Unterverzeichnis `...\virusdefs\4.x` abzurufen. Wir werden deshalb (voraussichtlich) absichtlich die Verzeichnisse `\DatFiles\4.x` und `\Superdat` nicht an diese neue Struktur anpassen und demnächst nicht mehr bereitstellen. Ferner werden wir voraussichtlich die englische Version dieser Aktualisierungen (und nicht die deutschsprachige Version) einspielen – diese englischen Virusdefinitionen sind durchaus auch für die deutschsprachige Programmversion geeignet. Dabei nehmen wir in Kauf, dass ein *AutoUpdate* der neuen Version 4.5.1 von unserem Verzeichnis `...\DatFiles\4.x` wegen des fehlenden `Update.ini` nicht gelingen kann.

Ich empfehle also (für Rechner mit Netzanbindung) ein wöchentliches *AutoUpdate* zu konfigurieren und dabei an Stelle des voreingestellten Servers der Herstellerfirma NAI ein (passives) anonymes FTP nach `winkiosk.uni-muenster.de/VirscanPub/virusdefs/4.x` einzutragen.

In diesem Zusammenhang gebe ich einen Hinweis für Administratoren, die in Ihrem Bereich die Aktualisierungsdateien spiegeln wollen: Derzeit gelingt mir dies zügig mit (allerdings nur nicht-passivem `ftp`) von `ftpde.nai.com/virusdefs/4.x`.

In der Bibliothek des Zentrums für Informationsverarbeitung ist ein Ordner mit folgenden Handbüchern eingestellt:

- McAfee VirusScan – Antivirensoftware – Erste Schritte (*vsc45srt.pdf*)
- McAfee VirusScan – Antivirensoftware – Benutzerhandbuch (*vsc45ug.pdf*)
- McAfee VirusScan – Administratorenhandbuch (*vsc45ag.pdf*)
- McAfee VirusScan – Release Guide – Version 4.5.1 (*vsc451wrg.pdf*)

Die PDF-Dateien finden angemeldete Nutzer im Verzeichnis `http://winkiosk.uni-muenster.de/VirScan/VirusScan v4.5 (deutsch)`.

Zugang zum Rechnernetz der Universität über das Internet

G Richter

Ohne Probleme über das Internet ins Universitätsnetz?

Globale Erreichbarkeit des Rechnernetzes der WWU

Das Rechnernetz der WWU ist über das Internet und den Internet-Anschluss der WWU (G-WiN) praktisch von jedem Punkt der Welt aus erreichbar. D. h. insbesondere, dass die Endgeräte im WWU-Netz im Grundsatz von beliebigen Ressourcen des Internet aus genutzt bzw. dass Verbindungen jeglicher Art aufgebaut werden können.

Einschränkungen für einzelne IV-Dienste

Natürlich besteht eine Nutzungsmöglichkeit der Ressourcen des Netzes der WWU über das Internet nur in dem Maße, wie dies durch die Betreiber der Endgeräte (Server, Workstations, Drucker etc.) im WWU-Netz für die Nutzung aus dem Internet vorgesehen ist. Bestimmte Dienste der Informationsverarbeitung (IV) sind mitunter nur innerhalb des Rechnernetzes der WWU erreichbar, teilweise auch nur aus Teilbereichen des WWU-Netzes. Gründe dafür sind zum Beispiel lizenzrechtlicher Art, in vielen Fällen sind Zugangsrestriktionen als Vorsorgemaßnahmen gegen Verletzungen des Datenschutzes oder gegen Missbrauch von Infrastrukturen und sonstige Sicherheitsrisiken eingerichtet. Ob solche Einschränkungen für einen bestimmten IV-Dienst wirksam sind oder nicht, erfährt man bei den einzelnen IV-Dienstanbietern in der Universität selbst – im Zweifel wende man sich an die zuständigen IV-Versorgungseinheiten, bei zentralen Ressourcen an das ZIV.

Allgemeine Einschränkungen

Über diese dienstspezifischen Zugangsbeschränkungen hinaus sind allgemeine, für das gesamte Netz der WWU geregelte Zugangsbeschränkungen wirksam, deren Funktion nur eingeschränkt öffentlich beschrieben werden kann. Beispielhaft genannt seien hier Maßnahmen, die Mail-Relaying für Dritte erschweren sollen (Anti-Spam-Maßnahmen); aufgrund solcher Maßnahmen sollte es beispielsweise nicht möglich sein, bei Nutzung eines Internet-Providers von den zentralen Mail-Servern der Universität im ZIV oder anderen Mail-Servern aus Nachrichten an Adressen außerhalb des Universitätsnetzes zu senden. Technisch gesehen beruhen solche Zugangseinschränkungen meistens darauf, dass die IP-Adresse überprüft und bei Nichtzugehörigkeit zum WWU-Netz die Kommunikation unterbunden wird.

VPN zur Aufhebung der Einschränkungen

Bei Zugang zum WWU-Netz aus anderen Netzen, gleich welcher Art, werden naturgemäß regelmäßig IP-Adressen anderer Netzbetreiber verwendet. Dies ist insbesondere zu bedenken, wenn für den Zugang zum WWU-Netz *Internet Service Provider* (ISP) anstelle der in das Netz der WWU unmittelbar integrierten Einwahlsysteme verwendet werden. Da die Verwendung von ISP anstelle der WWU-Einwahlsysteme aus verschiedenen Gründen, insbesondere aber ökonomischen, angeraten sein kann, stellt das ZIV so genannte VPN-Systeme (*Virtual Private Network*) bereit, mit welchen ein Arbeiten wie im Netz der WWU auch bei Zugang aus Netzen Dritter her ermöglicht wird. Unter Verwendung der VPN-Technik werden nach einer Nutzerauthentifizierung für die Kommunikation mit dem Netz der WWU auch IP-Adressen der WWU verwendet. Darüber hinaus kann die Datensicherheit durch Verschlüsselung erhöht werden.

Weitere Zugangsmöglichkeiten

Im WWW finden Sie unter `http://www.uni-muenster.de/ZIV/Rechnernetz/Zugaenge/Uebersicht.html` in kompakter Form in einer Übersicht alle Zugangsmöglichkeiten zum Rechnernetz der Universität Münster mit Hinweisen auf den Dienststatus, Zugangseinschränkungen und die Einbettung in Sicherheitskonzepte. VPN spielt in dieser Tabelle, die sicherlich für viele Nutzer neue Zugangswege aufzeigt, eine wichtige Rolle und zwar auch für Zugänge, die nicht durch ISP bereitgestellt werden. Dem Thema VPN werden Sie deshalb auch in diesem infoWWU wiederholt begegnen. Insbesondere auf das Tutorial (Seite 31 ff.) sei hingewiesen.

Virtuelle Private Netze an der WWU im Test

G. Richter

In Vorbereitung: Authentifizierter Zugang zum Uni-Netz

Zzt. sind VPN-Funktionen (*Virtual Private Network*) in das Rechnernetz der WWU i. Allg. noch nicht in den Regelbetrieb integriert. Das ZIV beabsichtigt, diesen Dienst bis September 2001 einzurichten, damit die Einschränkungen beim Zugang zum Netz der WWU über Netze Dritter, insbesondere über ISP (*Internet Service Provider*), soweit wie möglich abgebaut werden können.

Pilotartig sind VPN-Dienste u. a. in Betrieb für die Zugänge

- über Funk-LAN,
- über Internet (d. h. beliebige ISP) als auch
- für die ersten Pilot-Nutzer im Teleport-Projekt (ADSL-Zugänge in Wohnheimen des Studentenwerks).

Im WWW erfahren Sie unter

`http://www.uni-muenster.de/ZIV/Rechnernetz/VN/VPN/TechInfo.html`

alle aktuellen technischen Informationen wie den DNS-Namen und die IP-Adresse des jeweilig zu nutzenden VPN-Zugangs-Routers (VPN-Server). Bitte nutzen Sie nach Möglichkeit den DNS-Namen, da die IP-Adressen eher Änderungen unterliegen (z. B. bei Störungen) – der DNS-Name kann jedoch nur dann verwendet werden, wenn in dem Zugangsnetz bereits ein DNS-Dienst existiert (in ISP-Netzen gewöhnlich der Fall).

Der zugehörige VPN-Router für den Zugang über ISP hat den DNS-Namen `vpn-internet.uni-muenster.de` und unterstützt zunächst nur das Protokoll *PPTP* (*Point-to-Point Tunneling Protocol* über TCP-Port 1723). Die aktuelle IP-Adresse des VPN-Routers erfahren Sie über den DNS-Dienst (zzt. ist diese Adresse 128.176.239.193, diese IP-Adresse kann sich aber ändern, deshalb bei Vorhandensein eines DNS-Dienstes für den bestehenden Internetzugang beim ISP unbedingt den DNS-Namen `vpn-internet.uni-muenster.de` und nicht die IP-Adresse 128.176.239.193 für den VPN-Router konfigurieren). Verschlüsselte Passwort-Übermittlung wird zzt. noch nicht unterstützt. Die Einstellungen für die IP-Adresse als auch die DNS-Server werden automatisch vorgenommen – die IP-Adresse aus dem Bereich der WWU (128.176.x.y) wird ausschließlich dynamisch zugeteilt, eine statische Zuteilung ist nicht möglich.

Experimentierfreudige Nutzer dürfen diesen VPN-Zugang gerne ausprobieren, es besteht jedoch zzt. noch keinerlei Gewähr für eine ständige oder gar dauerhafte Verfügbarkeit oder angemessene Qualität dieses Dienstes. Voraussetzung für die Nutzung ist eine gültige Nutzerkennung des ZIV. Probleme melden Sie bitte an mich oder Herrn Speer; es kann zzt. jedoch nur eine eingeschränkte Unterstützung geboten werden.

Teleport-ADSL-Zugänge zum Netz der Universität

G. Richter

Mit MBit/s von der Uni ins Wohnheim

Im so genannten Teleport-Projekt, in dem das ZIV Dienstleistungen für die Deutsche Telekom AG zur kommunikationstechnischen Anbindung der Wohnheime des Studentenwerks erbringt, sind auch ADSL-Anschlüsse vorgesehen, für die zzt. erste Tests mit Pilotfunktion durchgeführt werden. Da das ADSL-Netz voraussichtlich auch als eigenständiges Netz innerhalb der Wohnheime zu nutzen sein wird, soll der Zugang zum Universitätsnetz deshalb über VPN-Technologie erfolgen.

Ein konkreter Termin für die Aufnahme des Regeldienstes kann bisher noch nicht genannt werden. Weitere Informationen erfolgen zu gegebener Zeit an dieser Stelle, soweit dies für den Zugang zum Universitätsnetz von Bedeutung ist.

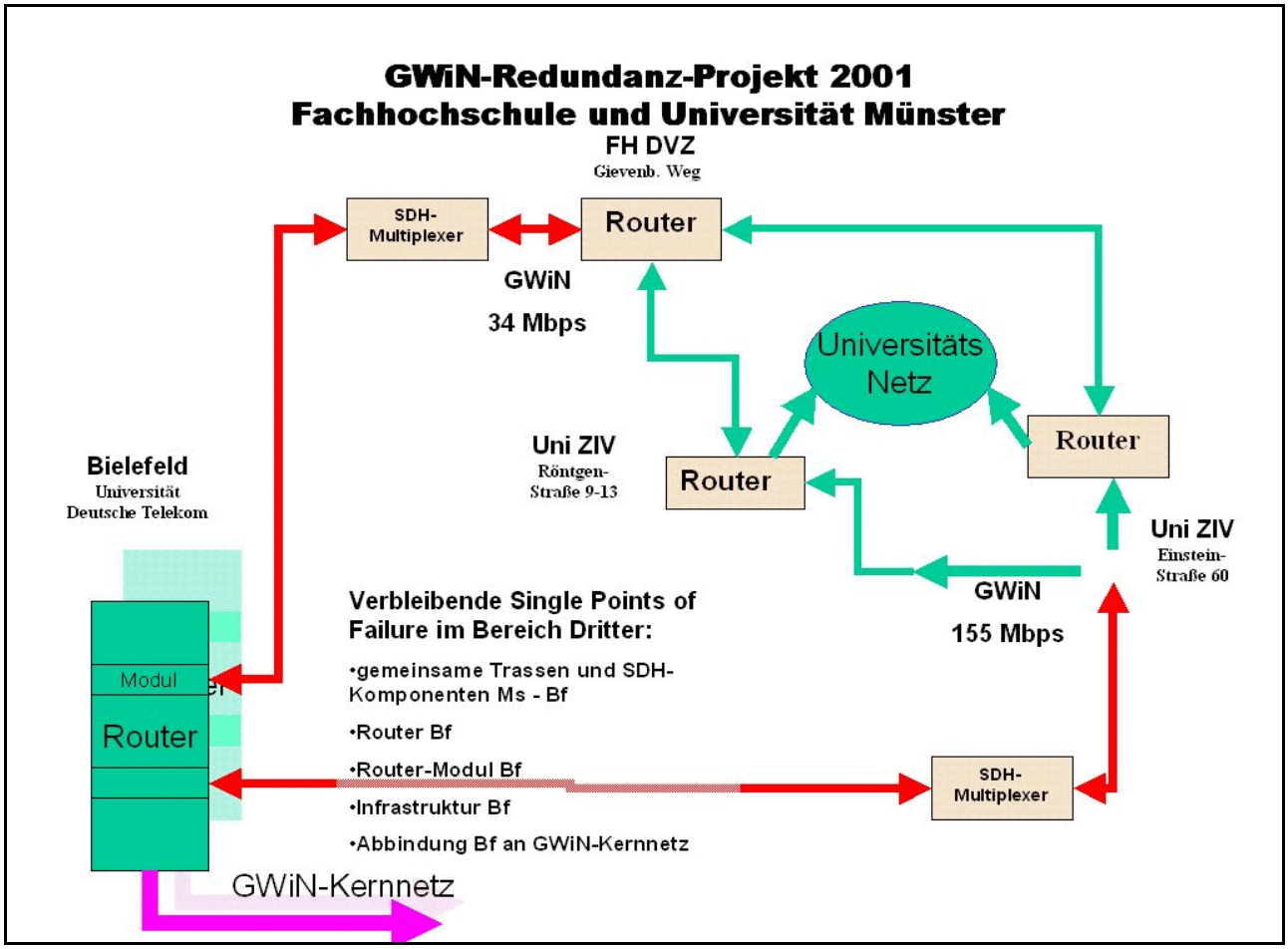


Abbildung: Redundanz beim GWiN-Zugang

ADSL: Status der Möglichkeiten des Zugangs zum Netz der Universität

G. Richter

Wann richtet die Universität ADSL-Einwahlmöglichkeiten ein?

Die Universität Münster war eine der ersten, wenn nicht gar die erste Hochschule in Deutschland, die ADSL-Technologie für den Zugang zum eigenen Rechnernetz und zum Internet eingesetzt hat. Im Wohnheimkomplex Rudolf-Harbig-Weg wurden 1997 für knapp 100 Studierende ADSL-Anschlüsse geschaffen; es handelte sich um ein Pilotprojekt der Firmen Siemens und Deutsche Telekom, des ZIV und des Instituts für Angewandte Informatik an der Universität. Das Projekt ist längst abgeschlossen, die Installation wird aber noch bis auf Weiteres in Betrieb gehalten.

Inzwischen ist ADSL-Technologie zur Standardzugangstechnologie vieler *Internet Service Provider* (ISP) geworden und in vielen größeren Städten unter verschiedenen Produktbezeichnungen (z. B. T-DSL, cDSL) als Dienst anmietbar. Im Bereich des Studentenwerks in Münster wird aktuell durch die Deutsche Telekom unter dem Projektnamen Teleport u. a. auch ADSL als Netzzugangstechnologie für die Studierenden angeboten (s. auch den vorstehenden Artikel) . Vor diesem Hintergrund wird das ZIV immer häufiger gefragt, wann denn die Universität allgemein ADSL-Einwahlmöglichkeiten anbieten werde.

Die Antwort darauf ist recht einfach: Wahrscheinlich nie. Die Gründe für diese Antwort sind einfach in der ADSL-Technik und den verfügbaren Infrastrukturen begründet. ADSL ist eine Technik der letzten Meile, d.h. der letzten wenigen Kilometer Telefonkabel bis

zum Endnutzer. Diese Kabelinfrastruktur ist nicht in der Hand der Universität, und selbst wenn dies möglich wäre, müsste die Universität dann doch an einer erheblichen Zahl von Ortsvermittlungsstellen (den Punkten, an welchen die Telefonkabel zusammengeführt werden) teure ADSL-Ausrüstungen (sog. DSLAMs) bereitstellen. Darüber hinaus müssten noch breitbandige Datenübertragungswege zum Universitätsnetz bereitstehen, um die DSLAMs an das Netz der Universität anzuschließen. Solche Infrastrukturen können selbstredend nicht durch die Universität, zumindest nicht mit einer angemessenen großen Flächendeckung, wirtschaftlich aufgebaut werden.

ADSL als Zugangstechnologie auch zum Rechnernetz der Universität ist damit trotzdem nicht ausgeschlossen, nur kann man hier nicht unbedingt von einer Einwahlmöglichkeit der Universität sprechen. Wenn heute jemand durch einen beliebigen ISP mit einer beliebigen Zugangstechnologie (Modem, ISDN, Funk-LAN) Zugang zum Internet hat, dann hat er auch Zugang zum Netz der Universität, da das Universitätnetz mit dem Internet über das Wissenschaftsnetz verbunden ist. Dies gilt genau so für ADSL-Internet-Zugänge beliebiger ISP.

Allerdings gibt es im Gegensatz zu den Einwahlsystemen der Universität einige Besonderheiten zu beachten, wenn der Zugang zum Netz der Universität über das Internet erfolgt; insbesondere kann der Zugriff auf bestimmte IV-Ressourcen im Netz der Universität eingeschränkt sein. Aber auch hierfür hat das ZIV eine Antwort: Mit so genannter VPN-Technologie (s. den Tutorial-Beitrag auf Seite 31) werden unter weitergehender Nutzung des Internets die Beschränkungen vollständig aufgehoben werden. Genau diese VPN-Technolgie wird übrigens auch seit dem Frühjahr 2001 erfolgreich für die bis dato bestehenden ADSL-Zugänge (Pilotprojekt Rudolf-Harbig-Weg und Teleport-Pilotnutzer) eingesetzt.

Uni@home II – eine Nachfolge für *uni@home* ?

G. Richter

Ab September wieder kostengünstig ins Uni-Netz einwählen!

Uni@home an der Universität Münster war eines der ersten großen Projekte, bei dem Universitätsangehörigen, insbesondere den Studierenden, die Möglichkeit gegeben wurde, vom häuslichen Arbeitsplatz und sonstwo IV-Ressourcen der Hochschule über Telefondienste zu erreichen, ohne dabei immer wieder auf besetzte Einwahlleitungen zu stoßen. Inzwischen sind einige Jahre ins Land gegangen, aber die Entwicklung der Dienstleistungsstrukturen hat gerade bei der Einwahl ins Internet eine rasante Entwicklung genommen. Es sind viele ISP (*Internet Service Provider*) entstanden und viele auch wieder verschwunden, es sind neue Angebote aufgetaucht, z. B. Flat Rates, die kamen und gingen, um nach einer Dürreperiode nun doch ein allmählich stabiles Dasein zu erreichen. Es sind neue Verfahren im Einsatz auch bei ISP: ADSL in verschiedenen Magervarianten und kaum bezahlbar in voller Schönheit für besonders ausgesuchte Kunden, Funk-LANs für MBit/s-Hungrige, wobei die Shared-LAN-Kost auf viele verteilt wird; nur Powerline über die Stromsteckdose beim Energieversorger lässt immer noch das Wasser im Mund zusammenlaufen, aber der Appetit wird bisher nicht gestillt. Jedenfalls ist ein Wandel überdeutlich und alte Konzepte zu überdenken ist überfällig. Es wird kolportiert, dass Studierenden die Immatrikulation wegen Dummheit entzogen werden müsste, wenn Sie sich noch über die Einwahlsysteme der Universität einwählen sollten. Ganz so dramatisch ist es wahrlich nicht, da der Zugang zum Universitätsnetz über Jahre stabil und kostengünstig war, und er wird, was für bestimmte Leistungen der Universität, z. B. der Universitäts- und Landesbibliothek (ULB), unabdingbar ist, nur berechtigten, weil authentifizierten Nutzern gewährt. Immerhin finden noch täglich bis zu ca. 400 Nutzer gleichzeitig den Weg über die allgemeinen Einwahlzugänge zum Universitätsnetz.

Das aktuelle Problem der bisherigen Einwahlzugänge sind die Telefongebühren, die für die Telefondienst-Anbieter zu entrichten sind, wobei insbesondere der regulierte ehemalige Monopolist Deutsche Telekom kaum Möglichkeiten von Kostenreduktionen bieten

konnte. Einer der günstigeren Tarife im City-Bereich ist noch der Nachttarif mit 3 Pfg/Min., der von Anfang an die Mitternacht zur Hauptnutzungszeit vieler Studentinnen und Studenten machte; 8 Pfg./Min. in der Hauptnutzungszeit sind aber sicherlich nicht mehr annehmbar. So ist es nicht verwunderlich, dass gerade die Nutzung der *uni@home*-Zugänge eher abnimmt oder bestenfalls stagniert. Verwendet werden stattdessen durch einen Großteil der Nutzer der universitären IV-Ressourcen, das kann als sicher gelten, verschiedenste ISP, über die dann der Weg über den Wissenschaftsnetzanschluss (G-WiN) in das Universitätsnetz gefunden wird und deren Tarife sich zur Zeit um 2,4 Pfg/Min. mit signifikanten Abweichungen zu bestimmten Zeiten nach unten einpendeln (s. Tarifvergleiche im WWW). Allerdings ist der Zugang zum Universitätsnetz über ISP bisher nicht uneingeschränkt verwendbar gewesen, z. B. ist der Zugang zur ULB eingeschränkt oder die Versendung von Mails an Ziele außerhalb der Universität ist über die meisten Mail-Server bei ISP-Nutzung aus guten Gründen unterbunden.

Naheliegend ist es natürlich nach Wegen zu suchen, wie ISP-Dienste für den Zugang zur Universität ohne Einschränkungen verwendet werden können. Mit der Einführung von VPN-Techniken (*Virtual Private Network*) will das ZIV genau dies ermöglichen; VPN sind eigene Beiträge in diesem infoWUM gewidmet.

Darüber hinaus arbeitet das ZIV zur Zeit zusammen mit Dez. 6.3 der Universitätsverwaltung und der Deutschen Telekom an einer neuen Variante von *uni@home*: *uni@home II*. Spätestens am 1. August wird im WWW mehr zu finden sein:

```
http://www.uni-muenster.de/ZIV/
Content--NetzEinwahl_uni_at_home.html
```

Mit *uni@home II* wird sicher wieder ein topaktuelles und kostengünstiges Einwahlangebot für die Universität Münster bereitstehen – seien Sie gespannt!

Erste Teilnehmer werden voraussichtlich ab 1. Oktober zu *uni@home II* zugelassen werden können; das Vorläufer-Projekt *uni@home* wird aber zunächst nicht aufgegeben, sondern nur reduziert werden. Des Weiteren wird natürlich die Einwahl über Citykom und den „universitätsinternen“ Zugang möglich bleiben; Citykom soll an den Tarifstrukturen ebenfalls erhebliche Veränderungen vorgenommen haben. Für Studierende in Wohnheimen des Studentenwerkes gibt es darüber hinaus die Möglichkeit am Teleport-Projekt teilzunehmen und dabei u. a. auch die ADSL-Technik zu wählen. In ersten Tests wird darüber hinaus mit einigen Wohnheimen die Verbindung zur Universität über Funk-LANs erprobt; die neuen Möglichkeiten, über Funk-LANs innerhalb des Universitätsgeländes Netzzugang zu erhalten, seien an dieser Stelle auch noch einmal erwähnt. Eine weitgehend vollständige Übersicht über alle Zugangsmöglichkeiten zum Rechnernetz der Universität Münster findet man unter

```
http://www.uni-muenster.de/ZIV/Rechnernetz/
Zugaenge/Uebersicht.html
```

Insgesamt dürfte mit *uni@home II* und den anderen genannten Maßnahmen zum Wintersemester 2001/2 eine breite, spürbare und Kosten senkende Verbesserung der Zugangsmöglichkeiten erreicht werden, wobei gerade die Vielfalt und die uneingeschränkte Nutzbarkeit nahezu beliebiger ISP die Weiterentwicklung der Dienste und des Wettwerbs fördern dürften.

Fingerprints

R. Perske

Unter dieser Rubrik erscheinen regelmäßig die aktuellen kryptografischen Prüfsummen der öffentlichen Schlüssel der WWUCA.

X.509-Zertifikat der WWUCA

Zum Ausstellen von X.509-Zertifikaten für SSL-/TLS-Server und -Clients und für S/MIME-Schlüssel verwendet die WWUCA den in folgendem Zertifikat enthaltenen Schlüssel:

Issuer: C=DE, O=Deutsches Forschungsnetz, OU=DFN-PCA, CN=DFN Top Level Certification Authority/Email=certify@pca.dfn.de
Subject: C=DE, O=Universitaet Muenster, CN=Zertifizierungsstelle 2000-2001/ Email=ca@uni-muenster.de
Version: 3 (0x2), Serial Number: 16 (0x10),
Validity: Not Before: Jun 5 15:35:24 2000 GMT,
Not After: Jun 5 15:35:24 2002 GMT
MD5-Fingerprint=DA:E3:E2:5D:BC:93:EF:03:37:96:4E:25:C1:AB:2B:D1
SHA1-Fingerprint=A764 5575 E0AD 9A2C 0CB4 C8ED BEE0 BFD4 726C 5CB2

Der mit diesem Zertifikat versehene Schlüssel wird von der WWUCA ausschließlich zum Ausstellen von X.509-Zertifikaten, zum Signieren der Policy und zum Signieren von X.509-Widerruflisten (Certificate Revocation List, CRL) verwendet, und zwar nur bis Ende 2001. Danach wird es einen neuen Zertifizierungsschlüssel geben.

PGP-Zertifizierungsschlüssel der WWUCA

Zum Zertifizieren von PGP-Schlüsseln verwendet die WWUCA folgenden Schlüssel:

Bits: 2048, KeyID: 313C02F5, Date: 2000/03/24
User ID: Zertifizierungsstelle Universitaet Muenster 2000-2001
Key fingerprint = 37 62 F5 E0 C2 78 76 97 53 0F 2D F2 F3 B3 27 F5

Dieser Schlüssel wird von der WWUCA ausschließlich zum Ausstellen von PGP-Zertifikaten, zum Signieren der Policy und zum Signieren von PGP-Widerruflisten verwendet, und zwar nur bis Ende 2001. Danach wird es einen neuen Zertifizierungsschlüssel geben.

PGP-Kommunikationsschlüssel der WWUCA

Bei jeder Kommunikation mit der Zertifizierungsstelle sollte der folgende Schlüssel verwendet werden:

Bits: 2048, KeyID: 4CB7658D, Date: 2000/07/06
User ID: Zertifizierungsstelle Universitaet Muenster (E-Mail) <ca@uni-muenster.de>
Key fingerprint = 38 3D 0F 16 CE FC 1F 9E B7 C3 04 B1 20 20 FC E6

Dieser Schlüssel ist durch die WWUCA zertifiziert und auf unbestimmte Zeit gültig.

Sie finden alle Zertifikate und Schlüssel auf den WWW-Seiten der WWUCA unter

`http(s)://www.uni-muenster.de/WWUCA/`.

ZIV-Tutorial

Einführung in Virtuelle Private Netze (VPN)

G. Richter

VPN erlaubt Angehörigen einer Organisation den Zugriff auf Ressourcen im „privaten" Netz der Organisation von beliebigen Endgeräten im Internet aus. Der Zugriff auf das private Netz kann dabei nach strengen Sicherheitsanforderungen erfolgen. Authentifizierung und Verschlüsselung können die Datensicherheit gewährleisten. Das Endgerät befindet sich bei Nutzung von VPN „virtuell" im privaten Netz der Organisation.

VPN – der Begriff

Die Bildung des Begriffes „Virtuelles Privates Netz" ist nur vor dem Hintergrund von zwei wichtigen Entwicklungen in der letzten Dekade zu verstehen:

- Entwicklung des ubiquitären, öffentlich nutzbaren Internet mit angeschlossenen Netzen aus allen Bereichen von Forschung, Handel, Industrie, Handwerk, Lehre, Verwaltung, Behörden, Privatnutzung etc. einschließlich einer Vielzahl von Dienstleisternetzen, die unterschiedlichsten Kunden den Zugang zum Internet ermöglichen (Internet-Service-Provider- bzw. ISP-Netze mit Modem-, ISDN-, ADSL-, Wireless-LAN- und anderen Zugangstechnologien),
- Entwicklung eines erhöhten Sicherheitsbedürfnisses für die vernetzte Informationsverarbeitung, insbesondere hin zu einem Schutzbedürfnis nach kontrollierten Netzbereichen, die ausschließlich nach Vorstellungen der nutzenden Organisation zugänglich sind und in der Regel sogar nur durch Organisationsmitglieder selbst genutzt werden können (private Netze, Intranets).

VPN erlaubt beides widerspruchsfrei und gleichzeitig vorteilhaft miteinander zu verbinden: Mitglieder einer Organisation, die nicht im unmittelbaren „privaten" Netzbereich der Organisation Informationen verarbeiten, aber über einen Internet-Zugang verfügen, können ihren externen Arbeitsplatz mit VPN über das Internet so mit dem privaten Netz verbinden, dass alle Sicherheitsbedürfnisse ähnlich wie im privaten Netz selbst befriedigt sind. Hierbei können sowohl Nutzer- und Rechner-Authentifizierungsmechanismen als auch hochwertige kryptografische Verfahren zur Herstellung der Abhör- und Verfälschungssicherheit eingesetzt werden. Ein solcher Arbeitsplatz befindet sich netztechnisch aus Sicht des Nutzers betrachtet vermeintlich (virtuell) im privaten Netz der eigenen Organisation. Insofern ist der Begriff Virtuelles Privates Netz gerechtfertigt. Beispielsweise können Rechner im Virtuellen Privaten Netz ganz real mit den Internet-Adressen (IP-Adressen) aus dem eigenen privaten Netz arbeiten, auch wenn der genutzte Internet-Zugangs-Service zunächst durchaus die Nutzung anderer IP-Adressen, nämlich die des ISP-Netzes, notwendig macht. Diese Technologie ist gegenüber den sonstigen Alternativen, nämlich den fest gemieteten eigenen Leitungen (Standleitungen), sehr viel kostengünstiger verfügbar.

Obwohl der Begriff VPN in der Regel im Zusammenhang mit ISP-Zugängen über Weitverkehrstechnologien verwendet wird, ist die Technologie nicht auf das Internet als Zuliefernetz beschränkt, sondern nahezu jedes beliebige IP-basierte Netz, das als Fremdnetz betrachtet wird, kann dazu verwendet werden. So kann z. B. der Zugang aus einem nicht abgesicherten Teil des Universitätsnetzes zu einem durch einen Firewall geschützten Bereich sicher eingerichtet werden. Im Folgenden wird „Internet" jedoch synonym für solche Fremdnetze allgemein verwendet.

Tunnel – das Mittel zum Zweck

Schlüssel zum technischen Verständnis von VPN sind die eingesetzten Übertragungsverfahren (Protokolle), die insbesondere Tunnel-Techniken einsetzen. Tunnel erlauben, wie der Name andeuten mag, die ungehinderte, geschützte Durchquerung eines Hindernisses (hier des Internets), das sich zwischen zwei Punkten befindet (hier das private Netz auf der einen Seite und der Arbeitsplatz auf der anderen Seite). Protokolltechnisch umgesetzt ist dies relativ einfach dargestellt:

Man benutzt das vorhandene Medium, das Internet, und überträgt in den Internet-Übertragungseinheiten, den IP-Paketen, selbst wieder IP-Pakete. Letztere nutzen dann die IP-Adressen aus dem privaten Netz und können verschlüsselt werden – erstere, die zur Übertragung im Internet dienen, verwenden naturgemäß IP-Adressen, die zur Paketvermittlung im offenen Internet benötigt werden.

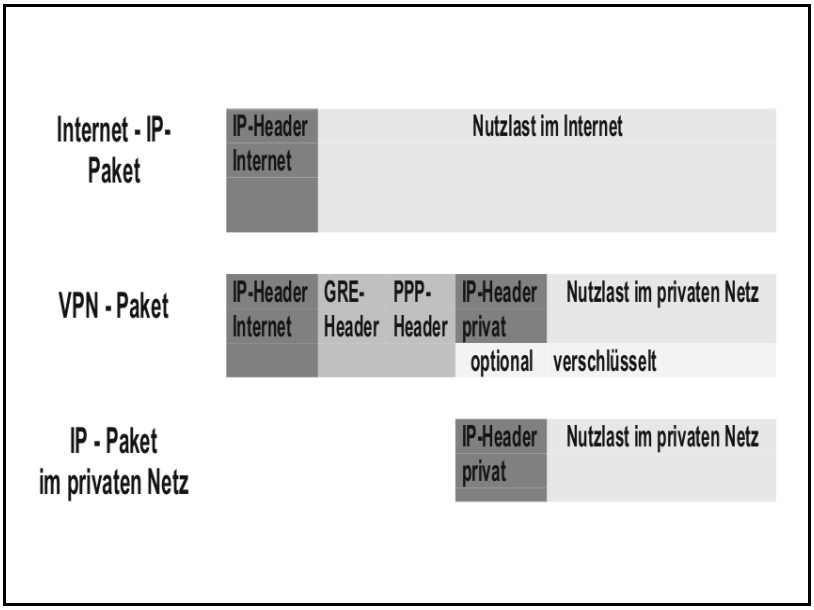


Abbildung 1: Struktur von VPN-IP-Paketen

Die Abbildung 1 zeigt vereinfacht die Schemata von IP-Paketen im Internet und im privaten Netz als auch die im VPN-Tunnel verwendeten IP-Pakete, die die „privaten IP-Pakete“ als Nutzlast tragen; verwendet wird hier beispielhaft das PPTP-Tunnel-Protokoll (*Point to Point Tunnel Protocol*). Die IP-Header-Informationen beinhalten insbesondere die entsprechenden IP-Adressen. Weitere Protokolldetails sollen hier nicht besonders erörtert werden. Dieses Verfahren wird aufgrund der Ummantelung des eigentlichen Datenverkehrs auch als *Encapsulation* bezeichnet.

Anwendung finden VPN-Tunnel meist

- **zwischen zwei Netzen** (in der Regel zwischen dedizierten Geräten, z. B. je einem VPN-Router in jedem Netz),
- **zwischen einem Endgerät und einem Netz** (meistens Arbeitsplatzrechner zu VPN-Router),
- **zwischen zwei Endgeräten** (in der Regel Arbeitsplatzrechner zu Server).

Im ersten Fall sorgen dedizierte Geräte (VPN-Router, manchmal auch Firewall-Systeme) als VPN-Client und VPN-Server für die sichere Verbindung von zwei Netzen über das Internet. Die Endgeräte in den verbundenen Netzen kommunizieren, ohne die VPN-Technik überhaupt besonders berücksichtigen zu müssen, da die Router die *Encapsulation* und *Decapsulation* vollständig übernehmen, während die Endgeräte lediglich ihre IP-Pakete des „privaten“ Netzes austauschen (vgl. Abbildung 2, unterer Teil).

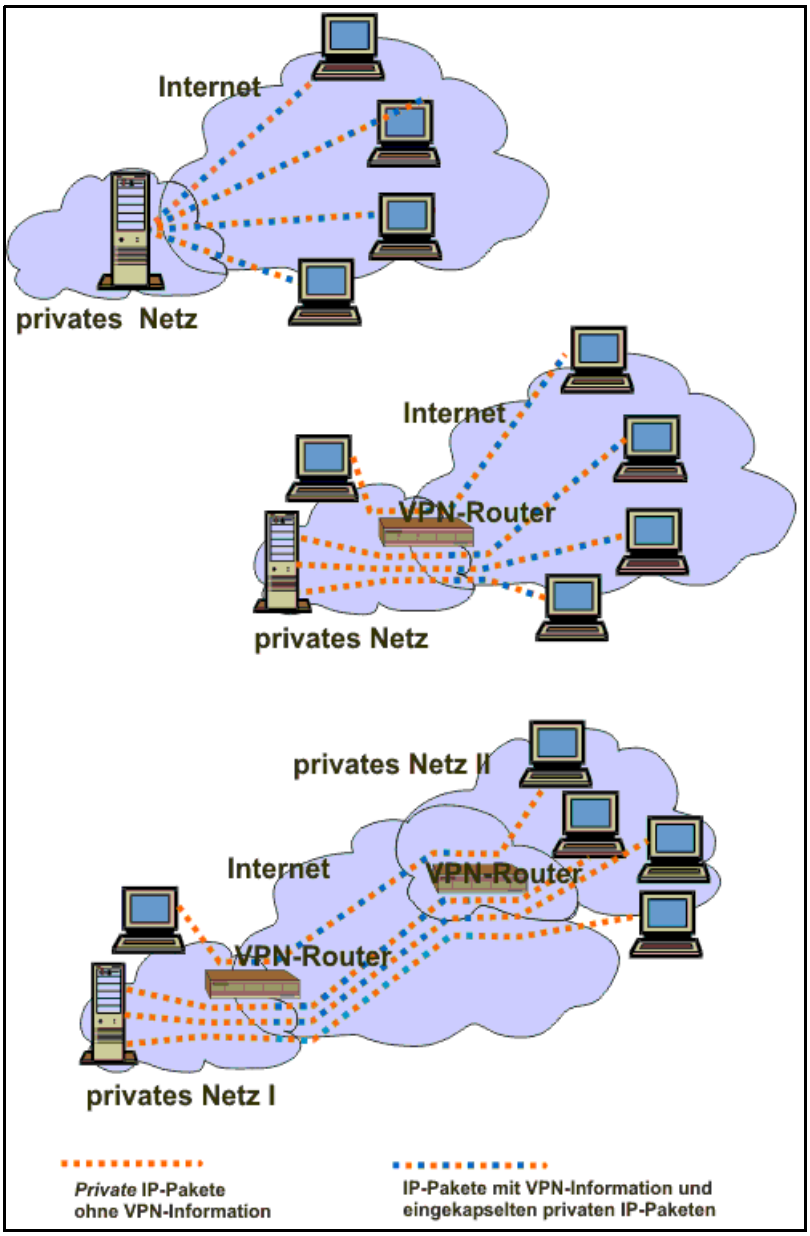


Abbildung 2: Nutzungsszenarien für VPN-Technologie

Die beiden anderen Verfahren unterscheiden sich vom vorhergehend beschriebenen dadurch, dass die *En-* und *Decapsulation* ganz oder teilweise in den Endgeräten selbst vorgenommen wird, wobei die Endgeräte die Rolle von VPN-Client oder auch VPN-Server übernehmen. Im Gegensatz zur ersten Variante kann hier ein VPN-Endgerät ohne eine zusätzliche Installation eines VPN-Routers die Vorteile der VPN-Technik nutzen. In der zweiten Variante wird meistens im Ziel-Netz ein VPN-Router installiert, der den sicheren Zugang zum „Intranet“ für alle VPN-Endgeräte im Internet oder in sonstigen „fremden“ Netzen ermöglichen soll; jeder Rechner irgendwo im Internet kann also somit jederzeit eine sichere Verbindung über VPN zu „seinem privaten Netz“ aufbauen.

Status 2001

Mit dem durch Microsoft ab Windows 95 unterstützen PPTP steht dem breiten Einsatz der VPN-Technologie auch für die Mehrzahl von Arbeitsplatzrechnern nur wenig entgegen. Für andere Betriebsysteme sind Treiberprogramme ebenfalls erhältlich oder stehen zumindest kurz vor der Verfügbarkeit. Die Installation der Treiberprogramme ist ähnlich einfach wie die Installation derartiger Programme für die Modem- oder ISDN-Nutzung. Eine Anleitung dazu finden Sie unter

`http://www.uni-muenster.de/ZIV/Content--NetzVN_VPN_Anleitung.html`

Aber auch die als in mancher Hinsicht (wegen der Möglichkeit der Rechnerauthentifizierung und der Verschlüsselung) noch sicherer einzuschätzenden Protokolle L2TP und IPSEC, insbesondere in Kombination, sind weitgehend auf relativ breiter Basis verfügbar. Allerdings sind die Anforderungen an VPN-Router bei ihrem Einsatz allgemein sehr hoch, so dass hier erhebliche Kosten entstehen können, insbesondere wenn die teilweise optionale Verschlüsselung in großem Umfang verwendet werden soll.

Die Einführung von VPN in den Netzbetrieb ist für viele Organisationen heute auf der Tagesordnung. Hauptsächlich werden dabei VPN-Router oder Firewall-Systeme mit VPN-Funktion als „sicheres Eingangstor“ zum eigenen Netz installiert. Der Betrieb eigener Standleitungen oder eigener Einwahlsysteme wird damit in der Regel überflüssig.

In größeren Organisationen mit entsprechend umfangreichen Netzen kann die „innere“ Sicherheit durch den Einsatz von mehreren VPN-Routern nach Bedarf quasi wie in Intranets innerhalb des Gesamtnetzes erhöht werden.

ZIV-Lehre

Veranstaltungen in der vorlesungsfreien Zeit (August/September 2001)

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, ✆ 83-31561

Für alle Veranstaltungen ist eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung, Einsteinstraße 60, erforderlich. Eintragungen in die Anmeldelisten sind ab dem 2. Juli 2001 möglich.

260014 Publizieren im Internet mit HTML und XML — Neukäter, B.
vom 03.09. bis 14.09.2001, ganztägig
Hörsaal: M4, Einsteinstr. 64, Beginn: 03.09.2001, 10 Uhr

260029 Windows 2000: Einführung und Grundlagen — Lange, W.
vom 03.09. bis 07.09.2001, ganztägig
Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 03.09.2001, 9 Uhr

260033 Programmieren in Fortran — Reichel, K.
vom 10.09. bis 21.09.2001, vormittags
Hörsaal: ZIV-Pool 2, Einsteinstr. 60, Beginn: 10.09.2001, 10.30 Uhr

260048 Statistische Datenanalyse mit dem Programmsystem SPSS — Zörkendörfer, S.
vom 17.09. bis 28.09.2001, ganztägig
Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 17.09.2001, 9 Uhr

260052 Sichere Kommunikation im Internet — Perske, R.
vom 24.09. bis 28.09.2001, ganztägig
Hörsaal: Raum 205, Röntgenstr. 11, Beginn: 24.09.2001, 10 Uhr

260067 Systemadministration für Linux-Systeme (für Fortgeschrittene) [2] — Hölters, J./ Grote, M.
vom 13.08. bis 17.08.2001, ganztägig
Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 13.08.2001, 9 Uhr

260071 Systemadministration für Windows-Systeme (für Fortgeschrittene) [2] — Kämmerer, M.
vom 20.08. bis 24.08.2001, ganztägig
Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 20.08.2001, 9 Uhr

Veranstaltungen in der Vorlesungszeit (Wintersemester 2001/2002) für Hörer aller Fachbereiche

Beratung zum Lehrangebot durch Herrn W. Bosse jeweils Di, Do 11-12, ✆ 83-31561

Für alle Veranstaltungen ist eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung, Einsteinstraße 60, erforderlich. Eintragungen in die Anmeldelisten sind ab dem 17. September 2001 möglich.

260086 Kommunikation und Information im Internet — Mertz, K.-B.
Mittwoch 13-15 Uhr
Hörsaal: ZIV-Pool 2, Einsteinstr. 60, Beginn: 24.10.2001

260090 Programmieren in Java — Pudlatz, H.
Mittwoch, 15-17 Uhr
Hörsaal: M4, Einsteinstr. 64, Beginn: 31.10.2001

---

[2] Bei diesen Veranstaltungen werden Studierende im Zusatzstudiengang Angewandte Informatik vorrangig berücksichtigt.

260105	Programmieren in Java für Fortgeschrittene Mittwoch 9-11 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 24.10.2001	Sturm, E.
260110	Objektorientiertes Programmieren in C++ Mittwoch 13-15 Uhr Hörsaal: M4, Einsteinstr. 64, Beginn: 24.10.2001	Mersch, R.
260124	Statistische Datenanalyse mit dem Programm SPSS Donnerstag 11-13 Uhr Hörsaal: ZIV-Pool 2, Einsteinstr. 60, Beginn: 25.10.2001	Nienhaus, R.
260139	Einführung in Windows-Systeme Montag 14-16 Uhr Hörsaal: ZIV-Pool 3, Einsteinstr. 60, Beginn: 22.10.2001	Kämmerer, M.
260143	Rechnernetze und Internet – Technische Grundlagen Donnerstag 10-12 Uhr Hörsaal: Raum 206, Röntgenstr. 11, Beginn: 25.10.2001	Kamp, M./ Richter, G./ Speer, M./ Wessendorf, G.
260158	Kolloquium des Zentrums für Informationsverarbeitung Freitag 14-16 Uhr Hörsaal: Raum 206, Röntgenstr. 11	Held, W.

Kommentare zu den Lehrveranstaltungen

260014 Publizieren im Internet mit HTML und XML

Neben den traditionellen Medien Buch, Zeitschrift, Presse, Rundfunk und Fernsehen wird das Internet zunehmend zur Veröffentlichung wissenschaftlicher Erkenntnisse in Wort, Bild und Ton genutzt. Eine wichtige Grundlage für Veröffentlichungen im Internet ist die Hypertext Markup Language (HTML), mit deren Hilfe ein Geflecht von Texten, Bildern und anderen multimedialen Elementen im World Wide Web (WWW) dargestellt werden kann.

Die HTML steht im Mittelpunkt dieser Lehrveranstaltung, in der gezeigt werden soll, dass es keiner besonderen Rechner- oder Informatikkenntnisse bedarf, um Web-Seiten für das Internet zu gestalten. Voraussetzung für diese Veranstaltung sind lediglich Kenntnisse, wie sie etwa in der Vorlesung „Kommunikation und Information im Internet“ vermittelt werden.

Im zweiten Teil der Veranstaltung sollen neben der HTML weitere Themen wie Webserver, CGI-Skripte. JavaScript und XML behandelt werden.

260029 Windows 2000: Einführung und Grundlagen

In der Veranstaltung wird der Einsatz des Betriebssystems Windows 2000 in einer Netzwerkumgebung vorgestellt. Vorgesehene Themen sind unter anderem: Netzwerkdienste, Domänenkonzept, Benutzerverwaltung, Sicherheit, Richtlinien und Serverdienste (u. a. Fileserver, Printserver, Terminalserver, Webserver).

Die Hörer sollten Zugang zu einem Windows-2000-System für Übungszwecke haben und bereits über Grundkenntnisse im Umgang mit Windows-Betriebssystemen verfügen.

260033 Programmieren in Fortran

Fortran ist eine weit verbreitete Programmiersprache, die insbesondere für die Programmierung naturwissenschaftlicher und technischer Anwendungen eingesetzt wird.

In dieser Vorlesung sollen die Hörerinnen und Hörer lernen, wie Programme systematisch konstruiert werden. Gleichzeitig wird ihnen zunächst der Fortran-77-Standard, anschließend darauf aufbauend der neueste Fortran-90-Standard vermittelt.

Es werden keine Programmierkenntnisse vorausgesetzt. Praktische Übungen sind Teil der Veranstaltung.

BRAUER: *Programmieren in Fortran 77*, Müthig
MICHEL: *Fortran 90*, BI-Wiss.-Verlag
BRAINARD/GOLDBERG/ADAMS: *Fortran 90*, Oldenbourg
HEISTERKAMP: *Fortran 90*, BI Wiss.-Verlag University Press

260048, 260124 Statistische Datenanalyse mit dem Programmsystem SPSS

Das statistische Programmsystem SPSS (*Statistical Package for the Social Sciences*) wird in dieser Veranstaltung in der neusten deutschsprachigen Version unter Windows vorgestellt und erprobt. Mit diesem System stehen bequem aufzurufende Programme zu den gebräuchlichen univariaten und multivariaten statistischen Verfahren sowie zur Datenaufbereitung zur Verfügung. SPSS wird z. B. zur Auswertung von Fragebögen eingesetzt.

In dieser Veranstaltung wird das programmtechnische Rüstzeug zur Durchführung derartiger Auswertungen vermittelt. Solide Grundkenntnisse bezüglich der anzusprechenden statistischen Verfahren sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

260052 Sichere Kommunikation im Internet

Das Internet ist eine mächtige und leistungsfähige Kommunikations-Infrastruktur, birgt aber auch erhebliche Gefahren, welche für einen unbedarften Nutzer nur schwer zu erkennen sind.

In der Veranstaltung wird gezeigt, welche Gefahren bestehen und wie man sich ohne große Mühe vor diesen Gefahren schützen kann. Praktisch geübt werden kurz das Absichern des eigenen Rechners sowie ausführlich das Einrichten und die Benutzung entsprechender Software zur sicheren Kommunikation:

- Sichere E-Mail mit *Pretty Good Privacy* und mit *Secure MIME*
- Sichere Dialog- und Datenverbindungen mit *Secure Shell*
- Sichere Interaktion im WWW mit SSL/TLS (HTTPS)

Den Teilnehmerinnen und Teilnehmern wird dabei deutlich, dass Verschlüsselung, elektronische Unterschriften und Zertifikate viel einfacher zu benutzen sind als man sich gemeinhin vorstellt.

Vorausgesetzt werden Erfahrungen im Umgang mit den Internetanwendungen E-Mail, WWW, Telnet und FTP sowie Grundkenntnisse der Funktionsweise (wozu braucht man IP-Adressen? Portnummern? Nameserver? Router?), wie sie beispielsweise durch den Besuch der Veranstaltung „Kommunikation und Information im Internet“ erworben werden können.

260086 Kommunikation und Information im Internet

In den letzten Jahren haben sich die internationalen Datenkommunikationsnetze – eines der wichtigsten ist das Internet – in rasantem Tempo ausgebreitet. Sie sind durch ihre Möglichkeiten zur Informationsgewinnung und zur Kommunikation ein unverzichtbares Hilfsmittel – nicht nur für Wissenschaftler.

Den Teilnehmern der Veranstaltung wird in Theorie und praktischen Übungen vermittelt, wie man sich in dieser komplexen Welt zurechtfinden und sie sich zunutze machen kann. Die Teilnehmer sollten bereits wissen, wie man mit der Windows-Fensteroberfläche und mit der MS-DOS-Eingabeaufforderung umgeht und welchem Zweck die DOS-Befehle `cd`, `mkdir`, `rmdir` usw. dienen.

260090 Programmieren in Java

Java ist eine Programmiersprache, die von SUN Microsystems direkt für das Internet entwickelt wurde. Sie erlaubt es, Anwendungen zu schreiben, die vom Benutzer über das Internet angefordert und auf seiner Maschine ausgeführt werden können, ohne dass der Entwickler die lokale Umgebung des Anwenders, wie Hardware und Betriebssystem, kennen muss.

Als objektorientierte Sprache ähnelt Java der Sprache C++, ist jedoch konzeptionell einfacher und enthält spezielle Sicherheitsfunktionen. In Java geschriebene Programme, so genannte Applets, lassen sich insbesondere zur Gestaltung von WWW-Seiten verwenden, die dynamische Elemente, also z. B. bewegte Bilder, enthalten.

Java hat sich seit einigen Jahren auf dem Markt etabliert, und es ist zu erwarten, dass es sich weiterhin dynamisch entwickelt.

Diese Vorlesung ist auch für Hörerinnen und Hörer ohne Vorkenntnisse im Programmieren geeignet.

260105 Programmieren in Java für Fortgeschrittene

In der Vorlesung sollen einige fortgeschrittene Konzepte der Programmiersprache Java vorgestellt werden.

Am Anfang der Lehrveranstaltung stehen Techniken zur Unterstützung der parallelen Programmierung (*Multithreading*) in Java. Im Anschluss daran erfolgt eine Übersicht zu IO in Java (Streams-Konzept).

Als internetbasierte Sprache bietet Java eine Reihe von Werkzeugen zur Netzwerkprogrammierung. Neben der Vorstellung der entsprechenden Grundlagen erfolgt eine Übersicht zu den darauf aufbauenden Themen wie *Remote Method Invocation*, Datenbankzugriff und Servlets.

Einen weiteren Themenschwerpunkt bilden schließlich neuere Konzepte zur Gestaltung grafischer Benutzeroberflächen wie Java-Beans und die Swing-Klassen.

260110 Objektorientiertes Programmieren in C++

Objektorientierte Programmierung wird einerseits als wichtiger Schritt in Richtung ingenieurmäßige Software-Erstellung gesehen, andererseits ist sie das „natürliche“ Programmier-Paradigma für einige Klassen von Anwendungen, wie z. B. grafische Oberflächen und Simulationen.

Zu dieser Lehrveranstaltung werden die Prinzipien der objektorientierten Programmierung vorgestellt und mit Hilfe der Programmiersprache C++ demonstriert. C++, eine Erweiterung der Programmiersprache C um objektorientierte Elemente, wurde Ende 1997 von ANSI und ISO standardisiert. Implementierungen der Sprache gibt es praktisch für alle Betriebssysteme und Rechnertypen.

In der Lehrveranstaltung werden die Programmiersprache und Teile der Standardbibliothek gemäß ISO/ANSI-Standard vorgestellt. Sie ist als weiterführende Veranstaltung konzipiert; Grundkenntnisse in C oder C++ werden vorausgesetzt.

260139 Einführung in Windows-Systeme

Diese Vorlesung bietet eine Einführung in Windows-NT-Prinzipien:

- Betriebssystemarchitektur: Dateisystem, Registry, Dienste, Benutzerverwaltung
- Kommunikationsdienste: Ethernet, TCP/IP, NetBios, LAN, Internet, Terminal-Clients
- Installation und Konfiguration: Betriebssystem, Anwendungsprogramme, Netzwerk, Systemsteuerung
- Absicherung des Systems: NTFS, Registry, Virenschutz, Personal FireWall
- PC-Hardware: Bus-Systeme, Plattentechnologien, Speicher, Peripherie
- System-Ausblick: DOS, WfW, Win9x/ME, WinNT/2000/XP

Allgemeine Windows-Vorkenntnisse sind erforderlich.

260143 Rechnernetze und Internet – Technische Grundlagen

Diese Veranstaltung gibt einen Einblick in die technischen Grundlagen der Rechnernetze unter besonderer Berücksichtigung des Internets.

Folgende Themen werden behandelt:

- Architekturmodell für Rechnernetze (OSI-Modell), Kommunikationsprotokolle
- Techniken für lokale Rechnernetze (LANs): Ethernet, Fast Ethernet, FDDI
- Kopplung/Strukturierung von Rechnernetzen: *Routing*, *Bridging* und *Switching*
- Verwendung von öffentlichen Netzen zur Rechnervernetzung: Analogtechnik, ISDN, ADSL – Weitverkehrsnetze
- Grundlegende Internet-Protokolle: IP, TCP, UDP, ICMP, ARP, DNS, DHCP, WINS
- TCP/IP-Software: Konfiguration und Diagnose
- IP-Multicast/Mbone
- ATM: Asynchronous Transfer Mode
- VLANs: Virtuelle LANs
- neuere Entwicklungen: IPv6 (Internet Protocol Version 6), Funk-LAN, ...
- Struktur und Funktionen des Rechnernetzes der Universität Münster

260158 Kolloquium des Zentrums für Informationsverarbeitung

Im Rahmen des Kolloquiums werden Vorträge über aktuelle Themen der Informationsverarbeitung gehalten. Vortragstermine werden im WWW und durch Aushang bekannt gegeben.

Liebe Leserin, lieber Leser,

wenn Sie infoforum regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts. Hat sich Ihre Adresse geändert oder sind Sie am weiteren Bezug von infoforum 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 infoforum

☐ 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:

_____

An die
Redaktion infoforum
Zentrum für Informationsverarbeitung
Röntgenstr. 9–13
48149 Münster

☐ Meine Anschrift hat sich geändert.
Alte Anschrift:

_____

_____

Absender:

Name: _____

FB: _____ Institut: _____

Straße: _____

Außerhalb der Universität:

_____

(Bitte deutlich lesbar in Druckschrift ausfüllen!)
Ich bin damit einverstanden, dass diese Angaben in der infoforum-Leserdatei gespeichert werden (§ 4 DSG NW).

_____ _____

Ort, Datum Unterschrift