

infoforum

Zentrum für Informationsverarbeitung der Universität Münster

Jahrgang 24, Nr. 1 – März 2000

ISSN 0931-4008

Inhalt

| | |
|--|----|
| Sicher ist sicher | 2 |
| RUM-Aktuell | 3 |
| Kosten- und Leistungsrechnung in der IV | 3 |
| Outsourcing und Insourcing | 3 |
| Campuslizenz McAfee VirusScan | 4 |
| DCE in Theorie und Praxis | 5 |
| Die IV-Versorgungseinheiten der WWU | 7 |
| Mangelnde Sicherheit von WWW-Programmen | 9 |
| Baumaßnahmen im Gebäude Einsteinstraße | 14 |
| WWWplot | 15 |
| Fingerabdrücke | 17 |
| Deponierung großer Datenmengen: Ein neues HSM-Dateisystem | 19 |
| RUM-Tutorial | 21 |
| Einsatz von Smartkarten in Betrieben, Hochschulen und Ämtern (2) | 21 |
| RUM-Lehre | 25 |
| Lehrveranstaltungen im Sommersemester 2000 | 25 |
| RUM-Index | 29 |
| Stichwörter infoforum Jahrgang 23 | 29 |



Impressum

inform

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: Zentrum für Informationsverarbeitung
(Rank Xerox DocuTech 135)

Auflage dieser Ausgabe: 1500

Sicher ist sicher

H. Pudlatz



Die Bauchschmerzen sind verfliegen, die uns der Jahrtausendwechsel und auch der kürzlich überstandene Millenniums-Schalttag – den es so nur alle 400 Jahre gibt – in der IV beschert hat. Ob der Wind, den man um die Sicherheit der Programme gemacht hat, gerechtfertigt war oder nicht, wird man im Nachhinein nicht mehr entscheiden können. Zwei Vorteile hatte das Ganze immerhin: Alte selbst gestrickte Programme wurden entsorgt oder konnten – wenn noch erforderlich – mit modernen Methoden neu konzipiert werden. Zum Anderen wurde bei einigen die Sensibilität für Sicherheitsfragen vielleicht erstmals geweckt und sollte nicht wieder verdrängt werden.

Warum aber schon wieder in diesem Heft das verstärkte Eingehen auf das Thema Sicherheit in der IV? Vielleicht deshalb, weil wir die vor dem „großen Zusammenbruch“ begonnenen Überlegungen erst jetzt richtig klargedacht haben? Sicherlich nicht, denn der 2. Teil unseres Tutorial-Beitrags über Smartkarten war schon lange vor dem Jahrtausendwechsel fertig. Oder hat es damit zu tun, dass wir endlich über den erst kürzlich erfolgten Abschluss des Campusvertrags über einen Virensch scanner berichten können? Das Thema Sicherheit ist mit der zunehmenden Nutzung der Netze relevant und wird durch die immer häufiger auftretenden massiven Angriffe auf Rechner – wie die neuerliche Denial-of-Service-Attacke zeigt – immer bedeutsamer.

Ob Themenschwerpunkt oder nicht: die Fingerabdrücke werden sicherlich ein Dauerbrenner bleiben, vermitteln sie uns und Ihnen doch die Sicherheit, mit dem richtigen Partner zu kommunizieren – vorausgesetzt, wir vergleichen schon mal eine PGP-signierte E-Mail mit der letzten Fingerabdruckliste!

Angesichts der mangelnden Sicherheit vieler WWW-Programme, über die in diesem Heft auch geredet werden soll, steckt in dem neuen Web-Programm „WWWplot“ für das Previewing und die Steuerung der Grafikausgabe mehr Sicherheit, als man annehmen könnte: Ohne Ihr Unix-Passwort bekommen Sie mit Sicherheit kein Bild zu sehen.

Das hier ebenfalls vorgestellte neue HSM-Dateisystem zur Datensicherung weist auf eine andere Facette des Themas hin, und nicht zuletzt passt auch der Artikel über das um Sicherheit und Zuverlässigkeit bemühte Distributed Computing Environment (DCE) gut zu unserem Themenschwerpunkt.

RUM-Aktuell

Kosten- und Leistungsrechnung in der IV

W. Held

Vom 01.01.2001 an wird in allen Hochschulen des Landes NRW für alle Bereiche eine Kosten- und Leistungsrechnung eingeführt.

Zur Kosten- und Leistungsrechnung in der IV haben Dr. Münch (Hochschulrechenzentrum Siegen), Dr. Held (ZIV Münster) et al. einen ausführlichen Bericht erstellt. Der Bericht wurde in der Zeitschrift „Praxis der Informationsverarbeitung und Kommunikation“ (PIK 21 (1998)) veröffentlicht, er ist auch unter <http://www.uni-muenster.de/ZIV/Allgemein/LeistungsKostenrechnungDV.html> abrufbar. Die Hochschulrechenzentren des Landes NRW haben ergänzend für die IV die Kostenarten und Kostenstellen für die bevorstehende Kostenrechnung einheitlich festgelegt.

Der Bericht wurde inzwischen ergänzt um das Thema „Quantitäten, Qualitäten und Kostenzuordnung von Leistungen in Unversitätsrechenzentren“, der in Kürze in der Zeitschrift PIK und im WWW veröffentlicht wird.

Es kann jeder Einrichtung der WWU nur dringend empfohlen werden, sich nicht allein auf die Kostenrechnung zu konzentrieren. Wer nicht gleichzeitig die Leistungen beschreibt, die die Einrichtung erbringt, handelt grob fahrlässig. Denn wer nur Kosten sieht, wird geneigt sein, diese zu reduzieren. Wer aber auch Leistungen zur Kenntnis nehmen muss, wird verantwortlicher handeln müssen.

Outsourcing und Insourcing

W. Held

In den Industrieländern sind derzeit feindliche und freundliche Firmenübernahmen an der Tagesordnung. Der sogenannte Shareholder Value steht offensichtlich im Vordergrund mancher Vorstandsüberlegungen, obwohl sie wissen sollten, dass ein Teil dieser Übernahmen (manche sprechen von 70 % der Fälle) nicht erfolgreich ist und zu hohen Verlusten führt. Die Menschen in den Betrieben werden dabei oft wie Objekte behandelt und die vorausschauende Entwicklung neuer Produkte kommt oftmals zu kurz.

Eine scheinbar mildere Form dieser Übernahme stellt das Outsourcing dar, das viele Politiker derzeit auch für die öffentlichen Einrichtungen propagieren, ohne, so hat es den Anschein, oftmals genau zu wissen, auf was sie sich dabei einlassen.

In dem Aufsatz „Outsourcing und Universitäten“ haben Dr. Münch (Hochschulrechenzentrum Siegen) und Dr. Held (ZIV Münster) das Thema ausführlich behandelt. Der Aufsatz ist in der Zeitschrift „Praxis der Informationsverarbeitung und Kommunikation“ (PIK 22 (1999) 4) und unter <http://www.uni-muenster.de/ZIV/Allgemein/OutsourcingUndUniversitaeten.html> zu finden.

Die Arbeit findet eine schöne Ergänzung in der Fachzeitschrift „Communications of the ACM“, Februar 2000, Vol. 43, No. 2. Dort sind R. Hirschheim und M. Lacity unter dem Titel „The Mythos and Realities of Information Technology Insourcing“ zu vergleichbaren Ergebnissen wie Held und Münch gekommen und haben über das Anti-Outsourcing, nämlich das Insourcing, berichtet.

Campuslizenz McAfee VirusScan

S. Zörkendörfer

Das Zentrum für Informationsverarbeitung (Universitätsrechenzentrum) hat für die Universität Münster einen Campusvertrag über die McAfee VirusScan Security Suite (VirusScan, Virex, Netshield, Management Edition) abgeschlossen, Laufzeit zunächst bis 31.3.2002.

Der Vertrag zur McAfee-VirusScan Security Suite wird aus zentralen Mitteln der Universität finanziert – eine erfreuliche Neuerung zum Vorgänger-Vertrag „Dr. Solomon’s“ besteht darin, dass nun nicht mehr Kopienzahlen beantragt und gezahlt und abgerechnet werden müssen. Dr. Solomon’s AVT wird nicht mehr bereitgestellt; wir möchten davon ausgehen, dass alle Nutzer dieses Produktes während der Laufzeit des alten Vertrags bereits auf VirusScan (McAfee) umgestiegen sind.

Nutzungsberechtigungen

Die Vereinbarungen bezüglich der (wesentlich erweiterten) Nutzungsberechtigung seien mitgeteilt:

- „3.2 VirusScan wird eingesetzt für einen Rechner (einschließlich Notebooks, Laptops, Handhelds), der Eigentum der WWU ist oder für ihre dienstlichen Belange verwendet wird.
- 3.4 VirusScan wird vom Mitarbeiter der WWU im privaten Bereich zum Zwecke der dienstlichen Nutzung eingesetzt, wobei gewährleistet ist, dass keine Nutzung durch andere Personen erfolgt. Beispielsweise durch entsprechende dienstliche Anweisungen oder schriftliche Erklärungen der Mitarbeiter kommen die Bezugsberechtigten ihren diesbezüglichen Verpflichtungen nach.
- 3.5 VirusScan wird von Studentinnen/Studenten der WWU genutzt.
- 4. Die Produkte können im Lizenzzeitraum bis 31.3.2002 unter den Bedingungen (3.2), (3.4), (3.5) mit jeweils aktuellen Updates (Aktualisierung der Datendateien, DAT-Files) und Upgrades (Erweiterung der Programmversionen) genutzt werden.“

Produktübersicht

Zunächst sei darauf aufmerksam gemacht, dass von weiteren Herstellern Produkte zum Virenschutz angeboten werden und dass einige Hersteller diese Produkte zur häuslichen Nutzung kostenlos freigeben. Bezüglich unserer Vereinbarung mit NAI weise ich darauf hin, dass wir nur die Produkte der VirusScan Security Suite (und nicht die umfassendere Total Virus Defense Suite) nutzen. Zu aktuellen Herstellerhinweisen mag Einsicht in <http://www.nai.com/> oder <http://www.mcafee.com/> angeraten sein.

Bezüglich Einzelplatzrechner wird VirusScan bereitgestellt für DOS, Windows 3.1x, Windows 95/98, Windows NT, zusätzlich Virex für Macintosh. Ferner umfasst die Suite die Management Edition und Netshield. Einige dieser Produkte werden in einer deutschsprachigen Version zur Verfügung stehen.

Zugang zu Installationsmaterialien

Das ZIV arbeitet daran, die Installationsmaterialien für die Berechtigten zum Kopieren oder Installieren bereitzustellen. Dateien zum Update der Virendefinitionen (sogenannte DAT-Files) werden wir auch weiterhin öffentlich bereitstellen. Einzelheiten hierzu werden wir in Kürze über die üblichen Medien (WWW, Aushang) veröffentlichen.

DCE in Theorie und Praxis

5. DCE-Workshops in Augsburg

M. Zahn (Augsburg) und R. Laißer (Karlsruhe)

Am 11./12. November 1999 hat in Augsburg der inzwischen 5. DCE-Workshop stattgefunden. Im Mittelpunkt stand der Austausch von Informationen, Erfahrungen und Betriebsstrategien rund um das Thema DCE/DFS.

Als das Distributed Computing Environment (DCE) Anfang der 90er Jahre von der Open Software Foundation (OSF) aus der Taufe gehoben wurde, wurde dem System von allen Seiten reges Interesse entgegen gebracht. „The network as a computer“, unter diesem Motto versprach DCE in Verbindung mit seinem Netzwerk-Dateisystem DFS (Distributed File System) die verschiedenen Hardware- und Betriebssystemplattformen zu einem und dem Administrator eine homogene Sicht auf seine System-, Benutzer- und Dateiverwaltung zu beschern. Schnell wurde jedoch klar, dass diesem an sich lobens- und lohnenswerten Ansatz mit dem notwendigen großen Aufwand für Einarbeitung und Migration oftmals eine schier unüberbrückbare Hürde entgegenstand. Seit diesen Anfangszeiten ist es um DCE/DFS merklich ruhiger geworden. Kaum einmal mehr verirrt sich ein Beitrag zu diesem Thema in eine der größeren DV-Zeitschriften.

Dennoch ist das Distributed Computing Environment inzwischen relativ verbreitet. Nicht nur an vielen Universitäten, die von Natur aus mit einer äußerst heterogenen Systemumgebung zu kämpfen haben, sondern auch in etlichen Wirtschaftsunternehmen hat sich DCE aufgrund diverser Vorteile (Sicherheit, Zuverlässigkeit, Skalierbarkeit, Plattformunabhängigkeit) gegenüber anderen Systemen durchgesetzt. Um die Kommunikation zwischen den DCE-Administratoren im deutschen Sprachraum zu verbessern, wurde vor Jahren eine Reihe von DCE-Workshops ins Leben gerufen. Das fünfte Treffen fand nun im November 1999 in Augsburg statt. Rund 60 Teilnehmer aus Deutschland, Schweden und Österreich nahmen aktiv an der zweitägigen Veranstaltung teil. Die Vorträge und das daraus resultierende Feedback zeigten, dass es mit und um DCE/DFS ausreichend „Success Stories“ gibt, über die es zu berichten lohnt. Kein Grund also, damit hinter dem Berg zu halten.

Zu Beginn der Veranstaltung waren alle Teilnehmer aufgefordert, kurze Statusberichte aus ihren Institutionen vorzutragen. Begleitet von zum Teil reger Diskussion wurden die Überlegungen vorgestellt, die zu einem Einsatz des Distributed Computing Environment geführt haben, die verfolgten Ziele und Betriebsstrategien erläutert und der Umfang der jeweiligen „DCE-Zellen“ präsentiert: die Zahl der registrierten Benutzer, das Datenvolumen im DFS, die Menge der beteiligten Rechnersysteme sowie die Größe des Administratoren-Teams. Der Umfang der DCE-Zellen variiert zwischen Zellen mit einigen hundert Benutzern und relativ wenigen Rechnersystemen bis hin zu großen Zellen mit weit mehr als 40.000 registrierten Nutzern und etlichen hundert angeschlossenen Arbeitsplatzrechnern. Bei einigen Organisationen gibt es alleine aufgrund dieser Größenordnung keine Alternative zu DCE, denn Konkurrenzprodukten fehlt eine ausreichende Skalierbarkeit. Die Client-Systeme sind bei fast allen Installationen äußerst heterogen, neben diversen kommerziellen Unix-Varianten müssen inzwischen meist auch die Microsoft-Plattformen (Windows 3.x/9x/NT), Linux-PCs und MacOS-Systeme bedient werden. Dabei können über Gateway-Lösungen auch Systeme eingebunden werden, für die keine direkte DCE/DFS-Unterstützung besteht. Insgesamt zeigt sich auf jeden Fall, dass die Administration einer DCE-Zelle in der Regel mit vergleichsweise geringen Personalressourcen vorstatten gehen kann.

Für die restliche Zeit des Workshops waren Vorträge zu speziellen Themengebieten angesetzt. Im Rahmen des Schwerpunkts „Systemintegration“ berichtete Jürgen Hölter über die an der Universität Münster besonders intensiv vorangetriebene Integration von Standardanwendungen (vor allem sendmail, IMAP- und POP-Server, Apache Web-Server mit Web-Anwendungen) in DCE/DFS. Daniel Mallman vom Forschungszentrum Jülich dokumentierte seine Erfahrungen mit der neu verfügbaren Kerberos-Integration von Unix-Kommandos. Dies ist mit Hinblick auf die Tatsache, dass die DCE-Security-Server seit Version 1.2.2 als sogenannte „Key Distribution Center“ (KDC) für Kerberos fungieren können, besonders interessant. Ralf Utermann und Markus Zahn berichteten über die Möglichkeiten zur Einbindung nicht DCE/DFS-fähiger Client-Plattformen und die in diesem Zusammenhang an der Universität Augsburg verfolgte Strategie. Unter anderem steht dort die Einbindung von Linux-PCs über eine PAM/NSS-Lösung unmittelbar vor der

Fertigstellung.

Unter dem Themenbereich „Administrative Delegation“ vermittelte Dieter Mack von der Universität Hohenheim, wie unter Beibehaltung der Systemsicherheit die Verwaltung von DFS-Servern delegiert werden kann. Der Beitrag vermittelte dabei sowohl den technischen Hintergrund als auch die spezielle Vorgehensweise zur konkreten Einrichtung der File-Server. Jochen Hollman erläuterte das sogenannte Chips-Projekt der Chalmers Universität aus Schweden. Von der Motivation bis zu detailreichen technischen Ausführungen wurde das spezielle Konzept zur Delegation komplexer administrativer Aufgabenstellungen dargestellt. Roland Laifer von der Universität Karlsruhe gab den Teilnehmern im Rahmen seines Vortrags „DCE/DFS Troubleshooting“ eine Fülle von hilfreichen Tips und Tricks zur Fehlersuche und Fehlerbehebung. Gerhard Rentschler von der Universität Stuttgart lieferte einige interessante Ausführungen zu LDAP und seinen möglichen Auswirkungen auf DCE.

Schließlich wurden einige Projekte vorgestellt, die auf DCE/DFS aufbauen. Dabei gab Stefan Ost von der Universität Münster einen Überblick über das Projekt „Rechnerverbund-NRW“, bei dem versucht wird, mittels DCE/DFS eine Hochleistungsrechner-Infrastruktur für Nordrhein-Westfalen zu etablieren. Jens Rosenhan von der MB&T GmbH gab einen interessanten Einblick in die betreuten Projekte im DCE/DFS-Umfeld und konnte insbesondere aufzeigen, dass DCE/DFS nicht nur im akademischen Bereich verbreitet ist, sondern dass auch bekannte, große Unternehmen auf diese systemübergreifende Technologie setzen.

Alles in allem kann man festhalten, dass die zahlreichen interessanten Beiträge zu einer gelungenen Veranstaltung geführt haben, was auch an vielen angeregten Diskussionen erkennbar war. Es wurde beschlossen, künftig über Mailing-Listen noch engeren Kontakt zu halten, um doppelte Entwicklungen gleicher Lösungen zu verhindern und um den Erfahrungsaustausch zu forcieren. Schließlich wurde der nächste DCE-Workshop bereits für den Spätsommer 2000 an der Universität Hohenheim verabredet. Sämtliche Vorträge des vergangenen Workshops sind unter der URL

<http://www.RZ.Uni-Augsburg.DE/DCE/ws-99/>

online abrufbar.

Auditorium des Augsburger DCE-Workshops



Die IV-Versorgungseinheiten der WWU

W. Bosse

Die IV-Versorgungseinheiten der WWU sind die Basiszellen der IV-Versorgung der Universität. Inzwischen ist eine gewisse Konsolidierung bei der Etablierung der Organisationsstrukturen dieser Einheiten erkennbar. Da die IVVen als primäre Ansprechpartner für IV-Probleme in den Fachbereichen gelten, geben wir hier unseren Kenntnisstand vom 24. 2. 2000 wieder.

| IV-Versorgungseinheiten | Fachbereiche | Leitung |
|---|---|--|
| 01 Geisteswissenschaften http://www.uni-muenster.de/IVV1/ IVV-Hotline: 24611 | 08, 09, Sprachen- zentrum | Peter Kollenbrandt IV-Versorgungseinheit 1 Englisches Seminar Bispinghof 20 Johannisstr. 12-20 ☎ 24612 Fax 28353 ☎ 29294 Fax 25616 📧 kollenb@ves101.uni-muenster.de |
| 02 Wirtschaftswissenschaften http://www.uni-muenster.de/IVV2/ Service-Tel. (BWL/VWL): 22947, 28364, 22738 Service-Tel. (WI): 38222, 38223 ivv-wiwi@wiwi.uni-muenster.de | 04 | Akad. Dir. Dr. Jan-Armin Reepmeyer Betriebliche Datenverarbeitung Universitätsstr. 14-16 ☎ 22948 Fax 22984 📧 reepmey@uni-muenster.de |
| 03 Rechtswissenschaften http://www.uni-muenster.de/IVV3/ ivv-jura@uni-muenster.de | 03 | AOR Dr. Ulrich Weber-Steinhaus IV-Versorgungseinheit – FB 03 Bispinghof 24/25 ☎ 29912 Fax 21202 📧 steinhu@uni-muenster.de |
| 04 Naturwissenschaften (ohne Geowissenschaften) http://www.uni-muenster.de/IVV4/ | 11, 12, 13 | Leitungsgremium: Dr. Wolfgang Zierau (Vorsitzender) Institut für Theoretische Physik II – Festkörperphysik Wilhelm-Klemm-Str. 10 ☎ 33589 Fax 33669 📧 zierau@nwz.uni-muenster.de |
| 05 Mathematik und Psychologie http://www.uni-muenster.de/IVV5/ IVV-Hotline (FB 07): 31357 support@psy.uni-muenster.de IVV-Hotline (FB 10): 33754 support@math.uni-muenster.de | 07, 10 (zzt. ohne Sportwissen- schaft) | AOR Dr. Ludger Becker Institut für Informatik Einsteinstr. 62 ☎ 38441 Fax 33755 📧 beckelu@math.uni-muenster.de |
| 06 Geowissenschaften und Geographie http://www.uni-muenster.de/IVV6/ support@ivvgeo.uni-muenster.de | 14 | AR Dr. Torsten Prinz IV-Versorgungseinheit Geowissenschaften Robert-Koch-Str. 26 ☎ 30015 Fax 39763 📧 prinz@uni-muenster.de |

| IV-Versorgungseinheiten | Fachbereiche | Leitung |
|--|--------------|---|
| <p>07 Theologie, Erziehungs- und Sozialwissenschaften http://www.uni-muenster.de/IVV7/</p> <p>Service-Tel. (FB01): 22553 edv-fb1@uni-muenster.de Service-Tel. (FB02): 22668 fb02edv@uni-muenster.de Service-Tel. (FB06): 24214 goden@uni-muenster.de Service-Tel. (FB06-SOWI): 21314 grimmh@uni-muenster.de</p> | 01, 02, 06 | <p>Matthias Goden (Geschäftsführung) Institut für Allgemeine Erziehungswissenschaft Georgskommende 25 ☎ 24214 Mobil 0171/7608726 Fax 21224 ✉ goden@uni-muenster.de</p> |
| <p>08 Medizinische Einrichtungen http://www.uni-muenster.de/IVV8/</p> <p>VME-Hotline: 48092 SMI-Hotline: 58403</p> | 05 | <p>IV-Leitungsgruppe: Prof. Dr. Ulrich Prokosch (Vorsitzender) Institut für Med. Informatik und Biomathematik Domagkstr. 9 ☎ 55263 Fax 55277 ✉ uprokos@uni-muenster.de</p> |
| <p>09 Universitätsverwaltung http://www.uni-muenster.de/IVV9/</p> | UniV | <p>Hans-Joachim Peter Dezernat 6.3 Schloßplatz 2 [Dienstgebäude: Röntgenstr. 19] ☎ 22262 Fax 28318 ✉ Dez63.Peter@uni-muenster.de</p> |
| <p>10 Universitäts- und Landesbibliothek http://www.uni-muenster.de/IVV10/</p> <p>ulbmail@uni-muenster.de</p> | ULB | <p>Friedhelm Komoßa Universitäts- und Landesbibliothek Krummer Timpen 3-5 ☎ 24083 Fax 28398 ✉ komosa@uni-muenster.de</p> |
| <p>Zentrum für Informationsverarbeitung Koordinierungsstelle ZIV und IVVen http://www.uni-muenster.de/ZIV/</p> <p>ZIVline: 31600 ziv@uni-muenster.de</p> | ZIV | <p>RD Walter Bosse Zentrum für Informationsverarbeitung Röntgenstr. 9-13 [Dienstgebäude: Einsteinstr. 60] ☎ 31561 Fax 31553 ✉ bosse@uni-muenster.de</p> |

Mangelnde Sicherheit von WWW-Programmen

R. Perske

Beim Zugang zum World Wide Web gefährden viele Programmier- und sonstige Fehler in verschiedenen WWW-Programmen die Sicherheit Ihrer Daten.

In den letzten Jahren, Monaten und Wochen wurde in den bekannten WWW-Programmen *Netscape Communicator* und *Microsoft Internet Explorer* eine unübersehbar große Anzahl an Programmierfehlern gefunden. Die meisten dieser Fehler führen nur zu gelegentlichen Störungen und Abstürzen. (Das kennt man ja leider von fast jeder modernen Software.)

Einige dieser Fehler stellten jedoch erhebliche Sicherheitsprobleme dar. Diese könnten von Unbefugten dazu genutzt werden, Ihnen gravierenden Schaden zuzufügen – alleine schon dadurch, dass Sie eine von Angreifern gestaltete WWW-Seite betrachten oder eine von Angreifern an Sie geschickte E-Mail anschauen! Glücklicherweise sind erst wenige solcher Angriffe bekannt geworden.

Selbst das Bundesamt für Sicherheit in der Informationstechnik warnt in einer Pressemitteilung vom 01.10.1999 vor den Implementierungen von *ActiveX*, *JavaScript* und *Java* in den Browsern *Microsoft Internet Explorer* und *Netscape Communicator*!

In den letzten Monaten war die Häufigkeit dieser Fehler derartig schlimm, dass wir von der Nutzung der Programme *Microsoft Internet Explorer* und *Netscape Communicator* abraten mussten. Mittlerweile scheint sich die Situation zu stabilisieren, so dass wir Ihnen die Nutzung dieser Programme wieder empfehlen können, falls Sie die weiter unten gegebenen Sicherheitshinweise beachten.

Die nachfolgenden Informationen, Hinweise und Zitate sind nach bestem Wissen und Gewissen zusammengestellt, trotzdem sind Irrtümer, Fehler, Missverständnisse, Unvollständigkeiten und unentdeckte Gefahrenquellen nie ganz auszuschließen.

Erste dringende Empfehlung:

- **Verwenden Sie immer die neueste Version!**
- **Lesen Sie regelmäßig die Sicherheitshinweise des Herstellers!**

Die Hersteller der Programme bemühen sich, bekannt gewordene Sicherheitsprobleme zügig zu beseitigen, zumindest gilt dies für die englische Programmversion, und veröffentlichen entsprechende Sicherheitshinweise (siehe bei Netscape die Web-Seite <http://home.netscape.com/security/index.html>, bei Microsoft die Seite <http://www.microsoft.com/windows/ie/security/default.asp>, ...).

Um nicht auf die vielen bekannten Fehler hereinzufallen und um unnötigen Risiken aus dem Weg zu gehen, sollten Sie daher die neueste Programmversion installieren und danach regelmäßig (etwa alle 14 Tage) die Sicherheitshinweise des Herstellers lesen und befolgen.

Wenn Sie dies befolgen, brauchen Sie vor den Sicherheitslöchern in früheren JavaScript- und Java-Implementierungen keine Angst mehr zu haben. (Es gibt jedoch weitere Sicherheitslöcher, die weiter unten beschrieben sind.)

Alternativ-Empfehlung für „Update-Muffel“:

- **Schalten Sie JavaScript und Java aus!**

Wenn Sie nicht bereit sind, sich um die neueste Programmversion und regelmäßig (etwa alle 14 Tage) um die Sicherheitshinweise der Hersteller zu kümmern – weil Ihnen das zuviel Arbeit macht oder aus welchem Grund auch immer –, dann sollten Sie jedoch unbedingt JavaScript und Java ausschalten und akzeptieren, dass manche WWW-Seiten dann nicht mehr richtig funktionieren.

Denn viele Versionen der WWW-Browser enthalten gerade in diesen Komponenten teilweise gravierende Fehler, wie aus den in der WWW-Version dieses Artikels (<https://www.uni-muenster.de/WWW/Sicherheit.html>) gesammelten Quellen hervorgeht, und es werden immer wieder neue Fehler gefunden.

Zweite dringende Empfehlung:

- **Schalten Sie ActiveX und VBScript aus!**

Der Microsoft Internet Explorer und andere Programme mit *ActiveX* enthalten ein massives, inhärentes Sicherheitsproblem, wenn Sie das Downloading *aktiver Inhalte*, also von Programmen erlauben, da diese mit voller Kontrolle über Ihren Rechner ablaufen, also wirklich alles machen können. Diese Probleme können, falls vom Programm vorgesehen, durch Deaktivierung von *ActiveX* bzw. von *Download active contents* umgangen werden. Im Vergleich dazu laufen Java-Programme in einer „Sandkiste“, können also – solange diese „Sandkiste“ sauber programmiert ist – keinen Schaden anrichten. Auf der angegebenen WWW-Seite finden Sie auch Quellen mit weiteren Hinweisen zu den Gefahren von *ActiveX*.

Das ebenfalls nur in Microsoft-Produkten enthaltene *VBScript* ist nur unwesentlich sicherer.

Daher sollten Sie *ActiveX* und *VBScript* immer ausschalten. Dazu müssen Sie in den Sicherheitseinstellungen des Microsoft Internet Explorer die Sicherheitsstufe auf „hoch“ einstellen und außerdem in den erweiterten Einstellungen an verschiedenen Stellen *Active Scripting* ausschalten.

Weitere Empfehlungen und Hintergrundinformationen:

- **Führen Sie niemals fremde Programme aus!**
- **Installieren Sie ein Virenschutzprogramm!**
- **Aktualisieren Sie wöchentlich die Virenerkennungstabellen Ihres Virenschutzprogramms!**
- **Speichern Sie niemals Passwörter auf Ihrem Rechner ab!**
- **Schalten Sie SmartBrowsing aus!**

Leider gibt es mit WWW-Programmen einige weitere, nicht ganz so gravierende Gefahrenquellen, auf die nachfolgend eingegangen werden soll. Auch auf die oben genannten Komponenten wird noch einmal mit weiteren Erläuterungen eingegangen.

Viren, Würmer und trojanische Pferde

Durch das geringste unvorsichtige Handeln können Sie sich sehr leicht *Viren*, *Würmer* und *trojanische Pferde* einfangen. Diese haben erst einmal nichts mit dem WWW zu tun; in allen drei Fällen handelt es sich allgemein um unerwünschte Programme, die sich in Ihrem System einnisten und für irgendwelchen Schaden sorgen.

Die drei Programmarten unterscheiden sich durch die Art der Vermehrung: *Viren* verändern vorhandene Programme (auch solche zum Laden des Betriebssystems im *Bootsektor* von Disketten und Festplatten) und werden aktiv, sobald das Wirtsprogramm ausgeführt wird. *Würmer* sind eigenständige Programme, die sich über das Netz verbreiten und auf dem Zielrechner unter Ausnutzung von Sicherheitslöchern automatisch aktivieren können. *Trojanische Pferde* tarnen sich als nützliche Programme, die bereitwillig vom Nutzer ausgeführt werden, in Wirklichkeit aber Schaden anrichten. Häufig werden alle drei Programmarten gemeinsam als *Viren* bezeichnet.

Grundsätzlich gibt es eine ganz einfache Regel, um sich vor solchen *Viren* zu schützen:

- **Führen Sie niemals fremde Programme aus!**

Dabei müssen Sie alle Programme, die Sie aus dem WWW herunter laden oder per E-Mail zugeschickt bekommen, als fremde Programme betrachten, denn Sie wissen ja nicht, ob diese mit einem *Virus* infiziert oder ein *trojanisches Pferd* sind.

(Auch Microsoft-Word-Dokumente und Microsoft-Excel-Tabellen sind ausführbare Programme. Öffnen Sie daher niemals Word-Dokumente oder Excel-Tabellen, die Ihnen von Dritten zugeschickt wurden. Die derzeit verbreitetsten *Viren* sind *Makro-Viren*, die sich in Word-Dokumenten verstecken.)

In der Praxis ist diese Forderung häufig undurchführbar. Daher sollten sie wenigstens dafür sorgen, dass eingedrungene Viren entdeckt und unschädlich gemacht werden, bevor sie

Schaden anrichten können:

- **Installieren Sie ein Virenschutzprogramm!**

Vergessen Sie nicht, dabei dafür zu sorgen, dass jedes ausgeführte Programm – dazu gehören auch *Plugin*-Programme, Word-Dokumente usw. – vor Verwendung durch das Schutzprogramm überprüft wird.

Da fast täglich neue *Viren* auftauchen:

- **Aktualisieren Sie wöchentlich die Virenerkennungstabellen Ihres Virenschutzprogramms!**

Das Zentrum für Informationsverarbeitung gibt das Virenschutzprogramm *MacAfee VirusScan* von NAI einschließlich aller Aktualisierungen kostenlos an alle Universitätsangehörigen weiter (vgl. den Artikel über „VirusScan“ in diesem [inforum](#)).

Passwörter

An verschiedenen Stellen benötigen Sie Passwörter, um auf Internetdienste zuzugreifen, sei es zur Einwahl bei Ihrem Internetprovider, sei es zum Abholen oder Versenden von E-Mail, sei es zum Zugriff auf News-Foren. In fast allen Fällen wird Ihnen Ihr Rechner anbieten, die Passwörter abzuspeichern, damit Sie sie nicht jedesmal wieder eintippen müssen.

Mit dem Abspeichern setzen Sie diese Passwörter jedoch besonderen Gefahren aus: Jeder, der Zugriff zu Ihrem Rechner erlangt, seien es Familienangehörige, Freunde und Bekannte, seien es Angreifer, die ein auf Ihren Rechner gelangtes *Virus* ausnutzen, kann Ihre Passwörter auslesen und für seine eigenen Zwecke missbrauchen.

Aus aktuellem Anlass weisen wir darauf hin, dass in letzter Zeit häufiger Passwörter gestohlen wurden. Meist waren die Rechner der Diebstahlopfer durch *Viren* und *trojanische Pferde* wie *BackOrifice*, *SubSeven* usw. infiziert, in Einzelfällen waren enge Bekannte die Täter.

Die Passwörter wurden dann ausgenutzt, um bei der Begehung von Straftaten die Identitäten der Diebstahlopfer vorzuschieben. Einige dieser Diebstahlopfer bekamen dann als dieser Straftaten Verdächtige unangenehmen Besuch von Polizei und Staatsanwaltschaft; dabei kam es zur Beschlagnahme der Rechner und sogar zu vorläufigen Festnahmen.

- **Speichern Sie niemals Passwörter auf Ihrem Rechner ab!**

Cookies

Cookies sind kleinere Datensätze, die von einem WWW-Server auf Ihrem Rechner abgelegt werden und danach bei jedem weiteren Zugriff auf diesen WWW-Server wieder zu diesem übertragen werden.

Mit *Cookies* sind grundsätzlich keine Angriffe auf Ihren Rechner möglich, außer bei Programmierfehlern.

Cookies sind eine praktische Hilfe, um beispielsweise Warenkörbe in elektronischen Kaufhäusern oder Ähnliches zu programmieren.

Jedoch ermöglichen *Cookies* den Betreibern von WWW-Servern, personenbezogene Daten ohne Ihr Einverständnis derart auf Ihrem Rechner zu speichern, dass Ihr WWW-Browser diese Daten zukünftig immer wieder an diese und sogar an gewisse andere WWW-Server schickt, ohne dass Sie darüber informiert werden.

Seit einiger Zeit haben sich sogar viele Firmen in Ringen zusammengeschlossen, indem sie eine gemeinsame Komponente (meist ein Bildchen) von einem zentralen WWW-Server laden. Dies ermöglicht den angeschlossenen Firmen, alle jemals an eine dieser Firmen übermittelten Daten automatisch zusammenzuführen und so ein perfektes Persönlichkeitsprofil von Ihnen zu erstellen.

Im Gegensatz zu den Beschwichtigungen vieler Firmen werden diese Möglichkeiten intensiv genutzt, siehe beispielsweise die aktuellen Presseberichte über die Absichten der amerikanischen Firma *DoubleClick*, einem Betreiber eines solchen *Cookie Rings*.

Wenn Ihnen das nicht gefällt, sollten Sie überlegen, ob Sie *Cookies* nicht grundsätzlich

ausschalten und nur bei Bedarf einschalten wollen. Außerdem sollten Sie die Dateien, in denen Ihr WWW-Programm langlebige *Cookies* ablegt, von Zeit zu Zeit löschen. Bei Netscape finden Sie eine Datei mit dem Namen *cookies.txt* o. ä. meist im Netscape-Installationsverzeichnis, bei Microsoft meistens ein ganzes Verzeichnis.

JavaScript

JavaScript ist eine von Netscape entwickelte und von anderen Herstellern kopierte Sprache für in WWW-Seiten eingebettete Anweisungen, beispielsweise für dynamische optische Effekte. Zwar ähneln *JavaScript*-Anweisungen äußerlich der nachfolgend beschriebenen Programmiersprache *Java*, es handelt sich jedoch um völlig verschiedene Dinge.

Mit *JavaScript* sind grundsätzlich keine Angriffe auf Ihren Rechner möglich, außer bei Programmierfehlern.

Leider gab es viele solcher Programmierfehler, daher sollte man unbedingt wie oben empfohlen immer die neueste Programmversion einsetzen oder aber *JavaScript* ausschalten.

Achtung: Bei einigen Versionen des *Netscape Communicator* ist es aufgrund eines Programmierfehlers erforderlich, *JavaScript* nach jedem Programmstart erneut ein- und wieder auszuschalten, um es zu wirklich zu deaktivieren, man kann sich auf die Anzeige in den Einstellungen nicht verlassen.

Java

Java ist grundsätzlich erst einmal eine vollwertige Programmiersprache wie viele andere Programmiersprachen auch. Sie wurde jedoch besonders mit Blick auf sichere Verwendung im Internet entwickelt. *Java Applets* (Programme), die über das Internet geladen wurden, besitzen nur sehr eingeschränkten Zugriff auf das eigene System.

Mit *Java* sind grundsätzlich keine Angriffe auf Ihren Rechner möglich, außer bei Programmierfehlern.

Leider gab es viele solcher Programmierfehler, daher sollte man unbedingt wie oben empfohlen immer die neueste Programmversion einsetzen oder aber *Java* ausschalten.

Ein unabhängiger Überblick über *Java*-Fehler wird von der Princeton University unter <http://www.cs.princeton.edu/sip/history/index.php3> angeboten, weitere Hinweise zur Sicherheit von *Java* veröffentlicht der *Java*-Entwickler Sun Microsystems unter <http://www.javasoft.com/sfaq>.

ActiveX

ActiveX gibt es nur für den Microsoft Internet Explorer. *ActiveX* ist ein ähnlicher Mechanismus wie *Java*, es fehlen jedoch die ganzen Sicherheitsvorkehrungen von *Java*. *ActiveX Controls* besitzen daher vollen Zugriff auf das eigene System. Zwar gibt es einen Mechanismus, der mittels Zertifikaten dafür sorgen soll, dass *ActiveX Controls* nur dann zur Ausführung gebracht werden, wenn sie von vertrauenswürdigen Programmierern stammen, dieses Konzept enthält jedoch grundlegende Schwächen.

Daher sollte man niemals *ActiveX Controls* vertrauen und wie oben empfohlen immer *ActiveX* ausschalten.

VBScript

VBScript gibt es nur für den Microsoft Internet Explorer. *VBScript* ist ähnlich gefährlich wie *ActiveX*. Daher sollte man wie oben empfohlen immer *VBScript* ausschalten.

JScript

JScript ist die Microsoft-Implementierung von *JavaScript*. Zwar gibt es Unterschiede zwischen *JScript* und *JavaScript*, aber in Sicherheitsbelangen sind sich beide Sprachen

ähnlich.

Daher sollte man unbedingt wie oben empfohlen immer die neueste Programmversion einsetzen oder aber *JScript* ausschalten.

SmartBrowsing

Bei *SmartBrowsing* werden die Adressen sämtlicher von Ihnen besuchter WWW-Seiten an einen zentralen WWW-Server übermittelt. Angeblich soll dieser Server nur dazu dienen, Ihnen anschließend Vorschläge zu machen, welche anderen WWW-Seiten ähnliche oder weiterführende Informationen anbieten. Diese Daten können jedoch auch ausgenutzt werden, um besonders einfach ein Persönlichkeitsprofil von Ihnen zu erstellen.

Da dieser Server sich in den USA befindet, greifen dort nicht die strengen deutschen Datenschutzgesetze.

- **Schalten Sie daher *SmartBrowsing* aus!**

Verschlüsselung

Grundsätzlich werden alle Daten im Internet unverschlüsselt übertragen, können also mit teilweise nur geringem Aufwand abgehört werden. Solange Sie nur WWW-Seiten abrufen, die sowieso für jedermann zugänglich sind, spielt das keine große Rolle.

Kritisch wird es jedoch, wenn Sie persönliche Daten in Formularfelder eintragen und an WWW-Server übermitteln, beispielsweise Kreditkartennummern, Kontonummern, Transaktionsnummern, Passwörter usw. Dann sollten Sie darauf achten, dass die Daten verschlüsselt übertragen werden.

Im WWW kann nur vom Server festgelegt werden, ob Daten verschlüsselt übermittelt werden. Die meisten WWW-Browser können Sie jedoch warnen, falls Sie im Begriff sind, Daten unverschlüsselt zu übermitteln, so dass Sie die Übermittlung abbrechen können. Sie sollten überlegen, diese Warnfunktion einzuschalten.

Die WWW-Programme beherrschen unterschiedliche Verschlüsselungsstärken. 40-Bit-Verschlüsselungen sind mit guten Rechnern in Minuten zu knacken, 128-Bit-Verschlüsselungen kann man derzeit als absolut sicher betrachten. Erst seit wenigen Wochen dürfen WWW-Programme mit 128-Bit-Verschlüsselung aus den USA exportiert werden. Falls Sie Netscape- oder Microsoft-Produkte benutzen, sollten Sie daher auch aus diesem Grunde auf die neueste Version umsteigen. Opera-Produkte beherrschen schon länger die 128-Bit-Verschlüsselung.

Weiterführende Quellen

Weitere Informationen finden Sie auf den im Auftrag des Bundesministeriums für Wirtschaft und Technologie zusammengestellten WWW-Seiten zum Thema Sicherheit in der Informationsgesellschaft (<http://www.sicherheit-im-internet.de/>) sowie auf den Seiten des Bundesamtes für Sicherheit in der Informationsverarbeitung (<http://www.bsi.de/>).

Auch das *World Wide Web Consortium* veröffentlicht Fragen und Antworten zur Sicherheit im WWW (<http://www.w3.org/Security/Faq/>).

Technische Möglichkeiten zur Sicherung der IV

Das ZIV hat in sehr komprimierter Form ein umfassendes Papier erstellt, das sich vorrangig an System- und Netz-Spezialisten wendet und ihnen einen Überblick über technische Möglichkeiten zur Sicherung der IV in die Hand gibt.

Dieser Entwurf ist mit Vertretern aller Hochschulrechenzentren des Landes NRW, des Bundesamtes für Sicherheit in der Informationsverarbeitung in Köln und des DFN-CERT in Hamburg abgestimmt und vervollständigt worden. Es ist in der Ausgabe für Münster in

<http://www.uni-muenster.de/ZIV/Hinweise/SicherungIV.html> abrufbar. Dieses Papier dient derzeit auch als Grundlage, um zusammen mit den IV-Versorgungseinheiten die Sicherheit der IV in der WWU deutlich zu verbessern. Außerdem liegt eine „Prüfliste für ein Sicherheitskonzept der IV“ unter <http://www.uni-muenster.de/ZIV/Hinweise/SicherungIV-Checkliste.html>.

Baumaßnahmen im Gebäude Einsteinstraße

H. Pudlatz

Kein Aprilscherz – wer liest schon am Samstag sein inforum?

Seit einigen Wochen ist das alte Rechenzentrumsgebäude in der Einsteinstraße 60 eingerüstet. Lange haben die Planungen gedauert, die zu einer Reihe von Veränderungen im alten Gebäude führen werden. Eigentlich war das erst 1968 bezogene Gebäude schon Anfang der 70-er Jahre zu klein geworden, so dass schon damals an die Eröffnung einer ersten Dependence gedacht werden musste. Weitere Rechenzentrumsadressen waren in über 30 Jahren Rechenzentrumsgeschichte der Schlossplatz, die Hüfferstraße, die Schlaunstraße, die Hittorfstraße, der Bispinghof, der Orléansring und die Röntgenstraße.



Schön wäre es somit gewesen, wenn das Gebäude Einsteinstraße 60 um weitere drei Stockwerke hätte erhöht werden können, um alle Mitarbeiter und Geräte aus dem Gebäudekomplex Röntgenstraße 9-13 wieder an die alte Stelle zurückzuführen – die derzeitige Einrüstung scheint diesen Trugschluss nahe zu legen. Statt dessen dient das Gerüst derzeit nur dazu, das Flachdach zu reparieren, womit die Hoffnung verbunden ist, dass es bei einigen Kollegen nicht mehr durch die Decke auf den Schreibtisch tropft. Die leider sehr unansehnliche Glasfront, die Fassadenverkleidung und die undichten Fenster (verantwortlich für so manche Wintergrippe!) werden erst in einer späteren Umbauphase erneuert werden – wahrscheinlich nicht vor Ablauf von zwei Jahren.

Für die noch in diesem Jahr vorgesehenen Baumaßnahmen wird das Gerüst nicht mehr benötigt. Das Kellergeschoss, das früher im wesentlichen die Klimaversorgung beherbergte, wird nun einem anderen Verwendungszweck zugeführt. Es wird die Server aus dem Erdgeschoss aufnehmen, so dass im Erdgeschoss nur der Nutzerschalter, die Druckperipherie, die DFÜ-Einrichtungen und der Ausgabebereich verbleiben. Der Großteil der frei werdenden Fläche wird als Nutzerarbeitsbereich ausgebaut. Der Eingangsbereich wird nach rechts verlegt, um dort einen behindertengerechten Zugang mit einem entsprechend vergrößerten Fahrstuhl zu installieren.

WWWplot

E. Sturm

Endlich kann man Bilder anschauen und drucken (auch Poster), ohne etwas von ftp und Unix zu verstehen – nur einen WWW-Browser muss man bedienen können.

Nach der im letzten inforum vorgestellten Änderung des `plot`-Kommandos (u. a. werden bestimmte Windows-Treiber-Fehler einfach ignoriert) wurde die Zahl der mir bekannt gewordenen Probleme zwar deutlich geringer – geblieben aber war die archaische Methode mittels `ftp`-Dateitransfer und Unix-Dialog. Für die meisten Nutzer war es mehr ein mechanisches Eintippen von Kommandos nach Rezept als eine logische Abfolge von Eingaben. Hier hat sich etwas getan:

Zusätzlich zum alten Weg gibt es jetzt einen, den jeder Computer-Nutzer kennen sollte, nämlich über einen WWW-Browser (z. B. Netscape). Voraussetzung ist ein Browser, der das Hochladen von Dateien unterstützt. Bei manchen älteren Produkten ist das leider nicht der Fall.

Wenn Sie auf der WWW-Startseite des ZIV suchen, werden Sie auf einen Punkt „Drucken im ZIV“ stoßen, der Ihnen die Möglichkeit bietet, „Drucken eines lokalen Bildes auf einem zentralen Drucker“ anzuklicken – oder so ähnlich, WWW-Seiten ändern sich ja schnell.

Das Programm, das Sie bedient (hoffentlich nicht umgekehrt), heißt `WWWplot`. Als erstes werden Sie gebeten, Kennung und Passwort einzugeben. Hier handelt es sich um die üblichen Unix-Dinge, die auch z. B. beim Abholen von E-Mail einzugeben sind. Es soll ja kein anderer auf Ihre Kosten (bzw. die Ihres Instituts) Papier, Farbe und Rechenzeit verbrauchen können.

Danach kann es dann losgehen. Auf der zweiten WWW-Seite können Sie angeben, um welche Bilddatei es sich handelt und was mit ihr geschehen soll. 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. `WWWplot` verarbeitet aber nur PostScriptDateien. Solche werden sichtbar, wenn Sie „Alle Dateien (*.*)“ anklicken. Der schließlich ausgewählte Dateiname erscheint dann im Eingabefeld der `WWWplot`-Seite.

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

- das Bild anschauen,
- als Papierbild ausdrucken auf Farblaserdrucker,
- als Folie ausdrucken auf Farblaserdrucker,
- als Poster auf Großformatdrucker ausgeben (standardmäßig von A4 nach A0 skalieren).

Nutzen sollten Sie auf jeden Fall den (voreingestellten) ersten Punkt. Wenn Sie auf „Weiter“ klicken, wird Ihre lokale Bilddatei auf einen zentralen Server übertragen, dieselbe in das GIF-Format übersetzt, zurückübertragen und in Ihrem Browser dargestellt. Auf dem Server wird dasselbe Programm aufgerufen wie ggf. später beim Drucken, nämlich GhostScript. Zzt. sehen Sie bei Bildern, die größer als DIN A4 sind, nur die linke untere Ecke.

Danach haben Sie wieder ähnliche Auswahlmöglichkeiten wie eben. 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 `WWWplot` drehen lassen und schauen, wie es dann aussieht. Hilft auch das nicht weiter, so wende man sich bitte an mich (s. u.).

Der nächste Auswahlpunkt leitet Ihre Bilddatei auf unseren Farblaserdrucker, zzt. ein Xerox 5760. Als Sonderwünsche stehen zur Verfügung:

1. Bitte das Bild um 90° drehen!

2. Bitte das Bild auf einem A3-Blatt drucken!
3. Bitte das Bild von A4 auf A3 vergrößern!
4. Bitte xx Exemplare drucken (zwischen 1 und 99)!

Die Punkte 2 und 3 sollten nicht verwechselt werden. Wenn Sie den Wunsch äußern, Ihr Bild auf einem A3-Blatt zu drucken, wird es nicht skaliert! Bei Punkt 3 wird es natürlich nicht nur skaliert, sondern auch auf einem A3-Blatt gedruckt.

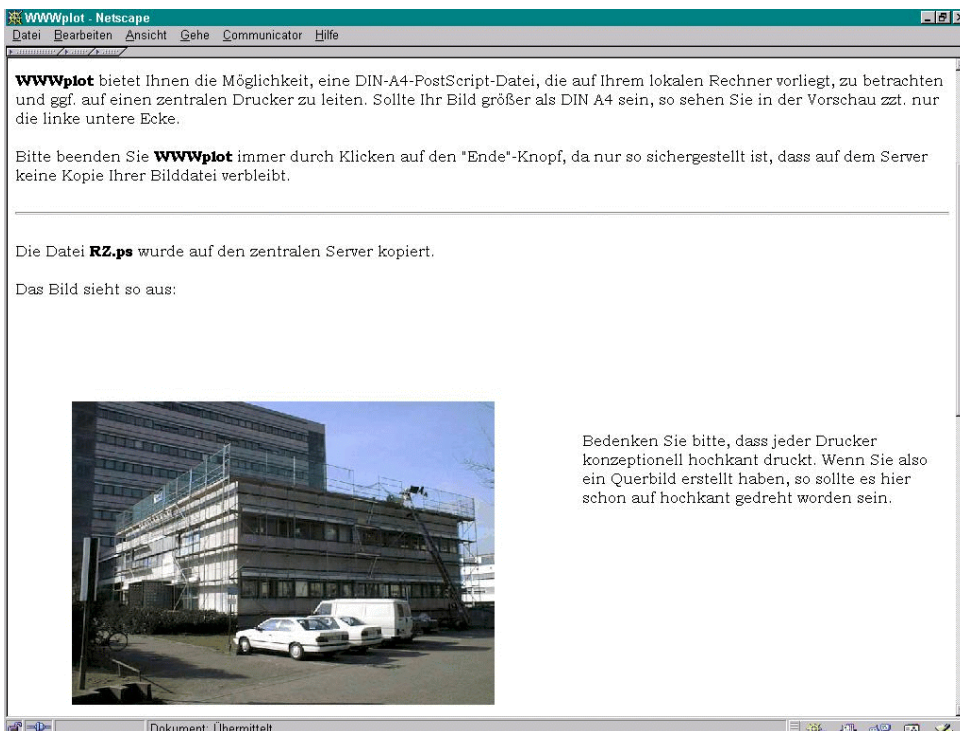
Wenn Sie eine Folie auf dem Farblaserdrucker ausgeben wollen, gibt es nur den Sonderwunsch, es gedreht zu bekommen. A3-Folien gibt es nicht, und mehrere Exemplare sind i. d. R. sinnlos.

Wenn Sie ein Poster auf dem Großformatdrucker (zzt. HP DesignJet 2500 CP) ausgeben möchten und keinen Sonderwunsch äußern, geht WWWplot davon aus, dass es sich um ein A4-Bild handelt, dass auf A0 vergrößert werden soll. Der normale Weg zum Posterdruck sollte nämlich sein:

- Erstellen einer DIN-A4-PostScript-Bilddatei,
- Anschauen mit WWWplot, ob alles in Ordnung ist,
- bei einem neu zu erstellenden Bild Probedruck auf dem Farblaserdrucker,
- Ausgabe auf dem Posterdrucker mit automatischer Vergrößerung.

So verwundert es also nicht, dass wir für alle Anwendungsfälle (A4/A3-Papier, Folie, Poster) nur einen Druckertreiber vorschlagen: Xerox MajestiK with Fiery RIP XJ (oder so ähnlich, je nach Betriebssystem).

Wenn Sie etwas anderes vorhaben, etwa sofort ein A0-Bild zu erstellen, müssen Sie den Weg über „Sonderwünsche“ gehen und angeben, welches Format ihr Originalbild hat und welche Größe es auf dem Papier haben soll.



Sollten Sie etwas falsch gemacht haben, so erschrecken Sie bitte nicht über die Fehlermeldung in rot. Sie verschwindet, wenn Sie den nächsten Aktionsknopf angeklickt haben. Falls jemand mit einer DaWIN-Kennung (also nicht mit einer Instituts-kennung) zu plotten versucht, sieht er sofort, dass er das nicht darf.

Theoretisch können Sie bei einem Browser jederzeit Schluss machen oder sich eine andere WWW-Seite anschauen. Bei WWWplot 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.

Falls es Sie interessiert, wie WWWplot realisiert wurde, so schauen Sie doch mal bei www.php3.de nach. Es handelt sich um PHP 3.0, eine Programmiersprache für in HTML eingebettete Programme. Bei Problemen mit WWWplot oder weiteren Wünschen wende man sich bitte an mich (☺ sturm@uni-muenster.de, ☎ 31679).

Fingerabdrücke

R. Perske

Dieser Beitrag enthält die aktuellen kryptografischen Prüfsummen der öffentlichen Schlüssel, die vom Zentrum für Informationsverarbeitung verwendet werden.

Die PGP-Schlüssel der Mitarbeiter des ZIV finden Sie im WWW zusammen mit den PGP-Schlüsseln verschiedener Zertifizierungsinstanzen unter der Adresse

<http://www.uni-muenster.de/ZIV/Mitarbeiter/zivring.asc>.

Die Prüfsumme des öffentlichen PGP-Schlüssels der Zertifizierungsstelle im ZIV lautet:

```
2048/EF750F1D 1997/10/14 Rainer Perske +49(251)83-31582 Certification Key
Key fingerprint = 2F 38 6E F8 DC 2E D8 5E 5B 35 DB 49 8A E4 52 AF
```

Alle öffentlichen PGP-Schlüssel der Mitarbeiter des Zentrums für Informationsverarbeitung sind mit diesem Schlüssel zertifiziert.

Folgende Zertifikate sind widerrufen, weil die E-Mail-Adresse nicht mehr gültig ist:

```
1024/17817C39 1997/09/01 Manfred Sand <sand@uni-muenster.de>
1536/7870F29D 1999/05/21 Martin Schlütz <schlutz@uni-muenster.de>
```

Folgende Schlüssel sind auf Wunsch des Eigentümers widerrufen; bitte markieren Sie diese Schlüssel in Ihrem Schlüsselring als ungültig (bei PGP 2 mit `pgp -kd 0x8A2097A5` usw., bei PGP 5 und 6 mit dem Kontextmenüpunkt *Disable*):

```
1024/8A2097A5 1997/06/13 Rainer Perske <perske@uni-muenster.de>
1024/D726DB95 1998/03/11 Guido Wessendorf <wessend@uni-muenster.de>
2048/914AD795 1999/03/17 Dr. Wilhelm Held <held@uni-muenster.de>
2048/4F643FF5 1999/05/26 Rita Sieber <siebert@uni-muenster.de>
2048/5F108685 1999/05/26 Dany Born <born@uni-muenster.de>
```

Die Prüfsummen der SSL-Zertifikate der zentralen WWW-Server lauten:

```
www.uni-muenster.de:
Zentrum für Informationsverarbeitung
Nr. 54 (0x36), gültig bis Sep 5 07:47:56 2001 GMT
Fingerprint=59:91:5A:A4:30:81:FA:12:56:4A:8E:10:01:C1:D5:DB
```

```
user.uni-muenster.de:
Universitätsrechenzentrum
Nr. 16 (0x10), gültig bis Dec 17 15:48:16 2002 GMT
Fingerprint=4F:D7:42:05:05:AA:EE:80:FF:35:C7:B4:53:09:6C:1F
```

Auf Anfrage zertifiziere ich auch WWW-Server und andere SSL-Server. Als Herausgeber wird dabei eingetragen: Rainer Perske, perske@uni-muenster.de, Universitätsrechenzentrum, Westfälische Wilhelms-Universität, Münster, Germany, DE.

Anders als bei PGP-Schlüsseln, die ich nur gegen Vorlage eines Ausweises zertifiziere, führe ich bei SSL-Servern jedoch nur eine minimale Plausibilitätskontrolle durch und halte mich an keine vorgegebenen Richtlinien. Die Ausstellung des Zertifikats hat den einzigen Zweck, den Betreibern der WWW-Server verschlüsselte Datenübertragung zu ermöglichen, ohne dass sie gleich viel Geld an irgendwelche Firmen überweisen müssen.

Wenn ein Server hier genannt wird, bedeutet dies nur, dass ich ein noch gültiges Zertifikat für den Server ausgestellt haben, jedoch nicht, dass der Server läuft oder für andere als interne Zwecke des jeweiligen Instituts verwendet wird.

```
mail.uni-muenster.de:
Universitätsrechenzentrum
Nr. 14 (0xe), gültig bis Dec 17 14:03:35 2002 GMT
Fingerprint=91:73:A4:91:77:A0:CD:5A:BF:22:AD:C0:FE:5A:3D:67
```

```
user.uni-muenster.de:
Zentrum für Informationsverarbeitung
Nr. 24 (0x18), gültig bis Oct 3 15:37:01 2001 GMT
MD5 Fingerprint=7D:31:D4:5A:38:10:6F:9E:4C:32:AE:42:D3:23:92:09
```

```
wwwunix.uni-muenster.de:
Zentrum für Informationsverarbeitung
Nr. 29 (0x1d), gültig bis Apr 29 15:02:13 2000 GMT
MD5 Fingerprint=52:0D:67:00:1D:F7:FB:BE:1E:C5:2F:DA:B0:85:AA:2E
```

```
winkiosk.uni-muenster.de:
```

Zentrum fuer Informationsverarbeitung (Rechenzentrum)
 Nr. 31 (0x1f), gültig bis May 24 13:59:23 2000 GMT
 MD5 Fingerprint=0C:6E:A3:94:F5:71:60:2F:45:B3:20:D4:04:23:C0:1B

www.wi.uni-muenster.de:
 Institut für Wirtschaftsinformatik
 Nr. 33 (0x21), gültig bis Jun 17 10:58:29 2000 GMT
 MD5 Fingerprint=0B:C8:0D:1F:24:6C:51:A3:9E:74:28:3E:2B:DB:D9:FD

pcwi003.uni-muenster.de:
 Systemadministration WI
 Nr. 46 (0x2e), gültig bis Jun 17 11:02:22 2000 GMT
 MD5 Fingerprint=04:75:54:CD:E8:C5:F1:8B:8F:3E:D7:16:BA:41:51:76

wwwzuv.uni-muenster.de:
 ZUV - Datenverarbeitung
 Nr. 47 (0x2f), gültig bis Jun 24 08:12:58 2000 GMT
 MD5 Fingerprint=76:C0:0B:DA:6F:33:3F:AE:51:14:41:A3:1C:59:5C:29

news.uni-muenster.de:
 Zentrum für Informationsverarbeitung
 Nr. 48 (0x30), gültig bis Jul 1 16:04:56 2000 GMT
 MD5 Fingerprint=CF:96:CA:3E:AE:21:C4:C4:21:FD:2D:4F:FD:FF:9A:C5

redenix.uni-muenster.de:
 Zentrum für Informationsverarbeitung
 Nr. 49 (0x31), gültig bis Jul 5 14:34:01 2000 GMT
 MD5 Fingerprint=BA:A9:E5:C4:B7:ED:27:98:06:89:94:20:2D:EE:E8:20

ec.uni-muenster.de:
 Westfaelische Wilhelms-Universitaet
 Nr. 50 (0x32), gültig bis Aug 3 16:17:44 2000 GMT
 MD5 Fingerprint=55:BA:5C:F6:94:BC:EE:7B:8D:89:F8:5C:CB:AC:1A:01

aberfix.uni-muenster.de:
 Universitäts- und Landesbibliothek
 Nr. 51 (0x33), gültig bis Aug 29 15:56:00 2000 GMT
 MD5 Fingerprint=CF:17:2A:53:D9:99:08:1C:18:2C:06:95:7F:D6:E3:81

wwuweb01.uni-muenster.de:
 Zentrum fuer Informationsverarbeitung (Rechenzentrum)
 Nr. 52 (0x34), gültig bis Aug 30 14:46:18 2000 GMT
 MD5 Fingerprint=FB:52:97:3A:9F:59:5C:72:29:27:98:ED:49:0E:55:52

sisis-i.uni-muenster.de:
 Universitäts- und Landesbibliothek
 Nr. 53 (0x35), gültig bis Aug 30 15:49:34 2000 GMT
 MD5 Fingerprint=02:2E:4F:A0:75:38:81:E9:1D:A4:E8:77:EB:67:39:FB

wi-2b.uni-muenster.de:
 Institut fuer Wirtschaftsinformatik
 Nr. 55 (0x37), gültig bis Sep 20 14:57:56 2000 GMT
 MD5 Fingerprint=57:88:5C:B0:03:AF:05:54:41:E4:8B:6C:BE:CC:B7:47

zuvbestc.uni-muenster.de:
 Verwaltung
 Nr. 56 (0x38), gültig bis Dec 16 16:12:45 2000 GMT
 MD5 Fingerprint=82:46:64:FC:60:69:6F:B7:EC:0B:5C:42:CB:82:F1:53

suchfix.uni-muenster.de:
 Universitäts- und Landesbibliothek
 Nr. 57 (0x39), gültig bis Jan 2 17:36:36 2001 GMT
 MD5 Fingerprint=98:6D:2E:7F:D3:91:97:38:93:6C:92:3E:18:7F:CC:34

suchfix2.uni-muenster.de:
 Universitäts- und Landesbibliothek
 Nr. 58 (0x3a), gültig bis Jan 2 17:37:48 2001 GMT
 MD5 Fingerprint=38:C8:C9:BD:6F:04:C6:BD:F1:F6:72:DA:E6:4D:22:63

Eine vollwertige Zertifizierungsstelle sowohl für PGP-Schlüssel als auch für SSL-Schlüssel im Rahmen der DFN-Zertifizierungshierarchie befindet sich im Aufbau. Die Schlüsseldaten werden im nächsten [infoRUM](#) veröffentlicht.

Deponierung großer Datenmengen: Ein neues HSM-Dateisystem

R. Mersch

Depotix heißt der Rechner, auf dem ein neues HSM-Dateisystem zur Speicherung großer Datenmengen bereitgestellt wurde.

Auf dem Rechner Backup existiert seit geraumer Zeit das hierarchische Dateisystem `/home/hsm1`. Es handelt sich dabei um ein Dateisystem, das von einem HSM (*Hierarchical Storage Manager*) verwaltet wird. Dieser HSM, eine Funktion des ADSM, verschiebt Dateien zum ADSM-Server (Migration) und bemüht sich so darum, in dem Dateisystem stets genügend Platz frei zu halten. Dem Benutzer wird dabei vorgegaukelt, dass sich die Dateien noch im Dateisystem befinden; erfolgt ein Zugriff auf eine Datei, so wird sie automatisch vom ADSM-Server zurückgeholt.

`/home/hsm1` beherbergt mittlerweile 435 GB Daten und hat damit eine Größe erreicht, bei der es beginnt unhandlich zu werden. Es stellt ferner eine ziemliche Belastung des Rechners Backup dar, auf dem sich auch unser ADSM-Server befindet. Um zusätzliche Belastungen dieses Rechners zu vermeiden, wurde darauf verzichtet, einen abhörsicheren Zugang via `ssh` (*Secure Shell*) einzurichten, der aber wegen der Passwort-Problematik zunehmend gewünscht wird.

Aus diesen Gründen wurde nun zusätzlich ein neues HSM-Dateisystem auf einem separaten Rechner eingerichtet. Es heißt `/home/hsm2` und befindet sich auf dem Rechner Depotix. Der `ssh`-Zugang zu diesem Rechner ist möglich, d. h. die Dateien können mittels `scp` (*secure copy*) transferiert werden.

Jeder Benutzer muss in der ersten Sitzung ein eigenes Verzeichnis anlegen, dessen Name der Benutzerkennung entspricht. Weitere Informationen zur Nutzung finden sich weiter unten. Folgendes sollte unbedingt beachtet werden:

- Da von jeder Datei ein 4 KB großer Rest (das sog. Stubfile) im Dateisystem verbleibt, sollte die Anzahl der Dateien klein gehalten werden. Will man viele kleine Dateien deponieren, so sollte man diese nach Möglichkeit zunächst mittels eines geeigneten Werkzeugs, wie z. B. `zip`, `tar` oder `VMS backup`, zu einer Container-Datei zusammenfassen.
- Die maximale Dateigröße beträgt 1 GB.
- Da die Migration nur zu bestimmten Zeitpunkten stattfindet, kann es vorkommen, dass im HSM-Dateisystem temporär kein Platz mehr frei ist. Man sollte daher jeden Dateitransfer auf erfolgreiche Beendigung überprüfen.

Das alte HSM-Dateisystem `/home/hsm1` auf Backup sollte für neue Daten möglichst nicht mehr genutzt werden. Es soll im Laufe des Jahres ebenfalls nach Depotix verschoben werden. Dieses wird um so einfacher, je weniger Daten sich darin befinden. Bitte löschen Sie daher alle Dateien, die nicht mehr benötigt werden. Eine Verschiebung noch benötigter Dateien in das neue HSM-Dateisystem ist aber vom Aufwand her nicht zu rechtfertigen; von Ausnahmefällen abgesehen sollte darauf verzichtet werden.

Nutzung des HSM-Dateisystems auf Depotix via FTP

Zur Erzeugung des eigenen Verzeichnisses geht man (mittels des vom Prinzip her unsicheren `ftp`-Programms) wie folgt vor, was hier beispielhaft für den Benutzer `mersch` erläutert wird:

```
ftp depotix
```

Man beantwortet die anschließenden Fragen nach Benutzerkennung (`mersch`) und Passwort (`verratichnicht`), und erzeugt dann sein Verzeichnis, dessen Name der Benutzerkennung entsprechen muss:

```
cd /home/hsm2
mkdir mersch
cd mersch
```

Bei späteren Sitzungen kann man nach Sitzungseröffnung natürlich direkt in das Verzeichnis wechseln:

```
cd /home/hsm2/mersch
```

Nun können mittels `put` und `get` wie üblich Dateien übertragen werden. Einige weitere wichtige FTP-Kommandos sind:

```
rmdir dir
```

Verzeichnis `dir` löschen

```
rename file1 file2
```

Datei `file1` in `file2` umbenennen

```
delete file
```

Datei `file` löschen

```
quote site chmod 600 file
```

Zugriffsrechte für die Datei `file` setzen (nur der Eigentümer darf lesen und schreiben, dies ist die Voreinstellung bei FTP-Zugang)

```
quit
```

FTP-Sitzung beenden

Abhörsichere Nutzung des HSM-Dateisystems auf Depotix via scp

Zum Kopieren der Datei `beispieldatei.tar` in das Verzeichnis des Benutzers `mersch` bedient man sich des folgenden (abhörsicheren) Kommandos:

```
scp beispieldatei.tar mersch@depotix:/home/hsm2/mersch
```

Umgekehrt geht es entsprechend:

```
scp mersch@depotix:/home/hsm2/mersch/beispieldatei.tar
```

Die übrigen Aktionen können via `ssh` bewerkstelligt werden, z.B.:

```
ssh depotix mkdir /home/hsm2/mersch
```

Verzeichnis erstellen

```
ssh depotix dls /home/hsm2/mersch
```

modifiziertes `ls`, das auch über den Zustand der Dateien Auskunft gibt
(m: migriert, r: resident)

```
ssh depotix mv /home/hsm2/mersch/file1 /home/hsm2/mersch/file2
```

Datei umbenennen

```
ssh depotix rm /home/hsm2/mersch/file
```

Datei `/home/hsm2/mersch/file` löschen

```
ssh depotix chmod g+r /home/hsm2/mersch/file
```

Zugriffsrechte für die Datei `file` setzen (auch die Gruppe darf lesen)

RUM-Tutorial

Einsatz von Smartkarten in Betrieben, Hochschulen und Ämtern (2)

W. Bosse, W. Held, H.-W. Kisker

Im ersten Teil in der inforum-Ausgabe Nr. 3/1999 ging es um den Sicherheitsaspekt beim Einsatz von Smartkarten. Im abschließenden zweiten Teil soll der mögliche praktische Einsatz vorgestellt werden.

Für Smart-Karten lassen sich in Hochschulen – aber auch in Betrieben und Behörden – leicht zahlreiche Anwendungen angeben, was im Folgenden geschehen soll. Es ist aber ausdrücklich darauf hinzuweisen, dass Smart-Karten auch viele Anwendungen gestatten, über die noch gar nicht nachgedacht wurde. Hier lässt sich also auch Neuland betreten.

Studierenden- und Bediensteten-Ausweis

Äußerlich lassen sich die Karten farbig bedrucken, z. B. mit dem Foto des Karteninhabers und seinem Namen oder mit Barcodes für die Buchausleihe. Auch sich halbjährlich ändernde Semestereinträge sind möglich, wobei spezielles Material verwendet werden kann, auf dem vor einem neuen Druckvorgang zunächst der alte Aufdruck gelöscht wird. Wenn an die Beschriftung besondere Sicherheitsanforderungen gestellt werden, können z. B. Hologramme, IUV-Belichtungen oder spezielle Kunststoffzusammensetzungen verwendet werden. Wenn auf der Oberfläche noch Platz bleibt, kann dieser für Werbung verwendet werden, damit die Karten preiswerter werden.

Für viele Anwendungen sind allerdings die in den Smart-Chips eingespeicherten Informationen, welche die Karten zum Ausweis machen, von Bedeutung. Zum Glück kommt man dabei mit ganz wenigen Informationen zur Identifizierung des Inhabers aus. Man muss nicht mehr – wie vor Jahren üblich – vollständige Anwendungen auf der Karte unterbringen. Vielmehr genügen Informationen, die zu einem Computer-Login ausreichen. Das kann z. B. eine Benutzer-Kennung zusammen mit einem langen Passwort sein. Oder – und das würden wir vorschlagen – es werden ein privater und ein öffentlicher Schlüssel für ein asynchrones Verschlüsselungsverfahren auf der Karte erzeugt. Der öffentliche Schlüssel wird von der Zertifizierungsstelle der Universität zertifiziert. Eine PIN ergänzt diese Information noch, damit ein Dritter die Karte nicht ohne weiteres missbrauchen kann. Mit Hilfe des Schlüsselpaares kann man sich nun bei Computer-Systemen und Computer-Anwendungen legitimieren und einen gesicherten Zugang erreichen. Aus Gründen der Bequemlichkeit kann man noch den öffentlichen Schlüssel der Zertifizierungsstelle unterbringen, damit man sich diesen nicht erst umständlich besorgen muss.

Wenn nur die beschriebenen Identifikationsmerkmale auf der Smart-Karte gespeichert sind, gibt es mit der Karte keine Datenschutz-Probleme, selbst dann nicht, wenn man aus Gründen der Einfachheit noch eine Matrikel- bzw. Mitarbeiternummer und die Version der Karte zusätzlich speichert.

Der Bezug zwischen Information auf und in der Karte und dem Karteninhaber wird von der Personalisierungsstelle der Universität hergestellt. Dazu verwendet die Personalisierungsstelle Rechner mit entsprechender Software und Peripherie. Hard- und Software sind als Sicherheitsmodule ausgelegt. Für die Beschriftung der Karte sind zur Erfassung der Daten u. a. Scanner und digitale Kameras und zum Beschriften Drucker erforderlich.

Die Zertifizierung erfolgt durch besonders vorbereitete und gesicherte Stellen.

Technik des Zugangs zu IV-Anwendungen

Um den Zugang zu IV-Anwendungen, die oft von vielen verschiedenen Stellen (in der WWU z. B. von der Verwaltung, von Fachbereichen und zentralen Einrichtungen) eingerichtet sind, von allen Arbeitsplätzen im Betrieb (oder in der WWU) und von zu Hause aus zu ermöglichen, sind die Benutzerkennungen und Benutzerverwaltungen zu vereinfachen.

Die Personalisierungsdaten und die Schlüssel zur Kryptographie reichen – wie schon gesagt – für den Zugang zu allen anderen IV-Anwendungen aus. Die Smart-Karte dient dabei als sicherer „Schlüssel“ für den Zugang zu den Anwendungen.

Die Smart-Karte kann nach Abschluss des Studiums beliebig im Besitz des Inhabers bleiben. Die Zahlfunktion (s. u.) und die Zertifizierung der Schlüssel können weiterhin genutzt werden. Der Zugang zu den Anwendungen wird einfach über die entsprechenden Datenbanken gesperrt.

Der Zugang zu IV-Anwendungen sollte in der Regel über WWW-Seiten gesteuert werden.

An folgende Anwendungen kann man denken:

- Bezahlen in der Mensa, Bibliothek und in anderen Einrichtungen der WWU,
- Gesicherter Zugang zu vertraulichen, personenbezogenen Daten im Studierendensekretariat, in Prüfungsämtern, zu Klausurergebnissen, zu Studienbescheinigungen,
- Studierendenausweis,
- Zugang zu CIP-Pools auch außerhalb der regulären Öffnungszeiten.

Aus der Sicht der IV wird, wenn alle Computer mit Kartenlesern ausgestattet sein werden, die Sicherheit der IV beim Zugang zu den vernetzten Computer-Systemen deutlich verbessert. Das dient dem Schutz der Daten und damit aller Nutzer.

Zahlungsfunktion

Smart-Karten sind in vielen Varianten für Zahlungen nutzbar. Von den Banken/Sparbanken wird dazu eine ZKA-Zulassung erwartet (ZKA = Zentraler Kreditausschuss¹). Die Smart-Karte muss außerdem eurofähig sein. Zahlungen sind in Zukunft direkt vom eigenen PC aus möglich. Dann sind – wie heute noch üblich – keine teuren Spezialleser erforderlich, viel mehr können die viel preiswerteren Kartenleser am eigenen PC genutzt werden.

Für elektronische Zahlungen sind derzeit noch viele Varianten im Umlauf. Es gibt multifunktionale Kartenleser, die die verschiedenen Zahlungsvarianten lesen können, natürlich jeweils entsprechende Software vorausgesetzt.

Zahlungsvarianten (stichwortartig):

- EC/Electronic Cash: PIN über Magnetstreifen oder Chip abfragen, meistens Offline-Zahlung, Zahlungsgarantie durch Kartenausgeber gegen Gebühren, keine Unterschrift für Geldtransfer, in Zukunft auch ohne PIN mit Verschlüsselung
- EC/PoS: (Point of Sale), keine Zahlungsgarantie, keine PIN-Eingabe, aber Unterschrift des Kunden; Gebühren nur, wenn Sperrabfrage zur Gültigkeitsdauer erfolgt
- ELV: Elektronische Lastschrift, Magnetstreifen, Lastschrift wird erstellt und an Bank geschickt, Kunde unterschreibt, keine Zahlungsgarantie, keine Gebühren, keine Online-Aktion
- Maestro-Karten: aus der ganzen Welt, PIN, Online, Gebühren, keine Unterschrift
- EC/Geldkarte: Beträge bis 400 DM, Chip aufladbar, offline, Gebühren an Kartenausgeber, EC-Karte mit Chip oder kontoungebundene Karte, Geldkarten werden auch als White-Karten bezeichnet. Die Geldkarte muss nach ZKA zugelassen sein.
- Kreditkarten (VISA, MC, ...): Separater Vertrag mit jeder Gesellschaft, Vergleich durch Unterschrift

¹ Das Design der ZKA-Karte stammt von der GAD in Münster, dem Rechenzentrum der Raiffeisen-Genossenschaften und Volksbanken.

Zahlungsfunktionen in der Universität

Auch in der Universität sind an verschiedenen Stellen Zahlungen zu leisten: in der Bibliothek, in der Mensa, für die Erzeugung von Druck- und Plot-Ausgaben, für Chemikalien, für die Rückmeldung usw.

Wenn sich eine Universität nicht auch noch als Bank betätigen will, kann sie die Funktion der Geld-Karte nutzen, die auch von Banken für den Zahlungsverkehr verwendet wird.

Es sollte bei der Konzeption der Smart-Karte für einen Betrieb oder die WWU und deren Funktionalität die Entwicklung der EC-Karte beachtet werden. Diese wird zusätzlich zur Geldkarte bis etwa 2002 mit Signatur-Funktionalitäten gemäß deutschem Signaturgesetz ausgerüstet (Platz für betriebseigene Zusatzanwendungen wird ebenso verfügbar sein!). Um Aufwand und Kosten zu reduzieren, sollte ein Stufen- bzw. Migrationskonzept erstellt werden, so dass später auf diese Standardkarte umgestiegen werden kann. Diese Karte wird dann ZKA-abgestimmt und für Studierende verfügbar sein, die nicht ein Konto bei einer bestimmten Sparkasse/Bank besitzen, mit der das Unternehmen oder die Universität zusammenarbeitet.

Die Sicherheit der Zahlfunktion wird nach dem HBCI-Standard (Home Banking Computer Interface, HBCI Version 2.1 ist verabschiedet) auf Basis von asymmetrischer RSA/DES-Verschlüsselung hergestellt. Alle Banken und Sparkassen in Deutschland haben sich zum Angebot des Zahlungsverkehrs auf der Basis von HBCI verpflichtet. HBCI Version 2.1 kann über das Internet geladen werden, dies kann unter

<http://www.zdnet.de/news/artikel/1999/06/01009-wf.htm>
nachgelesen werden.

Zahlungen können damit auch über unsichere Netze erfolgen. Damit ist Geld-Transfer zu und zwischen verschiedenen Banken/Sparkassen möglich. Es gibt bei Verwendung des Standards keine Beschränkung mehr auf einzelne Anbieter von Karten oder Kartenlesern oder der notwendigen Software. Selbst die PIN ist dann für den Zahlungsverkehr nicht mehr erforderlich.

Für den Zahlungsverkehr werden benötigt: Eine Bank/Sparkasse mit HBCI, Software für den Kunden, das sogenannte Kundenprodukt (z. B. StarMoney für Sparkassen) sowie die Registrierung und Freischaltung der Kundenschlüssel.

Die Gebühren für Clearing, Software und Karten-Kosten mit Kryptoprozessor sind mit den Banken/Sparkassen zu verhandeln. Auch die Telekom bietet z. B. HBCI mit einer eigenen Clearingstelle an.

Wenn die Gebühren für den Zahlungsverkehr für Kleinstbeträge (z. B. Drucken einzelner Seiten, Kopieren) zu groß sein sollten, kann ein Wertmarkenzähler per Software eingerichtet werden, so dass ein größerer Betrag einzahlbar und in Kleinstbeträgen ohne Bankgebühren abarbeitbar wird. Dieser Zähler kann in einer Datenbank außerhalb der Smart-Karte oder aber auf der Karte selbst untergebracht werden. Der interne Aufwand zur Abrechnung dieser Kleinstbeträge ist gegen die Clearing-Kosten aufzurechnen. Über die Smart-Karte kann man sich Software-Geld besorgen (Elektronische Wallets). Es ist allerdings nach neueren Untersuchungen unklar, ob sich dieses Software-Geld (auch als Disk-Geld) bezeichnet, durchsetzen wird, da man vermutet, dass es nur für Kleinstbeträge eingesetzt werden würde. Eine Variante stellt u. U. das Mikropayment dar, das auch mit der ZKA-Zahlungsfunktion möglich sein soll. Die Bedingungen dazu müssen aber noch geklärt werden.

Zahlungs-Funktionen außerhalb des Betriebes

Da Smart-Karten in vielen Varianten für Zahlungen geeignet sind und eine ZKA-Zulassung vorausgesetzt wird, sind Zahlungen natürlich auch außerhalb des Betriebes oder der Universität möglich.

Eine Einführung einer Smart-Karte für Studierende und Bedienstete wird der Nutzung der Karten in der umliegenden Region Auftrieb geben.

Nächste Schritte und mögliche Kooperationen

Im ZIV, im Institut für Angewandte Informatik, im Institut für Wirtschaftsinformatik sowie im Dezernat 6.3 der Universitätsverwaltung werden die in Frage kommenden Anwendungen dahingehend überprüft, ob ein Zugang zu diesen Anwendungen mit Hilfe der Smart-Karte sinnvoll ist.

Darüber hinaus laufen praktische Erprobungen der Smart-Karte. Denn Weiterentwicklungen einer neuen Technologie sind nur möglich, wenn man sie vollständig verstanden hat.

Es gibt bereits erste Verabredungen von Hochschulen in NRW über die Kooperation bei einer Einführung der Smart-Karte in ihren Hochschulen, denn fast alle Aufgaben fallen überall ähnlich an. Das ZIV ist allein schon aus Gründen der Erhöhung der Sicherheit der IV an einer schnellen Einführung der Karten interessiert.

RUM-Lehre

Lehrveranstaltungen im Sommersemester 2000

Beratung zum Lehrangebot durch Herrn W. Bosse Eine Anmeldung ist nur für diejenigen Lehrveranstaltungen erforderlich, die nachfolgend besonders gekennzeichnet sind.
jeweils Di, Do 11-12,
Tel. 83-31561

| | | |
|---------------|---|--|
| 260087 | Kommunikation und Information im Internet ¹ Do 13-15 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 13.4.2000 | Mertz, K.-B. |
| 260091 | Programmieren in C++ Mi 13-15 Hörsaal: M4, Beginn: 12.4.2000 | Mersch, R. |
| 260106 | Programmieren in Fortran Fr 9-11 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 28.4.2000 | Reichel, K. |
| 260110 | Programmieren in Pascal unter Delphi ¹ Di 14-16 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 18.4.2000 | Pudlatz, H. |
| 260125 | Einführung in grafische Anwendungssysteme Mi 11-13 Hörsaal: M4, Beginn: 12.4.2000 | Sturm, E. |
| 260130 | Statistische Datenanalyse mit dem Programmsystem SPSS ¹ Di 9-11 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 11.4.2000 | Zörkendörfer, S. |
| 260144 | Einführung in Unix Mo 15-17 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 17.4.2000 | Grote, M. |
| 260159 | Linux und Web-Server ¹ Mi 15-17 Hörsaal: Raum 107, Einsteinstr. 60, Beginn: 19.4.2000 | Neukäter, B. |
| 260163 | Windows NT und Windows 2000 Server (für Fortgeschrittene) ¹ Do 14-16 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 20.4.2000 | Kamp, M./ Lange, W. |
| 260178 | System-Administration für Linux-Systeme (für Fortgeschrittene) ¹ Blockveranstaltung vom 13.6. bis 16.6.2000, ganztägig Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 13.6., 9 Uhr | Hölters, J./ Ost, S. |
| 260182 | Rechnernetze: Technische Grundlagen Do 10-12 Hörsaal: Raum 206, Röntgenstr. 13, Beginn: 20.4.2000 | Richter, G./ Speer, M./ Wessendorf, G. |
| 260197 | Kolloquium des Zentrums für Informationsverarbeitung Fr 14-16 Hörsaal: Raum 206, Röntgenstr. 13 | Held, W. |

¹ Wegen der Begrenzung der Teilnehmerzahl ist für diese Veranstaltung eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung erforderlich.

Kommentare zum Lehrangebot

260087 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 praktischen Übungen gezeigt, 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 Befehle `dir`, `cd`, `mkdir`, `del` usw. dienen.

260091 Programmieren in C++

C++ erweitert die Programmiersprache C mit ihren durch Assembler-ähnliche Sprach-elemente einerseits und Elemente moderner blockstrukturierter Sprachen andererseits sehr vielseitigen Einsatzmöglichkeiten um objektorientierte Konzepte. Diese Verbindung einer sehr erfolgreichen Programmiersprache mit einem seit einigen Jahren boomenden Programmier-Paradigma macht C++ zu einer der, wenn nicht sogar zu der am meisten benutzten Programmiersprache(n).

In der Lehrveranstaltung wird C++ gemäß dem 1998 erschienenen ISO/ANSI-Standard von Grund auf vorgestellt. Kenntnisse einer anderen Programmiersprache wären hilfreich, werden aber nicht vorausgesetzt.

STROUSTRUP: *Die C++ Programmiersprache, dritte Auflage*, Addison-Wesley

260106 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

260110 Programmieren in Pascal unter Delphi

Die auf Object Pascal basierende Programmierumgebung Borland Delphi 4.0 erlaubt es, mit einfachen Mitteln Windows-Programme für die 32-Bit-Betriebssysteme Windows 95 und Windows NT zu entwerfen.

Wie schon das bewährte Turbo Pascal desselben Herstellers erzeugt der Delphi-Compiler schnellen und kompakten Code. Die anwenderfreundliche grafische Benutzeroberfläche unterstützt die von den Vorgängersystemen her vertraute objektorientierte Programmierung mit Werkzeugen, die die Windows-, Datenbank- und Internet-Programmierung erleichtern.

Die Veranstaltung wendet sich an Programmieranfänger, die von Anfang an die Eleganz der strukturierten und objektorientierten Programmierung in einer Windows-Umgebung

kennenlernen und einsetzen wollen. Dabei soll zur Vertiefung des Gelernten zu praktischen Übungen angeregt werden. Wegen der damit verbundenen Begrenzung der Teilnehmerzahl ist eine Anmeldung am Service-Schalter des Zentrums für Informationsverarbeitung erforderlich.

260125 Einführung in grafische Anwendungssysteme

In der Veranstaltung werden am Universitätsrechenzentrum verfügbare Grafikpakete vorgestellt, die dazu geeignet sind, Benutzern ohne Vorkenntnisse die Erstellung von Bildern aller Art zu ermöglichen. Der Schwerpunkt wird auf Corel Draw und den Grafik-Komponenten der Office-Pakete MS-Office, StarOffice und WordPerfect-Office liegen.

260130 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 (vom t-Test bis zur Varianzanalyse, vom Korrelationskoeffizienten bis zur Faktorenanalyse) sowie Kenntnisse der Anwendungsmöglichkeiten dieser Verfahren im jeweiligen Fachgebiet sind erwünscht und bei den praktischen Übungen von großem Nutzen.

260144 Einführung in Unix

Unix ist ein weitverbreitetes Mehrbenutzerbetriebssystem. Es ist auf Rechnern verschiedener Hersteller und unterschiedlicher Leistungsklassen ablauffähig. Damit steht dem Unix-Anwender vom Mikrorechner bis zum Großrechner die gleiche leistungsfähige und komfortable Programmier- und Arbeitsumgebung zur Verfügung. Hardware-Unterschiede der einzelnen Maschinen werden weitgehend verdeckt.

FEIG: *Unix von Anfang an*, Fischer

SCHRÖPFER: *Unix*, dtv

HECK: *Standard-Betriebssystem UNIX*, rororo

HECK: *Standard-Betriebssystem UNIX für Fortgeschrittene*, rororo

HARIG: *UNIX im Alleingang*, Springer

260159 Linux und Web-Server

Das Betriebssystem Linux oder – weitere Programme einschließlich – Gnu-Linux ist für viele Anwendungen gegenüber Windows die bessere und kostengünstigere Alternative. Wegen seiner Stabilität und der zunehmenden Verfügbarkeit qualitativ hochwertiger Anwendungsprogramme hat es in der letzten Zeit viele Nutzer überzeugt.

Gnu-Linux ist entstanden aus einer internationalen Zusammenarbeit im Internet. Die Autoren stellen die Quellprogramme zur Verfügung, ohne Lizenzgebühren zu verlangen (GPL). Firmen bieten gegen Entgelt Beratung, Wartung und Verteilung über CD-ROM an. Zahlreiche Anwendungsprogramme für Linux werden ebenfalls ohne Lizenzgebühren abgegeben und oft mit dem Betriebssystem zusammen verteilt.

Die Teilnehmer an dieser Lehrveranstaltung sollen in die Lage versetzt werden, Linux und gängige Anwendungen auf einem PC zu installieren und unter einer graphischen Oberfläche zu benutzen. Neben Textverarbeitung und Tabellenkalkulation sollen Internet-Anwendungen behandelt werden. Praktische Übungen sind vorgesehen. Besonders ausführlich besprochen und praktisch erprobt werden sollen die Installation und der

Betrieb eines Web-Servers, der es ermöglicht, eigene Publikationen im Internet zu veröffentlichen. Voraussetzung für die Teilnahme sind Erfahrung im Umgang mit dem PC und praktische Kenntnisse der Kommunikations- und Informationsdienste im Internet (E-Mail, WWW usw.). Für das im zweiten Teil der Veranstaltung behandelte Thema Web-Server wären Kenntnisse der HTML und Programmierkenntnisse vorteilhaft.

260163 Windows NT und Windows 2000 Server (für Fortgeschrittene)

In der Veranstaltung wird der Einsatz des Betriebssystems Windows NT in einer Netzwerkkumgebung vorgestellt. Vorgesehene Themen sind unter anderem: Domänenkonzept, Netzwerkdienste, Benutzerverwaltung, Sicherheit, Serverdienste (u. a. Fileserver, Printserver, Terminalserver, Webserver) sowie die wichtigsten mit Windows 2000 eingeführten Neuerungen (wie z. B. Active Directory Services).

Von den Hörern wird erwartet, dass sie über solide Grundkenntnisse der Microsoft-Betriebssysteme verfügen. Darüber hinaus ist ein uneingeschränkter Zugang (Administrator) zu einem eigenen Windows-NT-System für Übungszwecke empfehlenswert.

260178 System-Administration für Linux-Systeme (für Fortgeschrittene)

Die Vorlesung richtet sich an den fortgeschrittenen Linux-Anwender, der Unterstützung bei der Installation und System-Integration seines Linux-Systems benötigt. Die Teilnehmer werden in der Veranstaltung ein Linux-System selbst installieren und in die Netzwerk- und Systeminfrastruktur der Universität einbinden. Ferner wird demonstriert, wie man einen speziell auf die Hardware-Ausstattung des Rechners optimierten Kernel generiert.

Da voraussichtlich 6 PCs zur Verfügung stehen werden, ist die Teilnehmerzahl auf 12 begrenzt. Eine Anmeldung ist erforderlich.

260182 Rechnernetze: Technische Grundlagen

Diese Veranstaltung gibt einen Einblick in die technischen Grundlagen der Rechnervernetzung. Folgende Themen werden behandelt:

- Architekturmodell für Rechnernetze (OSI-Modell), Kommunikationsprotokolle
- Techniken für lokale Rechnernetze (LANs): Ethernet, Fast Ethernet, FDDI
- Kopplung 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
- ATM: Asynchronous Transfer Mode, VLANs: Virtuelle LANs
- neuere Entwicklungen: IPv6 (Internet Protocol Version 6), Funk-LAN, ...
- Struktur und Funktionen des Rechnernetzes der Universität Münster

Zu dieser Veranstaltung finden Sie vorlesungsbegleitende Materialien im WWW.

260197 Kolloquium des Zentrums für Informationsverarbeitung

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

RUM-Index

Stichwörter inforum Jahrgang 23

Im Index bedeutet der Verweis „23,3-13“: Jahrgang 23, Heft 3, Seite 13

| | | | | |
|--|-------------------------------|---|--|--|
| | ACL | 23,1-21 | B. Süselbeck | Vertrauen ist gut, Kontrolle ist besser (2) |
| | ATM | 23,1- 2 | H. Pudlatz | TEN-155 ging in Betrieb |
| | Axum | 23,3-12 | B. Süselbeck/ S. Zörkendörfer | Neues über Software |
| | Beratung | 23,1- 4 23,2-15 23,3- 3 | W. Held G. Richter H. Pudlatz | Zentrale Servicestelle im ZIV NIC und NOC im ZIV Guter Rat ist nicht teuer |
| | Blindenarbeitsplatz | 23,1- 9 | H. Kamp | Ein neuer Blindenarbeitsplatz |
| | Browser | 23,2- 7 | R. Perske | Automatische WWW-Proxy-Server-Konfiguration |
| | BWin | 23,1- 2 23,1- 3 | H. Pudlatz G. Richter | TEN-155 ging in Betrieb Durchsatzprobleme im Internet |
| | Compute-Server | 23,3- 7 | St. Ost | Neue Rechner zum Rechnen |
| | DCE | 23,1-21 | B. Süselbeck | Vertrauen ist gut, Kontrolle ist besser (2) |
| | DFN | 23,3-16 | | DFN-Verein vervierfacht Netzrate in die USA |
| | DFS | 23,1- 5 23,1-21 | St. Ost B. Süselbeck | Neue AIX-Server installiert Vertrauen ist gut, Kontrolle ist besser (2) |
| | Dokumentation | 23,2-14 | Unixgruppe | Online-Dokumentationen |
| | Drucker | 23,1- 5 23,1- 8 23,3-19 | H. Pudlatz H. Pudlatz E. Sturm | Druckausgabe auf zentralen Druckern Euro-Zeichen E verfügbar Änderungen beim plot-Kommando |
| | E-Mail | 23,2- 8 23,3- 6 23,3- 9 | W. Bosse W. Held/ G. Richter R. Perske | Betrieb von E-Mail-Servern im Netz der WWU Weitere Sicherungsmaßnahmen für die Informationsverarbeitung Übergroße E-Mails |
| | Exceed | 23,3-15 | M. Speer | X11-Server-Emulation mit Exceed im Universitäts-Rechnernetz |
| | Fingerabdrücke | 23,1-14 23,2-17 23,3-17 | R. Perske R. Perske R. Perske | Fingerabdrücke Fingerabdrücke Fingerabdrücke |
| | Grafik | 23,3-19 | E. Sturm | Änderungen beim plot-Kommando |
| | Höchstleistungsrechner | 23,1-18 | W. Held/ B. Neukäter u. a. | Hoch-, Höchst-, Super-, Mega-, Giga-, Meta- |
| | Internet | 23,1- 2 23,1- 3 23,2-14 23,2-19 23,2-27 23,3- 4 23,3- 9 | H. Pudlatz G. Richter R. Perske L. Donnerhacke B. Brandel W. Held/ G. Richter R. Perske | TEN-155 ging in Betrieb Durchsatzprobleme im Internet Ausbau des zentralen WWW-Servers Spuren im Netz Sichere Nutzung des World Wide Web Video-Konferenzen im Internet Übergroße E-Mails |

| | | | |
|--------------------------|---------|-------------------------------|---|
| | 23,3-10 | C. Müller-Böhm | Referenzzentrum für das neue Internet |
| | 23,3-16 | - | DFN-Verein vervierfacht Netzrate in die USA |
| IP | 23,1-16 | G. Richter | Ausschließliche Verwendung des IP-Protokolls im Rechnernetz der WWU |
| IPv6 | 23,3-10 | C. Müller-Böhm | Referenzzentrum für das neue Internet |
| Jahr-2000-Problem | 23,1-13 | H. Pudlatz | Y2K - das Jahr-2000-Problem |
| | 23,3- 3 | H. Pudlatz | Guter Rat ist nicht teuer |
| Kommunikation | 23,1- 2 | H. Pudlatz | TEN-155 ging in Betrieb |
| | 23,3- 4 | W. Held/ G. Richter | Video-Konferenzen im Internet |
| Kryptographie | 23,1-14 | R. Perske | Fingerabdrücke |
| | 23,2-17 | R. Perske | Fingerabdrücke |
| | 23,3-17 | R. Perske | Fingerabdrücke |
| LAN | 23,1-16 | G. Richter | Ausschließliche Verwendung des IP-Protokolls im Rechnernetz der WWU |
| | 23,1-17 | K.-B. Mertz | Regelungen zur Verwendung von Namen im LAN der WWU |
| | 23,2- 3 | K.-B. Mertz | Detailregelungen zur Verwendung von Namen im Datennetz der WWU |
| | 23,2- 8 | W. Bosse | Betrieb von E-Mail-Servern im Netz der WWU |
| | 23,3- 5 | M. Kamp | Terminal-Server |
| | 23,3-15 | M. Speer | Betriebsreports des Universitätsrechnernetzes |
| Lehrangebot | 23,1-27 | - | Lehrveranstaltungen im 1. Halbjahr 1999 |
| | 23,2-34 | - | Lehrveranstaltungen des ZIV |
| | 23,3-28 | - | Lehrveranstaltungen im 1. Halbjahr 2000 |
| MeDiDa-Prix | 23,3-14 | - | MeDiDa-Prix 2000 |
| Namen | 23,1-17 | K.-B. Mertz | Regelungen zur Verwendung von Namen im LAN der WWU |
| | 23,2- 3 | K.-B. Mertz | Detailregelungen zur Verwendung von Namen im Datennetz der WWU |
| NOC | 23,2-15 | G. Richter | NIC und NOC im ZIV |
| | 23,3- 3 | H. Pudlatz | Guter Rat ist nicht teuer |
| Parallelrechner | 23,1-18 | W. Held/ B. Neukäter u. a. | Hoch-, Höchst-, Super-, Mega-, Giga-, Meta- |
| plot-Kommando | 23,3-19 | E. Sturm | Änderungen beim plot-Kommando |
| Proxy-Server | 23,2- 7 | R. Perske | Automatische WWW-Proxy-Server-Konfiguration |
| Rechnernetz | 23,1- 2 | H. Pudlatz | TEN-155 ging in Betrieb |
| | 23,1- 3 | G. Richter | Durchsatzprobleme im Internet |
| | 23,1-16 | G. Richter | Ausschließliche Verwendung des IP-Protokolls im Rechnernetz der WWU |
| | 23,1-17 | K.-B. Mertz | Regelungen zur Verwendung von Namen im LAN der WWU |
| | 23,2- 8 | W. Bosse | Betrieb von E-Mail-Servern im Netz der WWU |
| | 23,2-19 | L. Donnerhacke | Spuren im Netz |
| | 23,2-27 | B. Brandel | Sichere Nutzung des World Wide Web |
| | 23,3- 5 | M. Kamp | Terminal-Server |
| | 23,3- 9 | R. Perske | Übergroße E-Mails |
| | 23,3-14 | W. Held/ G. Richter | CITYKOM-Zugang zum Rechnernetz der WWU |
| | 23,3-15 | M. Speer | Betriebsreports des Universitätsrechnernetzes |
| | 23,3-15 | M. Speer | X11-Server-Emulation mit Exceed im Universitäts-Rechnernetz |

| | | | |
|-------------------------------|--|--|---|
| | 23,3-16 | - | DFN-Verein vervierfacht Netzrate in die USA |
| Rechnerzugang | 23,3- 7 23,3-14 | K.-B. Mertz W. Held/ G. Richter | Zugang für Studierende zu den Rechnern der Fachbereiche CITYKOM-Zugang zum Rechnernetz der WWU |
| Server | 23,1- 5 | St. Ost | Neue AIX-Server installiert |
| Servicestelle | 23,1- 4 | W. Held | Zentrale Servicestelle im ZIV |
| Sicherheit | 23,2-19 23,2-27 23,3- 6 | L. Donnerhacke B. Brandel W. Held/ G. Richter | Spuren im Netz Sichere Nutzung des World Wide Web Weitere Sicherungsmaßnahmen für die Informationsver- arbeitung |
| Smart-Karte | 23,3-21 | W. Bosse/ W. Held/ H. W. Kisker | Einsatz von Smart-Karten in Betrieben, Hochschulen und Ämtern (1) |
| Software | 23,2- 8 23,3- 5 23,3-12 | H. Pudlatz M. Kamp Zörkendörfer/ B. Süselbeck | Zentrales Software-Angebot Terminal-Server Neues über Software |
| SPSS | 23,3-12 | S. Zörkendörfer/ B. Süselbeck | Neues über Software |
| Stichwörter | 23,1-22 | - | Stichwörter inform Jahrgang 22 |
| TEN-155 | 23,1- 2 | H. Pudlatz | TEN-155 ging in Betrieb |
| TEN-34 | 23,1- 3 | G. Richter | Durchsatzprobleme im Internet |
| Terminal-Server | 23,3- 5 | M. Kamp | Terminal-Server |
| TeX | 23,1-10 | W. Kaspar | TeX für Windows 95/98/NT |
| Textverarbeitung | 23,1- 8 23,1-10 23,2-16 23,3-16 | H. Pudlatz W. Kaspar W. Kaspar W. Kaspar | Euro-Zeichen E verfügbar TeX für Windows 95/98/NT Neue TUSTEP-Version Neue TUSTEP-Version 2000 |
| TUSTEP | 23,2-16 23,3-16 | W. Kaspar W. Kaspar | Neue TUSTEP-Version Neue TUSTEP-Version 2000 |
| Unix | 23,1-21 | B. Süselbeck | Vertrauen ist gut, Kontrolle ist besser (2) |
| Video-Konferenz | 23,3- 4 | W. Held/ G. Richter | Video-Konferenzen im Internet |
| Virenschutz | 23,3-12 | B. Süselbeck/ S. Zörkendörfer | Neues über Software |
| WWW-Server | 23,2-14 | R. Perske | Ausbau des zentralen WWW-Servers |
| X11 | 23,3-15 | M. Speer | X11-Server-Emulation mit Exceed im Universitäts-Rechnernetz |
| Y2K | 23,1-13 23,3- 3 | H. Pudlatz H. Pudlatz | Y2K – das Jahr-2000-Problem Guter Rat ist nicht teuer |
| ZIVline | 23,1- 4 23,3- 3 | W. Held H. Pudlatz | Zentrale Servicestelle im ZIV Guter Rat ist nicht teuer |
| Zugriffskontrolllisten | 23,1-21 | B. Süselbeck | Vertrauen ist gut, Kontrolle ist besser (2) |

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 DSGVO).

Ort, Datum

Unterschrift