



# Comment:

*Oktober 2000*

WAP – WHAT?

KRYPTOGRAPHIE

SSH – SECURE SHELL

SOFTWAREDISTRIBUTION NEU

WERDEN SIE SECURITY-EXPERTE!

## Impressum / Offenlegung gemäß § 25 Mediengesetz:

Herausgeber & Medieninhaber: Zentraler Informatikdienst der Universität Wien

Redaktion & Gestaltung: Vera Potuzak

Elisabeth Zoppoth

Adresse: Zentraler Informatikdienst der Universität Wien  
Universitätsstraße 7, A-1010 Wien

Tel.: 4277-14001

Fax: 4277-9140

eMail: COMMENT.ZID@UNIVIE.AC.AT

online: <http://www.univie.ac.at/comment/>

Druck: Riegelnik, Wien

Grundlegende Richtung: Mitteilungen des Zentralen Informatikdienstes

*Gedruckt auf chlorfrei gebleichtem Papier – Auflage 6000 Stk.*

## Ilse Hofmann gestorben



Am 25. Juli 2000 ist unsere Mitarbeiterin Ilse Hofmann völlig unerwartet in ihrem 53. Lebensjahr verstorben. Sie war in der Telefonzentrale der Universität Wien

tätig und kam somit erst zu Jahresbeginn zum ZID, als wir die Agenden der Telefonvermittlung von der Universitätsdirektion übernahmen. Ilse Hofmann trat ihren Dienst an der Uni Wien im August 1990 an und war dann acht Jahre lang für die Telefonvermittlung der medizinisch-theoretischen Institute in der Währinger Straße/Schwarzspanierstraße verantwortlich. Nach der Umstellung des dortigen Telefonsystems übersiedelte sie im Sommer 1998 ins Hauptgebäude und verstärkte das Vermittlungsteam in der Telefonzentrale. Ilse Hofmann war durch ihre ruhige und hilfsbereite Art bei allen Kolleginnen und Kollegen sehr beliebt. Umso größer war die Bestürzung über ihren viel zu frühen Tod. Wie viele Anrufer haben wohl am Telefon ihre freundliche Stimme gehört, ohne je an den Menschen dahinter zu denken? Alle, die Ilse Hofmann auch persönlich gekannt haben, werden ihr in Dankbarkeit ein ehrenvolles Andenken bewahren.

*Peter Rastl*

## Editorial

Liebe Leserin, lieber Leser!

Diese *Comment*-Ausgabe beschäftigt sich primär mit Computersicherheit: Auf Seite 2 erfahren Sie, wo Sie sich im Internet zu diesem Thema informieren können, auf Seite 20 werden die *Grundbegriffe der Kryptographie* erläutert, und auf Seite 23 wird das Netzwerkprotokoll *Secure Shell (SSH)* beschrieben, mit dem Sie Ihren Datenverkehr bei Bedarf verschlüsseln können. In diesem Zusammenhang möchten wir besonders auf unsere *Informationsveranstaltungen* (siehe Seite 36) hinweisen: Auch einige der Vorträge befassen sich mit dem Thema Security. Zusätzlich wird derzeit ein entsprechendes Informationsangebot im WWW aufgebaut (siehe <http://www.univie.ac.at/ZID/security.html>).

*Die Comment-Redaktion*

## Inhalt

### Aktuelles

- 2 Werden Sie Security-Experte!
- 4 Projekt UNIVIS macht Fortschritte
- 5 Personalnachrichten

### PCs & Workstations

- 6 Reform der Softwaredistribution
- 8 Campuslizenzvertrag mit NAG gekündigt
- 8 Neue Standardsoftware
- 9 Office-Workshop: TUn uND LasSEn, wAS Immer Man wILL

### Netzwerk- & Infodienste

- 15 eMail-Profitips
- 16 WAP – what?
- 20 Grundbegriffe der Kryptographie
- 22 Neue Software & Secure Server auf WWW.UNIVIE.AC.AT
- 23 Secure Shell (SSH): Kommunikation im Flüsterton
- 27 Secure Shell an den Außenstellen Physik & Biochemie des ZID
- 28 Wählleitungsverbindung mit Windows Millennium Edition (ME)

### Anhang

- 32 Kurse bis Jänner 2001
- 36 Informationsveranstaltungen
- 37 Öffnungszeiten
- 38 Personal- & Telefonverzeichnis
- 39 Handbücher
- 40 Ansprechpartner
- 40 Wählleitungszugänge & eMail-Adressen

# WERDEN SIE SECURITY-EXPERTE!

In letzter Zeit erscheinen im *Comment* vermehrt Beiträge, die sich mit Computersicherheit oder verwandten Themen beschäftigen (siehe auch *Informationsveranstaltungen*, Seite 36). Der Grund liegt auf der Hand: Die Attacks auf Systeme im Uni-Datennetz haben in den letzten Jahren deutlich zugenommen, und der Zentrale Informatikdienst muß infolgedessen (ebenso wie alle anderen vergleichbaren Netzbetreiber) seine Benutzer auffordern, sich mit Computersicherheit auseinanderzusetzen. Dieser Appell gilt nicht nur den Betreibern von Servern und PC-Netzwerken; auch die Benutzer von Arbeitsplatzrechnern sollten sich mit gewissen Grundbegriffen und Verhaltensweisen vertraut machen. Dieser Artikel soll dabei helfen, indem er Informationsquellen im Internet vorstellt.

Zunächst jedoch ein Wort an Neueinsteiger: Wer zum ersten Mal die langen Listen der Fehler und Schwächen all jener Betriebssysteme sieht, die sich derzeit der größten Verbreitung erfreuen, kann leicht einen Schock davontragen. Manche entwickeln sich daraufhin zu einer Art Computer-Hypochonder und vermuten hinter jeder unerwarteten Reaktion ihres Rechners einen Angriff übel gesinnter Hacker. Andere suchen ihr Heil im Glauben an die Hersteller und versuchen, jede soeben veröffentlichte Softwareänderung sofort in ihr System zu integrieren – eine Methode, die (ähnlich wie falsch dosierte Medikamente) zu einem besonders grausamen Tod des Rechners führen kann. Es braucht einiges an Erfahrung und Fingerspitzengefühl, um einen vernünftigen Mittelweg zu finden, der ein System vor den wichtigsten Bedrohungen schützt, ohne es durch den permanenten Einbau neuer, wenig getesteter Änderungen zu destabilisieren.

Noch eine weitere Hürde steht allen bevor, die sich zum ersten Mal in die Welt der Sicherheitslücken wagen: Viele

Meldungen und Beschreibungen sind auf einem technischen Niveau abgefaßt, das selbst erfahrene Systemadministratoren überfordert. **Lassen Sie sich nicht abschrecken!** Hier ist Geduld vonnöten – nach einigen Monaten versteht man meist schon deutlich mehr. Um die Details einer Sicherheitslücke zu durchschauen, benötigt man zwar oft profunde Kenntnisse von Win32-APIs, Unix-Systemcalls oder diversen Netzwerkprotokollen; üblicherweise kann man aber auch ohne dieses Wissen erkennen, worum es geht und ob das Problem für das eigene System relevant ist.

Wenn man sich intensiv mit einem Thema befassen will, wird man um die Lektüre der einschlägigen Bücher nicht herumkommen. Eine Unmenge von Informationen zur Computersicherheit bietet aber auch das Internet:

- Wer sich Grundkenntnisse aneignen möchte, findet wertvolle Informationen auf vielen Webservern sowie in den einschlägigen Newsgruppen, FAQs, HOW-TOs und anderen Dokumenten.
  - **Informationsdienste im WWW:** Im Kasten finden Sie unter *Linksammlungen für Einsteiger* eine (subjektive) Auswahl der bekanntesten Web-Portale zum Thema.
  - **Newsgruppen:** z.B. comp.risks. Weitere Security-Newsgruppen, die aber auch genauere Vorkenntnisse erfordern, finden Sie z.B. unter comp.security.
  - **FAQs** (*Frequently Asked Questions*): Die FAQs der Newsgruppen sind unter <http://ftp.univie.ac.at/archive/faq/> gesammelt. (FAQ ist übrigens laut neuem Duden nun ein Wort der deutschen Sprache.)
  - **HOW-TOs:** Unter Unix-Systemen – im speziellen unter Linux – üblich und weit verbreitet: <http://www.linuxdoc.org/> (auch mit FAQs).

## Linksammlungen für Einsteiger:

<http://www.alw.nih.gov/Security/security.html>  
<http://www.infosyssec.com/>  
<http://csrc.nsl.nist.gov/>  
<http://http.cs.berkeley.edu/~daw/compsec.html>  
[http://dir.yahoo.com/Computers\\_and\\_Internet/Security\\_and\\_Encryption/](http://dir.yahoo.com/Computers_and_Internet/Security_and_Encryption/)  
<http://www.sans.org/>  
<http://www.securiteam.com/>  
<http://www.securezone.com/>

## Alerts:

<http://www.securityfocus.com/>  
<http://www.cert.org/>  
<http://www.sans.org/>  
<http://securityportal.com/>  
<http://rootshell.com/>

<http://www.w3.org/Security/>  
<http://www.securiteam.com/>  
<http://www.ntsecurity.net/>  
<http://ntbugtraq.ntadvice.com/>

## Hersteller:

<http://www.microsoft.com/security/>  
<http://home.netscape.com/security/index.html>  
<http://www.adobe.com/support/main.html>  
<http://support.novell.com/>  
<http://www.apple.com/support/>  
<http://www.support.compaq.com/>  
<http://service.software.ibm.com/support/rs6000/>  
<http://welcome.hp.com/country/at/ger/supportservices.htm>  
<http://www.sgi.com/support/security/>  
<http://sunsolve.sun.com/>

- Technische Reports, Erfahrungsberichte, Normen und Hintergrundinformationen finden sich auf den Webseiten der Softwarehersteller, aber auch auf WWW-Servern zahlreicher unabhängiger Institutionen.
- Den wohl wichtigsten Bereich bilden jene Webseiten, Newsgruppen und Mailinglisten, die über die derzeit akuten Sicherheitsrisiken berichten (*Alert*). Wer von den aktuellen Attacken und den neuesten Viren nicht erst aus der Zeitung erfahren will, muß sich in diese Mailinglisten eintragen oder regelmäßig die entsprechenden Webseiten lesen. Selbstverständlich werden die publizierten Probleme auch in (meist Web-basierten) Archiven gesammelt.
- Zum Thema Sicherheit gibt es natürlich jede Menge Software – von Antiviren-Programmen bis zu Produkten zur Entdeckung von Eindringlingen. Wichtig ist dabei, daß man solche Programme nur von seriösen Quellen bezieht: Es gab bereits etliche Fälle, in denen Software, die eigentlich dem Schutz des Systems dienen sollte, in bösartig veränderter Form in Umlauf gebracht wurde.

## Hersteller

Mittlerweile ist es für jeden ernstzunehmenden Softwarehersteller selbstverständlich geworden, seinen Kunden via Internet technische Unterstützung zu bieten. Dies betrifft nicht nur sicherheitsrelevante Fehler – meist steht eine ganze Reihe verschiedener Services zur Verfügung:

- Meldungen über Fehler und Probleme,
- Berichte über die derzeit bekannten Sicherheitslücken (*Security Bulletins*),
- Zugang zu einer Datenbank mit technischen Informationen (*Knowledge Base*),
- die Möglichkeit, Korrekturen der Software (*Patches*, *Service Packs*) vom Server zu kopieren,
- die Möglichkeit, Mailinglisten zu „subskribieren“ (man erhält dann alle neuen wichtigen Informationen via eMail).

Die angebotenen Informationen sind meistens nach den diversen Produkten der Erzeuger gegliedert, aber auch nach Benutzerkreis. So bietet etwa Microsoft unter dem Begriff „Technet“ Unterstützung für Systemadministratoren, während sich „msdn“ (*Microsoft Developer Network*) an Programmierer von Windows-Anwendungen richtet.

## Alerts

Einen ebenso wichtigen Platz wie die Hersteller nehmen die unabhängigen Betreiber von Informationsdiensten zur Computersicherheit ein. Zwei seien besonders hervorgehoben:

- Einen guten allgemeinen Überblick mit hervorragender Suchfunktion bietet <http://www.securityfocus.com/>. Die Inhalte der Webseite werden auch über die Mailingliste „bugtraq“ (am ZID die am häufigsten verwendete Security-Mailingliste) verbreitet. Wie Sie in den Kreis der Mailempfänger aufgenommen werden, erfahren Sie ebenfalls auf der genannten Webseite.
- Nach genauer Überprüfung von neuen Meldungen werden auf der Webseite <http://www.cert.org/> all jene Sicherheitsmängel publiziert, die eine besonders große Gefahr darstellen.

Daneben behandeln auch die diversen Software-Newsgruppen die für das jeweilige System aktuellen Sicherheitsfragen.

## Viren & Hoaxes

Computerviren stellen eine eigene Art der Bedrohung dar. Untrennbar damit verbunden sind diverse Falschmeldungen (*Hoaxes*), die oft jahrelang im Netz kursieren: Diese Falschmeldungen beziehen sich häufig auf erfundene Viren, verunsichern die Benutzer und machen den Systembetreibern unnötige Arbeit. Die Produzenten von Antiviren-Software stel-

<http://www.bsdi.com/services/support/>  
<http://securityportal.com/lasg/>  
<http://www.linuxsecurity.com/advisories/>  
<http://linuxtoday.com/>  
<http://www.redhat.com/apps/support/updates.html>  
<http://www.suse.de/de/support/security/>  
<http://www.calderasystems.com/support/>  
<http://linux.corel.com/support/>  
<http://www.debian.org/support>

### Viren:

<http://vil.mcafee.com/>  
[http://www.commandcom.com/virus/virus\\_alerts.html](http://www.commandcom.com/virus/virus_alerts.html)  
<http://www.commandcom.com/virus/db/list.cfm>  
<http://www.datafellows.com/vir-info/>

<http://www.antivirus.com/vinfo/virusencyclo/default.asp>  
<http://www.avpve.com/>  
<http://www.symantec.com/avcenter/index.html>  
<http://www.sophos.com/virusinfo/>  
<http://www.cai.com/virusinfo/>

### Hoaxes:

<http://vil.mcafee.com/hoax.asp>  
<http://www.symantec.com/avcenter/hoax.html>  
<http://hoaxbusters.ciac.org/>  
[http://www.commandcom.com/virus/virus\\_hoaxes.html](http://www.commandcom.com/virus/virus_hoaxes.html)  
<http://www.datafellows.com/virus-info/hoax/>  
<http://www.icsa.net/html/communities/antivirus/hoaxes/>  
<http://www.sophos.com/virusinfo/scares/>  
<http://www.hoax-info.de/>

len Datenbanken bereit, in denen die bekannten Viren, ihr Verhalten und die Möglichkeiten ihrer Entfernung dokumentiert sind. Einige Server bieten Verzeichnisse jener „Warnungen“, die bereits als Falschmeldungen identifiziert wurden.

Zum Abschluß sei noch auf das *IT-Grundschutzhandbuch* des deutschen *Bundesamts für Sicherheit in der Informations-*

*technik* hingewiesen (<http://www.hu-berlin.de/bsi/gshb98/sonstige/titel.htm>): Das Buch zeigt, daß Sicherheit für Computer und Netzwerke mehr ist als die sorgfältige Pflege der Software – auch Bereiche wie Datensicherung, Benutzerschulung und ein sicherer Aufstellungsort sowie eine Reihe organisatorischer Aspekte sind zu berücksichtigen.

Herbert Stappler ■

## PROJEKT UNIVIS MACHT FORTSCHRITTE

Wie bereits mehrfach berichtet, soll in den nächsten Jahren die bestehende heterogene EDV-Infrastruktur der Universitätsverwaltung schrittweise durch eine moderne IT-Gesamtlösung ersetzt werden: Im Rahmen des Projekts UNIVIS wird ein integriertes Informationssystem entwickelt, das alle Bereiche der Universitätsverwaltung (operative Systeme, Managementinformation, Services für die Universitätsangehörigen) umfaßt. Die UNIVIS-Initialisierungsphase konnte im September 1999 abgeschlossen werden; dabei wurden sieben Teilprojekte – Studienwesen, Personalwesen, Finanzwesen, Materialwirtschaft, Facility Management, Work Management und Managementinformationssystem – definiert, von denen dem Teilprojekt Studienwesen die höchste Priorität zugeordnet wurde (siehe *Comment 00/1*, Seite 10).

Die Universität Wien hat daher am 29. 9. 1999 die Firma CSC Ploenzke beauftragt, als erste Phase des Teilprojekts Studienwesen ein entsprechendes Fachkonzept zu entwickeln. Bereits in der Initialisierungsphase wurde entschieden, im Studienwesen die Software i3v®-education der Firma GINIT (<http://www.ginit.de/>) einzusetzen. Die wesentlichen Aufgaben bei der Erstellung eines Fachkonzepts für das Studienwesen waren daher

- die Darstellung der relevanten Geschäftsprozesse der Universität Wien in den Bereichen Studierendenverwaltung bzw. Lehr- und Prüfungsverwaltung sowie die Schaffung eines Konsens mit den sogenannten Key Usern (erfahrene Mitarbeiter der Universitätsverwaltung) über die Abläufe dieser Geschäftsprozesse,
- die Identifizierung jener Prozesse, die mit i3v zu unterstützen sind,
- die Analyse der vorhandenen i3v-Unterstützung für diese Prozesse und die Definition der Anforderungen für einen effizienten und gesetzeskonformen Einsatz der Software,
- die Identifizierung und Dokumentation der allgemeinen Anforderungen an das Berechtigungssystem von i3v,
- die Erstellung eines Datenkatalogs, der die wesentlichen Daten aus dem Bereich Studienwesen auflistet,
- die Identifizierung und Dokumentation der wesentlichen allgemeinen Anforderungen an die Migration,
- die Erstellung eines Differenzpflichtenhefts, das alle notwendigen Änderungen gegenüber der Standardfunktionalität von i3v definiert.

Das detaillierte Geschäftsprozeßmodell wurde (aufbauend auf dem in der Initialisierungsphase erstellten groben Ge-

schäftsprozeßmodell) in einer Reihe von Workshops mit den Key Usern abgestimmt. Für die Analyse von i3v wurde eine Testlizenz erworben, sodaß die Key User im Rahmen von Einschulungen die einzelnen Komponenten von i3v erstmals praktisch kennenlernen konnten. Zusätzlich wurde von der Universität Wien eine Datenbank entwickelt, mit deren Hilfe die zusätzlichen Anforderungen (*Change Requests*) an die i3v-Software gesammelt und verwaltet wurden. Um diese Anforderungen zu definieren, wurden die Key User in Workshops und Arbeitsgesprächen zu den wesentlichen Prozessen und Abläufen befragt und die Funktionalität von i3v in den einzelnen Bereichen zumindest in groben Zügen geprüft. Von November 1999 bis März 2000 wurden insgesamt 13 Workshops abgehalten und rund 20 Arbeitsgespräche mit einzelnen Vertretern der Key User durchgeführt. Dabei wurden etwa 120 unterschiedliche Formulare und Reports zur Definition der Anforderungen herangezogen und knapp 300 Prozesse in 33 unterschiedlichen Prozeßdiagrammen (Prozeßfolgen) analysiert. 26 dieser Prozeßfolgen wurden als Basis für das Differenzpflichtenheft herangezogen. Die *Change Requests*-Datenbank enthielt nach Abschluß der Erhebungen über 400 Änderungsanforderungen. Das Fachkonzept für das Studienwesen wurde Ende Mai 2000 fertiggestellt.

Die in allen Bereichen der öffentlichen Verwaltung bemerkbaren Sparmaßnahmen sind natürlich auch an UNIVIS nicht spurlos vorübergegangen; die Finanzierung der wichtigsten Folgeprojekte wurde aber – wohl auch aufgrund der großen strategischen Bedeutung des Vorhabens – vom zuständigen Bundesministerium vorerst sichergestellt. Daher konnte die Universität Wien am 20. 7. 2000 mit der Firma GINIT die Kaufverträge für die Software i3v-education unterzeichnen und somit das Teilprojekt Studienwesen planmäßig fortsetzen. Das Teilprojekt Facility Management wird ebenfalls wie geplant in Angriff genommen: Die mit GINIT unterzeichneten Verträge erstrecken sich auch auf die bereits verfügbaren Facility Management-Komponenten von i3v (eine Testversion davon wird derzeit an der Universität geprüft), die im Laufe des Projekts um Komponenten zur Verwaltung von Raum- und Gebäudeplänen erweitert werden sollen. Auch im Personalwesen soll – aufgrund der engen Kopplung mit dem Studienwesen – i3v zum Einsatz kommen. Da die Software derzeit nicht über entsprechende Komponenten verfügt und an der Uni Wien in diesem Bereich fundiertes Fachwissen vorhanden ist, wird GINIT in enger Zusammenarbeit mit der Uni Wien eine Personal- und Planstellenverwaltung mit i3v

neu entwickeln. Im Hinblick auf eine integrierte Lösung ist dabei besonderes Augenmerk auf die Budgetierungswerkzeuge für den Personalbereich (z.B. Koppelung der Personal- und Planstellendaten mit den Lehrveranstaltungs- und Prüfungsdaten) zu legen. Die Detailarbeiten dazu sollen im Oktober 2000 unter der Federführung der Personalabteilung der Uni Wien beginnen, was eine bestmögliche Berücksichtigung unserer Anforderungen garantiert.

Bei der i3v-Betriebseinführung im Studienwesen sind zwei Bereiche zu unterscheiden: Die Studierendenverwaltung, die zentral von der Studienabteilung der Uni Wien wahrgenommen wird, und die Lehr- und Prüfungsverwaltung, die weitgehend von den Fakultäten (Dekanate, Institute, ...) getragen wird. Mit Beginn des Sommersemesters 2001 soll zunächst die Studierendenverwaltung auf i3v umgestellt werden. In den letzten Wochen wurden auf Basis des Differenzpflichtenhefts die Änderungsanforderungen für die betroffenen Komponenten von i3v weiter ausgearbeitet und an GINIT zur Realisierung übergeben. Die Betriebseinführung der Lehr- und Prüfungsverwaltung wird nicht an allen Fakultäten zugleich erfolgen, sondern in einer ersten Phase zu Beginn des Wintersemesters 2001/02 an der medizinischen und an den beiden theologischen Fakultäten. Das bedeutet, daß im März 2001 das i3v-Modul zur Erfassung der Lehrveranstaltungen verfügbar sein muß, im Juli 2001 (Beginn der allgemeinen Zulassungsfrist für das Wintersemester 2001/02) das Modul zur Prüfungsanmeldung und ab Oktober 2001 das Modul zur Erfassung und Bearbeitung von Prüfungen.

Einer der wesentlichen Gründe für die hohe Priorität des Studienwesens war das Bestreben, das Service für Studierende zu verbessern. Bei Redaktionsschluß standen zwar einige Entscheidungen noch aus, doch schon mit der Inbetriebnahme der Studierendenverwaltung sollten sich für die Studierenden spürbare Verbesserungen ergeben. So wird man sich in Zukunft vor der Zulassung zu einem Universitätsstudium via Internet „voranmelden“ und alle relevanten Daten vorerfassen können. Dabei können bereits viele Formalfehler erkannt und vermieden werden – z.B. kann überprüft werden, ob im Falle von kombinationspflichtigen oder kombinierbaren Studien die gewünschte Kombination überhaupt zulässig ist. Das persönliche Erscheinen in der Studienabteilung dient dann lediglich der (gesetzlich unerlässlichen) Vorlage der Originaldokumente. Nach der Prüfung der vorgelegten Unterlagen werden am Schalter sämtliche Dokumente (Studienbuchblatt, Zulassungs-/Fortsetzungsbestätigung, Semesteretikett) sofort ausgedruckt und überreicht; etwaige Fehler bei der Erfassung können somit unmittelbar erkannt und behoben werden. Auch bei Wechsel der Studienrichtung, Änderung der Anschrift etc. werden alle relevanten Dokumente umgehend erstellt und ausgehändigt. Mit der geplanten Einführung der Chipkarte als Studierendenausweis (an der Uni Wien wird dies allerdings noch nicht im Sommersemester 2001 geschehen) können viele dieser Vorgänge dann im Selbstbedienungsbetrieb erfolgen. Alle aktuellen Veränderungen in diesem Zusammenhang werden auf der Homepage der Universität Wien bekanntgemacht.

## Personalnachrichten

Seit Erscheinen des *Comment 00/2* haben wieder mehrere neue Mitarbeiterinnen und Mitarbeiter ihre Tätigkeit am ZID aufgenommen: **Holger Englisch** hat im Juli 2000 die Nachfolge von Susanne Böck angetreten und leitet nun das Techniker-Team der Internet-Domainverwaltung. **Monika Schneider** studiert Telekommunikation an der Fachhochschule St. Pölten und absolviert seit August 2000 ihr Berufspraktikum in unserer Netzwerkgruppe.

Anlässlich der Einführung neuer Software für die Universitätsverwaltung (siehe Seite 4) wurden am ZID neue Planstellen geschaffen: **Gertraud Lohner**, die bisher am Dekanat der Geisteswissenschaftlichen Fakultät für die Prüfungsverwaltung verantwortlich war, wechselte mit August 2000 zum ZID, wo sie nun mit ihren profunden Praxiskenntnissen der Verwaltungsabläufe das neue Referat *UNIVIS User-Support* leitet. Zur selben Zeit trat auch **Clemens Url** seinen Dienst als neuer Mitarbeiter in der Abteilung Universitätsverwaltung des ZID an; er verstärkt das neugeschaffene UNIVIS-Betriebsreferat.

**Ralph Staudigl** kehrte nach Ableistung seines Präsenzdienstes im September 2000 an den ZID zurück und beteiligt sich nun mit frischem Schwung am PC-Support. Zusätzlich wurde – im Rahmen der Teilrechtsfähigkeit – mit Oktober 2000 **Ulrich Kiermayr** am ZID angestellt, um der immer problematischeren Entwicklung im Bereich der Computer- und Netzwerksicherheit Rechnung zu tragen: Er wird sich in einem Pilotprojekt gemeinsam mit den zuständigen Systemadministratoren um den Aufbau von Security-Services kümmern.

**Wolfgang Kantner** entschloß sich zu unserem großen Bedauern – nach einem knapp zweijährigen „Gastspiel“ im Service- und Beratungszentrum des ZID – mit Anfang Oktober 2000 wieder an die Universität für Bodenkultur zurückzukehren. Die vielen Hilfesuchenden an der Universität Wien, denen er mit großer Kompetenz bei der Bewältigung ihrer Computerprobleme geholfen hat, werden ihn ebenso vermissen wie die Kolleginnen und Kollegen am ZID, die sein Organisationstalent auch außerhalb der fachlichen Belange zu schätzen lernten. Wir wünschen ihm alles Gute als Administrator der EDV-Systeme an der Boku! Die Nachfolge von Wolfgang Kantner im Service- und Beratungszentrum tritt **Thomas Kaider** an. Ihm und allen anderen neuen Mitarbeiterinnen und Mitarbeitern wünschen wir viel Erfolg und Freude bei ihrer Tätigkeit!

*Peter Rastl*

Aktuelle Termine und Informationen zum Projekt UNIVIS finden Sie unter <http://www.univie.ac.at/univis/>, für Anfragen und Hinweise ist das UNIVIS-Team unter der eMail-Adresse UNIVIS@UNIVIE.AC.AT erreichbar.

*Martin Polaschek* ■

# REFORM DER SOFTWAREDISTRIBUTION

Die Beschaffung und Verteilung lizenzierter Standardsoftware ist ein wesentliches Service des Zentralen Informatikdienstes: Campusweite Lizenzverträge mit Softwareherstellern ermöglichen es den Instituten und Dienststellen der Uni Wien, eine breite Palette gängiger Softwareprodukte gegen einen Unkostenbeitrag vom ZID zu beziehen, der für die Finanzierung dieses Service jährlich mehrere Millionen Schilling aufwendet. Bisher wurde bei den Softwarelizenzen zwischen Sammellizenzen (eine Lizenz pro Installation) und Campuslizenzen (eine Lizenz pro Institut) unterschieden; für drei Jahre ab Bestelldatum standen kostenlos Updates zur Verfügung. Dieses Konzept hatte einige Nachteile:

- Für uns war nicht ersichtlich, wie viele Lizenznehmer von der Möglichkeit der kostenlosen Updates Gebrauch machten, daher mußten wir von den Softwareherstellern Updates auf Basis von Schätzungen beziehen oder teure Wartungsverträge abschließen.
- Bei Campuslizenzen war nicht bekannt, wie oft die Software tatsächlich installiert wurde.
- 1999 erhielten die Institute erstmals von uns eine Verständigung über bereits abgelaufene Lizenzen. Der orga-

nisatorische Aufwand dieser Vorgangsweise war sowohl für uns als auch für die Institute unverhältnismäßig hoch, was sich auch in der geringen Rückmeldequote von nur 52 % widerspiegelte.

Aus diesen Gründen und wegen der Forderung nach einer besseren Kostentransparenz (sowohl für die Institute als auch für den ZID) war eine Reform der Softwaredistribution unerlässlich. Daher wird sie nun nach einem neuen System abgewickelt, das es einerseits den Instituten ermöglichen soll, durch eine bessere Kontrolle über die eingesetzten Lizenzen unnötige Zahlungen zu vermeiden, und das andererseits auch die von den Softwareherstellern geforderten exakten Reports liefern kann.

## Was geschieht ...

Die Einteilung in Sammel- und Campuslizenzen entfällt, stattdessen muß nun generell **für jeden Rechner**, auf dem die Software installiert wird, **eine eigene Lizenz** bestellt

### Direktinstallation vom Software-Server für Windows-Rechner: Voraussetzungen & Vorgangsweise

Derzeit funktioniert die Direktinstallation von PC-Software nur mit dem Internet Explorer (getestet ab Version 4). Im Internet Explorer darf kein Proxy-Server eingetragen sein (Sie finden diese Einstellung unter **Extras – Internetoptionen** – Registerkarte **Verbindungen – LAN-Einstellungen**). Eine weitere Voraussetzung ist ein einmaliger Eintrag in die Datei `lmhosts`:

- Diese Datei finden Sie unter Windows 95/98 normalerweise im Verzeichnis `\windows\`, unter Windows NT/2000 im Verzeichnis `\winnt\system32\drivers\etc\`. (Sollte dieses Verzeichnis nicht existieren, müssen Sie die **MS-DOS Eingabeaufforderung** starten und den Befehl `set` eingeben. Am Bildschirm erscheint nun eine Parameterliste. Den Namen des richtigen Verzeichnisses finden Sie in der Zeile, die mit `windir=` beginnt.)
- Suchen Sie in diesem Verzeichnis nach der Datei `lmhosts` und öffnen Sie diese mit einem beliebigen Texteditor (z.B. Notepad). Falls die Datei noch nicht existiert, müssen Sie sie mit dem Texteditor neu anlegen.
- Fügen Sie eine neue Zeile mit folgendem Inhalt ein: **131.130.1.4 swd**
- Speichern Sie die Datei. Beachten Sie bitte, daß der Dateiname keine Extension (wie `.txt` oder `.doc`) haben darf und daß das Dateiformat ASCII- oder ANSI-Text sein muß.
- Die Richtigkeit Ihres Vorgehens können Sie überprüfen, indem Sie in der **MS-DOS Eingabeaufforderung** den Befehl `ping swd` eingeben: Erscheint die Fehlermeldung `Unbekannter Host`, kontrollieren Sie bitte Ihre Einstellungen.

Die für die Direktinstallation vorbereiteten Produkte sind in der Softwareliste (<http://www.univie.ac.at/zid-swd/>) durch das Kürzel **[DI]** neben dem Produktnamen gekennzeichnet. Wenn Sie am Software-Server SWD.UNIVIE.AC.AT – nach der Anmeldung mit Ihrer UserID und Ihrem Paßwort – in ein solches Produktverzeichnis wechseln, finden Sie neben einem Link für den Download auch einen Link für die Direktinstallation. Ein Klick darauf führt Sie zu einer Seite mit weiteren Informationen; eventuell werden hier auch die für die Installation nötigen Seriennummern angezeigt. Klicken Sie auf **Direktinstallation starten!** und beantworten Sie die Frage *Wie möchten Sie mit dieser Datei verfahren?* mit **Das Programm von diesem Ort ausführen**. Auf die nun folgende Sicherheitswarnung mit der Frage, ob Sie das Programm tatsächlich ausführen möchten, antworten sie mit **Ja**. Nun brauchen Sie nur noch etwas Geduld, bis das Setup-Programm startet.



werden. Der Unkostenbeitrag von öS 300,- pro Lizenz bleibt unverändert; bei sehr teuren Produkten kann er allerdings – wie bisher auch – höher liegen (MS-Office Pro kostet z.B. öS 1200,-, MS-Windows 2000 Server öS 2500,-). Neu ist die dem jeweiligen Vertrag mit dem Hersteller entsprechende Unterscheidung von Einzel- und Mietlizenzen:

- Bei **Einzellizenzen** erhalten Sie die zum Bestelldatum aktuelle (oder eine bestimmte gewünschte) Version der Software und können diese beliebig lang verwenden. Die Sprache ist frei wählbar; am Software-Server wird nur die bestellte Programmversion freigeschaltet. Updates (ausgenommen Servicepacks und Gratis-Updates) sind nicht mehr inkludiert, sondern müssen ebenfalls um öS 300,- pro Lizenz bestellt werden. Auf dem neuen Bestellformular sind Updates entsprechend zu kennzeichnen.
- Bei **Mietlizenzen** sind sämtliche Updates enthalten; dafür wird nach dem ersten Jahr eine jährliche Wartungsgebühr von öS 100,- pro Lizenz verrechnet. Eine nicht mehr benötigte Lizenz können Sie abmelden, die Software muß dann aber (von wenigen Ausnahmen abgesehen) vom Rechner gelöscht werden. Unter die Mietlizenz fallen z.B. Mathematica und SPSS.

Ob ein Programm als Einzel- oder als Mietlizenz verfügbar ist, können Sie der Softwareliste im WWW (<http://www.univie.ac.at/zid-swd/>) entnehmen; dort sind auch die Preise derjenigen Produkte angeführt, die mehr als öS 300,- kosten.

Eine weitere wesentliche Änderung ist, daß für den Zugriff auf den Software-Server (<http://swd.univie.ac.at/>) nun die Mailbox-UserID des Bestellers verwendet wird: Die bisher vergebenen UserIDs für den Software-Server bleiben noch drei Jahre lang bestehen, Neubestellungen sind aber **nur mehr mit einer gültigen Mailbox-UserID** möglich. Die Authentifizierung am Software-Server erfolgt mit dem Mailbox-Paßwort, das Sie unter keinen Umständen weitergeben sollten. Auch Gruppenbestellungen sind möglich: Ein Gruppenverantwortlicher bestellt die Software und definiert die Bezugsberechtigten, die dann mit ihrem eigenen Mailbox-Paßwort auf den Server zugreifen können.

Da für Einzellizenzen keine Updates mehr verfügbar sind, muß nach und nach die Verzeichnisstruktur am Software-Server geändert werden: Anstatt wie bisher verschiedene Versionen eines Produkts in Unterverzeichnissen anzubieten, wird in Zukunft für jede Programmversion ein eigenes Verzeichnis angelegt.

## Unix-Workstations

Durch abgelaufene und nicht mehr erneuerbare Verträge entfällt bei Unix-Workstations der Support für IBM, Sun und Compaq (früher Digital). Software-Wartungsverträge gibt es jetzt nur mehr für HP und SGI, wobei die Betreuung weiterhin durch die TU Wien erfolgt. Für HP- und SGI-Work-

stations wird ebenfalls eine jährliche Wartungsgebühr eingehoben (öS 300,- pro Rechner). Wie bisher müssen die Workstations bei uns einmalig um öS 3000,- registriert werden, damit der Software-Support in Anspruch genommen werden kann.

## ... wann?

Stichtag für die Reform der Standardsoftware-Distribution war der 1. 10. 2000: Seit diesem Zeitpunkt werden alle Bestellungen nur mehr nach dem neuen System bearbeitet. Die Wartungsgebühren für Mietlizenzen und für Unix-Workstations werden ab 1. 1. 2001 verrechnet.

Sammellizenzen aus alten Bestellungen bleiben aktiv, erhalten aber keine Updates mehr. Alle bestehenden Campuslizenzen werden je nach Vertrag in Einzel- oder Mietlizenzen umgewandelt. Bitte beachten Sie, daß Sie bei Mehrfachinstallationen von Campuslizenz-Software Lizenzen nachkaufen müssen, da nun für jeden Rechner, auf dem die Software installiert ist, eine eigene Lizenz benötigt wird! Eine Aufstellung Ihrer derzeit bei uns registrierten Lizenzen können Sie bei Peter Wienerroither (siehe *Kontakt*) anfordern.

## Direktinstallation vom Server

Für alle Benutzer von Windows-Systemen steht ebenfalls seit 1. 10. 2000 ein neues Service zur Verfügung: Die Direktinstallation vom Software-Server (<http://swd.univie.ac.at/>). Bisher mußten alle bestellten Produkte zunächst vom Server auf den PC übertragen, dann entpackt und schließlich installiert werden. Nun ist es möglich, manche Produkte direkt vom Server zu installieren. Die technischen Voraussetzungen hierfür finden Sie im Kasten auf Seite 6.

Aus Kapazitätsgründen können derzeit nur die gängigsten Pakete direkt installiert werden (siehe Softwareliste); darunter sind allerdings auch solche, die bisher nur auf CD-ROM verfügbar waren. Die Möglichkeit zum Download bleibt erhalten, auch können Sie weiterhin CD-ROMs kaufen oder entleihen. Allen Benutzern, die Lizenzen für Access, Excel, PowerPoint und Word haben, wird auf Wunsch das MS-Office-Paket für die Direktinstallation freigeschaltet.

## Kontakt

Neben Peter Wienerroither (Tel.: 4277-14138, eMail: PETER.WIENERROITHER@UNIVIE.AC.AT) ist nun auch Christian Marzluf (Tel.: 4277-14136, eMail: CHRISTIAN.MARZLUF@UNIVIE.AC.AT) für die Standardsoftware zuständig.

Alle Informationen zur Standardsoftware und speziell zur Reform finden Sie im WWW unter <http://www.univie.ac.at/zid-swd/>.

Peter Wienerroither & Christian Marzluf ■

# CAMPUSLIZENZVERTRAG MIT NAG GEKÜNDIGT

Wegen des hohen Preises und der relativ geringen Nachfrage muß der Campuslizenzvertrag mit der Firma NAG (*Numerical Algorithms Group*) mit Ende des Jahres gekündigt werden. Immer mehr Teilnehmer sind aus dem ursprünglich österreichweiten Vertrag ausgestiegen, sodaß der Kostenanteil für die wenigen verbleibenden Universitäten immer höher wurde. Auch wirkte die Marketing-Strategie von NAG – die Preise für Einzellizenzen zu erhöhen, damit die Campuslizenz in der Relation günstiger erscheint – nicht sehr überzeugend.

Die betroffenen Produkte sind v.a. der NAGWare Fortran90-Compiler und die NAG Fortran- und C-Bibliotheken. Gute Fortran90-Compiler für Unix- und Windows-Systeme werden heute von vielen Herstellern relativ preisgünstig angeboten, sodaß der Ersatz des NAG-Compilers kein großes Problem darstellen dürfte.

Etwas schwieriger ist der Ersatz der NAG-Routinen in numerischen Programmen – hier ist zumindest ein gewisser Umstellungsaufwand erforderlich. Offiziell dürfen ab dem 1. Jänner 2001 keine Programme mehr verwendet werden, die NAG-Routinen aufrufen. Folgende Softwareprodukte kommen als Ersatz in Frage:

- **Netlib** (<http://www.netlib.org/>) enthält ein großes Archiv von numerischen Programmpaketen. Alle sind Public Domain-Software und die meisten von recht guter Qualität, auch wenn manche schon seit längerer Zeit nicht mehr gewartet werden.
- Das am häufigsten verwendete Programmpaket von Netlib ist **LAPACK**, das hochoptimierte Routinen für Lineare Algebra und Eigenwertprobleme enthält. LAPACK ist auch auf dem FTP-Server der Universität Wien zu finden (<http://ftp.univie.ac.at/packages/lapack/>).
- **Mathematica** und **Matlab** sind zwar keine numerischen Programm-bibliotheken, aber viele mathematische oder numerische Aufgaben lassen sich damit ebenso gut – wenn nicht besser – lösen wie mit einem selbstgeschriebenen Fortran-Programm, das NAG-Routinen aufruft. Mathematica kann auch dazu verwendet werden, Formeln und fertigen Fortran- oder C-Code zu generieren.
- Die **IMSL** (*International Mathematical and Statistical Library*, <http://www.vni.com/>) ist der NAG-Bibliothek in Funktion und Umfang sehr ähnlich. Auf dem Alpha-Cluster steht eine Lizenz für maximal zwei gleichzeitige Benutzer zur Verfügung. Bei mehreren Fortran-Compilern ist die IMSL-Bibliothek enthalten (siehe [http://www.vni.com/products/ims1/F90\\_resellers.html](http://www.vni.com/products/ims1/F90_resellers.html)).
- Großer Beliebtheit bei Verfassern numerischer Programme erfreuen sich die **Numerical Recipes** (siehe <http://www.nr.com/>). Die dort beschriebenen Algorithmen sind zwar vielleicht nicht so ausgefeilt wie die bei NAG oder IMSL verwendeten, aber für die meisten Zwecke durchaus ausreichend. Es gibt verschiedene Versionen des Buches (unter anderem für Fortran77, Fortran90 und C); um sich das mühsame Abtippen der Programme zu ersparen, kann man auch eine CD mit dem gesamten Source-Code in allen Sprachen erstehen.

Wer trotz allem noch die eine oder andere NAG-Routine braucht, kann sich an die **Außenstelle Physik** des ZID wenden: Am Unix-Cluster „Merlin“ gibt es weiterhin eine Einzellizenz der NAG Fortran Library.

Peter Marksteiner ■

## Neue Standardsoftware

**Neue Produkte** (Stand: 15. 9. 2000):

- Adobe LiveMotion 1.0 für Win. und Mac (Web-Grafiken und -Animation)
- Apple MacOS 9 (Betriebssystem)
- Apple Works 5.0.3 für Win. und 6.0 für Mac (Integriertes Paket mit Textverarbeitung, Tabellenkalkulation, Datenbank etc.)
- MS-Tutorials, diverse neue Titel (elektronische Handbücher und multimediale Trainer)

**Updates** (Stand: 15. 9. 2000):

- Adobe Acrobat 4.05 für Win. (bisher 4.0)
- Adobe FrameMaker 6.0 für Win. und Mac (bisher 5.5)
- Adobe Illustrator 9.0 für Win. und Mac (bisher 8.0)
- Adobe InDesign 1.5 für Win. und Mac (bisher 1.0)
- Adobe Premiere 5.1 für Win. und Mac, englisch (bisher 5.0)
- Borland JBuilder Prof. 3.5 für Win. (bisher 3.0)
- Mathematica 4.0.2 für Win., Linux, Mac und diverse Unix (bisher 4.0)
- MS-MapPoint 2001 Euro und US für Win. (bisher 2000, nur US und UK)
- MS-Project 2000 für Win. (bisher 98)
- MS-Visio Standard, Professional, Technical und Enterprise 2000 SR1 für Win. (bisher ohne SR1)
- SAS 8.1 für Win. (bisher 8.0)
- SPSS 10.0.7 für Win. (bisher 10.0.5)
- SPSS Data Entry Builder 2.0S für Win. (bisher 1.0.5)
- Symantec Norton Antivirus 2000 6.0 für PC (bisher 12/99)
- Symantec WinFax Pro 10.0 für Win. (bisher 9.0)
- TUSTEP 2000 für Win. und Linux (bisher 11/97)

Alle angeführten Updates wurden vor dem 1. 10. 2000 bezogen und sind daher von der Reform der Softwaredistribution (siehe Seite 6) noch nicht betroffen.

Peter Wienerroither

Alle Informationen zur Standardsoftware finden Sie im WWW unter

<http://www.univie.ac.at/zid-swd/>

# OFFICE-WORKSHOP: TUn uND LasSen, wAS Immer Man wILL

Ich hasse Word! Das Programm glaubt doch tatsächlich immer zu wissen, was ich will, fragt aber niemals nach! Da stehen plötzlich Großbuchstaben am Zeilenanfang, die ich nicht eingegeben habe, geschweige denn dort haben will; Zahleneingaben werden automatisch in der nächsten Zeile fortgesetzt, noch dazu mit speziellen Einzügen, die nie und nimmer von mir stammen – die Liste läßt sich beliebig fortsetzen. Was ist bloß los mit dem Programm? Eine Reihe von Programmfehlern („Bugs“)? Nein, denn es ist eine gewisse Systematik in der Vorgangsweise von Word erkennbar... Mit ein bißchen Suchen und Probieren kann man das Rätsel lösen und von nun an *TUn uND LasSen, wAS Immer Man wILL*: Das Lüften der Geheimnisse von AutoKorrektur und AutoFormat sowie ein Überblick über die Funktionalität von Rechtschreibprüfung & Co bilden diesmal die zentralen Themen unseres Office-Workshops.

## Die AutoKorrektur

Um es gleich vorwegzunehmen: Die Funktionen von Word, die den Begriff „Auto“ beinhalten, sind mit Vorsicht zu genießen. Das Problem ist, daß sie Dinge verändern, ohne vorher mit dem Autor Rücksprache zu halten. Vieles passiert – oft ungewollt – „AutoMatisch“. So werden beispielsweise zwei Großbuchstaben am Wortanfang korrigiert (auch bei Akronymen wie „PCs“ oder „CDs“) oder klein geschriebene Wörter am Zeilenanfang mit einem großen Anfangsbuchstaben versehen.

### Funktionalität

Die Zielsetzung der AutoKorrektur ist rasch erklärt: Mit ihrer Hilfe sollen häufig vorkommende Eingabefehler automatisch richtiggestellt werden. Die AutoKorrektur trat in der Version 6.0 von Word für Windows erstmals in Erscheinung und wurde seither nur geringfügig verändert. Neu in den Versionen Word 97 und Word 2000 ist vor allem die erweiterte Zugriffsmöglichkeit auf die AutoKorrektur. So können Sie mittels Schaltfläche direkt aus der Rechtschreibprüfung falsche und korrigierte Wörter in die AutoKorrektur übernehmen. Auch die Aufnahme von Sonderzeichen in die AutoKorrektur-Liste (durch einen Mausklick auf die Schaltfläche *AutoKorrektur*) wurde wesentlich erleichtert.

Konkret kann Word die folgenden „Fehleingaben“ automatisch richtigstellen:

- Zwei Großbuchstaben am Wortanfang korrigieren,
- jeden Satz mit einem Großbuchstaben beginnen,
- unbeabsichtigtes Betätigen der Feststelltaste korrigieren,
- Wochentage immer groß schreiben (nur Word 2000),
- falsch geschriebene Wörter bereits während der Eingabe ersetzen.

### Anpassung

Um unerwünschte Ergebnisse zu vermeiden, sollten Sie das automatische Ersetzen von Eingabefehlern Ihren Bedürfnissen anpassen und nicht benötigte Optionen deaktivieren. Dies kann im Dialogfenster *AutoKorrektur* (siehe Abb. 1) durchgeführt werden, zu dem Sie über das Menü **Extras** und die Option **AutoKorrektur** gelangen.

Zu empfehlen ist das Deaktivieren der Option **Jeden Satz mit einem Großbuchstaben beginnen**. Unter **Ausnahmen** ist zwar eine Reihe von Abkürzungen vordefiniert (z.B. „allg.“ und „etc.“), nach denen Wörter nicht automatisch mit großem Anfangsbuchstaben geschrieben werden; die automatische Ersetzung tritt aber auch in Kraft, wenn man nur nach einer Zeilenschaltung klein weiterschreibt.

Sehr brauchbar ist die Funktion **Während der Eingabe ersetzen**, die falsch geschriebene Wörter bereits im Zuge der Eingabe korrigiert. Die bestehende Liste gängiger Eingabefehler kann jederzeit um eigene Einträge erweitert werden. Geben Sie dazu das falsch geschriebene Wort in das Eingabefeld *Ersetzen* ein; im Eingabefeld *Durch* tragen Sie das Wort nochmals ein, diesmal allerdings in korrekter Schreibweise. Klicken Sie danach auf die Schaltfläche **Hinzufügen**. Dadurch wird Ihr Eintrag in die Liste aufgenommen und von nun an bereits während der Eingabe automatisch richtiggestellt. AutoKorrektur-Einträge lassen sich auch sehr rasch im Zuge der Rechtschreibprüfung erstellen: Durch einen Klick auf die Schaltfläche **AutoKorrektur** im Dialogfenster *Rechtschreibung und Grammatik* wird das

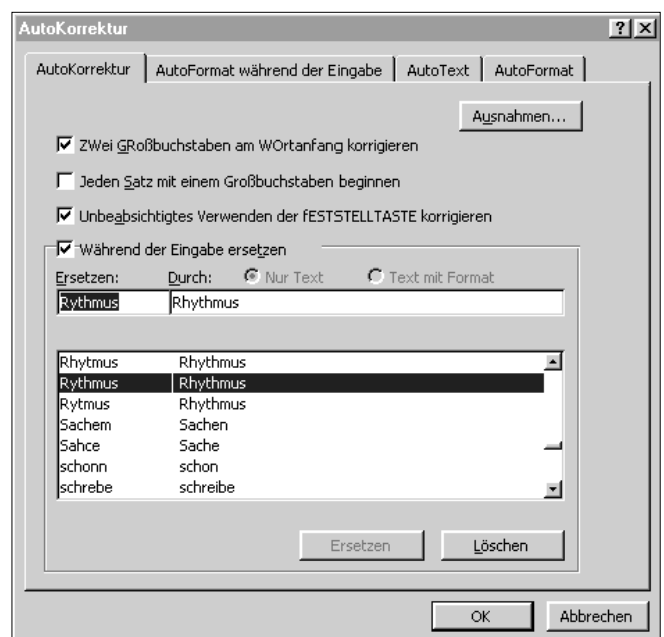



Abb. 1: Dialogfenster *AutoKorrektur*

falsch und korrekt geschriebene Wort automatisch in die AutoKorrektur-Liste übernommen.

Sie können die Funktion *Während der Eingabe ersetzen* auch dazu verwenden, Abkürzungen automatisch ausschreiben zu lassen, indem Sie z.B. im Eingabefeld *Ersetzen* das Kürzel „mfg“ und im Eingabefeld *Durch* „Mit freundlichen Grüßen“ eintragen. Zu beachten ist jedoch, daß die Eingabefehler bzw. Abkürzungen keinesfalls eigenständige Wörter sein dürfen. Beispielsweise macht es wenig Sinn, den Tippfehler „Wein“ durch das Wort „Wien“, das Sie eigentlich schreiben wollten, ersetzen zu lassen – in Zukunft trinken Sie sonst immer ein Gläschen Wien!

Mit Hilfe der Schaltfläche **Ausnahmen** können AutoKorrektur-Ausnahmelisten erstellt werden (keine Großbuchstaben nach bestimmten Abkürzungen bzw. Zulassen von zwei aufeinanderfolgenden Großbuchstaben bei bestimmten Begriffen). Hilfreich ist dabei, daß Wörter automatisch in diese Listen aufgenommen werden, wenn bei einer Texteingabe mit unerwünschter AutoKorrektur diese sofort rückgängig gemacht wird (z.B. mit der **Rückgängig**-Schaltfläche  oder mit der Tastenkombination <STRG>+Z). Zuständig dafür ist die Option **Wörter automatisch hinzufügen**, die im Dialogfenster *AutoKorrektur – Ausnahmen* unbedingt aktiviert sein muß.

## Das AutoFormat

Nicht nur die AutoKorrektur, sondern auch das AutoFormat versucht Ihre Eingaben automatisch an vordefinierte Standards anzupassen. Bestes Beispiel hierfür sind Begriffe, die Sie zwischen zwei Hochkommas (gerade Anführungszeichen) schreiben möchten: Word setzt Ihre Eingabe automatisch außer Kraft, und aus den "geraden Anführungszeichen" werden „typografische Anführungszeichen“.

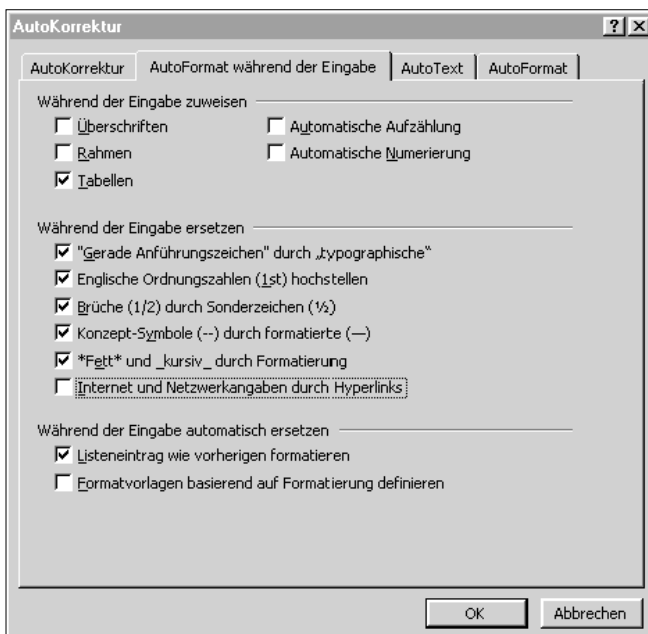


Abb. 2: Registerkarte *AutoFormat während der Eingabe*

Noch tückischer ist die automatische Numerierung bzw. Aufzählung. Ich habe beim Verfassen meines Lebenslaufs (ich bin 1968 geboren) nicht schlecht gestaunt, als ich feststellen mußte, daß ich laut Word bereits 1969 die Volksschule und 1970 das Gymnasium besucht habe. Nach den ersten, eher mühseligen Korrekturversuchen machte ich mich dann auf die Suche nach der Wurzel des Übels und stieß auf die Registerkarte **AutoFormat während der Eingabe** (siehe Abb. 2), die ebenfalls unter **Extras – AutoKorrektur** zu finden ist.

Im Bereich *Während der Eingabe zuweisen* finden Sie Optionen, die automatisch angewendet werden, sobald Sie bestimmte Eingaben tätigen. Wenn Sie beispielsweise Text eingeben und danach zweimal die <Enter>-Taste drücken, wird dem Text automatisch die Formatvorlage *Überschrift 1* zugewiesen. Drücken Sie einmal die <Tab>-Taste und geben wiederum Text und danach zwei <Enter>-Schritte ein, so wird der Absatz automatisch mit der Formatvorlage *Überschrift 2* belegt – dies alles allerdings nur dann, wenn die Option **Überschriften** aktiviert ist, der Absatz mit einem Großbuchstaben beginnt und am Ende kein Satzzeichen aufweist.

Ähnlich verhält es sich bei aktivierter Option **Rahmen**: Wenn Sie mindestens drei Gleichheitszeichen (===) hintereinander eingeben und die Taste <Enter> drücken, so erhalten Sie eine doppelte Unterstreichung vom linken bis zum rechten Rand. Eine dicke Linie erreichen Sie durch die Eingabe von mindestens drei Unterstreichungszeichen (\_\_\_), eine dünne Linie durch mindestens drei Bindestriche (---). Drei Sternchen (\*\*\*) ergeben eine punktierte Linie, drei Rauten (###) eine schattierte Linie und drei Tildezeichen (~~~) eine Wellenlinie, wenn danach jeweils die Taste <Enter> gedrückt wird. Um eine solche Rahmenlinie wieder zu entfernen, müssen Sie entweder die **Rückgängig**-Schaltfläche, die Rücklöschtaaste oder das Menü **Format – Rahmen und Schattierung** (bzw. die entsprechende Schaltfläche in der Symbolleiste) verwenden.

Die Option **Tabellen** erstellt beispielsweise automatisch eine zweiseitige Tabelle, wenn Sie folgende Zeichenkombination eingeben: +---+---+. Die Pluszeichen sind die Spaltentrenner, die Bindestriche legen die Größe der einzelnen Zellen fest.

Die Optionen **Automatische Aufzählung** und **Automatische Numerierung** bewirken, daß automatisch in der nächsten Zeile weitergezählt bzw. weiter aufgezählt wird, wenn am Beginn der vorhergehenden Zeile eine Zahl oder ein Aufzählungszeichen steht. Damit verbunden sind auch Texteingänge, die das Programm selbsttätig vornimmt. Um den Spuk zu beenden, ist das Deaktivieren beider Optionen empfehlenswert.

Die Automatismen, die durch das Aktivieren der Optionen im Bereich *Während der Eingabe ersetzen* in Gang kommen, sind im wesentlichen selbsterklärend (einige zusätzliche Erläuterungen bietet Word in seiner Direkthilfe, die Sie

aufrufen können, indem Sie den Mauszeiger auf eine Option bzw. Schaltfläche bewegen und mit der **rechten** Maustaste klicken. Klicken Sie dann auf die Schaltfläche **Direkthilfe**, so erhalten Sie in einem Pop-up-Fenster kurze Hilfetexte.) Erwähnenswert ist der letzte Eintrag in diesem Bereich, **Internet und Netzwerkangaben durch Hyperlinks**: Diese Funktion erstellt aus URLs oder eMail-Adressen im Text automatisch Hyperlink-Felder, d.h. der URL (z.B. <http://www.univie.ac.at/>) oder die Mailadresse wird färbig und unterstrichen dargestellt, und durch einen Mausklick auf diesen Hyperlink wird das betreffende Dokument oder Ihr Mailprogramm aufgerufen. Genau das ist aber das Problem beim Korrigieren solcher Hyperlinks – sobald Sie den Link anklicken, werden Sie auch schon „weitervermittelt“. Sie können diese Hyperlink-Formatierung dennoch nachträglich deaktivieren (und anschließend korrigieren), indem Sie mit der **rechten** Maustaste auf den Hyperlink klicken. Im daraufhin erscheinenden Kontextmenü finden Sie als letzten Eintrag die Option **Hyperlink** und im Untermenü den Eintrag **Hyperlink bearbeiten**. Das nun folgende Dialogfenster bietet links unten die Schaltfläche **Hyperlink entfernen**; durch Klick auf diese Schaltfläche wird die Hyperlink-Funktionalität eliminiert.

Die Option **Listeneintrag wie vorherigen formatieren** wiederholt automatisch die Zeichenformatierung, die Sie für den Beginn des vorhergehenden Listenelements definiert haben (z.B. erstes Wort kursiv). Als Trennzeichen zum „Haupttext“ des Listeneintrags fungieren Satzzeichen (wie ! oder :). Hinter diesem Trennzeichen wird die Sonderformatierung deaktiviert und Sie können in Standardschrift weiterschreiben.

Die Option **Formatvorlagen basierend auf Formatierung definieren** erstellt neue Absatz-Formatvorlagen auf Basis der manuellen Formatierungen des Dokuments.

Noch ein wichtiger Hinweis: Die Registerkarte *AutoFormat während der Eingabe* ist nicht zu verwechseln mit der Registerkarte *AutoFormat!* Letztere definiert lediglich die Einstellungen, die bei einer schnellen, nachträglichen Formatierung von Dokumenten (mittels **Format – AutoFormat**) angewendet werden sollen, greift aber nicht während des Schreibvorgangs ein.

## Die Rechtschreibprüfung

### Allgemeines

Eine der augenfälligsten Funktionen von Word ist, daß falsch geschriebene oder dem Programm nicht bekannte Wörter (sogenannte „Eigenbegriffe“) automatisch mit einer roten Wellenlinie gekennzeichnet werden. Der Grund dafür ist die Online-Rechtschreibprüfung, die in der Statuszeile durch ein Buchsymbol mit rotem Stift angezeigt wird und bereits während der Texteingabe mit Hilfe eines eingebauten elektronischen Wörterbuchs Wort für Wort überprüft. Dieses Hauptwörterbuch umfaßt über 200 000 Einträge, ist jedoch nicht erweiterbar. Um den Wortschatz des Pro-

gramms zu vergrößern, verwendet man das sogenannte Benutzerwörterbuch (BENUTZER.DIC), das sich um beliebige Einträge ergänzen läßt. Es besteht auch die Möglichkeit, zusätzliche Benutzerwörterbücher anzulegen, die z.B. nur bestimmte Fachbegriffe enthalten. Im Zuge der Rechtschreibprüfung werden alle Wörter des Textes mit den Inhalten des Hauptwörterbuchs und der aktivierten Benutzerwörterbücher verglichen.

Erscheint nun während der Texterfassung eine rote Wellenlinie unterhalb eines Wortes, kann dieses mit Hilfe des Kontextmenüs (dazu richtet man den Mauszeiger auf das gekennzeichnete Wort und klickt einmal mit der **rechten** Maustaste) sehr rasch korrigiert, ignoriert oder dem Benutzerwörterbuch hinzugefügt werden (siehe Abb. 3). In jedem Fall verschwindet die rote Wellenlinie.

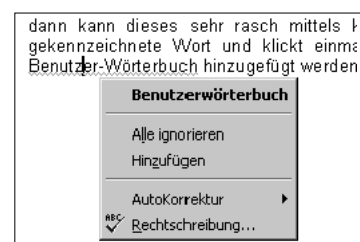


Abb. 3: Korrektur mittels Kontextmenü

Über das Menü **Extras – Optionen** und die Registerkarte **Rechtschreibung und Grammatik** können Sie definieren, ob die Online-Rechtschreibprüfung generell aktiviert oder deaktiviert sein soll, und einige andere allgemeine Einstellungen vornehmen. Schneller geht es allerdings, wenn Sie mit der **rechten** Maustaste auf das Buch-Symbol in der Statusleiste klicken: Sie erhalten wiederum ein Kontextmenü, in dem Sie die Rechtschreibkennzeichnung (die rote Wellenlinie) aus- oder einblenden und auch direkt auf die entsprechenden Optionen für Rechtschreibung und Grammatik zugreifen können.

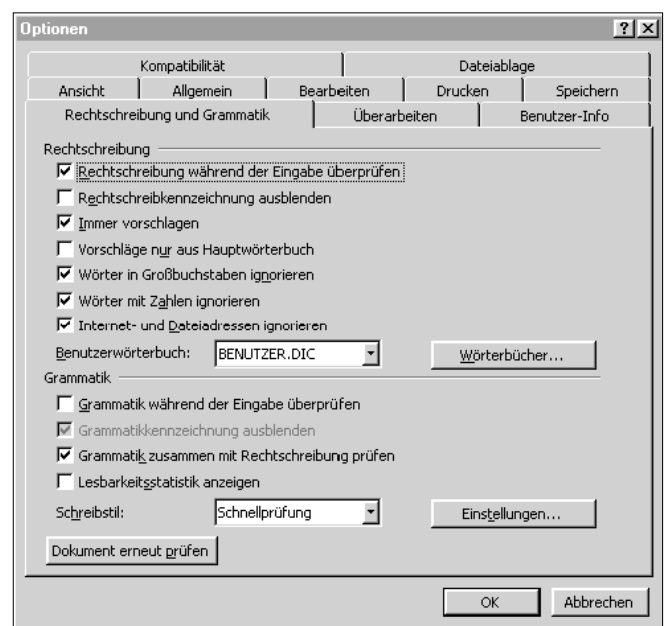


Abb. 4: Optionen für Rechtschreibung und Grammatik

## Optionen

Wie vorhin erwähnt, bietet die Registerkarte **Rechtschreibung und Grammatik** im Menü **Extras – Optionen** (siehe Abb. 4) die Möglichkeit, generelle Einstellungen für die Arbeitsweise von Rechtschreib- und Grammatikprüfung zu definieren. Weiters können Sie mit Hilfe dieser Registerkarte auf das Benutzerwörterbuch **BENUTZER.DIC** zugreifen und dort Korrekturen oder zusätzliche Einträge erfassen.

Mit Hilfe der ersten Option können Sie festlegen, ob Sie die **Rechtschreibung während der Eingabe überprüfen** lassen wollen oder nicht. Ist diese Option deaktiviert, erscheint die folgende Option **Rechtschreibkennzeichnung ausblenden** automatisch grau (nicht wählbar).

Die Optionen **Immer vorschlagen** und **Vorschläge nur aus Hauptwörterbuch** definieren, ob und in welchem Umfang während der Rechtschreibprüfung Korrekturvorschläge angeboten werden. Ist die Option **Vorschläge nur aus Hauptwörterbuch** aktiviert, werden eventuell vorhandene Benutzerwörterbücher ignoriert.



Die letzten drei Optionen legen fest, ob bestimmte Wörter (in Großbuchstaben bzw. in Kombination mit Zahlen) und Internet- und Dateiadressen in die Rechtschreibprüfung einbezogen oder ignoriert werden.

Die Schaltfläche **Wörterbücher** ermöglicht es, Einträge im Benutzerwörterbuch **BENUTZER.DIC** zu bearbeiten oder ein neues Wörterbuch hinzuzufügen (siehe Abb. 5).


Wenn Sie falsche Einträge aus dem Benutzerwörterbuch löschen wollen, müssen Sie den Eintrag **BENUTZER.DIC** markieren und auf die Schaltfläche **Bearbeiten** klicken. Word öffnet nun ein neues Fenster mit dem Inhalt der Datei **BENUTZER.DIC** – eine alphabetische Liste aller von Ihnen hinzugefügten Wörter. Löschen Sie die falschen oder nicht mehr benötigten Begriffe wie gewohnt aus dem Dokument, speichern und schließen Sie die Datei.

Um ein neues Benutzerwörterbuch anzulegen, rufen Sie über das Menü **Extras – Optionen** die Registerkarte **Rechtschreibung und Grammatik** auf, klicken auf die

Schaltfläche **Wörterbücher** und danach auf die Schaltfläche **Neu**. Es erscheint ein Dialogfenster, in dem Sie den gewünschten Dateinamen eingeben müssen (Speicherort und Dateityp dürfen nicht verändert werden, da das Wörterbuch sonst unbrauchbar ist!). Sobald Sie auf die Schaltfläche **Speichern** klicken, wird das neue Wörterbuch in die Liste der Benutzerwörterbücher aufgenommen. Stellen Sie sicher, daß das Wörterbuch aktiviert (mit einem Hakerl versehen) ist und klicken Sie auf die Schaltfläche **OK**. Damit neue Einträge in das soeben erstellte Wörterbuch aufgenommen werden, müssen Sie es aus der Liste der vorhandenen Benutzerwörterbücher auswählen.

Ein kleiner Tip am Rande: Behalten Sie das Buch-Symbol in der Statusleiste im Auge, denn hier wird angezeigt, ob der Text noch fehlerhafte bzw. unbekannte Wörter enthält. So bedeutet ein rotes Kreuz , daß das Dokument noch mindestens einen „Fehler“ aufweist (ein Doppelklick auf das Buch-Symbol führt Sie direkt zur Fehleingabe); fehlerfreier Text hingegen wird durch ein rotes Hakerl  symbolisiert.

## Arbeiten mit der Rechtschreibprüfung

Die schnelle Variante im Umgang mit der Rechtschreibprüfung (mittels Kontextmenü) wurde bereits eingangs erläutert. Ein ausführlicheres Dialogfenster (siehe Abb. 6) erhalten Sie, wenn Sie die Rechtschreibprüfung über das Menü **Extras – Rechtschreibung und Grammatik** oder durch Klick auf das entsprechende Symbol  in der Standard-Symbolleiste aufrufen.

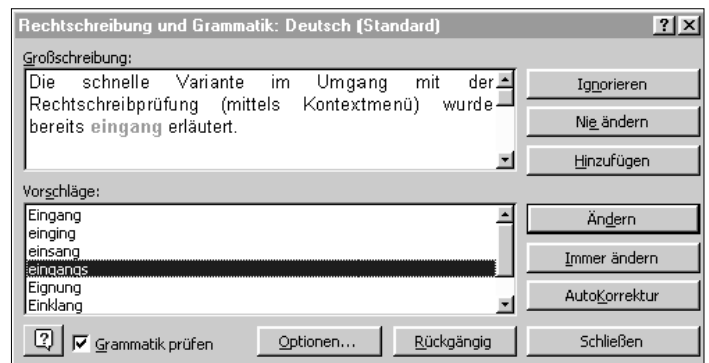
Im Gegensatz zur Korrektur mittels Kontextmenü bietet die umfangreichere Version den Vorteil, daß automatisch ein fehlerhafter/unbekannter Begriff nach dem anderen erscheint. Im oberen Bereich des Dialogfensters wird das beanstandete Wort rot geschrieben, während der untere Bereich – sofern vorhanden – Korrekturvorschläge anbietet.

Handelt es sich tatsächlich um eine fehlerhafte Eingabe, dann besteht in der Regel die Möglichkeit, in der Liste der Vorschläge den richtigen Begriff zu markieren und diesen durch Anklicken der Schaltfläche **Ändern** (einmalig) oder **Immer ändern** (automatische Korrektur innerhalb des gesamten Dokuments) anstelle des falschen Wortes ins Dokument zu übernehmen.



Abb. 5 (links):  
Dialogfenster  
Benutzer-  
wörterbücher

Abb. 6 (rechts):  
Umfangreiche  
Rechtschreib-  
prüfung



Gibt es keine passenden Vorschläge, müssen Sie die Änderung händisch vornehmen, indem Sie in den oberen Bereich klicken und dort das falsch geschriebene Wort korrigieren. Dieses wird nun schwarz dargestellt, und Sie müssen wiederum entweder **Ändern** oder **Immer ändern** anklicken, damit die Korrektur im Dokument durchgeführt wird.

Handelt es sich bei dem beanstandeten Wort um einen Eigenbegriff, der weder im Haupt- noch im Benutzerwörterbuch aufscheint, können Sie entscheiden, ob Sie diesen Begriff **Ignorieren** (einmalig), **Nie ändern** (jedes weitere Vorkommen wird automatisch übergangen) oder mittels **Hinzufügen** ins Benutzerwörterbuch aufnehmen wollen.

## English spoken – Le français parlant

Word bietet neben der deutschen Rechtschreibprüfung auch Korrekturhilfen für Dokumente in englischer und französischer Sprache. Voraussetzung dafür ist die Umstellung der Sprache für ganze Dokumente oder fremdsprachige Textpassagen. Weitere fremdsprachige Wörterbücher sind im Fachhandel erhältlich und können jederzeit nachträglich installiert werden. Zu beachten ist, daß eine eventuelle Sprachumstellung nicht nur die Rechtschreib- und Grammatikprüfung beeinflusst, sondern auch Auswirkungen auf die Silbentrennung, den Thesaurus und die Darstellung von Datums-, Währungs- und Zahlenangaben hat.

Um die Sprache zu wechseln, müssen Sie entweder die Textpassage markieren, die in einer Fremdsprache geschrieben wurde, oder die Einfügemarke an der Stelle positionieren, wo fremdsprachiger Text geschrieben werden soll. Wählen Sie nun das Menü **Extras – Sprache** und im Untermenü die Option **Sprache bestimmen** aus. Es erscheint eine Liste aller zur Verfügung stehenden Sprachen (siehe Abb. 7), wobei jedoch nur Englisch und Französisch standardmäßig von Word unterstützt werden. Markieren Sie die gewünschte Sprache und klicken Sie auf die Schaltfläche **OK**. Für die gewählte Textpassage bzw. für den zu schreibenden Text werden ab nun die landesspezifischen Korrekturdateien (Wörterbücher) herangezogen.

## Die Grammatikprüfung

Die Grammatikprüfung funktioniert ähnlich wie die Rechtschreibprüfung, allerdings kann man der deutschen Grammatikprüfung leicht überdrüssig werden: Beinahe jeder Satz

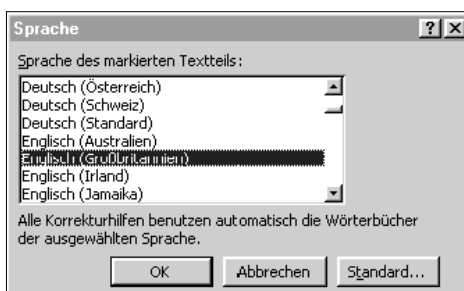


Abb. 7:  
Sprache bestimmen

muß vom Autor auf von Word gefundene Grammatikfehler hin überprüft werden, wobei man sehr rasch erkennt, daß die eigenen Grammatikkenntnisse um einiges besser sind als die von Word. Die Erläuterungen zu den angeblich gemachten Grammatikfehlern lassen ebenfalls zu wünschen übrig, da sie ohne fachspezifische Deutschkenntnisse kaum zu interpretieren sind. Auch die folgende Meldung ist nicht sehr förderlich, wenn man einen Text auf seine grammatikalische Richtigkeit überprüfen will:

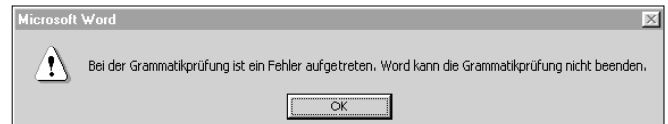


Abb. 8: Fehlermeldung bei der Grammatikprüfung

So gesehen kann von einem Einsatz der Grammatikprüfung – der auch noch auf Kosten der Rechnerleistung geht – derzeit nur abgeraten werden. Dennoch soll im folgenden ein kurzer Überblick über die Funktionalität der Grammatikprüfung gegeben werden.

## Optionen

Im Gegensatz zur Rechtschreibprüfung verwendet die Online-Grammatikprüfung von Word eine grüne Wellenlinie, um Fehler zu kennzeichnen. Spezifische Einstellungen zur Arbeitsweise der Grammatikprüfung können Sie wiederum über das Menü **Extras – Optionen** und die Registerkarte **Rechtschreibung und Grammatik** (siehe Abb. 9) definieren.

Im Bereich **Grammatik** können Sie festlegen, ob Sie die **Grammatik während der Eingabe überprüfen** lassen wollen und ob die Grammatikzeichnung ein- oder ausgeblendet werden soll. Weiters haben Sie die Möglichkeit, im Rahmen einer umfangreichen Rechtschreib- und Gram-

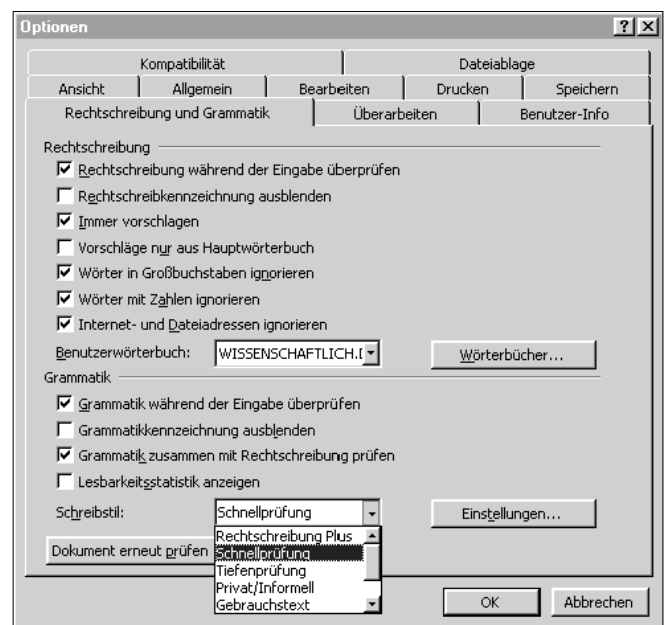


Abb. 9: Optionen für Rechtschreibung und Grammatik

Lesbarkeitsstatistik			
<b>Zahlen</b>			
Zeichen	924	Kurze Sätze	6
Silben	362	Lange Sätze	1
Wörter	154	Einfache Sätze	1
Sätze	27	Lange Wörter	21
Absätze	14		
<b>Durchschnitt</b>			
Silben pro Wort			2,35
Wörter pro Satz			5,70
Sätze pro Absatz			1,92
<b>Lesbarkeit</b>			
Flesch Lesbarkeitsgrad (100 = sehr leicht)			30
Passiv (% der finiten Verbphrasen)			0
Satzkomplexität (100 = sehr komplex)			2
Wortschatzkomplexität (100 = sehr komplex)			25

Abb. 10: Die Lesbarkeitsstatistik

matikprüfung auf die Grammatikprüfung zu verzichten, indem Sie die Option **Grammatik zusammen mit Rechtschreibung prüfen** deaktivieren.

Wenn Sie von der Option **Lesbarkeitsstatistik anzeigen** Gebrauch machen, bietet Word nach erfolgter Rechtschreib- und Grammatikprüfung verschiedene Informationen zum Schwierigkeitsgrad des Dokuments (siehe Abb. 10), die anhand der durchschnittlichen Anzahl von Silben pro Wort bzw. von Wörtern pro Satz ermittelt werden. Das Verfahren „Flesch Reading Ease“ bewertet die Lesbarkeit eines Textes nach einem Punktesystem mit maximal 100 Punkten – je höher die Punktezah, desto verständlicher das Dokument. In Standarddokumenten sollten Sie eine Punktezah von etwa 60 bis 70 anstreben.


Mit Hilfe der Option **Schreibstil** können Sie die Art und Weise der Grammatikprüfung beeinflussen: Wählen Sie aus der Liste den Schreibstil aus, der auf Ihr Dokument am ehesten zutrifft. Durch Anklicken der Schaltfläche **Einstellungen** können Sie herausfinden, welche grammatikalischen Richtlinien und Stilregeln (z.B. Amtsdeutsch) für die Überprüfung herangezogen werden.

### Arbeiten mit der Grammatikprüfung

Ebenso wie bei der Rechtschreibprüfung erfolgt die schnelle Variante der Grammatikprüfung mit Hilfe des Kontext-



Abb. 11: Umfangreiche Grammatikprüfung

menüs: Wenn Sie mit der **rechten** Maustaste auf ein grün unterstrichenes Wort klicken, werden Korrekturvorschläge beziehungsweise grammatikalische Erläuterungen angezeigt. Sie können nun entweder den im Kontextmenü angebotenen Vorschlag übernehmen oder **Satz ignorieren** auswählen. Die Option **Grammatik** führt Sie zur umfassenden Grammatikprüfung, bei der – analog zur Rechtschreibprüfung – die Möglichkeiten **Ignorieren**, **Nie ändern** und **Ändern** zur Verfügung stehen (siehe Abb. 11). Die ausführliche Grammatikprüfung kann auch über das Menü **Extras – Rechtschreibung und Grammatik** oder durch Klick auf das Symbol  in der Standard-Symbolleiste aktiviert werden.

### Der Thesaurus

Die meisten kennen sie noch aus der Schulzeit – die rote Wellenlinie unter einem Wort, das man schon dreimal verwendet hat, weil einem beim besten Willen kein anderer passender Begriff einfallen wollte. Solche Wortwiederholungen lassen sich beim Arbeiten mit Word etwas leichter vermeiden: Der sogenannte Thesaurus, ein elektronisches Synonymwörterbuch, kann Sie zwar nicht auf Wortwiederholungen im Text aufmerksam machen, bietet aber für zahlreiche Begriffe eine Auswahl an bedeutungsgleichen Wörtern.

Um den Thesaurus zu verwenden, müssen Sie zunächst das Wort markieren, für das Sie ein Synonym finden möchten. Wählen Sie dann aus dem Menü **Extras – Sprache** im Untermenü die Option **Thesaurus** aus. Es erscheint das Dialogfenster *Thesaurus: Deutsch* (siehe Abb. 12). Im Eingabefeld *Synonyme für* finden Sie bereits den zuvor markierten Begriff; hat dieses Wort mehrere Bedeutungen, müssen Sie in der Liste *Bedeutungen* die passende auswählen. Im rechten Fenster sind die entsprechenden Vorschläge aufgelistet, die Sie durch einfaches Anklicken in das Eingabefeld *Ersetzen durch Synonym* übernehmen können. Wenn Sie nun auf die Schaltfläche **Ersetzen** klicken, wird das markierte Wort im Dokument gegen das gewählte Synonym ausgetauscht. Sie haben aber auch die Möglichkeit, für den Begriff, der im Eingabefeld *Ersetzen durch Synonym* aufscheint, weitere Synonyme zu suchen – klicken Sie dazu auf die Schaltfläche **Nachschlagen**.

Eva & Michel Birnbacher ■



Abb. 12: Der Thesaurus





## EMAIL-PROFITIPS

Moderne eMail-Programme geben Ihnen die Möglichkeit, jede Ihrer Nachrichten wie ein Glückwunschtelegramm aussehen zu lassen. Wie zu den Beginnzeiten der elektronischen Textverarbeitung, als jeder Brief wirkte wie eine Einladung zu einem Kindergeburtstag, werden alle diese Features natürlich auch eingesetzt. Bitte bedenken Sie aber, daß die Nutzung aller Möglichkeiten zur „Verschönerung“ keineswegs bei allen Empfängern gut ankommt. Menschen, die einen großen Teil ihrer Kommunikation über eMail abwickeln (eMail-Profis?), handeln meistens nach dem Grundsatz

### Weniger ist mehr!

Es ist nicht garantiert, daß Ihre mühsam geschriebene, mit einem bewegten Hintergrundbild und stimmungsvoller Musik unterlegte Nachricht überhaupt von mir gelesen werden kann. Beispielsweise kommt die oben abgebildete Nachricht bei mir unter Umständen folgendermaßen an:

```
<!doctype html public "-//w3c//dtd
html 4.0 transitional//en">
<html>
<body background="cid:part1.
39BF742B.E940FC5B@univie.ac.at">
<h1>
<font color="#000000">Hallo!!!</font>
</h1>
<h1>
<font color="#000000">Wie gehts? Schau, wie
sch&ouml;n ich eMails kann</font></h1>
</body>
</html>
```

Ich lese meine eMail-Nachrichten mit verschiedenen Mailprogrammen, und nicht jedes davon ist in der Lage, mir Bilder und HTML-Formatierungen anzuzeigen – von Sound ganz zu schweigen. Was auf jeden Fall passiert, ist, daß Ihre Nachricht viel mehr Netzwerkverkehr produziert, die Übertragung der Nachricht auf meinen Rechner länger dauert und ich mir aus einem Buchstabensalat Ihre Sätze herausuchen oder ein zusätzliches Programm starten muß, um die Nachricht anzusehen. Fröhlich macht mich das nicht.

Falls Sie einen Kommunikationspartner haben, von dem Sie wissen, daß er sich darüber freut und daß sein Mailprogramm diese „Verschönerungen“ darstellen kann, können Sie bei ihm Ihre gesamte Kreativität in die Ausgestaltung

der eMail-Nachricht legen. Bei allen anderen (vor allem bei Menschen, mit denen Sie zum erstenmal per eMail in Kontakt treten): Hände weg von Formatierungen und Hintergrundbildern! Es geht um den Austausch von Informationen mittels Nachrichten. Nachrichten bestehen aus Text. Text besteht aus Buchstaben. Aktivieren Sie den „Plain Text-Editor“ in Ihrem Mailprogramm! Wie das geht, können Sie in unseren Konfigurationsanleitungen für Mailprogramme nachlesen (siehe <http://www.univie.ac.at/ZID/helpdesk.html>).

Außerdem empfehle ich Ihnen, zum Lesen Ihrer eMail-Nachrichten eine Schriftart mit fester Schriftbreite (*Fixed Width Font*, z.B. Courier) zu verwenden, bei der jedes Zeichen gleich viel Platz braucht. Die Nachricht

```
Tabellenstand nach der 3. Runde
Rennweg          3 2 1 0  9: 1  7
FavAC            3 2 1 0  9: 3  7
BSV/Vienna Amateure 3 2 0 1 12: 6  6
```

sieht dann wirklich so aus, wie sie gedacht war. Bei einer Schriftart mit variabler Breite (z.B. Arial) ist sie weitaus unübersichtlicher:

```
Tabellenstand nach der 3. Runde
Rennweg          3 2 1 0 9: 1 7
FavAC            3 2 1 0 9: 3 7
BSV/Vienna Amateure 3 2 0 1 12: 6 6
```

Man kann auch ohne Auszeichnungsmittel wie fetter Schrift oder Unterstreichungen schön strukturierten Text erstellen. Wenn Sie ein Wort hervorheben wollen, können Sie davor und danach einen Stern (\*) oder einen Unterstrich ( \_ ) setzen:

```
**Achtung, wichtig!**
Wir treffen uns nicht am Mittwoch, sondern
am Donnerstag
um 18:00!
```

Mit einem Stilmittel sollten Sie besonders vorsichtig umgehen: dem Schreiben in Großbuchstaben. Das wird als SCHREIEN interpretiert! Ich glaube, man sollte möglichst wenig SCHREIEN.

Weitere Tips für den Umgang mit eMail finden Sie in den beiden *Comment*-Artikeln

- **POP Art**  
([http://www.univie.ac.at/comment/99-1/991\\_25.html](http://www.univie.ac.at/comment/99-1/991_25.html)) und
- **Return to Sender, Address unknown...**  
([http://www.univie.ac.at/comment/99-2/992\\_17.html](http://www.univie.ac.at/comment/99-2/992_17.html)).

Robert Brunthaler ■

# WAP – WHAT?

## *Wirklich Absolut Phänomenal*

Wer sich heutzutage überlegt, ein Handy zu kaufen, kommt eigentlich nicht mehr daran vorbei: Die Werbung preist es in schillernden Farben, beim Niedermayer wird es einem nachgeschmissen und, hey, Niki Lauda fährt voll darauf ab. Die Rede ist von WAP, dem *Wunder Aller Produkte*, und ginge es nach dem Willen der Marketing-Leute, würde in Zukunft sowieso nichts mehr ohne WAP laufen.

Was ist es nun, dieses WAP? Hinter der Abkürzung verbirgt sich der klingende Ausdruck *Wireless Application Protocol*, und dieser verspricht die Erfüllung des Traums aller Informationsjunkies: Die Loslösung des Internet von fixer Netzwerkinfrastruktur. Hurra, gleichzeitig joggen und Kinokarten bestellen, endlich! (Und auch „S-Bahn-Surfen“ erhält eine ganz neue Bedeutung.)

## *Was Allgemein Passiert*

Das Grundprinzip einer WAP-Verbindung ist denkbar einfach: Wie bei einem „normalen“ HTML-Browser ruft der Benutzer über ein WAP-Handy oder ein anderes WAP-Device – z.B. ein PDA, ein Handheld oder ein Webpad – einen URL auf (z.B. <http://wap.univie.ac.at/>). Anders als im WWW wird die Anfrage aber nicht direkt zum Webserver geschickt, sondern zunächst an ein sogenanntes WAP-Gateway, das als Schnittstelle zwischen Funknetz und Internet fungiert und die Anfrage an den Webserver weiterleitet. Dieser schickt die gewünschte WML-Seite (WML steht für *Wireless Markup Language* und definiert ähnlich wie HTML, die *Hypertext Markup Language*, den Seitenaufbau) an das WAP-Gateway zurück. Das WAP-Gateway übersetzt nun die im ASCII-Text-Format vorliegende Seite in einen binären Bytecode, den die Handies verarbeiten können, und sendet diesen über das Funknetz zum Handy. Dieser Vorgang läuft für die Benutzer vollkommen transparent ab, d.h. sie merken nichts vom dazwischengeschalteten WAP-Gateway, das meistens vom jeweiligen Mobilfunkbetreiber zur Verfügung gestellt wird.

Nicht sonderlich transparent sind hingegen die Fehlermeldungen, die ein WAP-Handy ausspuckt, falls etwas nicht funktioniert: Meldungen wie *Keine Antwort empfangen*, *Fehler beim Seitenaufruf* usw. lassen nur Vermutungen darüber zu, was denn nun nicht stimmt – sogar der berühmte Windows-Bluescreen liefert aussagekräftigere Informationen. Früher kam es auch immer wieder vor, daß das Handy beim Seitenaufruf komplett abstürzte und nur durch ein kurzes Lösen des Akkus „wiederbelebt“ werden konnte. Die Handy-Hersteller haben die Software ihrer Produkte inzwischen verbessert; dennoch hat es manchmal den Anschein, daß trotz hochgelobter Qualitätskontrollen und ISO-Zertifizierungen viel Mist auf den Markt kommt – Hauptsache, man kann es verkaufen.

Abgesehen von den unverschämte hohen Online-Gebühren ist das größte Defizit der derzeit erhältlichen WAP-Handies ihre begrenzte Speicherkapazität, die in Verbindung mit kleinen Displays und erbärmlich unergonomischen Eingabe-Elementen („Krankheitsbilder der Zukunft: der WAP-Daumen“) die Freude am mobilen Surfen erheblich schmälert.

## *Wie Außerordentlich Praktisch*

Trotz dieser Mängel hat WAP natürlich einiges zu bieten (siehe auch Kasten *Was Andere Publizieren* auf Seite 19). Da der Hauptzweck eines Handys nach wie vor das Telefonieren ist, gibt es das Herold-Telefonverzeichnis auch für WAP. Ebenfalls sehr brauchbar sind die News-Dienste: Beispielsweise kann man die Schlagzeilen von ORF, „Standard“ und „Presse“ via Handy abrufen, ebenso die neuesten Ö3-Verkehrsnachrichten oder die Wettervorhersage. Neben diesen „klassischen“ Diensten gibt es auch spezielle Newsticker – Technik-Freaks erfahren die neuesten Nachrichten z.B. beim Zeitschriftenverlag Heise oder bei Slashdot, Musik-Fans z.B. bei MTV.

Um WAP-Fans zum nötigen Überblick zu verhelfen, bieten bekannte Suchmaschinen wie Yahoo, Altavista oder Fireball ihre Dienste auch für mobile Surfer an. Das derzeit beste Service kommt von Google: Diese Suchmaschine liefert nicht nur beim Auffinden von WML-Seiten gute Ergebnisse, sondern durchsucht auch „normale“ HTML-Seiten, die dann in WML umgewandelt und am Handy angezeigt werden – WAP-Surfer können also mit Hilfe von Google nicht nur das bestehende WAP-Angebot, sondern große Teile des Internet durchkämmen.

## *Werkzeuge Am Prüfstand*

Wenn man vom WAP-Fieber angesteckt wurde und nun selbst WML-Seiten entwickeln möchte (siehe dazu *WML Crash-Kurs*), muß man einige wichtige Dinge beachten:

- Die Konfiguration des Webservers, auf dem die WML-Seiten gespeichert werden, muß um folgende MIME-Types erweitert werden (auf den Servern des ZID sind diese MIME-Types bereits vorkonfiguriert):
 

text/vnd.wap.wml	für WML-Dateien
	mit der Endung .wml und
image/vnd.img.wbmp	für WAP-Bitmaps
	mit der Endung .wbmp.
- Die Einhaltung der korrekten WML-Syntax ist unbedingt erforderlich. Schlampigkeiten, die von HTML-Browsern toleriert werden, führen im WML-Browser zu kryptischen Fehlermeldungen und verursachen Frust auf der Anwenderseite.

- Die WML-Seiten dürfen nicht zu groß werden. Handies zeigen die Seite nicht an, falls der Speicher voll ist, und der Speicherplatz ist bescheiden. So verfügt das Nokia 7110 nur über knapp 1400 KB; diese Angabe bezieht sich aber auf den vom WAP-Gateway erzeugten Bytecode und nicht auf die tatsächliche Größe der WML-Datei.
- Als weiteres Hindernis kommt hinzu, daß eine WML-Seite nicht überall gleich aussieht. Zum einen bestimmt schon die Displaygröße, wie die Seite angezeigt wird, zum anderen ist die WML-Spezifikation nicht in allen Handies gleich implementiert. Beispielsweise kann das Ericsson R320s mit Textauszeichnungen wie Bold-Tags oder Formatierungen wie zentriertem Text umgehen, nicht aber das Nokia 7110.

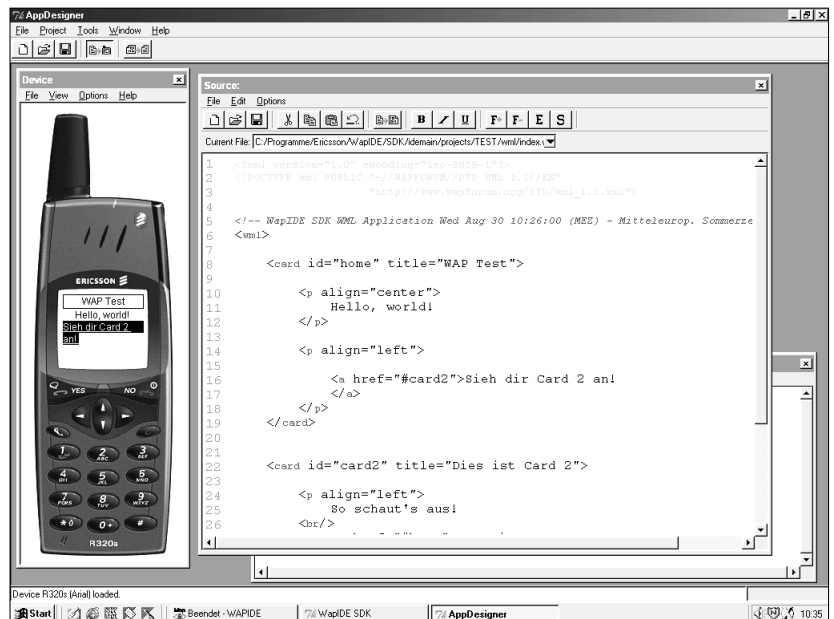


Abb. 1: Das Ericsson-Toolkit

Angesichts der Mühen, die das Testen und Debuggen von WAP-Anwendungen mit sich bringt, und der Kosten, die für Handy und Onlinezeit entstehen, ist man gut beraten, seine WML-Seiten mit Hilfe sogenannter „WAP-Toolkits“ zu erstellen. Diese Toolkits werden z.B. von Nokia, Ericsson und Phone.com angeboten und umfassen neben einer integrierten Programmierumgebung auch einen WAP-Browser, der den jeweiligen Handy-Typ simulieren kann. Außerdem können die erstellten WML-Seiten in den vom Handy verwendeten Bytecode übersetzt werden, was die Kontrolle über die Seitengröße erleichtert. Für WML-Entwickler empfiehlt es sich daher, alle verfügbaren Toolkits (die übrigens nur für Windows 98 bzw. NT-Systeme erhältlich sind) zu installieren, um die Seiten auf verschiedenen Handies testen zu können.

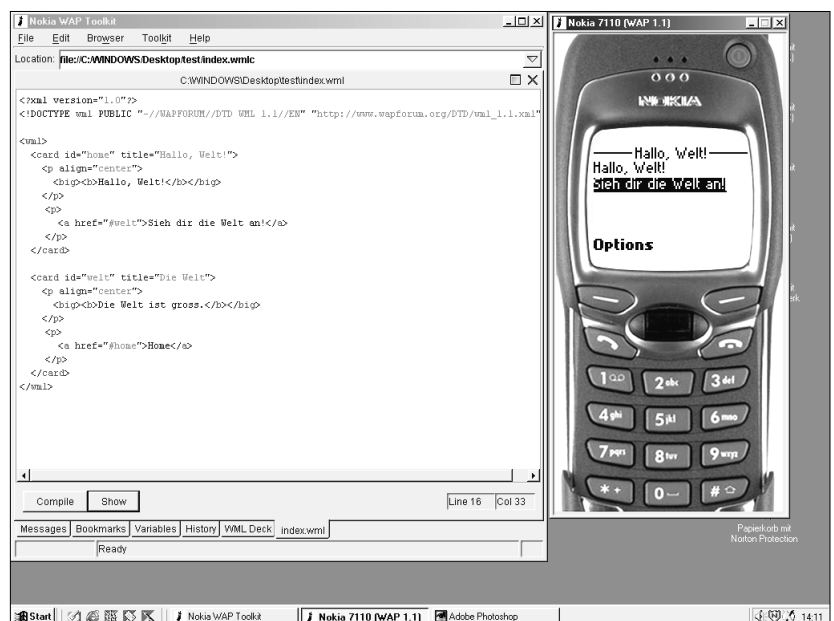


Abb. 2: Das Nokia-Toolkit

Allerdings haben diese Toolkits auch ihre Haken. Abgesehen davon, daß der Zugang zu den Developer-Bereichen auf den Websites der Hersteller mit einer Registrierung verbunden ist, werden Modem-Benutzer am Download der großen Dateien ganz schön zu kiefeln haben (neben den umfangreichen Toolkits wird z.B. auch noch das *Java Runtime Environment* verlangt). Außerdem läuft die Installation dieser Toolkits nicht immer reibungslos ab. So baut beispielsweise das Ericsson-Toolkit auf *Tcl* auf, einer Sprache, die in der Windows-Welt eher unbekannt ist. Die notwendigen Tcl-Bibliotheken werden zwar mitgeliefert; dennoch läßt sich das Ericsson-Toolkit nicht über den Eintrag im *Start*-Menü starten – erst nach der Anpassung der *PATH*-Variable in der Datei *AUTOEXEC.BAT* konnte ich mit dem Ericsson-Toolkit arbeiten. Damit dieses überhaupt seinen Dienst tut, muß ein lokaler Webserver vorhanden sein; deshalb installiert sich neben dem Toolkit auch noch der Xitami-Webserver. Das Arbeiten mit dem IDE (*Integrated Development Environ-*

*ment*) von Ericsson gestaltet sich mitunter etwas schwierig, da man immer zuerst in den sogenannten Test-Mode umschalten muß, wenn man sich seine WML-Seiten im Simulator ansehen will. Diesen Test-Mode muß man aber explizit wieder ausschalten, um Änderungen im WML-Code durchzuführen. Andererseits unterstützt das Ericsson-Toolkit den WML-Anfänger, da im *Insert*-Pull-down-Menü stets nur diejenigen Tags ausgewählt werden können, die laut WML-Spezifikation an der aktuellen Cursorposition eingefügt werden dürfen (z.B. `<card>` nur innerhalb von `<wml>`, `<p>` nur innerhalb von `<card>`). Im Lieferumfang des Ericsson-Toolkit ist leider nur ein Simulator für das R320s enthalten; ein Simulator für das R380s kann aber von der Ericsson-Homepage (siehe *Was Andere Publizieren* auf Seite 19) heruntergeladen werden.

Im Falle des Nokia-Toolkit, das auf dem Java Runtime Environment aufsetzt, muß nach der Installation die PATH-Variable ebenfalls händisch angepaßt werden, damit die Java-Bibliotheken gefunden werden; dann läßt es sich allerdings problemlos starten. Das Nokia-Toolkit zeichnet sich durch seinen Funktionsumfang und die Fülle an mitgelieferter Dokumentation aus. So erhält man neben dem *User's Guide* für das Toolkit auch noch einen *Designer's Guide* (der Grundsätzliches über das Design von WAP-Services erklärt und auf die Besonderheiten des 7110 eingeht) und einen *Developer's Guide*, der eine WML-Referenz darstellt und auch einige praktische Beispiele liefert. Weiters umfaßt das Toolkit auch einen WBMP-Editor, mit dem man WAP-Bitmaps erstellen kann. Die derzeit aktuelle Version 2.0 des Nokia-Toolkit installiert neben dem IDE auch eine WAP-Server-Simulation, die benötigt wird, um mit dem 7110-Emulator lokale WML-Seiten zu betrachten.

Beide Toolkits beinhalten zahlreiche Anwendungsbeispiele, das Ericsson-Toolkit sogar einen Perl-Interpreter und viele CGI-Beispielskripts.

## WML Crash-Kurs

(Wenn Anfänger Programmieren)

Die WML-Syntax umfaßt im Vergleich zu HTML weniger Tags, deren Anordnung und Verwendung aber aufgrund der Tatsache, daß es sich bei WML um eine XML-konforme Sprache handelt, exakt eingehalten werden muß (XML =

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE wml PUBLIC
"-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
<card id="card1" title="Hello, world!">
  <p align="center">
    <b>Hello, world!</b>
  <br/>
</p>
<p>
  This is Card 1.<br/>
  <a href="#card2">Goto Card 2</a>
</p>
</card>
<card id="card2" title="Hello, again!">
  <p align="center">
    <b>This is Card 2!</b>
  <br/>
  <a href="#card1">Goto Card 1</a>
</p>
</card>
</wml>
```

Abb. 3: Beispiel für eine WML-Datei

*Extensible Markup Language*). Die Basisstruktur einer WML-Seite ist die sogenannte *Card*; innerhalb einer Card können Texte, Links, Bilder, Formulare usw. definiert werden. Mehrere Cards innerhalb einer Seite ergeben dann – analog zum herkömmlichen Kartenspiel – ein *Deck*. (Zum besseren Verständnis: Eine Card definiert einen ähnlichen Bereich wie in HTML der <body>-Tag – dort steht, was im Browser angezeigt wird. Allerdings sind in HTML mehrere <body>-Abschnitte nicht erlaubt, während in WML mehrere <card>-Bereiche zur Strukturierung der Seite dienen.) Die WML-Syntax soll im folgenden anhand eines *Hello, world*-Beispiels (ein Deck mit zwei Cards, siehe Abb. 3) erläutert werden.

WML-Seiten müssen immer mit dem sogenannten XML-Header beginnen:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE wml PUBLIC
"-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
```

Einen solchen Header müssen alle XML-Dokumente aufweisen. Die erste Zeile definiert, daß es sich um ein XML-Dokument handelt, die zweite (hier aus Platzgründen dreigeteilt) gibt an, welche *Document Type Definition* für dieses Dokument verwendet werden soll. (Document Type Definitions sind notwendig, um XML-Dokumente auf ihre korrekte Syntax zu überprüfen und um festzustellen, um welche XML-Abart es sich handelt – in diesem Fall um WML.)

Daraufhin wird das eigentliche WML-Dokument eröffnet und die erste Card definiert:

```
<wml>
<card id="card1" title="Hello, world!">
```

Über die zugeordnete ID kann man die Card innerhalb des Decks identifizieren und auch mittels Links ansteuern. Zu beachten ist, daß jedes Attribut innerhalb eines Tags immer unter Anführungszeichen geschrieben werden muß.

Innerhalb der Card können nun Texte, Bilder, Links etc. eingefügt werden. Allerdings schreibt die WML-Spezifikation vor, daß solche Inhalte nur innerhalb von <p>-Tags stehen dürfen.

```
<p align="center">
  <b>Hello, world!</b>
<br/>
</p>
<p>
  This is Card 1.<br/>
  <a href="#card2">Goto Card 2</a>
</p>
```

Auffällig ist hier, daß Tags ohne entsprechendes Abschluß-Tag (wie hier der Zeilenumbruch <br/>) immer als <..> geschrieben werden müssen. Der Link zeigt als Beispiel, wie man innerhalb eines Decks zu anderen Cards springen kann. Links können natürlich auch zu anderen WML-Dokumenten zeigen, wobei sowohl absolute URLs (z.B. <a href="http://meinserver.at/links.wml">) als auch relative URLs (z.B. <a href="news/wetter.wml">) möglich sind.

Weil manche WAP-Devices mit den relativen Angaben nichts anfangen können, sollten besser absolute URLs verwendet werden.

Selbstverständlich muß jede Card abgeschlossen und zuletzt auch das WML-Dokument beendet werden:

```
</card>
</wml>
```

Neben den aus HTML bekannten Tags wie <p>, <b>, <a href="..."> etc. stehen in WML auch einige Meta-Tags zur Verfügung, um bestimmte Aktionen durchzuführen. So haben WAP-Handies derzeit noch keine *Back*-Taste, mit der man zum vorigen Dokument zurückkehren kann. Angesichts der ohnehin eingeschränkten Bedienungsfreundlichkeit der WAP-Handies freuen sich WAP-Surfer im allgemeinen nicht besonders, wenn sie in einer „Sackgasse“ festsitzen. Deshalb besteht die Möglichkeit, mit dem <do>-Tag den Handy-eigenen Funktionstasten bestimmte Aktionen zuzuweisen. <do>-Tags definiert man folgendermaßen:

```
<do type="..." label="...">
...
</do>
```

Der Typ (z.B. *accept* oder *prev*) dient den Handies nur zur Information und muß daher nicht unbedingt angegeben werden. Das Label ist der Text, der der Funktionstaste zugewiesen wird. Innerhalb des <do>-Tags steht dann die eigentliche Aktion, die durch Betätigen der Taste ausgeführt wird. Das folgende Beispiel legt auf die linke Funktionstaste einen Link zu einer weiteren Card und auf die rechte eine Back-Taste:

```
<do type="accept" label="Next">
<go href="#card2"/>
</do>
<do type="prev" label="Back">
<prev/>
</do>
```

<do>-Definitionen können entweder innerhalb einer Card oder auf Deck-Ebene (für alle Cards gültig) angegeben werden.

Selbstverständlich ist auch das Erstellen von Formularen mit WML möglich. Um ein Texteingabefeld zu erzeugen, genügt ein <input>-Tag innerhalb einer Card; um die Eingabe auszuwerten (z.B. um sie an ein CGI-Skript zu senden oder in einer anderen Card auszugeben), verwendet man den Namen des <input>-Feldes mit vorangestelltem \$ als Variable. Das folgende Beispiel erzeugt zwei Formularfelder, deren Inhalt nach einem Klick auf *Abschicken* an ein CGI-Skript gesendet wird:

```
<p>Nachname: <input name="nach"/><br/></p>
<p>Vorname: <input name="vor"/><br/></p>
<p><br/>
<a href="http://meinserver.at/cgi-bin/
foo.cgi?vor=${vor} & nach=${nach}" >
Abschicken</a>
</p>
```

## Was Andere Publizieren

### Informationen über WAP:

- WAP-Forum  
<http://www.wapforum.org/>
- Nokia Developer Forum  
<http://www.forum.nokia.com/>
- Ericsson Developers' Zone  
<http://www.ericsson.com/developerszone/>
- SelfWML (WML-Seiten selbst erstellen)  
<http://www.selfwml.f2s.com/>
- WAP-Magazin  
<http://www.wap-magazin.de/>

### Links für's WAP-Handy:

- „Der Standard“ on WAP  
<http://derstandard.at/Wap/>
- „Die Presse“ on WAP  
<http://wap.diepresse.at/>
- ORF ON Mobile  
<http://wap.orf.at/>
- Telefonbuch  
<http://wap.otb.at/>
- Google on WAP  
<http://wap.google.com/>
- Yahoo on WAP  
<http://wap.yahoo.com/>
- Fireball on WAP  
<http://wap.fireball.de/>
- MTV on WAP  
<http://www.mtvhome.de/wap/>
- Heise Verlag (c't, iX)  
<http://wap.heise.de/>

Diese Beispiele umfassen natürlich nur einen kleinen Teil der WML-Syntax. Weiterführende Seiten zu diesem Thema finden Sie im Kasten *Was Andere Publizieren*.

## Wiener Akademiker Probieren's

Der Zentrale Informatikdienst der Universität Wien bietet nun auch Services für mobile Surfer an. Derzeit kann man unter <http://wap.univie.ac.at/> auf das Telefonverzeichnis der Uni Wien zugreifen, außerdem werden Links zu den bestehenden WAP-Seiten von Instituten aufgelistet.

Falls Sie auf Ihrem Mailbox- bzw. Unet-Webpace ebenfalls WAP-Seiten zur Verfügung stellen möchten, müssen Sie die fertigen Seiten mit der Endung *.wml* (bzw. *.wbmp* für WAP-Bitmaps) abspeichern. Die Start-Seite in einem Verzeichnis (diese wird angezeigt, wenn Sie im URL nicht auf eine konkrete Datei, sondern nur auf ein Verzeichnis verweisen) sollte *index.wml* heißen. Viel Spaß beim Wappen!

Lukas Ertl ■

# GRUNDBEGRIFFE DER KRYPTOGRAPHIE

Die Geschichte der Geheimschriften ist fast so lang wie die Geschichte der Schrift – schon Julius Caesar hat Geheimschriften verwendet. In zahlreichen Klassikern der Kriminalliteratur (z.B. bei Edgar Allan Poe oder bei Arthur Conan Doyle) kommen Geheimschriften vor. Verglichen mit heutigen Methoden der Kryptographie sind solche Geheimschriften allerdings kindische Spielereien: Heute ist die Kryptographie ein Industriezweig, der Milliarden umsetzt, viele der besten Mathematiker beschäftigt und die leistungsfähigsten und teuersten Supercomputer einsetzt. Lange Zeit auf Militär und Geheimdienste beschränkt, gehört Kryptographie im Zeitalter des *electronic commerce* zum Alltag des Geschäftslebens.

Die Grundaufgabe der Kryptographie läßt sich sehr einfach formulieren: Aus einem Klartext (engl. *plain text*) wird mit Hilfe eines Schlüssels (engl. *key*) ein verschlüsselter Text (engl. *cipher text*) erzeugt. Dieser Text wird – heutzutage fast ausschließlich elektronisch – einem Adressaten übermittelt, und niemand außer dem Empfänger, für den die Nachricht bestimmt ist, soll instande sein, daraus den Klartext wiederherzustellen. Trotz der Bezeichnung *plain text* sind Kryptisierungsverfahren nicht auf Text-Daten beschränkt: Jede Form von Daten wird binär kodiert und als Folge von Einsen und Nullen dargestellt. Jede solche Folge kann auch als Binärzahl interpretiert werden. Kryptisierungs-Algorithmen können daher ohne Einschränkung der Allgemeinheit nur für die Verschlüsselung von Zahlen definiert werden. Die angewendeten Methoden sind keineswegs geheim – alle Algorithmen sind publiziert und können von allen nachvollzogen werden. Im folgenden werden einige der wichtigsten kryptographischen Verfahren vorgestellt.

## Symmetrische Verfahren

Symmetrische Verfahren werden so genannt, weil derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln dient. Dieser Schlüssel ist einfach eine Zahl. Die meisten symmetrischen Verfahren sind sogenannte *block ciphers*, d.h. der zu verschlüsselnde Text wird in Blöcke zerlegt und jeder einzelne Block mit dem Schlüssel kryptisiert. Die übliche Länge eines Blocks ist 64 Bit, das entspricht acht Zeichen, wenn der für Text-Daten allgemein gebräuchliche ASCII-Zeichensatz verwendet wird. In der Praxis wird dieses Verfahren etwas modifiziert: Die Blöcke werden zusätzlichen Operationen unterworfen, sodaß identische Blöcke nicht dasselbe Ergebnis bei der Kryptisierung liefern.

Jeder Verschlüsselungs-Algorithmus besteht aus einer wohldefinierten, nicht allzu langen Folge von einfachen arithmetischen und logischen Operationen (Permutationen, Additionen, und/oder etc.). Symmetrische Kryptisierung geht sehr schnell, sodaß auch große Datenmengen in kurzer Zeit ver- und entschlüsselt werden können.

Eine wichtige Kennzahl jedes symmetrischen Algorithmus ist die Länge des Schlüssels: Jede symmetrische Kryptisierung kann (zumindest theoretisch) dadurch geknackt werden, daß alle möglichen Schlüssel durchprobiert werden. Bei einer Länge von 40 Bit gibt es 1 099 511 627 776 mögliche Schlüssel. Schafft man eine Million Schlüssel pro Sekunde (für leistungsfähige moderne Computer ist das durchaus realistisch), braucht man für eine solche *Brute Force*-Angriffe knapp zwei Wochen. Die Vermutung liegt nahe, daß Geheimdienste und ähnliche Organisationen, die sich auf das Knacken von Codes spezialisieren, über wesentlich leistungsfähigere Spezial-Hardware verfügen und dafür höchstens einige Minuten brauchen: Was mit 40 Bit verschlüsselt durch das Netz geschickt wird, kann vermutlich fast in Echtzeit geknackt werden.<sup>1)</sup> Eine Schlüssellänge von 128 Bit hingegen dürfte auch den besten Code-Knackern mit den schnellsten Computern Kopfzerbrechen bereiten: Selbst wenn man eine Billion ( $10^{12}$ ) Schlüssel pro Sekunde probieren könnte, würde man mit *Brute Force*  $10^{19}$  Jahre brauchen – das ist mehr als eine Milliarde Mal so lang wie das Alter der Erde.

Eine ausreichende Länge des Schlüssels ist für ein sicheres Kryptisierungsverfahren notwendig, aber nicht hinreichend. Der Algorithmus selbst kann Mängel haben, die es ermöglichen, mit verschiedenen Methoden – die wesentlich intelligenter sind als die oben beschriebene *Brute Force*-Angriffe – den Code zu knacken. Kryptographie ist ein sehr aktives Forschungsgebiet: Ständig werden neue Algorithmen erfunden; manche können recht schnell geknackt werden und geraten wieder in Vergessenheit, andere bewähren sich und widerstehen jahrelang allen Angriffen. Solche Algorithmen gelten dann allgemein als vertrauenswürdig. Einen strengen Beweis der Sicherheit eines Kryptisierungsverfahrens kann es allerdings nie geben.

Lange Zeit war der *Data Encryption Standard* (DES) das am weitesten verbreitete symmetrische Verfahren. Heute hat er weitgehend ausgedient, hauptsächlich wegen der bescheidenen Länge seines Schlüssels von 56 Bit, was für heutige Anforderungen viel zu wenig ist. Nur in der Variante des Triple DES (3DES), bei dem im wesentlichen der DES-Algorithmus dreimal hintereinander mit drei verschiedenen Schlüsseln verwendet wird, ist er heute noch in Gebrauch. Von den zahlreichen moderneren symmetrischen Verfahren seien hier drei der wichtigsten erwähnt:

- IDEA ist eine Entwicklung der Schweizer Firma Ascom (siehe <http://www.ascom.ch/>) und verwendet Schlüssel mit 128 Bit.
- RC4 war lange Zeit nur der Firma RSA (siehe weiter

1) In den USA ist der Export von „starker“ Kryptographie verboten. Beispielsweise verwenden die für den Export zugelassenen Netscape-Versionen Schlüssel mit einer Länge von 128 Bit, von denen aber nur 40 Bit geheim sind – den Rest kennt die US-Regierung.

unten) zugänglich und ist heute mit 128 Bit das Standardverfahren bei Secure HTTP.

- Blowfish (<http://www.counterpane.com/blowfish.html>) ist „freie Software“ – weder der Algorithmus noch die Implementation unterliegen irgendwelchen Lizenz-Beschränkungen. Die Länge des Schlüssels ist variabel bis zu 448 Bit.

## Asymmetrische Verfahren

Bei asymmetrischen Verfahren (*public-key cryptography*) werden verschiedene Schlüssel zum Ver- und Entschlüsseln verwendet. Zum Verschlüsseln dient der *public key*, der, wie der Name schon sagt, öffentlich bekanntgegeben wird. Zum Entschlüsseln wird der *private key* benötigt, der von seinem Besitzer sorgfältig verwahrt werden muß und auf den sonst niemand Zugriff haben darf: Sobald jemand anderer den *private key* kennt, ist er wertlos. Wer eine asymmetrisch verschlüsselte Nachricht verschicken will, muß den *public key* des Empfängers kennen. Für manche Formen der sicheren Kommunikation benötigen beide Partner einen *public key* – jeder verschlüsselt mit dem Schlüssel des anderen.

Die meisten asymmetrischen Verfahren beruhen auf folgenden zwei Tatsachen:

- Es ist sehr leicht festzustellen, ob eine ganze Zahl eine Primzahl ist oder nicht. Selbst bei Zahlen mit mehreren hundert Ziffern (solche werden in der asymmetrischen Kryptographie üblicherweise verwendet) braucht ein Computer dazu nur Sekundenbruchteile.
- Wenn eine Zahl keine Primzahl ist, hat sie mindestens zwei echte Primfaktoren. Es ist jedoch kein Verfahren bekannt, bei großen Zahlen diese Faktoren auch in sinnvoller Zeit zu finden (von Sonderfällen abgesehen, z.B. wenn einer der Primfaktoren sehr klein ist oder wenn die Zahl sonstige spezielle Eigenschaften hat, die die Faktorisierung erleichtern).

Um ein Schlüsselpaar – *public* und *private key* – zu erzeugen, geht man folgendermaßen vor:

- Man generiert zwei Primzahlen von bestimmter Größe (üblich sind 512 Bit, das entspricht im Dezimalsystem 153 oder 154 Ziffern). Dazu probiert man einfach eine Reihe von Zufallszahlen so lange durch, bis man Primzahlen findet. Die Wahrscheinlichkeit, daß eine beliebige Zahl dieser Größenordnung eine Primzahl ist, beträgt nach dem Primzahlsatz etwa  $1/350$ ; man muß also meistens einige hundert Zahlen probieren, sofern man nicht das Verfahren verfeinert und z.B. Zahlen mit kleinen Primfaktoren von vornherein ausschließt. So oder so dauert dieser Vorgang höchstens einige Sekunden.
- Man bildet das Produkt dieser beiden Primzahlen. Nun kann – wie oben beschrieben – niemand auf der Welt in absehbarer Zeit die beiden Primfaktoren aus dem Produkt rekonstruieren. Das Produkt ist der Hauptbestandteil des *public key*; die beiden Primfaktoren (die nur derjenige kennt, der sie multipliziert hat) bilden den Hauptbestandteil des *private key*.

Das bekannteste und mit Abstand am meisten verwendete asymmetrische Verfahren ist die RSA-Methode, so benannt nach den Initialen der Erfinder (Rivest, Shamir, Adleman). Die arithmetischen Operationen, die beim RSA-Verfahren ausgeführt werden (Exponentiation und Restklassenbildung), sind wesentlich aufwendiger als bei symmetrischen Verfahren, weshalb RSA für große Datenmengen ungeeignet ist. Ausführliche Informationen zum RSA-Verfahren und zur Kryptographie im allgemeinen finden Sie unter <http://www.rsa.com/>; sehr informativ sind vor allem die *Frequently Asked Questions* unter <http://www.rsasecurity.com/rsalabs/faq/>.

## Kombinierte Verfahren

Während der relativ hohe Rechenaufwand ein Nachteil asymmetrischer Verfahren ist, ist das Hauptproblem bei symmetrischer Kryptisierung der sichere Austausch des Schlüssels: Es muß ein Weg gefunden werden, dem Partner den Schlüssel mitzuteilen, ohne daß er von einem Dritten abgefangen werden kann. In der Praxis wird deshalb fast immer eine Kombination aus symmetrischer und asymmetrischer Kryptisierung verwendet, die die Vorteile beider Methoden vereint: Beim PGP-Verfahren zur Verschlüsselung von eMail (siehe *Comment 97/2*, Seite 17), beim Secure HTTP-Protokoll zur sicheren Kommunikation mit Webservern (siehe *Comment 97/2*, Seite 22, und *Comment 00/2*, Seite 25) und auch bei der Secure Shell (siehe Seite 23). Eine sichere Verbindung mit einem dieser Protokolle wird nach folgender Methode – mit verschiedenen Varianten – durchgeführt: Einer der beiden Partner wählt eine Zufallszahl als Schlüssel für symmetrische Kryptisierung und verschlüsselt diesen Schlüssel mit dem *public key* des anderen Partners. Der verschlüsselte Schlüssel wird dem Partner mitgeteilt. Für diesen ist das eine „Herausforderung“ (*challenge*) – er muß imstande sein, ihn mit seinem *private key* zu entschlüsseln. Der Rest der Verbindung zwischen den Partnern wird nach einem symmetrischen Verfahren mit diesem Schlüssel kryptisiert. Generell werden symmetrische Schlüssel nur einmal verwendet (manchmal wird sogar während der Datenübertragung der Schlüssel gewechselt), während asymmetrische Schlüsselpaare jahrelang eingesetzt werden.

## Digitale Unterschriften

Vielleicht haben Sie schon einmal eine eMail-Nachricht bekommen, die am Ende die Zeile --BEGIN PGP SIGNATURE-- enthielt, gefolgt von einigen Zeilen mit unverständlichen Buchstaben und Ziffern. Diese unverständlichen Zeichen bilden eine „digitale Unterschrift“, mit der sichergestellt werden soll, daß eine Nachricht einerseits nicht verfälscht wurde und andererseits wirklich vom angegebenen Absender stammt. Dies ist z.B. für rechtsverbindliche Unterschriften im elektronischen Zahlungsverkehr unerlässlich. Um ein Dokument digital zu signieren, sind zwei Schritte erforderlich:

- Im ersten Schritt wird eine *hash function* des Dokuments berechnet. Der Wert dieser *hash function* ist sozusagen

ein „Fingerabdruck“ des Dokuments: Er ist nur vom Dokument und dem verwendeten Algorithmus abhängig, benötigt also keine Zusatzinformationen wie z.B. Schlüssel. Er ist relativ kurz (üblich sind einige hundert Zeichen) und von konstanter Länge, egal wie lang der Text ist. Es gibt verschiedene Hash-Algorithmen, die bekanntesten sind MD5 (*Message Digest*) und SHA-1 (*Secure Hash Algorithm*). Ein guter Hash-Algorithmus soll einerseits nicht erlauben, aus dem Wert der *hash function* Rückschlüsse auf den Originaltext zu ziehen (die Änderung eines einzigen Bits führt zu einem völlig unterschiedlichen Ergebnis); andererseits soll es praktisch unmöglich sein, zwei verschiedene Texte zu finden, bei denen die *hash function* denselben Wert hat, obwohl man sehr leicht zeigen kann, daß viele solcher Texte existieren. Die Entwicklung von guten Hash-Algorithmen gehört zu den schwierigsten Aufgaben der Kryptographie: Immer wieder werden Hash-Algorithmen aus dem Verkehr gezogen, meist weil sie das zweite Kriterium nicht ausreichend erfüllen (so z.B. vor einigen Jahren das MD4-Verfahren).

- Im zweiten Schritt wird die *hash function* mit dem *private key* des Absenders verschlüsselt. Meistens wird dazu das RSA-Verfahren verwendet (allerdings in der umgekehrten Richtung, also mit dem *private key* zum Verschlüsseln und dem *public key* zum Entschlüsseln); es gibt aber auch einen eigenen *Digital Signature Algorithm* (DSA). Die so verschlüsselte *hash function* ist die digitale Unterschrift, die gemeinsam mit dem Dokument an den Empfänger geschickt wird.

Um eine digitale Unterschrift zu überprüfen, geht der Empfänger eines Dokuments folgendermaßen vor:

- Die digitale Unterschrift wird mit dem *public key* des Senders entschlüsselt.

- Ebenso wie der Sender bestimmt der Empfänger die *hash function* des Dokuments.
- Die Ergebnisse dieser beiden Schritte müssen exakt übereinstimmen. Sind sie unterschiedlich, wurde entweder das Dokument verfälscht oder es wurde ein falscher *private key* zum Signieren verwendet.

Ein fundamentales Problem der *public-key cryptography* wird allerdings auch mit digitalen Unterschriften nicht gelöst: Es kann keine absolute Garantie für die Authentizität eines Schlüssels geben, irgend jemandem muß man wohl oder übel vertrauen. Wenn die Firma A ihren *public key* veröffentlicht, gibt es keinen Nachweis, daß tatsächlich die Firma A dahintersteckt – es könnte auch die Firma B sein, die die Geheimnisse der Firma A ausspähen will. A kann sich ihren *public key* von der Firma C mit einem Zertifikat (d.h. einer digitalen Unterschrift) beglaubigen lassen; nun muß man aber dem *public key* von C vertrauen, es sei denn, C besorgt sich ein Zertifikat von D, und so weiter ad infinitum. Wie gesagt, absolute Garantie gibt es keine, aber anerkannte Zertifizierungs-Stellen (z.B. jene, die von den großen Browser-Herstellern akzeptiert werden), sind wohl recht vertrauenswürdig.

In Österreich soll das Bundesgesetz über elektronische Signaturen, das am 1. Jänner 2000 in Kraft getreten ist, die Voraussetzungen dafür schaffen, daß „*elektronische Signaturen die Rechtswirkungen der Schriftlichkeit entfalten*“, wie es in der schönen Formulierung des § 4.(2) heißt. In diesem Gesetz ist die Einrichtung von staatlich anerkannten Zertifizierungsstellen vorgesehen. Einige solcher Stellen existieren bereits (z.B. A-Trust, <http://www.a-trust.at/>), allerdings sind diese Systeme noch nicht sehr ausgereift.

Peter Marksteiner ■

## NEUE SOFTWARE & SECURE SERVER AUF WWW.UNIVIE.AC.AT

Weitgehend unbemerkt von den Benutzern wurden im September 2000 die auf dem Webserver WWW.UNIVIE.AC.AT eingesetzten Softwareprodukte auf den neuesten Stand gebracht und einige Altlasten beseitigt. Beispielsweise wurde der Port 82 endgültig stillgelegt; die früher dort angesiedelten Datenbankabfragen befinden sich jetzt alle auf dem Server DATA.UNIVIE.AC.AT. Es werden auch einige neue Dienste angeboten, die hauptsächlich für die Betreiber von Instituts-Homepages und sonstigen Subservern von Interesse sind (eine ausführliche Dokumentation finden Sie unter <http://www.univie.ac.at/www-service.html>). Die wichtigsten Neuerungen sind folgende:

- Der Server verfügt jetzt über ein von Thawte ausgestelltes **Zertifikat** und unterstützt auch das **Secure HTTP**-Protokoll, d.h. alle Dokumente können sowohl über <http://www.univie.ac.at/> als auch über <https://www.univie.ac.at/> abgerufen werden.
- Es ist nun möglich, **Mailbox- und Unet-Paßwörter zur Authentifizierung** bei paßwortgeschützten Bereichen einzusetzen. Die Paßwörter werden mittels Datenbankabfrage überprüft und sind daher immer aktuell. Der Personenkreis, dem der Zugang zu einem bestimmten Verzeichnis gestattet wird, kann wahlweise noch weiter eingeschränkt werden: Entweder durch eine Liste zugriffsberechtigter UserIDs, die vom Betreuer der Webseite selbst verwaltet wird, oder mit Hilfe gewisser Auswahlkriterien (z.B. *Alle Angehörigen des Instituts für Psychologie* oder *Alle Medizinstudenten im zweiten Studienabschnitt*). Näheres dazu finden Sie unter <http://www.univie.ac.at/authentication/>.

Peter Marksteiner



# SECURE SHELL (SSH): KOMMUNIKATION IM FLÜSTERTON

## Secure Shell? Was ist das?

Computersicherheit ist der Schwerpunkt dieser *Comment*-Ausgabe (siehe auch Seite 2, Seite 20 und <http://www.univie.ac.at/ZID/security.html>). Der folgende Artikel kann ebenfalls dieser Kategorie zugeordnet werden: Secure Shell (SSH) ist ein Netzwerkprotokoll, das den Datenverkehr zwischen zwei Rechnern in verschlüsselter Form abwickelt und somit einen guten Schutz gegen gewisse Angriffe aus dem Netzwerk (*packet sniffing* und *spoofing*)<sup>1)</sup> bietet. SSH kann für folgende Aufgaben eingesetzt werden:

- als Terminalemulation (*remote login*, Ersatz für Telnet),
- für Dateiübertragung (*remote copy*, Ersatz für FTP),
- zum Ausführen von Befehlen auf anderen Servern (*remote execution*) und
- zum „Tunneln“ beliebiger Protokolle: Praktisch der gesamte Netzwerkverkehr – vor allem auch eMail – kann bei Bedarf verschlüsselt übertragen werden.

## Wer braucht das?

Während *spoofing* eher selten ist und nur von hochmotivierten Hackern mit profunden technischen Kenntnissen durchgeführt wird, ist *packet sniffing* in vielen Netzen eine reale Gefahr. In folgenden Situationen wird die Verwendung der Secure Shell empfohlen:

- Prinzipiell als Ersatz für Telnet und FTP: Die Secure Shell funktioniert genauso komfortabel, bietet aber erhöhte Sicherheit. Wenn Sie selbst einen Server betreiben, sollten Sie – wenn möglich – Telnet- und FTP-Zugriffe überhaupt verbieten und nur SSH-Verbindungen zulassen.
- Wenn jemand aus einem „Fremdnetz“ (z.B. während eines Auslandsaufenthalts) auf den Mailbox-Rechner zugreifen will, um einerseits mit POP3 eMail abzuholen und andererseits mit FTP seine Homepage zu warten. In diesem Fall wäre es vollkommen sinnlos, *secure copy* anstatt FTP zu verwenden, solange alle paar Minuten eine POP3-Anfrage das Paßwort unverschlüsselt über das Netz schickt. Hier empfiehlt sich das Verschlüsseln des eMail-Verkehrs mit Hilfe eines SSH-Tunnels. Inner-

1) Unter *packet sniffing* versteht man das Abhören des gesamten Datenverkehrs in einem bestimmten Netzwerkbereich durch einen anderen Netzteilnehmer. Da mit SSH alle Daten (also auch alle Paßwörter) verschlüsselt übertragen werden, sind die erlauschten Informationen für den Übeltäter wertlos. *Spoofing* (IP oder DNS *spoofing*) bedeutet, daß ein Server X im Netzwerk mit Hilfe verschiedener Tricks vortäuscht, Server Y zu sein, und daher Verbindungen von Klienten entgegennehmen kann, die an Server Y gerichtet sind. Bei Verwendung der Secure Shell hat der Klient jedoch die Möglichkeit, die Identität des Servers anhand eines Zertifikats zu überprüfen.

2) <http://ftp.univie.ac.at/netinfo/rfc/rfc1700.txt> oder <http://ftp.univie.ac.at/netinfo/assignments/port-numbers>

halb des Datennetzes der Universität Wien ist die Gefahr geringer; bei erhöhtem Sicherheitsbedürfnis ist ein SSH-Tunnel jedoch auch hier angebracht.

Obwohl sich der Aufbau eines Tunnels weitgehend automatisieren läßt, ist die Konfiguration eines Mail-Klienten mit SSH-Tunnel relativ umständlich. Es gibt auch Alternativen, um eMail sicher zu bearbeiten: Entweder mittels *slogin* auf dem Mailserver oder mittels Webmail über Secure HTTP. Für Unet- und Mailbox-Benutzer wird eine solche Webmail-Lösung demnächst angeboten werden. Generell wenig Sinn macht ein SSH-Tunnel bei Verwendung des Wählleitungszugangs zur Uni Wien.

## Wie geht das?

Um die Funktionsweise der Secure Shell zu verstehen, benötigt man Grundkenntnisse der Kryptographie (siehe Artikel auf Seite 20) und der Client/Server-Kommunikation. Das Client/Server-Prinzip, auf dem fast alle Verbindungen in Computernetzwerken basieren, sei im folgenden kurz erläutert:

Ein *Server* ist ein Rechner im Netzwerk, der ständig in Betrieb ist und Anfragen von *Klienten* entgegennimmt und bearbeitet. Als Klienten bezeichnet man die Netzwerkprogramme (z.B. Mailprogramme, Web-Browser), die auf den lokalen Arbeitsplatzrechnern installiert sind. Server und Klienten kommunizieren nach wohldefinierten Regeln (*Protokollen*). Solange diese Regeln eingehalten werden, können sich die unterschiedlichsten Klienten auf verschiedensten Rechner-typen mit beliebigen Servern verständigen. Beispiele für Protokolle sind die bereits erwähnten Protokolle Telnet und FTP (*file transfer protocol*); das *hypertext transfer protocol* (HTTP), auf dem das WWW beruht; das *simple mail transfer protocol* (SMTP) bzw. das *post office protocol* (POP3) zum Verschicken bzw. zum Abholen von eMail – und auch das Secure Shell-Protokoll. Leider gibt es von letzterem zwei Versionen (SSH1 und SSH2), die teilweise inkompatibel sind, sodaß nicht jeder SSH-Klient mit jedem Server kommunizieren kann.

Damit ein Klient eine Verbindung zu einem Server aufbauen kann, muß zusätzlich zur Netzwerkadresse (IP-Adresse) des Servers auch der *Port* angegeben werden – das ist ein durch eine eindeutige Nummer identifizierter Kommunikationskanal. Ein Server ist imstande, auf mehreren Ports gleichzeitig Verbindungen entgegenzunehmen und so verschiedene Services anzubieten (z.B. WWW und eMail). Für viele Protokolle gibt es bereits vordefinierte Ports: Beispielsweise ist Port 22 für Secure Shell vorgesehen, Port 23 für Telnet, Port 25 für SMTP, Port 80 für HTTP und Port 110 für POP3. Die Zuordnung von Protokollen zu Ports ist eine Konvention, die im RFC 1700<sup>2)</sup> definiert ist, aber keine absolute Not-

wendigkeit. Zahlreiche Webserver verwenden z.B. andere Ports als den Standard-Port 80; der URL erweitert sich dann um einen Doppelpunkt und eine Zahl, die den Port bezeichnet (z.B. <http://aleph.univie.ac.at:4505/ALEPH>).

Der Aufbau einer Secure Shell-Verbindung funktioniert nun folgendermaßen:

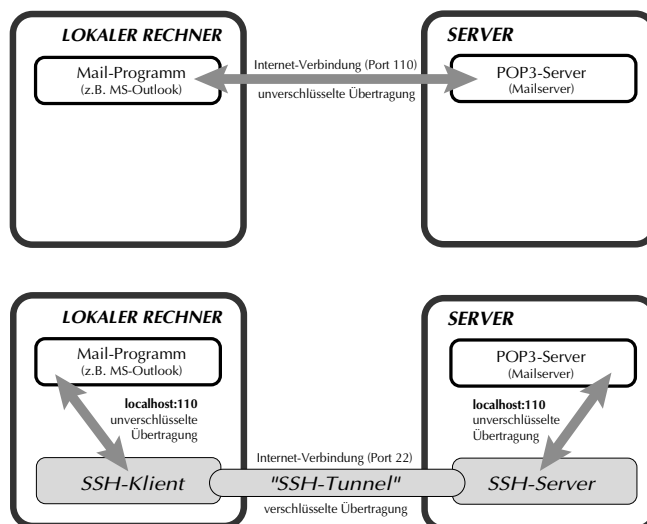
1. Nachdem der SSH-Klient den Server kontaktiert hat, schickt ihm der Server seinen *public key*.
2. Der Klient hat Zugriff auf eine Datei (diese heißt üblicherweise *known\_hosts*) mit den *public keys* aller Server, denen der Klient vertraut. Wenn es für den kontaktierten Server keinen Eintrag in dieser Datei gibt, wird die Verbindung nur dann errichtet, wenn man bestätigt, diesen Schlüssel zu akzeptieren. Er wird dann in die Liste der *known hosts* aufgenommen. Falls es einen Eintrag mit einem unterschiedlichen Schlüssel gibt, liegt der Verdacht auf *spoofing* nahe; der Verbindungsaufbau wird dann meistens mit einer Fehlermeldung abgebrochen (manche Klienten liefern nur eine Warnung und stellen es dem Benutzer frei, die Verbindung dennoch zu errichten).
3. Wie auf Seite 21 beschrieben, wird der *public key* zum sicheren Austausch eines symmetrischen Schlüssels verwendet; der Rest der Verbindung wird nach einem symmetrischen Verfahren (3DES, Blowfish) verschlüsselt.
4. Die Authentifizierung des Klienten gegenüber dem Server kann wie gewohnt mittels Paßwort erfolgen, das verschlüsselt übertragen wird. Es kann aber auch der Server eine Datei (üblicherweise *authorized\_keys*) mit den *public keys* aller Klienten führen, die sich ausreichend authentifiziert haben. Der Klient authentifiziert sich dadurch, daß er eine vom Server geschickte „Herausforderung“ (*challenge*) mit seinem *private key* entschlüsseln kann. Diese Art von Verbindung eignet sich sehr gut für automatische Prozeduren, die ohne händische Eingriffe (Eintippen von Paßwörtern) auskommen müssen.

## Tunnel

Mit Hilfe eines Tunnels kann der Datenverkehr beliebiger Protokolle<sup>3)</sup> – also auch POP3 – verschlüsselt übertragen werden. Dies geht folgendermaßen vor sich:

- Der SSH-Klient wartet auf einem bestimmten Port auf Netzwerkverbindungen (z.B. auf Port 110 auf Verbindungen von einem POP3-Klienten), d.h. der SSH-Klient übernimmt auch die Funktion eines Servers. Da solche Verbindungen üblicherweise nur vom lokalen Rechner (dem *localhost*) aus aufgebaut werden, wird der SSH-Klient bei einer POP3-Verbindung als *localhost:110* adressiert.
- Sobald eine Verbindung zu diesem Port des SSH-Klienten aufgebaut wird, errichtet der SSH-Klient eine Verbindung zum SSH-Server (dem sogenannten *sshd daemon*) am gewünschten Server. Diese Verbindung wird als Tunnel be-

3) Bei manchen Protokollen ist das Tunneln schwierig, weil mehrere Verbindungen auf unterschiedlichen Ports beteiligt sind: Beim FTP-Protokoll gibt es z.B. die Datenverbindung (Port 20) und die Kontrollverbindung (Port 21). Daher ist es einfacher, anstatt eines FTP-Tunnels *scp* zu verwenden.



**Abb. 1: POP3-Verbindung ohne (oben) und mit (unten) SSH-Tunnel**

zeichnet; alle Daten, die an den SSH-Klienten geschickt werden, werden automatisch verschlüsselt und durch diesen Tunnel weitergeleitet.

- Der SSH-Server entschlüsselt die Daten und reicht sie an den endgültigen Adressaten weiter – z.B. an den POP3-Server, der aus der Sicht des SSH-Servers ebenfalls als *localhost:110* angesprochen werden muß.

Unverschlüsselte Verbindungen gibt es nur lokal: zwischen Mailprogramm (POP3-Klient) und SSH-Klient bzw. zwischen SSH-Server und POP3-Server (siehe Abb. 1).

Um eMail über einen SSH-Tunnel abzuholen, sind also zwei Schritte notwendig: Zuerst müssen Sie in der Konfiguration Ihres Mailprogramms als POP3-Server **localhost** eintragen (der Port 110 ist schon vorkonfiguriert) und anschließend mit Hilfe des SSH-Klienten den Tunnel errichten. Solange kein Tunnel besteht, versucht das Mailprogramm, die für Sie am Mailserver neu eingelangten Nachrichten vom lokalen SSH-Klienten zu erhalten, was natürlich nicht funktioniert.

Ein Spezialfall ist der X11-Tunnel (X11 ist das Protokoll, das für netzwerkfähige grafische Unix-Applikationen verwendet wird): Dabei laufen die Daten vom Server zum Klienten und erlauben das Ausführen von X-Applikationen. Durch X11-Authentication wird sichergestellt, daß nur der Benutzer den Tunnel verwenden kann, der die Verbindung aufgebaut hat.

## SSH-Server

Mit OPEN-SSH 2.0 (<http://www.openssh.com/>) steht auf den Servern des Zentralen Informatikdienstes eine Software zur Verfügung, die folgende Funktionen unterstützt:

- SSH-Protokoll 1 und 2
- RSA- und DSA-Schlüssel
- Symmetrische Kryptisierung mit 3DES (Standardeinstellung) oder Blowfish
- Authentifizierung mit *private key* oder Paßwort
- Interaktives Arbeiten (*slogin*)
- Datentransfer (*scp*)

- Ausführen von Befehlen (*ssh*)
- Verschlüsselung beliebiger Protokolle mittels Tunnelling
- Spezielle Unterstützung für X11-Tunnelling

Diese Software kommt zur Zeit auf folgenden Servern zum Einsatz:

- MAILBOX.UNIVIE.AC.AT
- UNET.UNIVIE.AC.AT (*ohne X11*)
- WWW.UNIVIE.AC.AT (*ohne X11*)
- RS6000.UNIVIE.AC.AT
- ALPHA.UNIVIE.AC.AT

Auf UNET.UNIVIE.AC.AT befindet sich das Homedirectory auf einem DFS-Filesystem und steht daher während des Loginvorgangs noch nicht zur Verfügung. Deshalb funktionieren manche SSH-Features nicht, die Zugriff auf dieses Verzeichnis brauchen (z.B. Authentifizierung mit *private key*).

Eine etwas andere SSH 2.0-Version, die zusätzlich noch *sftp* unterstützt, ist auf den Servern

- MERLIN.AP.UNIVIE.AC.AT (Außenstelle Physik des ZID)
- EMB1.BCC.UNIVIE.AC.AT (Außenstelle Biochemie)

verfügbar. Näheres dazu – auch eine kurze Beschreibung eines geeigneten Windows-Klienten – finden Sie im Kasten auf Seite 27.

Die *public keys* aller genannten Server sind unter <https://www.univie.ac.at/keys/> zu finden.

## SSH-Klienten

Im folgenden werden einige von uns getestete SSH-Klienten für Unix und Windows vorgestellt; weitere SSH-Klienten für verschiedene Plattformen (auch für Macintosh) finden Sie unter <http://www.freessh.org/>.

### Unix

Die Secure Shell wurde ursprünglich für Unix-Systeme entwickelt und erst später auf verschiedene Windows-Plattformen portiert. Die Befehle *ssh*, *slogin* und *scp* sind die „sicheren“ Äquivalente zu den bekannten Unix-Befehlen *rsh* (*remote shell*), *rlogin* (*remote login*) und *rcp* (*remote copy*). Es gibt etliche SSH-Klienten für Unix, bei den Befehlen und Optionen findet man jedoch nur geringe Unterschiede. Details dazu sind auf Unix- oder Linux-Systemen in der entsprechenden Online-Dokumentation (*man pages*) zu finden, z.B. mit *man slogin*. Die wichtigsten Funktionen seien hier anhand einiger Beispiele illustriert:

- Login auf einem anderen Rechner:  
**slogin -l remoteuser remotehost**  
 (z.B. `slogin -v -l broesef7 mailbox.univie.ac.at`)  
**Ann.:** Alle SSH-Befehle können mit der Option *-v* („verbose“) aufgerufen werden, die bei der Fehlersuche sehr nützlich ist.
- Übertragen einer Datei:  
**scp localfile remoteuser@remotehost:remotefile**

(z.B.: `scp index.html`

`broesef7@mailbox.univie.ac.at:html/index.html`)

**Ann.:** Beim SSH-Klienten von *ssh.com* (siehe Seite 27) ist *scp* ein Alias für *sftp*; daher muß hier der Befehl `scp1` verwendet werden, wenn der Server das *sftp*-Protokoll nicht unterstützt.

- Ausführen eines Befehls auf einem anderen Rechner:

**ssh -l remoteuser remotehost "ls -l"**

(z.B.: `ssh -l broesef7 mailbox.univie.ac.at "ls -l"`)

- Aufbau eines POP3-Tunnels:

**ssh -L 60000:localhost:110 remotehost**

(z.B.: `ssh -L 60000:localhost:110 mailbox.univie.ac.at`)

**Ann.:** Unter Unix sind die Ports 1 – 1023 dem Benutzer *root* vorbehalten. Daher muß für POP3 ein freier Port mit hoher Nummer (1024 – 65535) verwendet werden, sofern man keine *root*-Privilegien hat. Wählt man einen hohen Port (z.B. 60000), muß dieser auch in die Konfiguration des Mailklienten eingetragen werden.

### PuTTY & PSCP (für Windows)

Diese beiden Programme (Autor: Simon Tatham; zu finden unter <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>) bestechen durch ihre Einfachheit: Sie bestehen jeweils nur aus einer *.exe*-Datei und haben gemeinsam auf einer Diskette Platz.

Eine Installation ist nicht erforderlich. Will man PuTTY aus dem *Programm*-Menü starten, muß man selbst eine entsprechende Verknüpfung erstellen. Es empfiehlt sich, beim Programmaufruf die Option *-ssh* anzugeben. Wenn dann das Dialogfenster zur Eingabe der Verbindungsdaten erscheint, ist der Punkt *SSH* bereits ausgewählt; man muß nur noch den Hostnamen eingeben und auf **Open** klicken. Bei der ersten Verbindung zu einem bestimmten Rechner fragt das Programm, ob der *public key* dieses Servers (*hostkey*) gespeichert werden soll.<sup>4)</sup> Im anschließend erscheinenden Terminalfenster verlangt das Programm mit dem Text `login as:` Ihre UserID, danach Ihr Paßwort. Eine Besonderheit des SSH-Protokolls ist, daß nach einem Login-Fehlversuch nur das Paßwort nochmals verlangt wird – hat man sich bei der UserID vertippt, muß man den Vorgang durch Schließen des Fensters beenden und von vorne beginnen.

PSCP ist ein Programm zur Dateiübertragung und hat im wesentlichen dieselben Optionen wie die Unix-Variante *scp*. Es arbeitet über Befehlszeilen und muß daher in einem Eingabe-Fenster gestartet werden. Interessant ist die Option *-ls*, welche es ermöglicht, Inhaltsverzeichnisse vom Host abzurufen. Der Kopiervorgang kann entweder vom lokalen

<sup>4)</sup> Bei PuTTY ist es nicht so einfach möglich, die *hostkeys* bereits im vorhinein zu speichern: Die *hostkeys* werden im Windows-Registry in einem eigenen Format abgelegt, da es keine *known\_hosts*-Datei gibt.

Rechner zum Host oder umgekehrt erfolgen. Dabei gilt, daß ein Dateiname, der einen Doppelpunkt enthält, als Hostdatei verarbeitet wird. Die Syntax lautet `user@host:path`, wobei `path` relativ zum Homeverzeichnis des Benutzers `user` angenommen wird. Einige Beispiele veranschaulichen die Funktionalität am besten:

- `pscp -ls hugok4@mailbox.univie.ac.at`  
(Inhalt des Homeverzeichnisses von `hugok4` ansehen)
- `pscp default.html a1234567@unet.univie.ac.at:html/index.html`  
(Kopieren der Datei `default.html` vom lokalen Rechner zum Host unter einem anderen Namen)
- `pscp -r y1234uaa@rs6000.univie.ac.at:daten c:\`  
(Kopieren des Verzeichnisses `daten` mit allen Unterverzeichnissen vom Host zum lokalen Rechner)

Fazit: Klein, aber fein. Besonders empfehlenswert, wenn man unterwegs eMail lesen möchte.

### TeraTerm & TTSSH (für Windows)

Dieses Paket bietet wesentlich mehr Funktionsumfang als PuTTY & PSCP. TeraTerm ist ein ausgezeichnete Terminal-emulator des japanischen Autors T. Teranishi; TTSSH wurde von Robert O'Callahan entwickelt und ist eine Erweiterung dazu, die das SSH-Protokoll implementiert. Die aktuellen Versionen finden Sie unter <http://hp.vector.co.jp/authors/VA002416/teraterm.html> (TeraTerm) und <http://www.zip.com.au/~roca/download.html> (TTSSH).

Die Installation erfolgt in zwei Schritten: Zunächst wird TeraTerm nach Entpacken der ZIP-Datei und Starten von `setup.exe` wie gewohnt installiert. Danach müssen die Dateien aus der TTSSH-ZIP-Datei in dasselbe Verzeichnis kopiert werden, in das zuvor TeraTerm installiert wurde. Will man das Programm über das *Start*-Menü zur Verfügung haben, muß man eine entsprechende Verknüpfung für die Datei `ttssh.exe` herstellen. Die Verknüpfung, die während der Installation von TeraTerm angelegt wurde, startet den Terminalemulator *ohne* SSH-Erweiterung.

Der Verbindungsaufbau verläuft ähnlich wie bei PuTTY. Nach dem Programmstart erhält man ein Fenster mit den Verbindungsdaten. Hier müssen Sie den gewünschten Hostnamen eingeben und auf **OK** klicken. Es folgt die Überprüfung des *hostkey*; wenn dieser in der Datei `known_hosts` nicht gefunden wird, erscheint eine Warnung. Man kann dann entweder die Verbindung abbrechen oder den unbekannten *hostkey* akzeptieren und optional in die `known_hosts`-Datei aufnehmen. (Ist der *hostkey* des gewünschten Servers aus einer anderen, sicheren Quelle bereits bekannt, kann man ihn schon vor dem Programmstart mit einem Texteditor in die Datei `ssh_known_hosts` eintragen, die sich im TeraTerm-Installationsverzeichnis befinden muß.) Das folgende Fenster dient der Authentifizierung am Server. Man gibt UserID und Paßwort (hier *Passphrase* genannt) ein, wählt **Use plain password to log in** und klickt auf **OK**. Auch hier gilt, daß eine Fehleingabe bei der UserID nicht korrigiert werden kann.

Wer viel in Terminalfenstern arbeitet, wird die gute und einfache Konfigurierbarkeit von TeraTerm schätzen lernen. Alle Einstellungen sind im Menüpunkt **Setup** vorzunehmen. Unter *Font* können Sie eine Ihnen genehme Schriftart aussuchen und unter *Terminal* unter anderem die Größe des Fensters bestimmen, in dem Sie arbeiten wollen. Falls Sie sich auf mehreren Rechnern per SSH einloggen, empfehle ich Ihnen, Ihre Terminalfenster je nach Rechner verschieden einzufärben. Sie sehen dann sofort, auf welchem Rechner Sie sich gerade befinden, und die Gefahr, ein `rm -rf *` (der Unix-Befehl zum Löschen aller Dateien und Unterverzeichnisse) versehentlich in einem Terminalfenster einzugeben, wo man es auf keinen Fall tun hätte sollen, wird wesentlich geringer. Stellen Sie sich für jeden Host, auf den Sie zugreifen, die gewünschten Parameter ein und speichern Sie diese mittels Klick auf **Setup – Save Setup** in einer separaten Konfigurationsdatei (z.B. `www.ini`).

Nachdem Sie eine solche Konfigurationsdatei erstellt haben, können Sie sich für jeden Rechner, zu dem Sie Kontakt aufnehmen, eine Verknüpfung auf Ihren Bildschirm „zaubern“: Klicken Sie mit der rechten Maustaste auf Ihren Desktop, wählen Sie **Neu – Verknüpfung** und anschließend die Datei `ttssh.exe` (meistens zu finden unter `C:\Programme\TTERMPRO\ttssh.exe`). Nun wird ein neues Symbol erstellt. In den *Eigenschaften* dieses Symbols erweitern Sie unter **Verknüpfung – Ziel** den Programmaufruf um die Einträge `hostname:22` und `/F=hostname.ini`, also z.B. `C:\Programme\TTERMPRO\ttssh.exe www.univie.ac.at:22 /F=www.ini` (siehe Abb. 2). Diese Zeile bewirkt, daß nach Doppelklick auf das neue Symbol eine Verbindung zum SSH-Port des Rechners WWW.UNIVIE.AC.AT aufgebaut und die unter `www.ini` gesicherte Konfiguration geladen wird.

Auch wenn Sie sich nie per Telnet/SSH in einen Rechner einloggen, kann Ihnen TeraTerm gute Dienste erweisen: Sie können damit beliebige Protokolle „tunneln“ und somit abhörsicher machen. Ein Protokoll, das Sie sicher verwenden, ist jenes, mit dem Sie eMail vom Server holen: POP3 oder IMAP.

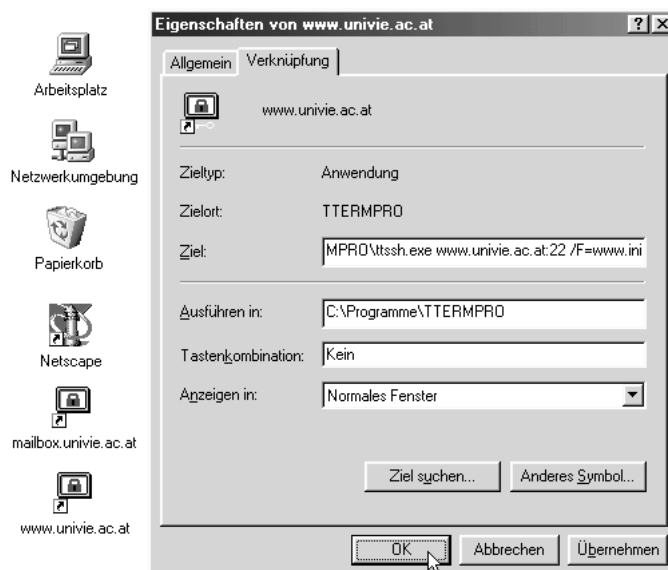


Abb. 2: Verknüpfung für TTSSH-Konfigurationsdatei erstellen

Das Abholen erledigt Ihr Mailprogramm für Sie – irgendwann haben Sie den Namen Ihres POP3- oder IMAP-Servers eingetragen (POP.UNET.UNIVIE.AC.AT für Studierende, MAILBOX.UNIVIE.AC.AT für Uni-Mitarbeiter), haben Ihren Benutzernamen angegeben und womöglich Ihr Paßwort im Mailprogramm abgespeichert. Jedesmal, wenn Ihr Mailprogramm am Server nachsieht, ob neue Nachrichten für Sie da sind, wird Ihre UserID-/Paßwort-Kombination im Klartext zum Server übertragen und kann, wenn sich Ihr Rechner in einem unsicheren Netz befindet, abgehört werden! Die Klärung der Frage, ob Ihr Rechner in einem „sicheren“ Netz hängt, benötigt sicher mehr Zeit als die Erstellung eines Tunnels mit Hilfe von TeraTerm – und ein Tunnel schadet auch in einem sicheren Netz nicht. Wie im Abschnitt *Tunnel* beschrieben, sind zwei Schritte notwendig, um den Datenverkehr zwischen Ihrem Rechner und dem Mailserver zu verschlüsseln:

- Zuerst muß ein Tunnel eingerichtet werden: Klicken Sie im TeraTerm-Fenster auf **Setup – SSH Forwarding...** und dann im *TTSSH: Forwarding Setup*-Dialog auf **Add**.
- Im Fenster *SSH Port Forwarding* (siehe Abb. 3) aktivieren Sie **Forward local port** und geben das Protokoll an, über das Sie Ihre eMail-Nachrichten erhalten (**pop-3** oder **imap**).
- Das Feld *to remote machine* lassen Sie frei und tragen das Protokoll auch im Feld *port* ein.
- Durch Klick auf **OK** wird der Tunnel Ihrer Konfiguration hinzugefügt, und Sie können auch den *TTSSH: Forwarding Setup*-

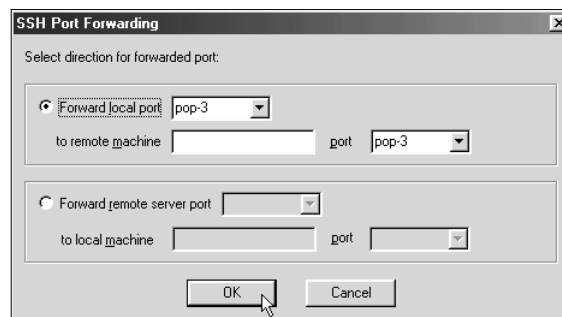


Abb. 3: Dialogfenster *SSH Port Forwarding*

- Dialog durch Klick auf **OK** wieder beenden.
- Speichern Sie die Konfiguration wie vorhin beschrieben.
- Erstellen Sie eine Verknüpfung am Desktop (siehe weiter oben) und tragen Sie als *hostname* den Namen Ihres Mailservers ein (z.B. C:\Programme\TTERMPRO\ttssh.exe mailbox.univie.ac.at:22 /F=mailbox.ini).
- Ein Doppelklick auf diese Verknüpfung und die Eingabe von UserID und Paßwort im *SSH Authentication*-Dialogfenster baut den Tunnel auf. Vorsicht: Das ganze funktioniert nur, wenn Ihr Rechner eine bestehende Internetverbindung hat. Falls Sie per Modem einwählen, müssen Sie diese zuerst herstellen.
- Im zweiten Schritt müssen Sie in der Konfiguration Ihres Mailprogramms den Namen des *Posteingangsservers* auf **localhost** ändern. Wo Sie dies einstellen können, entnehmen Sie bitte unseren Konfigurationsanleitungen (<http://www.univie.ac.at/ZID/helpdesk.html>).

Diese Einstellungen müssen Sie nur einmal vornehmen. Ihr Mailprogramm funktioniert in dieser Konfiguration allerdings nur bei aktiviertem Tunnel. Falls Ihr Rechner über eine permanente Internetverbindung verfügt, spricht nichts dagegen, den Tunnel immer aktiv zu lassen, während Ihr Rechner läuft. Sie müssen nur einmal nach dem Rechnerstart auf das TTSSH-Icon doppelklicken und sich authentifizieren. Alles funktioniert dann wie vorher. Nur sicher.

P. Marksteiner, H. Mislik,  
R. Brunthaler ■

## Secure Shell an den Außenstellen Physik & Biochemie des ZID

Der Unix-Cluster „Merlin“ (MERLIN.AP.UNIVIE.AC.AT) der Außenstelle Physik und der EMBnet-Rechner (EMB1.BCC.UNIVIE.AC.AT) der Außenstelle Biochemie können ebenfalls mit den Versionen 1 und 2 des SSH-Protokolls umgehen. Im Unterschied zur OpenSSH-Software enthält die hier verwendete SSH-Server-Software allerdings auch *sftp* (eine Abart von FTP) zur leichteren Dateiübertragung im Rahmen einer verschlüsselten Sitzung.

Als geeignetster Windows-Klient für diese Implementation empfiehlt sich der SSH-Klient der Firma SSH Communications Security (ssh.com), der im Gegensatz zu PuTTY und TTSSH, die nur SSH1 beherrschen, SSH Version 1 oder 2 „spricht“ und ebenfalls *sftp* unterstützt. Dadurch ist es möglich, Dateien zwischen dem PC und dem Hostrechner wie unter Windows per *Drag & Drop* auszutauschen. Den Klienten, der für die Anwendung an Hochschulen frei erhältlich ist, findet man unter <http://www.ssh.com/products/ssh/download.html>. Nachdem man die Datei *SSHWin.exe* aus dem Netz kopiert und ausgeführt hat, installiert sich die Software; damit ist sie für einen Monat

zum Testen lizenziert. Unter <http://commerce.ssh.com/> kann man sich eine *non-commercial licence* für das Produkt, das später problemlos nachgeladen werden kann, via eMail zusenden lassen.

Nach dem Programmstart erhält man ein Fenster mit den Verbindungsdaten. Wenn der *hostkey* nicht schon lokal bekannt ist, werden Sie gewarnt und haben die Möglichkeit, ihn zu akzeptieren. Auch mit dieser SSH-Implementation können beliebige Protokolle getunnelt werden: Über das Menü **Edit** gelangt man zu den **Settings**, wo die Eigenschaften des Programms festgelegt werden können. Unter **Tunneling** kann ein X11-Forwarding ausgewählt werden, und im Unterpunkt **Outgoing** werden mittels **Add** weitere Tunnel hinzugefügt. Will man z.B. mit IMAP4 eMail lesen und bearbeiten, errichtet man einen Tunnel auf den Port 143 und trägt im Mailprogramm als IMAP4-Host **localhost** ein. Wie bei den anderen Klienten kann ein Tunnel beliebig oft und lang verwendet werden, solange die dazugehörige Terminalverbindung aufrecht ist.

Aron Vrtala & Ulrich Kiermayr

# WÄHLEITUNGSVERBINDUNG MIT WINDOWS MILLENNIUM EDITION (ME)

## Warum Windows ME?

Weil Sie es höchstwahrscheinlich auf Ihrem neuen Rechner vorfinden werden. Komplet-PCs werden seit Erscheinen dieses Betriebssystems damit ausgeliefert, ob man mag oder nicht. Für aktuelle PCs ist Windows ME auch gar keine schlechte Wahl – es ist die Weiterentwicklung von Windows 95 und 98 und soll die bevorzugte Spiel-, Internet- und Heimanwender-Plattform werden. Ein Upgrade Ihres (bereits unter einer Vorgängerversion laufenden) Rechners auf Windows ME sollten Sie sich genau überlegen. Auf Rechnern mit langsameren Prozessoren als Pentium 150 ist eine Installation gar nicht möglich. Falls dieser Mindeststandard erfüllt ist, läßt sich Windows ME zwar installieren, viel Freude werden Sie mit einem solchen System aber nicht haben: Das Arbeiten auf einem solchen Rechner wird eher zu einer „Entdeckung der Langsamkeit“, da dieses Betriebssystem alle Ihre PC-Ressourcen verbraucht, bevor Sie noch ein Programm gestartet haben.

## Need for Speed

Internetzugang ist längst nicht mehr auf Verbindungen über ein lokales Netzwerk (LAN) mittels Netzwerkkarte oder über Telefonleitungen mittels Modem beschränkt. Kabelgesellschaften bieten Zugang über ihr bestehendes Netz an; auch die Post hat einen solchen „HighSpeed“-Zugang im Programm, der auf ADSL (*Asymmetric Digital Subscriber Line*)-Technologie beruht. Diese Zugänge bedürfen eines Vertrags mit dem jeweiligen Anbieter und werden üblicherweise auf Basis einer FlatRate (eine fixe, monatliche Gebühr) abgerechnet. Falls Sie intensiv von Ihrem Internetzugang Gebrauch machen, kann sich ein solcher Zugang auszahlen – und schneller ist er außerdem. Die Geräte, die Sie an Ihren Rechner anschließen, um einen solchen Zugang nutzen zu können, werden unter Umständen ebenfalls Modems genannt; die folgende Anleitung hilft Ihnen in diesem Fall aber nicht weiter. Hier geht es um „echte“ Modems oder ISDN-Terminaladapter – jene Geräte, die entweder in Ihrem Computer eingebaut sind, als PCMCIA-Karten in Ihrem Notebook zu finden sind oder an der seriellen Schnittstelle Ihres PCs stecken und mit dem Telefonsystem verbunden sind.

Als Studierende/r oder Mitarbeiter/in der Universität Wien brauchen Sie nur:

- einen Computer,
- einen Telefonanschluß,
- ein Modem (wir unterstützen den 56k-Standard V.90 – bitte beim Kauf eines Modems beachten),
- eine Benutzerkennung (siehe <http://www.unet.univie.ac.at/userid.html> für Studierende bzw.

<http://mailbox.univie.ac.at/benutzung.html> für Mitarbeiter der Universität Wien) und

- eine Konfigurationsanleitung für den Wähleitungszugang. Falls Sie *nicht* Windows Millennium Edition auf Ihrem Rechner installiert haben, hören Sie jetzt bitte zu lesen auf und besorgen sich die für Ihr Betriebssystem vorgesehene Konfigurationsanleitung – entweder auf Papier im Service- und Beratungszentrum des ZID (NIG, Stiege II, 1. Stock) oder aus dem Internet unter <http://www.univie.ac.at/ZID/helpdesk.html>.

Den Wähleitungszugang zur Uni Wien können Sie nach Bedarf nutzen – außer den während der Verbindung anfallenden Telefongebühren entstehen keine weiteren Kosten. Diese Telefongebühren zahlen Sie mit Ihrer nächsten Telefonrechnung. **Vorsicht:** Diese Anleitung geht davon aus, daß Sie über einen **Festnetzanschluß der PTA** einwählen und Ihr Standort **in der Regionalzone Wien** ist (siehe <http://mailbox.univie.ac.at/50km.html>). Falls Sie über einen anderen Anbieter (z.B. Priority) oder ein Handy bei uns einwählen wollen, werden Sie nicht nach dem PTA-Onlinetarif (siehe <http://www.telekom.at/fr/tarife/online99-fr.html>) abgerechnet. Erkundigen Sie sich in diesem Fall, welche Kosten für Sie anfallen, vielleicht ist ein anderer Internetzugang günstiger. Für alle, die (aus welchem Grund auch immer) keinen Gebrauch von der Onlinetarif-Rufnummer machen können, haben wir auch „normale“ Wiener Rufnummern, um ins Internet einzuwählen (+43 1 40122 für Studierende, +43 1 42726 für Mitarbeiter). Die Einwahl bei diesen Nummern kostet so viel wie ein Telefongespräch zu einer Wiener Festnetznummer – abhängig von Ihrem Standort unterschiedlich viel.

## Los geht's

Die Installation Ihres Modems sollte ohne Probleme von-statten gehen: Windows ME bringt die meisten Treiber mit, außerdem wird ein großer Teil der Installations-CD-ROM auf die Festplatte kopiert. Sie sollten also nie mehr nach dieser CD-ROM gefragt werden. Falls Ihr Modem nicht erkannt wird, sollte die (hoffentlich) mitgelieferte Treiberdiskette helfen; ansonsten versuchen Sie es mit den angebotenen Standardmodemtypen.

- Ihre Wähleitungsverbindung wird mit Hilfe eines Assistenten hergestellt, der die von Ihnen während der Installation eingegebenen Daten an die richtigen Stellen im System schreibt. Aufrufen können Sie den Assistenten durch einen Doppelklick auf das abgebildete Icon; falls Sie es nicht mehr auf Ihrem Bildschirm vorfinden, können Sie ihn



Verbindung mit dem Internet herstellen

auch über **Start – Programme – Zubehör – Kommunikation – Assistent für den Internetzugang** starten.

- Das Begrüßungsfenster des Assistenten heißt Sie willkommen und bietet Ihnen drei Möglichkeiten (siehe Abb. 1). Wählen Sie **Manuelle Einrichtung der Internetverbindung oder Verbindung über ein lokales Netzwerk (LAN) herstellen** und klicken Sie auf **Weiter >**.
- Im nächsten Fenster können Sie die Art der Internetverbindung bestimmen. Wählen Sie **Verbindung über Telefonleitung und Modem** und klicken Sie auf **Weiter >**.
- Falls Ihre Standortinformationen noch nie abgefragt wurden, müssen Sie diese jetzt eingeben (siehe Abb. 2):
  - Das Land, in dem Sie sich befinden, ist hoffentlich **Österreich** (sonst wird die Wählleitungsverbindung ziemlich teuer).
  - Ihre Ortskennzahl sollten Sie wissen – die von Wien ist **1**.
  - Wenn Ihr Telefon an eine Telefonanlage angeschlossen ist, können Sie als **Kennzahl für die Amtsleitung** die Ziffer eingeben, die Sie wählen müssen, um aus Ihrer Telefonanlage ins öffentliche Telefonnetz zu kommen (meistens **0**).
  - Sie können auch bestimmen, ob Sie das **MFV (Ton)**- oder das **IWV (Impuls)**-Wählverfahren verwenden wollen. In Österreich ist MFV Standard.
  - Durch Klick auf **Schließen** können Sie die Abfrage der Standortinformationen beenden.
- Weiter geht's im **Assistent für den Internetzugang**. In drei Schritten werden alle für die Verbindung notwendigen Parameter abgefragt und an die richtigen Stellen im System geschrieben. Falls Sie schon eine Internetverbindung unter Windows 98 oder 2000 eingerichtet haben, kommen Ihnen diese Schritte sicher bekannt vor:
  - Bei Schritt 1 (siehe Abb. 3) wird gefragt, welche Telefonnummer das Modem wählen soll. Wenn Sie Gebrauch vom Onlinetarif machen können, geben Sie als **Ortskennzahl 07189** und als **Rufnummer 14012** (wenn Sie Studierender der Uni Wien sind) bzw. **14013** (wenn Sie Mitarbeiter der Uni Wien sind) ein. Die Optionen, die sich hinter dem Knopf **Erweitert** befinden, lassen Sie bitte unberührt – sie sind richtig gesetzt. **Weiter >**.
  - Bei Schritt 2 geht es um Ihren Benutzernamen und Ihr Kennwort. Als **Benutzername** geben Sie als Studierender **aMATRIKELNUMMER** (z.B. a0815333) an, als Mitarbeiter der Uni Wien Ihre **Mailbox-UserID** (z.B. broeseE7). Als **Kennwort** geben Sie als Studierender Ihr **Unet-Paßwort** (das haben Sie bei der Anmeldung selbst gesetzt), als Universitätsmitarbeiter Ihr **Mailbox-Paßwort** ein. **Weiter >**.
  - Schritt 3 verlangt nur die Angabe eines Namens, den die Verbindung bekommen soll – **Uni Wien** ist ein schöner Name. Klick auf **Weiter >**.



Abb. 1: Fenster **Assistent für den Internetzugang, Willkommen**

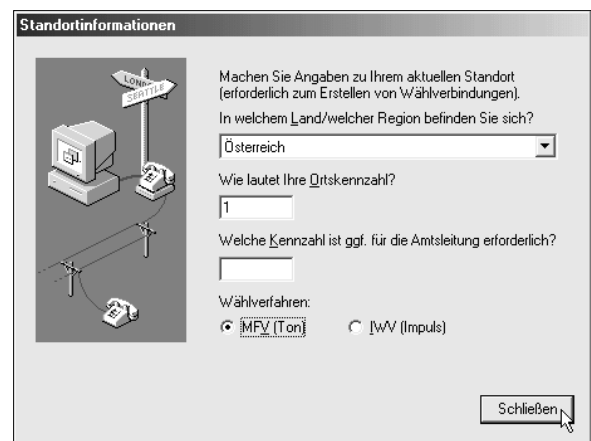
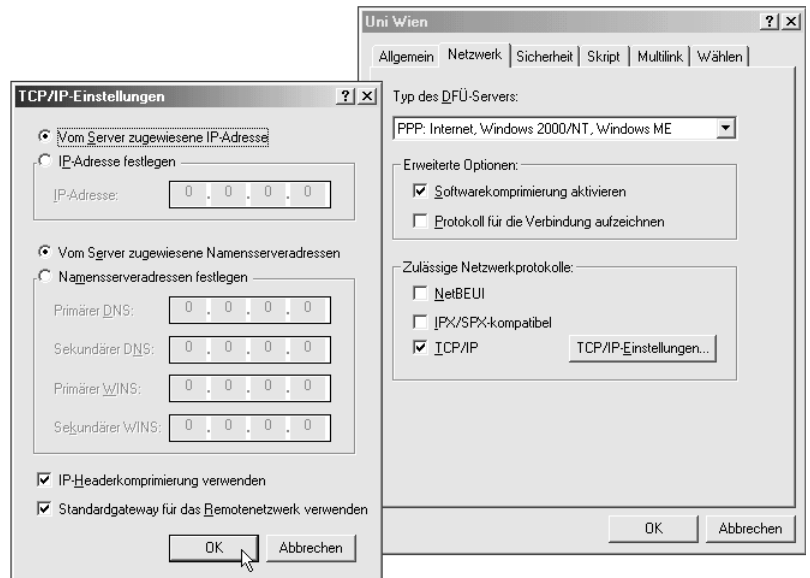


Abb. 2: Fenster **Standortinformationen**



Abb. 3: Fenster **Information zur Verbindung mit dem Internetkonto**

- Die Wählleitungsverbindung ist jetzt fertig konfiguriert. Sie können durch Ausfüllen weiterer Dialogboxen auch gleich das vorinstallierte Outlook Express als Ihr Stan-

Abb. 4 (oben): Fenster *Verbinden mit*Abb. 5 (rechts): Registerkarte *Netzwerk* und Fenster *TCP/IP-Einstellungen*

Standard-Mailprogramm einrichten (eine Anleitung dafür finden Sie unter [http://www.univie.ac.at/comment/99-1/991\\_22.html](http://www.univie.ac.at/comment/99-1/991_22.html)). Egal, ob Sie das jetzt tun oder im *Internet Mail-Konto einrichten*-Dialogfenster **Nein** aktivieren und auf **Weiter** > klicken – Sie landen im

- *Assistent für den Internetzugang ist beendet*-Fenster, das Ihnen die Möglichkeit gibt, bei aktivierter Checkbox durch Klick auf **Fertig stellen** die soeben erstellte Internetverbindung auszuprobieren.
- Das *Verbinden mit*-Fenster (siehe Abb. 4) ermöglicht es Ihnen nicht nur, durch Klick auf die Schaltfläche **Verbinden** Ihr Modem wählen und Ihren Computer Teil des Internet werden zu lassen, sondern auch alle Eigenschaften Ihrer Verbindung zu ändern. Sie können Ihr *Kennwort speichern* (gut für tippfaule Menschen, schlecht bei Computern, zu denen mehrere Menschen Zugang haben) und Ihre *Wählparameter* (Standort, Amtskennzahl usw.) ändern. Hinter der Schaltfläche *Einstellungen* verbergen sich alle anderen Parameter der Verbindung. **Vorsicht!** Alle Optionen sind standardmäßig richtig gesetzt, eine Änderung beschert Ihnen eher Fehlermeldungen als eine optimierte Internetverbindung.
- Sobald die Verbindung steht, wird der Internet Explorer gestartet. Eine Anleitung, wie Sie diesen Browser richtig konfigurieren, finden Sie unter [http://www.univie.ac.at/comment/00-1/001\\_28.html](http://www.univie.ac.at/comment/00-1/001_28.html). Beenden können Sie die Verbindung entweder durch Schließen des Internet Explorer (der *Automatische Trennung*-Dialog erscheint und fragt, ob die Verbindung beendet werden soll) oder durch Klick mit der **rechten** Maustaste auf das kleine Icon rechts unten in der Taskleiste, das zwei Computer darstellt, und Auswahl von **Trennen**. Eine Internetverbindung starten Sie am einfachsten durch Doppelklick auf das Symbol für den Internet Explorer (das blaue **e**). Dieser bringt automatisch den *Verbinden mit*-

Dialog, der nach Eingabe Ihres Paßworts und Klick auf **Verbinden** die Internetverbindung herstellt.

## Einfacher geht's nicht mehr

Dieser Assistent zum Einrichten einer Internetverbindung ist wirklich gelungen: Nach wenigen Schritten funktioniert alles, und die Werte, die nicht abgefragt werden, sind für die Verbindung zur Universität Wien richtig eingestellt. Für den Fall, daß Sie trotzdem Probleme mit der Verbindung haben, folgt hier eine Liste, in der Sie nachsehen können, ob nicht doch ein Hakerl an der falschen Stelle gesetzt ist.

Klären Sie zuerst, ob wirklich die Verbindung Probleme macht, oder ob nicht nur das eMail-Programm oder der Browser spinnt. Hilfe für Outlook Express finden Sie unter [http://www.univie.ac.at/comment/99-1/991\\_22.html](http://www.univie.ac.at/comment/99-1/991_22.html), für den Internet Explorer unter [http://www.univie.ac.at/comment/00-1/001\\_28.html](http://www.univie.ac.at/comment/00-1/001_28.html). Aus dem *Verbinden mit*-Dialog kommen Sie durch Klick auf **Einstellungen** in die unzähligen Fenster, die Sie an den Parametern der Verbindung drehen lassen. Die folgende Aufzählung beschreibt, was in den einzelnen Fenstern stehen sollte.

### Registerkarte *Allgemein*

- *Ortskennzahl*: 07189
- *Rufnummer*: 14012 (Studierende) oder 14013 (Mitarbeiter)
- *Landeskennzahl*: Österreich (43)
- *Ortskennzahl und Wählparameter verwenden*: aktiv (= mit Hakerl)
- *Verbinden über*: Ihr Modem

### Registerkarte *Netzwerk* (siehe Abb. 5)

- *Typ des DFÜ-Servers*: PPP: Internet, Windows 2000/NT, Windows ME



- Erweiterte Optionen:  
*Softwarekomprimierung aktivieren*: aktiv;  
*Protokoll für die Verbindung aufzeichnen*: inaktiv  
(= ohne Hakerl; dieses Protokoll kann Ihnen zwar bei der Fehlersuche helfen, im Normalbetrieb ist es aber unnötig)
- Zulässige Netzwerkprotokolle: **Nur TCP/IP aktiv**, die beiden anderen: inaktiv!
- TCP/IP-Einstellungen: *Vom Server zugewiesene IP-Adresse*: aktiv, *Vom Server zugewiesene Namensserver-adressen*: aktiv. Auch die beiden Checkboxen für *IP-Headerkomprimierung* und *Standardgateway*: aktiv.

### Registerkarte Sicherheit

- Authentifizierung: *Benutzername*: Ihr Benutzername;  
*Kennwort*: Ihr Unet- bzw. Mailbox-Paßwort; *Domäne*: in diesem Feld soll **auf keinen Fall** etwas stehen;  
*Verbindung automatisch herstellen*: inaktiv, es sei denn, Ihre Telefonkosten sind Ihnen völlig egal.
- Erweiterte Sicherheitsoptionen: **Keine der angebotenen Einstellungen darf aktiv sein!**

### Registerkarte Skript

- Unter *Dateiname* darf nichts stehen, da Sie für die Auswahl bei der Universität Wien **kein** Skript benötigen.

### Registerkarte Multilink

- *Keine zusätzlichen Geräte verwenden*: aktiv

### Registerkarte Wählen

- *Standardinternetverbindung*: aktiv; *Immer Standardverbindung wählen*: aktiv
- *Wahlwiederholungseinstellungen*: Geschmackssache
- *Trennen nach Leerlauf aktivieren*: Geschmackssache

Wenn Sie wieder auf die Registerkarte **Allgemein** zurückgehen und dort auf die Schaltfläche **Konfigurieren** klicken, erscheint das Fenster **Eigenschaften des Modems** mit noch mehr Registerkarten:

#### Registerkarte

##### *Eigenschaften des Modems – Allgemein*

- *Lautstärke*: Geschmackssache (bei der Fehlersuche laut drehen – dann hört man, ob das Modem überhaupt richtig wählt)
- *Maximale Geschwindigkeit*: Die voreingestellte Geschwindigkeit (115200) sollte funktionieren; bei Problemen kann man die Geschwindigkeit etwas herunterdrehen.

#### Registerkarte

##### *Eigenschaften des Modems – Verbindung*

- *Datenbits*: 8, *Parität*: Keine, *Stoppbits*: 1

- Die Punkte unter *Anrufeinstellungen* brauchen nicht aktiv zu sein.
- Erweitert:
  - *Fehlerkontrolle verwenden* und *Datenkomprimierung*: aktiv
  - *Flußkontrolle verwenden* und *Hardware (RTS/CTS)*: aktiv
  - *Modulationstyp*: Standard
  - *Weitere Einstellungen*: Hier können Sie dem Modem Befehle schicken, die es umprogrammieren, bevor es zu wählen beginnt. Das kann sinnvoll sein, um dem Modem Verbindungsversuche mit Protokollen „auszureden“, die von den Modems der Universität Wien nicht unterstützt werden (z.B. k56flex), oder um einen ISDN-Terminaladapter auf das richtige B-Kanal-Protokoll (*HDLC* oder *SyncPPP* und **nicht X.75**) zu trimmen. Die richtigen Init-Strings finden Sie in Ihrem Modemhandbuch; tragen Sie sie hier ein.
- *An Protokoll anhängen*: Das brauchen Sie nur zur Fehlersuche.

#### Registerkarte

##### *Eigenschaften des Modems – Optionen*

- Keine der Optionen muß aktiv sein.

#### Registerkarte

##### *Eigenschaften des Modems – Anrufweiterleitung*

- Alles inaktiv!

## Noch ein Tip

Wenn Sie Dateien aus dem Internet kopieren, sind diese sehr oft komprimiert. Auch Sie sollten Dateien vor dem Versand „zippen“, der Empfänger wird es Ihnen danken.

Im Gegensatz zu den Vorgängerversionen, bei denen man dafür ein zusätzliches Programm (WinZip war weit verbreitet) installieren mußte, bringt Windows ME ein sehr schönes Tool für den Umgang mit komprimierten Dateien und Ordnern mit. Bei einer Standardinstallation ist dieses Tool aus unerfindlichen Gründen nicht dabei. Sie sollten es mittels Doppelklick auf **Arbeitsplatz – Systemsteuerung – Software** und Auswahl von **Windows Setup – Systemprogramme – Komprimierte Ordner** nachinstallieren, es zahlt sich aus.

## Und noch ein Tip

Wenn Sie sich den Inhalt des *Windows*-Verzeichnisses auf Ihrer Festplatte ansehen, werden Sie bemerken, daß dieses Fenster auch den Hinweis *Der Inhalt dieses Ordners sollte sorgfältig verändert werden* zeigt. Bitte befolgen Sie diese Aufforderung nicht.

Robert Brunthaler ■

# KURSE BIS JÄNNER 2001

## Kurskalender

Auf den folgenden Seiten finden Sie detaillierte Beschreibungen zu den von Ende Oktober 2000 bis Jänner 2001 geplanten Kursen des Zentralen Informatikdienstes. Wir sind bemüht, keine Änderungen mehr vorzunehmen. Da jedoch Kurse hinzukommen oder entfallen können, beachten Sie bitte auch die aktuellen Informationen im Service- und Beratungszentrum und die Kursterminblätter in den Formularspendern vor den PC-Räumen und im Service- und Beratungszentrum. Alle Informationen zu den Kursen sowie die aktuellen Kursbelegungen finden Sie auch unter <http://data.univie.ac.at/kurs/bin/kursang.pl>.

## Anmeldungen

können nur im Service- und Beratungszentrum (NIG, Stg. II, 1. Stock links; Mo–Fr 9–17 Uhr) erfolgen. **Bitte beachten Sie die Anmeldefristen!** Teilnahmeberechtigt sind alle Studierenden und Mitarbeiter der Universität Wien. Die Kurse sind bei der Anmeldung bar zu bezahlen; Studierende müssen dabei ihren Studiausweis vorlegen. Für Institute und Dienststellen der Uni Wien besteht auch die Möglichkeit, sich mittels *ZVA für Kursanmeldung* (dieser ist ausgefüllt und unterschrieben mitzubringen) bargeldlos anzumelden.

## Absagen/Rücktritte

Liegen zwei Wochen vor Kursbeginn zu wenige Anmeldungen vor, kann der Kurs abgesagt werden. Die angemeldeten Teilnehmer werden nach Möglichkeit rechtzeitig verständigt. Falls ein Kurs abgesagt wird oder sich ein Teilnehmer innerhalb der Anmeldefrist abmeldet, kann die bezahlte Kursgebühr innerhalb eines Jahres (ab Kurstermin) zurückgefordert werden. **Bei Abmeldung eines Teilnehmers nach Anmeldeschluß des betreffenden Kurses sind 10% der Kursgebühr zu entrichten.**

## Kosten

Die Preise für die einzelnen Kurse entnehmen Sie bitte den Kursbeschreibungen auf den folgenden Seiten.

## Vortragende

Die Kurse werden von bewährten externen Schulungsfirmen bzw. von Experten des ZID abgehalten.

## Kursorte

### Kursraum A des ZID

NIG (1010 Wien, Universitätsstr. 7), Stg. I, Erdg.

### Kursraum B des ZID

NIG (1010 Wien, Universitätsstr. 7), Stg. III, Erdg.

### PC-Raum 2 des ZID

NIG (1010 Wien, Universitätsstr. 7), Stg. I, 1. Stock

### Hörsaal 3 des Neuen Institutsgebäudes

NIG (1010 Wien, Universitätsstr. 7), Stg. I, Erdg.

## PC-SOFTWARE

### Grundlagen

#### Arbeiten mit MS-Windows – Einführung

Zielgruppe: PC-Benutzer, die – als Basis für alle weiteren Kurse – den Umgang mit MS-Windows erlernen möchten

Voraussetzung: keine

Dauer: 6 Stunden (1 Tag)

Inhalt: Windows-Oberfläche / Arbeiten mit Maus & Tastatur / Fenstertechniken / Konfiguration / Überblick über Zubehör-Programme / Windows Explorer

Ort: 1. Termin: Kursraum A

2. Termin: Kursraum B

Preis: öS 400,- für Studierende

öS 800,- für Mitarbeiter der Uni Wien

Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
22.11.2000	09.00 – 16.00 h	16.10.00 – 10.11.00
11.12.2000	09.00 – 16.00 h	13.11.00 – 01.12.00

### Textverarbeitung

#### MS-Word für Windows – Einführung

Zielgruppe: Neueinsteiger im Bereich Textverarbeitung, die Word verwenden wollen, um ihre Texte (Briefe, Seminararbeiten, ...) zu erfassen

Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*

Dauer: 6 Stunden (1 Tag)

Inhalt: Word-Arbeitsoberfläche / Erstes Dokument / Formatierungsmöglichkeiten / Seitengestaltung / Drucken

Ort: 1. Termin: Kursraum A

2. Termin: Kursraum B

Preis: öS 400,- für Studierende

öS 800,- für Mitarbeiter der Uni Wien

Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
23.11.2000	09.00 – 16.00 h	16.10.00 – 10.11.00
12.12.2000	09.00 – 16.00 h	13.11.00 – 01.12.00

#### MS-Word für Windows – Fortsetzung

Zielgruppe: PC-Benutzer, die grundlegende Word-Kenntnisse besitzen und zusätzliche Möglichkeiten erlernen und nützen wollen

Voraussetzung: Kurse *Arbeiten mit MS-Windows* und *MS-Word für Windows – Einführung*

Dauer: 6 Stunden (1 Tag)

Inhalt: Tabellen / Seriendruck / Formatvorlagen / Verknüpfung mit anderen Programmen

Ort:	1. Termin: Kursraum A 2. Termin: Kursraum B
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 16
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>24.11.2000</b>	<b>I 09.00 – 16.00 h I 16.10.00 – 10.11.00</b>
<b>13.12.2000</b>	<b>I 09.00 – 16.00 h I 13.11.00 – 01.12.00</b>

### Wissenschaftliches Arbeiten mit Word für Windows

Zielgruppe:	Word-Benutzer, die wissenschaftliche Arbeiten (z.B. Diplomarbeiten) erstellen wollen
Voraussetzung:	Beherrschen der Word-Grundlagen (siehe Kurse <i>MS-Word für Windows – Einführung</i> und <i>Fortsetzung</i> )
Dauer:	6 Stunden (1 Tag)
Inhalt:	Zentraldokument – Filialdokument / Verzeichnisse erstellen / Fußnoten einfügen und bearbeiten / Kopf- und Fußzeilen einfügen und gestalten / Excel-Tabellen einfügen
Ort:	1. Termin: Kursraum B 2. Termin: Kursraum A
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 10
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>23.10.2000</b>	<b>I 09.00 – 16.00 h I 22.09.00 – 13.10.00</b>
<b>14.12.2000</b>	<b>I 09.00 – 16.00 h I 13.11.00 – 01.12.00</b>

### MS-Word für Windows – Büroinsatz

Zielgruppe:	Winword-erfahrene Benutzer, die sich ihre Büroarbeit durch einfache Automatisierung erheblich erleichtern wollen
Voraussetzung:	Beherrschen der Word-Grundlagen (siehe Kurse <i>MS-Word für Windows – Einführung</i> und <i>Fortsetzung</i> )
Dauer:	6 Stunden (1 Tag)
Inhalt:	Seriendruck / Dokumentvorlagen / Auto-Text erfassen und bearbeiten / Symbolleisten / Formatvorlagen
Ort:	Kursraum B
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 16
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>04.12.2000</b>	<b>I 09.00 – 16.00 h I 30.10.00 – 17.11.00</b>

## Tabellenkalkulation

### MS-Excel – Einführung

Zielgruppe:	Neueinsteiger im Bereich Tabellenkalkulation, die mit Excel Berechnungen erfassen, modifizieren und grafisch darstellen wollen
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurs <i>Arbeiten mit MS-Windows – Einführung</i>
Dauer:	6 Stunden (1 Tag)

Inhalt:	Excel-Arbeitsoberfläche / Arbeiten mit Arbeitsmappen und Tabellenblättern / Erstellen einfacher Tabellen / Formatierungsmöglichkeiten / Diagramm erstellen und bearbeiten / Drucken
---------	---

Ort:	1. Termin: Kursraum A 2. Termin: Kursraum B
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 16
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>13.11.2000</b>	<b>I 09.00 – 16.00 h I 09.10.00 – 03.11.00</b>
<b>20.11.2000</b>	<b>I 09.00 – 16.00 h I 23.10.00 – 10.11.00</b>

### MS-Excel – Fortsetzung

Zielgruppe:	Erfahrene Excel-Anwender, die an komplexeren Berechnungen bzw. an weiteren Funktionen interessiert sind
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurse <i>Arbeiten mit MS-Windows – Einführung</i> und <i>MS-Excel – Einführung</i>
Dauer:	6 Stunden (1 Tag)
Inhalt:	Anpassen der Arbeitsoberfläche / Komplexe Berechnungen / Arbeitsmappen verknüpfen / Mustervorlagen und Formulare
Ort:	1. Termin: Kursraum A 2. Termin: Kursraum B
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 16
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>14.11.2000</b>	<b>I 09.00 – 16.00 h I 09.10.00 – 03.11.00</b>
<b>21.11.2000</b>	<b>I 09.00 – 16.00 h I 23.10.00 – 10.11.00</b>

### MS-Excel – Datenanalyse

Zielgruppe:	Excel-erfahrene PC-Benutzer, die Excel-Daten verwalten, analysieren und filtern wollen
Voraussetzung:	Beherrschen der Excel-Grundlagen (Kurse <i>MS-Excel – Einführung</i> und <i>Fortsetzung</i> )
Dauer:	6 Stunden (1 Tag)
Inhalt:	Listen verwalten / Tabellenblätter gliedern / Pivot-Tabelle / Aufgaben automatisieren
Ort:	Kursraum B
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien
Teilnehmer:	maximal 10
<b>Termin</b>	<b>I Zeit</b> <b>I Anmeldefrist</b>
<b>01.12.2000</b>	<b>I 09.00 – 16.00 h I 30.10.00 – 17.11.00</b>

## Datenbanken

### MS-Access für Windows – Einführung

Zielgruppe:	PC-Benutzer, die eine anwenderfreundliche Datenbank unter Windows einsetzen wollen
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurs <i>Arbeiten mit MS-Windows – Einführung</i>

Dauer:	12 Stunden (2 Tage)	
Inhalt:	Datenbankgrundlagen / Erstellen eines Tabellenentwurfs / Arbeiten mit Tabellen / Abfragen / Erstellen von Formularen / Berichte / Drucken / Einfache Makros	
Ort:	Kursraum A	
Preis:	öS 800,- für Studierende öS 1.600,- für Mitarbeiter der Uni Wien	
Teilnehmer:	maximal 16	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>20.11. – 21.11.00</b>	09.00 – 16.00 h	23.10.00 – 10.11.00

### MS-Access für Windows – Fortsetzung

Zielgruppe:	PC-Benutzer, die ihre Access-Kenntnisse vertiefen wollen	
Voraussetzung:	Kurse <i>Arbeiten mit MS-Windows</i> und <i>MS-Access für Windows – Einführung</i>	
Dauer:	12 Stunden (2 Tage)	
Inhalt:	Datenbankdesign und -pflege / Tabellen einbinden / Abfragen / Automatisieren von Arbeitsabläufen mittels Makroprogrammierung	
Ort:	Kursraum A	
Preis:	öS 800,- für Studierende öS 1.600,- für Mitarbeiter der Uni Wien	
Teilnehmer:	maximal 16	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>04.12. – 05.12.00</b>	09.00 – 16.00 h	30.10.00 – 17.11.00

## Diverse Applikationen

### SPSS – Einführung

Zielgruppe:	PC-Benutzer, die ein Statistikprogramm unter Windows einsetzen wollen	
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurs <i>Arbeiten mit MS-Windows – Einführung</i>	
Dauer:	12 Stunden (2 Tage)	
Inhalt:	Fragebogenerstellung / Dateneditor / Datentransformation und -selektion / Ausgewählte statistische Verfahren / Grafiken	
Ort:	PC-Raum 2	
Preis:	öS 800,- für Studierende öS 1.600,- für Mitarbeiter der Uni Wien	
Teilnehmer:	maximal 12	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>11.12. – 12.12.00</b>	09.00 – 16.00 h	13.11.00 – 24.11.00

### Photoshop – Einführung

Zielgruppe:	PC-Benutzer, die mit einem professionellen Programm Bilder bearbeiten wollen	
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurs <i>Arbeiten mit MS-Windows – Einführung</i>	
Dauer:	6 Stunden (1 Tag)	
Inhalt:	Photoshop-Arbeitsoberfläche / Bildbearbeitung / Ebenen- und Filtereffekte / Text erzeugen und bearbeiten / Bilder importieren, scannen, ins Web exportieren / Drucken	

Ort:	1. Termin: Kursraum B 2. Termin: Kursraum A	
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien	
Teilnehmer:	maximal 16	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>30.10.2000</b>	09.00 – 16.00 h	25.09.00 – 13.10.00
<b>01.12.2000</b>	09.00 – 16.00 h	30.10.00 – 17.11.00

### PowerPoint – Einführung

Zielgruppe:	PC-Benutzer, die professionelle Folien bzw. Bildschirmpräsentationen für Vorträge, Seminararbeiten etc. erstellen wollen	
Voraussetzung:	EDV-Grundkenntnisse bzw. Kurs <i>Arbeiten mit MS-Windows – Einführung</i>	
Dauer:	6 Stunden (1 Tag)	
Inhalt:	PowerPoint-Arbeitsoberfläche / Die erste Präsentation / Grafik und Text / Drucken / Bildschirmpräsentation	
Ort:	1. und 3. Termin: Kursraum A 2. Termin: PC-Raum 2	
Preis:	öS 400,- für Studierende öS 800,- für Mitarbeiter der Uni Wien	
Teilnehmer:	maximal 16	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>09.11.2000</b>	09.00 – 16.00 h	09.10.00 – 27.10.00
<b>30.11.2000</b>	09.00 – 16.00 h	30.10.00 – 17.11.00
<b>15.12.2000</b>	09.00 – 16.00 h	13.11.00 – 01.12.00

## Windows NT

### Windows NT Systembetreuung

Zielgruppe:	Benutzer, die einzelne NT-Rechner administrieren wollen	
Voraussetzung:	Erfahrung mit Windows NT oder mit MS-Windows-Anwendungen	
Dauer:	9 Stunden (1,5 Tage)	
Inhalt:	Grundlagen des Betriebssystems / Dateisystem NTFS / Installation einer NT-Workstation (Demo) / Anpassung und Konfiguration / Lokale Benutzerverwaltung / Dateien und Verzeichnisse gemeinsam nutzen / Drucker gemeinsam nutzen / Systemüberwachung und -pflege / Die Registrierungsdatenbank / Festplattenverwaltung / TCP/IP	
Ort:	Kursraum B	
Preis:	öS 1.200,- für Studierende und Mitarbeiter der Uni Wien	

Teilnehmer:	maximal 10	
<b>Termin</b>	<b>  Zeit</b>	<b>  Anmeldefrist</b>
<b>27.11. – 28.11.00</b>	09.00 – 15.00 h	30.10.00 – 17.11.00

## UNIX

### Einführung in Unix

Zielgruppe:	alle Benutzer von Unix-Systemen	
-------------	---------------------------------	--

Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*

Dauer: 12 Stunden (3 Halbtage)

Inhalt: Was ist Unix? / Erste Schritte / Unix-Befehle / Dateien und Dateisysteme / Filter und Pipes / Dateien bearbeiten und inspizieren / Kernel und Shells / Umgebungsvariable / Prozesse / X Windows

Ort: Kursraum A

Preis: öS 400,- für Studierende und Mitarbeiter der Uni Wien

Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
15.01. – 17.01.01	12.00 – 16.00 h	04.12.00 – 05.01.01

### Einführung in Linux

Zielgruppe: Anwender, die in die Linux-Welt einsteigen möchten

Voraussetzung: Kurs *Einführung in Unix* oder gleichwertige Kenntnisse

Dauer: 12 Stunden (2 Tage)

Inhalt: Was ist Linux / Installation von Linux auf einem PC / Kommandozeile und grafische Oberfläche / Ein Linux-PC als Workstation / Ein Linux-PC als Server / Sicherheit

Ort: Kursraum B

Preis: öS 1.200,- für Studierende und Mitarbeiter der Uni Wien

Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
25.01. – 26.01.01	9.00 – 16.00 h	18.12.00 – 12.01.01

## INTERNET

### Verwendung des Internet an der Uni Wien – Teil 1

Zielgruppe: alle Benutzer des Datennetzes der Uni Wien

Voraussetzung: EDV-Grundkenntnisse

Dauer: ca. 2,5 Stunden

Inhalt: Computernetzwerke / Adressierung im Netzwerk / Electronic Mail / Dateiübertragung mit FTP / Remote Login mit Telnet

Ort: Hörsaal 3

Preis: gratis für Studierende und Uni-Mitarbeiter

Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
17.11.2000	12.30 – 15.00 h	keine Anmeldung

### Verwendung des Internet an der Uni Wien – Teil 2

Zielgruppe: alle Benutzer des Datennetzes der Uni Wien

Voraussetzung: Kurs *Verwendung des Internet an der Universität Wien – Teil 1* bzw. gleichwertige Vorkenntnisse

Dauer: ca. 2,5 Stunden

Inhalt: NetworkNews / WorldWideWeb / Wahlleitungszugang / Unet- und Mailbox-Service / Abhilfe bei Problemen

Ort: Hörsaal 3

Preis: gratis für Studierende und Uni-Mitarbeiter

Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
24.11.2000	12.30 – 15.00 h	keine Anmeldung

### Einführung in das Erstellen von Webpages – Teil 1

Zielgruppe: Anwender, die eigene Webpages erstellen möchten

Voraussetzung: EDV-Grundkenntnisse

Dauer: ca. 2,5 Stunden

Inhalt: Grundlagen / Erste Schritte / Strukturierte Webpage / Webpage auf Server kopieren

Ort: Hörsaal 3

Preis: gratis für Studierende und Mitarbeiter der Universität Wien

Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
20.10.2000	12.30 – 15.00 h	keine Anmeldung
01.12.2000	12.30 – 15.00 h	keine Anmeldung

### Einführung in das Erstellen von Webpages – Teil 2

Zielgruppe: Anwender, die Webpages erstellen wollen

Voraussetzung: EDV-Grundkenntnisse und *Einführung in das Erstellen von Webpages – Teil 1*

Dauer: ca. 2,5 Stunden

Inhalt: Tabellen / Frames (Aufbau und Aussehen) / Interaktive Grafiken / Einbinden von Java-Applets

Ort: Hörsaal 3

Preis: gratis für Studierende und Mitarbeiter der Universität Wien

Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
27.10.2000	12.30 – 15.00 h	keine Anmeldung
15.12.2000	12.30 – 15.00 h	keine Anmeldung

### Einführung in das Erstellen von Webpages – Teil 3

Zielgruppe: PC-Benutzer, die eigene Webpages erstellen und professionell formatieren wollen

Voraussetzung: EDV-Grundkenntnisse (bzw. Kurs *Arbeiten mit MS-Windows – Einführung*) und Kurse *Einführung in das Erstellen von Webpages – Teil 1 & 2*

Dauer: 6 Stunden (1 Tag)

Inhalt: Erstellen von HTML-Seiten mit einem Texteditor / Formatieren erfaßter Texte / Strukturieren von HTML-Seiten / Tabellen / Grafik

Ort: 1. Termin: Kursraum A  
2. Termin: Kursraum B

Preis: öS 400,- für Studierende  
öS 800,- für Mitarbeiter der Uni Wien

Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
08.11.2000	09.00 – 16.00 h	09.10.00 – 27.10.00
13.11.2000	09.00 – 16.00 h	09.10.00 – 03.11.00

## INFORMATIONSVORANSTALTUNGEN

Diese Vorträge finden im **Hörsaal 3 des Neuen Institutsgebäudes** (NIG, 1010 Wien, Universitätsstr. 7, Stiege I, Erdgeschoß) statt und sind für Studierende und Mitarbeiter der Universität Wien kostenlos zugänglich.

### Verwendung des Internet an der Uni Wien, Teil 1 & 2

Termine: Teil 1: Freitag, 17. November 2000, 12.30 Uhr (s.t.)  
Teil 2: Freitag, 24. November 2000, 12.30 Uhr (s.t.)

Dauer: jeweils ca. 2,5 Stunden

In dieser Einführung wird versucht, jenes Wissen zu vermitteln, das ein Neueinsteiger für die Verwendung des Internet braucht. Neben der Erläuterung einiger technischer und organisatorischer Grundbegriffe werden die wichtigsten Internetanwendungen – wie WWW, Electronic Mail, FTP, Telnet und News – besprochen. Den Abschluß bildet die Vorstellung der Internetservices für Studierende und Mitarbeiter der Universität Wien (siehe auch Seite 35).

### Erstellen von Webpages (HTML), Teil 1 & 2

Termine: Teil 1: Freitag, 20. Oktober 2000 und Freitag, 01. Dezember 2000; jeweils 12.30 Uhr (s.t.)  
Teil 2: Freitag, 27. Oktober 2000 und Freitag, 15. Dezember 2000; jeweils 12.30 Uhr (s.t.)

Dauer: jeweils ca. 2,5 Stunden

Diese beiden Vorträge richten sich an alle Benutzer, die eigene Webpages erstellen möchten. Es werden nicht nur alle wichtigen Elemente von HTML besprochen, sondern auch allgemeine Richtlinien für die Erstellung von Webpages gegeben, die Vorgangsweise bei der Veröffentlichung der Seiten erläutert und einige HTML-Editoren vorgestellt (siehe auch Seite 35).

### Linux für Neueinsteiger

Vortragender: Robert Brunthaler

Termin: Freitag, 12. Jänner 2001, 12.30 Uhr (s.t.)

Dauer: ca. 2,5 Stunden

Das Betriebssystem Linux hat als extrem kostengünstige und doch leistungsfähige Variante von Unix auch an der Uni Wien viele Freunde gefunden. Dieser Vortrag richtet sich an alle, die in die Linux-Welt einsteigen wollen. Er bietet einen Überblick über die derzeit verfügbaren Linux-Distributionen, bespricht die Hardwareanforderungen und gibt Hinweise zur richtigen Konfiguration des Rechners. Für Anwender, die Linux daheim einsetzen wollen, wird die Konfiguration zur Nutzung der Wählleitungszugänge der Universität Wien erläutert.

### Linux II

Vortragender: Robert Brunthaler

Termin: Freitag, 19. Jänner 2001, 12.30 Uhr (s.t.)

Dauer: ca. 2,5 Stunden

Einen Linux-Rechner mit permanenter Internet-Anbindung (Universitätsdatennetz, TeleWeb/Chello, ...) zu betreiben, birgt einiges an Gefahren. Nicht nur der Rechner selbst, sondern auch das Netz, in dem er sich befindet, kann betroffen sein. Warum, wie und womit man einen solchen Rechner absichern kann/muß, soll dieser Vortrag zeigen.

### Wie schütze ich mich vor Hackern?

Vortragende: Ulrich Kiermayr & Aron Vrtala

Termin: Freitag, 10. November 2000, 12.30 Uhr (s.t.)

Dauer: ca. 1,5 Stunden

Welchen realen Gefahren sind die Computer im Datennetz der Uni Wien heute ausgesetzt? Basierend auf den Erfahrungen der letzten Jahre wird in diesem Übersichtsvortrag ein allgemein verständlicher Leitfaden gegeben, wie Sie Ihr System besser vor Übergriffen schützen können.

### Sicherheit bei Microsoft-Betriebssystemen

Vortragende: Ulrich Kiermayr & Aron Vrtala

Termin: Freitag, 26. Jänner 2001, 12.30 Uhr (s.t.)

Dauer: ca. 1,5 Stunden

Es gibt kein Betriebssystem, das nicht angreifbar ist; zusätzliche Sicherheitsmaßnahmen können die Gefahr jedoch verringern. In diesem für jeden MS-Anwender verständlichen Vortrag werden mögliche Arten des Übergriffs auf Ihre MS-Workstation bzw. Ihren MS-Server erläutert und gezeigt, wie Sie mit einfachen Maßnahmen (Personal Firewalls, Virens Scanner, Browser- und Mailklient-Einstellungen) Ihren Rechner besser schützen können. Dabei werden sowohl die Auswirkungen der gesetzten Maßnahmen als auch relevante Systemmeldungen erläutert.

# ÖFFNUNGSZEITEN

(Achtung: An vorlesungsfreien Tagen keine Tutorenbetreuung!)

## Service- und Beratungszentrum des ZID

1010 Wien, Universitätsstraße 7 (NIG), Stg. II, 1. Stock, links

Mo – Fr 9.00 – 17.00

## Sekretariat

1010 Wien, Universitätsstraße 7 (NIG), Stg. II, 1. Stock

Mo, Mi, Fr 9.00 – 11.00  
Di, Do 13.30 – 15.30

## Außenstelle Physik

1090 Wien, Boltzmannngasse 5

PC-Raum: Mo – Fr 9.00 – 17.00  
Beratungszeiten: Mo – Fr 10.00 – 12.00

## PC-Räume

### PC-Räume des Zentralen Informatikdienstes (NIG)

1010 Wien, Universitätsstraße 7, Stg. I, 1. Stock

PC-Räume: Mo – Fr 7.30 – 19.30  
Sa 8.00 – 13.00  
Tutorenbetreuung: Mo – Fr 9.00 – 12.00  
13.00 – 19.00

### PC-Räume des Zentralen Informatikdienstes (Altes AKH)

1090 Wien, Spitalgasse 2, Hof 7, 1. Stock

PC-Räume: Mo – Fr 8.00 – 20.00  
Tutorenbetreuung: Mo – Fr 9.00 – 12.00  
13.00 – 19.00

### PC-Raum Soziologie (NIG)

1010 Wien, Universitätsstraße 7, 2. Stock, Raum A207

Nur für Studierende des Instituts!

Anmeldung mit Studienausweis und

öS 100,- als Einsatz für Magnetkartenschlüssel

PC-Raum: wie Instituts-Öffnungszeiten

### PC-Raum Ethnologie (NIG)

1010 Wien, Universitätsstraße 7, 4. Stock

Nur für Studierende des Instituts!

PC-Raum: Mo – Fr 9.00 – 17.00

### PC-Raum Geographie (NIG)

1010 Wien, Universitätsstraße 7, 5. Stock, Raum B512

Nur für Studierende des Instituts!

Anmeldung mit Studienausweis

PC-Raum: Mo – Do 9.00 – 17.00  
Fr 9.00 – 15.00

### PC-Raum Psychologie (NIG)

1010 Wien, Universitätsstraße 7, 6. Stock

Nur für Studierende des Instituts!

PC-Raum: Mo – Do 8.30 – 19.30  
Fr 8.30 – 18.00

## PC-Raum Germanistik

1010 Wien, Dr. Karl Lueger-Ring 1; Stg. 9, 3. Stock

Zugang haben alle Studierenden der deutschen Philologie und andere Personen, die am Institut für Germanistik wissenschaftlich arbeiten; Anmeldung im Sekretariat

PC-Raum: Mo – Do 8.00 – 17.00  
Fr 8.00 – 16.00

## PC-Raum Politikwissenschaft

1090 Wien, Währinger Straße 17, 5. Stock

Anmeldung mit Studienausweis im Sekretariat

PC-Raum Mo – Mi 9.30 – 12.00  
13.30 – 15.30  
& Sekretariat: Do 9.30 – 15.30  
Fr 9.30 – 12.00  
Tutorenbetreuung: Mo & Mi 13.00 – 15.00  
Fr 10.00 – 12.00

## PC-Raum der Rechtswissenschaftlichen Fakultät

1010 Wien, Heßgasse 1, Erdgeschoß, links

Nur für Studierende der Rechtswissenschaftlichen Fakultät!

PC-Raum: Mo – Fr 8.00 – 18.00  
Tutorenbetreuung: Mo – Fr 8.00 – 18.00

## PC-Raum Botanik

1030 Wien, Rennweg 14

Nur für Studierende des Instituts!

PC-Raum: Mo – Fr 7.00 – 20.00

## PC-Raum Medizinische Aus- und Weiterbildung (AKH)

1090 Wien, Währinger Gürtel 18 – 20, Ebene 6, Bereich M

Nur für Studierende der Medizinischen Fakultät!

PC-Raum: Mo – Fr 9.00 – 19.30

## PC-Raum Anthropologie (UZA I)

1090 Wien, Althanstraße 14, Spange 1, Ebene 2

PC-Raum: Mo – Fr 7.30 – 19.30  
Sa 8.00 – 13.00  
Tutorenbetreuung: Mo – Fr 9.00 – 12.00  
13.00 – 19.00

## PC-Raum Ökologie und Naturschutz (UZA I)

1090 Wien, Althanstraße 14, Spange 4, Ebene 1

PC-Raum: Mo – Fr 7.30 – 19.30  
Sa 8.00 – 13.00  
Tutorenbetreuung: Mo – Fr 9.00 – 12.00  
13.00 – 19.00

## PC-Raum Mineralogie (UZA II)

1090 Wien, Althanstraße 14, Raum 2A187

PC-Raum: Mo – Fr 7.30 – 19.30  
Sa 8.00 – 13.00  
Tutorenbetreuung: Mo – Fr 9.00 – 12.00  
13.00 – 19.00

## PC-Räume Betriebswirtschaftszentrum (BWZ)

1210 Wien, Brünner Straße 72; Erdgeschoß, 2. & 3. Stock

PC-Räume: Mo – Fr 8.00 – 20.00

Aktuelle Informationen zu den PC-Räumen finden Sie unter <http://www.univie.ac.at/ZID/PC-Raeume/>.

# PERSONAL- & TELEFONVERZEICHNIS

<b>Vermittlung</b>	4277-14001
<b>Fax</b>	4277-9140

## Direktor des Zentralen Informatikdienstes

Rastl Peter	4277-14011	Zi.B0112
-------------	------------	----------

## Sekretariat

Berschlinghofer Christa	4277-14015	Zi.B0116
Pulzer Ingrid	4277-14017	Zi.B0116

## Buchhaltung

Deusch Maria	4277-14016	Zi.D0107
Haumer Claudia	4277-14018	Zi.D0107

## Abteilung

### Dezentrale Systeme & Außenstellen

Karlsreiter Peter ( <i>Leiter</i> )	4277-14131	Zi.D0108
Halasz Karl	4277-14135	Zi.D0104
Marzluf Christian	4277-14136	Zi.D0110
Pfeiffer Günter	4277-14134	Zi.D0113
Staudigl Ralph	4277-14224	Zi.D0106
Wienerroither Peter	4277-14138	Zi.D0110

#### Außenstelle Altes AKH (AAKH),

Spitalgasse 2, 1090 Wien:

Hönigsperger Helmuth	4277-14114	2H EG 35
Paunzen Ernst	4277-14111	2H EG 31
Pechter Karl	4277-14068	2H EG 29

#### Außenstelle Biochemie,

Dr. Bohr-Gasse 9, 1030 Wien:

Grabner Martin	4277-14141	6.St.Zi.6108
Haitzinger Robert	4277-14142	6.St.Zi.6108

#### Außenstelle Physik,

Boltzmannngasse 5, 1090 Wien (Fax: 4277-9141):

Kiermayr Ulrich	4277-14104	1.St.Zi.3129
Kind Mario	4277-14101	2.St.Zi.3227
Njoroge Mike	4277-14103	2.St.Zi.3227
Vrtala Aron	4277-14102	1.St.Zi.3129

#### Außenstelle UZA,

Althanstraße 14, 1090 Wien:

Dempf Stefan	4277-14151	UZA I/Zi.2.260
Doppelhofer Johann	4277-14152	UZA I/Zi.2.260

## Abteilung

### Software & Benutzerbetreuung

Stappler Herbert ( <i>Leiter</i> )	4277-14051	Zi.B0110
Berndl Christoph	4277-14064	Zi.B0113
Brugger Nikolaus	4277-14069	Zi.D0106
Brunnthaler Robert	4277-14062	Zi.C0102
Ertl Lukas	4277-14073	Zi.B0111
Hurka Franz	4277-14067	Zi.D0112
Kaider Thomas	4277-14066	Zi.C0102
Kaltenbrunner Franz	4277-14061	Zi.C0102
Köberl Dieter	4277-14058	Zi.D0111
Marksteiner Peter	4277-14055	Zi.B0120
Mislik Heinrich	4277-14056	Zi.B0120
Neuwirth Ernst	4277-14052	Zi.B0115
Platzer Eveline	4277-14071	Zi.C0102A
Potuzak Vera	4277-14072	Zi.B0111
Scherzer Horst	4277-14053	Zi.B0115
Schreiner Willibald	4277-14076	Zi.D0112
Stadlmann Uwe	4277-14037	Zi.D0111
Stampfer Dieter	4277-14063	Zi.B0104
Szabo August	4277-14085	Zi.B0113
Talos Alexander	4277-14057	Zi.B0120
Zoppoth Elisabeth	4277-14074	Zi.B0111

## Abteilung

### Zentrale Systeme & Datennetze

Steinringer Hermann ( <i>Leiter</i> )	4277-14021	Zi.B0108
Ankner Markus	4277-14077	Zi.B0106
Bogad Manfred	4277-14029	Zi.B0105
Cikan Edwin	4277-14022	Zi.B0102
Domschitz Eduard	4277-14133	Zi.B0104
Englisch Holger	4277-14039	Zi.D0105
Geicsnek Karin	4277-14245	Zi.D0114
Grabner Eva	4277-14047	Zi.D0105
Halpern Erwin	4277-14024	Zi.D0115
Hofstetter Mark	4277-14046	Zi.D0117
Jenisch Ewald	4277-14028	Zi.B0105
Jenny Harald	4277-14047	Zi.D0105
Kogler Edgar	4277-14065	Zi.D0105
Kunft Walter	4277-14031	Zi.B0107
Kunitzky Walter	4277-14086	Erdg.Stg.I
Michl Harald	4277-14078	Zi.B0117
Panigl Christian	4277-14032	Zi.B0117
Papst Andreas	4277-14036	Zi.B0117
Pötzl Heinz	4277-14023	Zi.B0102



Regius Rene	4277-14242	Zi.D0117
Rosenwirth Thomas	4277-14025	Zi.B0109
Schaidl Christian	4277-14026	Zi.B0106
Schneider Monika	4277-14048	Zi.B0109
Szvasztics René	4277-14054	Zi.D0105
Vidovic Dejan	4277-14027	Zi.B0109
Vogler Martin	4277-14113	AAKH/2H EG 35
Wandler Alexander	4277-14244	Zi.D0114
Winkler Gerhard	4277-14035	Zi.B0117
Wöber Wilfried	4277-14033	Zi.B0107
Zettl Friedrich	4277-14041	Zi.D0113

### Telefonvermittlung Hauptgebäude

(Dr. Karl Lueger-Ring 1, 1010 Wien)

Drnek Jeanette	4277-14313
Engel Herbert	4277-14315
Erasmus Karl	4277-14311
Kettner Hedwig	4277-14317
Mayr Karl	4277-14314
Sylla-Widon Margaretha	4277-14318
Waba Theodor	4277-14312

### Telefonvermittlung Kinderspitalgasse

(Kinderspitalgasse 15, 1090 Wien)

Bösze Hildegard	4277-14319
Lenhard Leopoldine	4277-14319

## Abteilung Universitätsverwaltung (AUV)

(Garnisongasse 7/20, 1090 Wien; Fax: 4277-9142)

Riedel-Taschner Harald (Leiter)	4277-14211	
Aschauer Johann	4277-14213	
Böck Susanne	4277-14034	NIG/Zi.D0109
Dreiseitel Thomas	4277-14216	
Fuchs Alexander	4277-14228	
Hoys Peter	4277-14215	
Kauer Josef	4277-14210	
Klünger Gerhard	4277-14219	
Lackner Herbert	4277-14217	
Linhart Leopold	4277-14221	
Lohner Gertraud	4277-14222	
Osmanovic Richard	4277-14212	
Pauer-Faulmann Barbara	4277-14227	
Payer Markus	4277-14229	
Plattner Dieter	4277-14232	
Polaschek Martin	4277-14200	NIG/Zi.D0109
Rast Wolfgang	4277-14218	
Römer Alfred	4277-14214	
Url Clemens	4277-14220	
Zalcmann Erich	4277-14226	

## HANDBÜCHER

(Stand: 15. September 2000)

- Einführung in die EDV mit Windows 95 und Office 97 öS 60,-
- Windows 95 – Einführung öS 30,-
- Windows 98 – Systembetreuer öS 80,-
- Windows NT 4.0 – Anwender öS 75,-
- Windows NT 4.0 – Systembetreuer öS 80,-
- UNIX – Einführung öS 60,-
- UNIX – Systemverwaltung öS 75,-
- Linux – Nutzung mit der grafischen Oberfläche KDE öS 80,-
- Internet – Eine Einführung öS 80,-
- Publizieren im World Wide Web öS 75,-
- Word 2000 – Einführung öS 80,-
- Word 2000 – Fortgeschrittene öS 80,-
- Excel 7.0 – Fortsetzung öS 85,-
- Excel 97 – Einführung öS 70,-
- Excel 97 – Fortsetzung öS 80,-
- Excel 97 – Automatisierung – Programmierung öS 80,-
- Excel 2000 – Einführung öS 80,-
- Excel 2000 – Automatisierung – Programmierung öS 80,-
- Access 7.0 – Einführung öS 85,-
- Access 7.0 – Fortsetzung öS 85,-
- Access 97 – Fortsetzung öS 80,-
- Access 97 – Automatisierung – Programmierung öS 80,-
- Access 2000 – Einführung öS 80,-
- Access 2000 – Automatisierung – Programmierung öS 80,-
- PowerPoint 97 – Einführung öS 80,-
- PowerPoint 2000 – Einführung öS 80,-
- Photoshop 5.0 – Einführung öS 80,-
- SPSS für Windows – Einführung öS 60,-

Alle Handbücher stammen vom *Regionalen Rechenzentrum Niedersachsen (RRZN)* und sind im Service- und Beratungszentrum des ZID (NIG, Stg. II, 1. Stock, links; Mo – Fr 9 – 17 Uhr) gegen Barzahlung erhältlich.

## ANSPRECHPARTNER

In grundsätzlichen Angelegenheiten wenden Sie sich bitte an den Direktor des Zentralen Informatikdienstes:

Rastl Peter 4277-14011

oder an die Abteilungsleiter:

*Dezentrale Systeme & Außenstellen*

*Software & Benutzerbetreuung*

*Zentrale Systeme & Datennetze*

*Universitätsverwaltung*

Karlsreiter Peter 4277-14131

Stappler Herbert 4277-14051

Steinringer Hermann 4277-14021

Riedel-Taschner Harald 4277-14211

### Service- und Beratungszentrum

Als erste Anlaufstelle bei allgemeinen EDV-Problemen und technischen Schwierigkeiten, für Vermittlung zu Ansprechpartnern bei speziellen Problemen;

bei Störungen im Datennetz oder an einem Rechnersystem des Zentralen Informatikdienstes;

für Vergabe von Benutzungsberechtigungen für die Rechnersysteme und das Backup-Service;

für Kursanmeldungen, Verwaltung von *Comment*-Abos sowie Verkauf von Handbüchern, Netzwerkkarten und -kabel:

**eMail:** **HELPDESK.ZID@UNIVIE.AC.AT**

**Telefon:** **4277-14060**

**Öffnungszeiten:** **Mo – Fr 9.00 – 17.00 Uhr**  
NIG (1010 Wien, Universitätsstraße 7), Stg. II, 1. Stock, links

#### Bei Problemen im Bereich einer Außenstelle (Außenstellen AAKH, Biochemie, Physik & UZA)

stehen Ihnen die Mitarbeiter der jeweiligen Außenstelle zur Verfügung (siehe Personal- & Telefonverzeichnis, Seite 38).

#### bei EDV-Problemen im Bereich der Universitätsverwaltung:

Lackner Herbert 4277-14217

#### für Bewilligungen von a.o. Dotationsanträgen für EDV-Anschaffungen und bei Fragen zum EDV-Reparaturfonds:

Rastl Peter 4277-14011

Karlsreiter Peter 4277-14131

#### für Netzwerkplanung & Gebäudeverkabelung:

Steinringer Hermann 4277-14021

#### für Kursraumvergabe:

Pechter Karl 4277-14068

#### bei Fragen zur Standardsoftware:

Wienerroither Peter 4277-14138

#### bei Fragen bezüglich des EMBnet-Knotens:

Grabner Martin 4277-14141

#### bei Fragen zur Telefonanlage der Uni Wien:

Geicsnek Karin 4277-14245

#### für Öffentlichkeitsarbeit:

*Comment*-Red.: Potuzak Vera 4277-14072

Zoppoth Elisabeth 4277-14074

WWW-Redaktion: Ertl Lukas 4277-14073

## WÄHLEITUNGSZUGÄNGE & EMAIL-ADRESSEN

#### Unet-Wählleitungszugang

07189 14012 Onlinetarif (Regionalzone Wien)  
(01) 40122 Normaltarif

07189 14014 **Mail-Only** zum Onlinetarif

(01) 42781 **Mail-Only** zum Normaltarif

#### Mailbox-Wählleitungszugang

07189 14013 Onlinetarif (Regionalzone Wien)  
(01) 42726 Normaltarif

#### eMail-Adressen der Mitarbeiter

Die Mitarbeiter des ZID sind unter eMail-Adressen der Form **VORNAME.NACHNAME@UNIVIE.AC.AT** erreichbar (**Ausnahme:** Lukas Ertl hat die Adresse **L.ERTL@UNIVIE.AC.AT**). Umlaute sind mit zwei Buchstaben zu schreiben (ö = oe).



**Bitte beachten Sie auch die umseitigen Hinweise!**

**Unleserliche, unvollständig ausgefüllte sowie unzureichend frankierte Karten können nicht bearbeitet werden!**

- Ich möchte den *Comment* abonnieren.
- Meine Daten (Name, Adresse) haben sich geändert.
- Bitte schicken Sie mir den *Comment* nicht mehr.
- Ich benötige regelmäßig mehrere Exemplare (Anzahl:           Stk.).



vienna  
university  
computer  
center

Zentraler Informatikdienst  
der Universität Wien  
Universitätsstraße 7   Tel: 4277-14001  
A-1010 Wien           Fax: 4277-9140

Titel, Vorname, Nachname: \_\_\_\_\_

Institution: \_\_\_\_\_

Institut: \_\_\_\_\_

Abteilung: \_\_\_\_\_

Adresse: \_\_\_\_\_

PLZ, Ort (Telefonnummer): \_\_\_\_\_

## COMMENT-ABO

Der *Comment* erscheint ca. alle 4 Monate und wird Interessenten kostenlos zugesandt. Wir ersuchen um Nachricht, falls

- Ihr Name und/oder Ihre Adresse nicht korrekt angegeben wurden,
- Sie in unserer Abonnenten-Datenbank noch nicht erfasst sind, aber den *Comment* regelmäßig lesen möchten,
- Sie diese Zeitschrift *nicht* beziehen wollen,
- oder falls Sie mehrere Exemplare benötigen.
- Wir bitten auch alle Institute, uns zu verständigen, falls wir *ehemalige* Mitarbeiter mit Zusendungen beglücken.

Bitte verwenden Sie die unten abgedruckte Abo-Karte oder kontaktieren Sie unser Service- und Beratungszentrum (NIG, Stg. II, 1. Stock; Öffnungszeiten: Mo–Fr 9–17 Uhr; Tel.: 4277-14060, eMail: HELPDESK.ZID@UNIVIE.AC.AT). Außerdem besteht die Möglichkeit, die Abo-Bestellung über ein WWW-Formular durchzuführen (URL: <http://www.univie.ac.at/comment/mail-abo.html>). **Danke!**



# *Comment*

Der *Comment*, das Mitteilungsblatt des Zentralen Informatikdienstes, erscheint ca. alle 4 Monate und wird an Interessenten kostenlos abgegeben.

Bitte kreuzen Sie umseitig das Zutreffende an und geben Sie Ihre Daten *vollständig* und in *lesbaren Blockbuchstaben* an. Bei Änderungen vermerken Sie bitte auch Ihre bisherigen Daten in Klammern. Die Felder „Institution“, „Institut“ und „Abteilung“ sind nur dann auszufüllen, wenn die Zeitschrift *nicht* an Ihre Privatadresse geschickt werden soll. Senden Sie die Karte per Post oder Fax (4277-9140) an den ZID oder geben Sie diese im Service- und Beratungszentrum (Stg. II, 1. Stock) ab.

Bitte  
als Brief  
frankieren!

An den  
Zentralen Informatikdienst  
Service- und Beratungszentrum

Universitätsstraße 7  
A-1010 Wien