

*IN*formationen *K*atholische *U*niversität *E*ichstätt-Ingolstadt *R*echen*Z*Eentrum



Inhaltsverzeichnis

Editorial	4
Über die E-Future der universitären Lehre	5
ILIAS-News	9
Virtuelles Angebot für Absolventen der Fakultät für Soziale Arbeit	14
VoIP: Telefonieren über das Datennetz	15
Und dauernd funkt das Netz	18
Sicherer SSL-Zugang zum elektronischen Postfach	27
Der Umgang mit Malware in der Praxis	34
Mozilla Firefox – unser Standardbrowser	40
typokurz – Einige wichtige typografische Regeln	47
TeXinfo	55
Mal schnell eine Fernleihe aufgegeben? Oder etwa nicht? Anmerkungen zum aktuellen Gesetzentwurf des Urheberrechts	58
IN aller KUERZE	60
DV-Veranstaltungen SS 2007	62

Impressum

Herausgeber:	Katholische Universität Eichstätt-Ingolstadt, Rechenzentrum 85071 Eichstätt
Redaktion:	Bernhard Brandel, Peter Ihrler, Peter Kahoun, Dr. Wolfgang A. Slaby, Dr. Bernward Tewes, Peter Zimmermann
V. i. S. d. P.:	Dr. Wolfgang A. Slaby
Satz:	Theresia Stalker
Ausgabe:	z. Zt. halbjährlich
Auflage:	800 Exemplare
E-Mail:	inkuerze@ku-eichstaett.de
URL:	http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/schriften/inkuerze

Editorial

P. Ihrler

Die *INKUERZE* vor 10 Jahren beschäftigte sich unter anderem mit der Datenautobahn, dem Publizieren im WWW, dem Online-Katalog der Bibliothek und mit E-Mail. Sehr ähnlich sind die Themen dieser Ausgabe, man könnte fast an Absicht glauben. Allerdings handelt es sich hier um einen Zufall, der auch erst kurz vor Redaktionsschluss aufgefallen ist. In den Inhalten liegt jedoch ein kleiner Unterschied: Damals wurde mehr darüber informiert, wie die Fachleute einen Webauftritt machen. Der unidirektionale Weg vom Entwickler zum Konsumenten war das einzig Mögliche. Heute liegt der Schwerpunkt auf neuen Anwendungsgebieten im Internet, des (scheinbaren?) Zusammenfallens von Machern und Konsumenten von Web-Inhalten und leider auch auf den Gefahren und den technischen und rechtlichen Problemen.

Die ersten drei Artikel dieser Ausgabe beschäftigen sich mit den neuen Möglichkeiten, die Alumni, Studierenden und Lehrenden heute und in Zukunft zur Verfügung stehen werden. Es geht nicht nur um die informationstechnologische Nachbildung von bereits Vorhandenem, sondern auch

um neue Wege der aktiven Mitgestaltung von Lernprozessen.

Über den Stand des Telefonierens an der KU via Internet informiert ein Artikel, der deutlich macht, dass VoIP nicht nur das Internet als alternatives Transportmedium verwendet, sondern auch Möglichkeiten der Integration mit anderen Internetdiensten, wie z. B. mit E-Mail aufzeigt. Leider dürfen auch die Gefahren und Probleme der neuen Technologien in dieser *INKUERZE* nicht zu kurz kommen. Wir geben Tipps zum Netzzugang der KU über Funk, zur sicheren Übertragung von Passwörtern vom E-Mail-Client zum Postfach und zum Umgang mit Malware, zu der auch die Computerviren gehören. Die in einem Artikel beschriebenen urheberrechtlichen Neuerungen sind vor allem für einen wünschenswerten Ausbau der Virtualisierung von Bibliotheksdiensten problematisch.

Informationen über den Web-Browser Mozilla Firefox, leserfreundliche Textgestaltung und T_EX werden im Arbeitsalltag sicher weiter helfen.

Wir wünschen Ihnen viel Freude bei der Lektüre und hoffen, Ihnen Anregungen für Ihre Tätigkeiten geben zu können.

Über die E-Future der universitären Lehre

P. Ihrler

Dass heute vor viele englische Begriffe ein „E“ gesetzt wird, ist sicherlich eine Modeerscheinung. Es stecken aber auch einige nachvollziehbare Gründe dahinter. So bleibt neben vielen anderen Bereichen auch die Lehre an der Universität von dem „E“ und den damit verbundenen Innovationen der (elektronischen) Informationstechnologien nicht verschont. Der Artikel will einige Neuerungen beschreiben und Begriffe erläutern, die für den „E-Alltag“ der universitären Lehre relevant sein können.

Einleitend seien nur einige dieser Wörter genannt, von denen uns einige aus der Presse, aber auch zunehmend aus dem universitären Alltag bekannt sind: eGovernment, E-Learning, eScience, eTraining, E-Teaching, eCulture, eAdministration, ePayment, eZoo, eCommunity, eCompetence, E-tivities¹, eUniversity, eCampus, eContent, eVoting, ...eBay. E-Mail gehört auch dazu, obwohl sich dieses Wort schon so „eingedeutscht“ hat, dass dafür häufig nur noch das Wort „Mail“ benutzt wird. Die direkte Rückübersetzung ins Englische führt dann häufig zur Verwirrung ...

„E-Learning goes Web2.0“²

Web2.0 fasst viele neuere Entwicklungen im Bereich des Internets zusammen. Der Begriff Web2.0 wurde im Jahr 2004 gebildet und ist jünger als die meisten dahinter stehenden Technologien. Zwei wesentliche Aspekte, die Möglichkeit der aktiven Mitwirkung eines jeden Internetbenutzers an der Gestaltung des Web und die sich verbessernde Benutzeroberfläche des Web-Browsers, sollen im Hinblick auf die Auswirkungen für die universitäre Lehre genauer beleuchtet werden.

Der erste Aspekt von Web2.0 ist die Möglichkeit, dass jeder im Internet aktiv mitmachen kann. Das hat zur Folge, dass die klare Grenze zwischen dem Autor, der Web-Inhalte (eContent) erstellt, und dem Benutzer, der diese Inhalte konsumiert, nicht mehr existiert. Jeder kann heute Inhalte in das Web stellen ohne gleich eine eigene Homepage haben zu müssen, so z.B. in ein Forum, in ein Weblog oder in eine mp3-Börse. Diese Technologien wurden schon lange vor der Entstehung des Begriffs Web2.0 im E-Learning benutzt. So

können Studierende und Dozenten beispielsweise unter <http://elearn.ku-eichstaett.de> Lerninhalte und Foren erstellen. Durch solche Technologien wird eine Kommunikation über elektronische Wege ermöglicht oder „neudeutsch“ ausgedrückt, eine eCommunity der Lehrenden und Lernenden geschaffen.

Eine weitere Technologie, die zum Phänomen Web2.0 gezählt wird, heißt **Ajax** (**A**synchronous **J**avascript and **X**ML). Sie tritt zunehmend auf Internetseiten auf, leider jedoch oft um Werbespots in Webseiten einzublenden. Das Positive ist, dass Ajax und ähnliche Technologien die Benutzeroberfläche des Web-Browsers deutlich verbessern. Das ist in Zeiten, in denen immer mehr Anwendungen in den Web-Browser wandern, ganz wichtig und wird diesen Trend noch verstärken.

Wie Ajax in Erscheinung treten kann, soll am Beispiel von E-Mail-Clients gezeigt werden. Vielleicht haben Sie sich schon einmal gefragt, warum die meisten für das Lesen von E-Mails überhaupt noch einen E-Mail-Client (Pegasus Mail, Thunderbird ...) installieren und nicht einen Web-Mailer (<http://imap.ku-eichstaett.de>, <http://www.gmx.de>) verwenden. Lokale E-Mail-Clients merken sich die letzten Eingaben, wie z.B. die Adresse, so brauchen Sie nur die ersten Buchstaben einer Adresse einzugeben und schon wird die Adresse vervollständigt. Außerdem kann man Adressbücher führen und andere Einstellungen vornehmen. Neuere Web-Mailer mit Ajax, wie z.B. die Beta-Version von Google Mail, kann das alles auch. Alle Eingaben werden nicht im lokalen Web-Browser oder E-Mail-Client gespeichert, sondern im Netz. Ajax bringt u.a. den Vorteil, dass an jedem PC, an dem Sie den Web-Mailer

1. Salmon, Gilly: E-tivities. The key to active online learning, Kogan Page: London 2002

2. So wurde ein Schwerpunkt des 7. Learning Management Congress in Düsseldorf am 27. und 28. September 2006 betitelt

starten und sich einloggen, Ihre letzten Eingaben bekannt sind (siehe Abb. 1). Da heute schon alle modernen Lernplattformen ausschließlich über den Web-Browser funktionieren, werden diese Verbesserungen der Web-Benutzeroberfläche deutliche Auswirkungen auf E-Learning haben.

Ein weiteres Beispiel, wie komfortabel Web-Oberflächen mit Ajax sind, können Sie unter <http://www.protopage.com> selber ausprobieren.

Es scheinen die eFuturologen recht zu behalten, denen zu Folge es in Zukunft nur noch so etwas wie einen Web-Browser auf einer Art von Bildschirm geben wird – ohne lokale Textverarbeitung, Tabellenkalkulationen, etc. – und alle Daten im Netz gespeichert werden (erste Versuche z. B. <http://desktoptwo.com>. Die derzeit zum Straßenbild gehörenden Menschen, die ein Notebook inklusive aller wichtigen Daten mit sich tragen, werden wohl bald der Vergangenheit angehören.

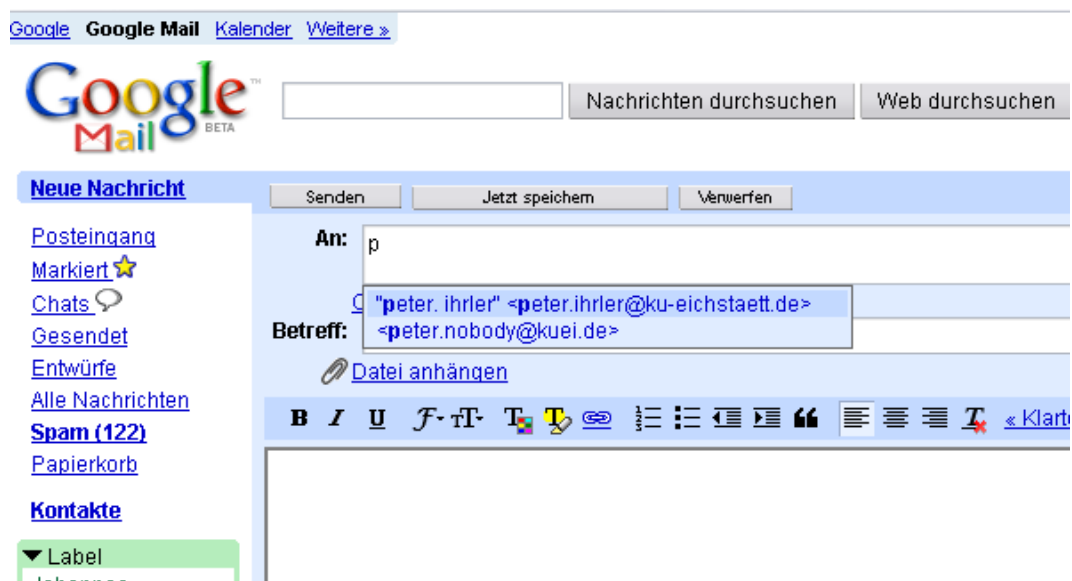


Abb. 1: Google Mail ist eines der bekannten Web2.0-Projekte

Social Software – Social Learning

Der Begriff „Social Software“ fasst ähnlich wie Web2.0 ältere und neuere Technologien zusammen. In diesem Fall sind Web-Angebote gemeint, die das Kommunizieren über Internet ermöglichen und dem Aufbau von sozialen Netzwerken und Communities dienen. Zu den ersten Technologien gehören E-Mail, Chat und Webforen. Neuere Technologien, die zur sozialen Software gehören, sind Weblogs, Wikis, Social Bookmarks (<http://www.furl.net/>), E-Portfolios, Kontaktbörsen, Plattformen zum Sammeln von Informationen und Fotos etc. Viele dieser Systeme werden heute innerhalb von Lernplattformen zur Verfügung gestellt mit dem Vorteil, dass sie ohne lange Vorbereitung schnell in Lernprozessen

eingesetzt werden können und der Zugriff nur für Berechtigte einfach und sicher festgelegt werden kann. Sie eignen sich als interaktive Lehr-, Lern- und Prüfungsräume. Dieses Gebiet hat nichts mit der Sozialinformatik zu tun, die ein Fachgebiet der Sozialen Arbeit und des Sozialmanagements ist.

E-Portfolio: Lebenslauf online

E-Portfolios sind im englischen Sprachraum bereits sehr verbreitet. Sie sind vergleichbar mit einem in das Netz gestellten Lebenslauf oder mit einer persönlichen Webseite, die die Interessen und Qualifikationen einer Person aufzeigt. An Universitäten wird das E-Portfolio vielfach von Studierenden eingesetzt um ihre Entwick-

lung im Studium (Lehrveranstaltungen, Studienarbeiten, Transcript of Records) und Aktivitäten außerhalb der Universität aufzuzeigen. Software für E-Portfolio ermöglicht es, dass nur einzelne Teile der eingegebenen Daten für bestimmte Personenkreise (z.B. Firmen, die Personal suchen) offen gelegt werden. <http://elgg.net/> bietet die Gelegenheit, für sich selbst ein Portfolio zu erstellen und teilweise zu veröffentlichen. Eine vergleichbare Software findet sich unter <http://www.osportfolio.org/>. E-Portfolios werden wohl bald auch in CampusManagementSystemen und Lernplattformen deutscher Hochschulen einziehen (weitere Infos: <http://www.e-teaching.org/didaktik/gestaltung/kommunikation/portfolio/>).

Tags: Meta-Informationen leicht gemacht Attribut/Wert-Kombinationen

Um Medien (Bücher, Filme ...) wiederfinden zu können, werden diese mit Metadaten versehen. Dies ist jedoch mühsame Arbeit, die vor allem im Bereich Web und E-Learning nicht oder nur sehr ungern gemacht wird. Auch Lernplattfor-

men stellen Formulare zur Eingabe von Metadaten zur Verfügung. Die Nutzung dieser Möglichkeiten ist jedoch wegen des hohen Aufwands gering und damit bleibt die Wiederauffindbarkeit von Lernmodulen schwierig.

Initiativen im Web versuchen das Problem pragmatisch mit so genannten Tags zu lösen, z.B. <http://images.google.com/>. Tags sind Schlagwörter, die ohne festgelegte Indexierungsregeln und auf einfache Art und intuitiv in der eCommunity des Web gebildet werden. <http://mail.google.com/> oder <http://www.flickr.com/> verwenden „tags“ oder „labels“ als Suchbegriffe, die man sich „unbürokratisch“ und schnell selber definieren kann (siehe Abb. 2). Gruppen von Tags werden häufig visuell je nach Grad ihrer Bedeutung oder Häufigkeit hervorgehoben. Dieser Ansatz ist auch Teil des „Web 2.0“ und hält allmählich auch bei Lernplattformen Einzug. Weitere Ansätze mit Metadaten umzugehen finden sich im Bereich des „Semantischen Web“ oder bei der Suchmaschine <http://de.gnod.net/>, die u. a. Knowledge Maps verwendet (siehe Abb. 3).

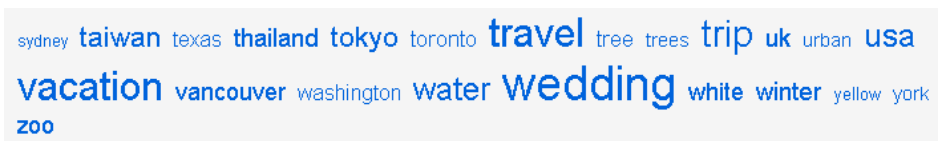


Abb. 2: Tags nach Popularität bei www.flickr.com

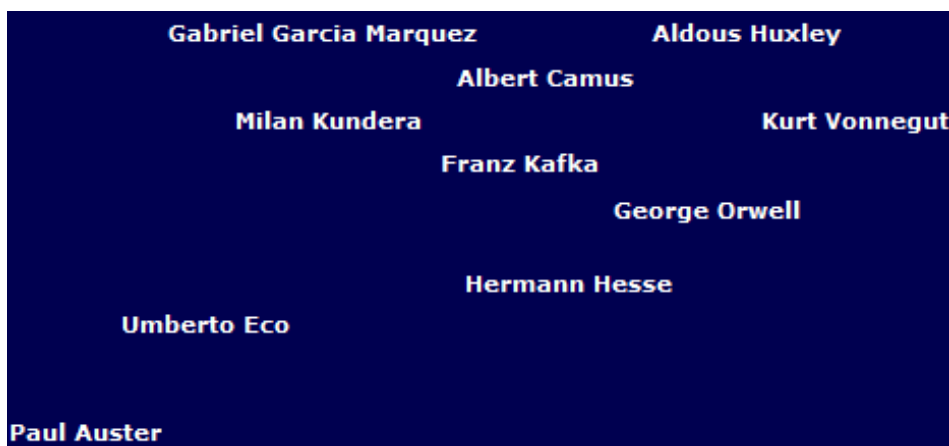


Abb. 3: Ausschnitt einer Literaturlandkarte von Hermann Hesse aus <http://de.gnod.net/>

Digitaler Semesterapparat

Manche Bibliotheken und Lehrinhalte bieten Semesterapparate nicht mehr in einem Bücherregal, sondern digital an. Aufsätze aus Büchern, die zur Literaturliste eines Seminars gehören, werden eingescannt und im Netz zur Verfügung gestellt. Links zu Artikeln elektronischer Zeitschriften werden online aufgelistet oder es werden gleich die dahinter liegenden pdf-Dateien online zur Verfügung gestellt. Damit werden Engpässe und das Heißlaufen des Kopierers im Lesesaal vermieden. Der digitale Semesterapparat kann ein Service von Bibliotheken sein, die neben der Zusammenstellung des Materials gleich online bereitstellen und die Lernplattform dahin verlinken, oder das Material wird gleich in der Lernplattform z. B. innerhalb eines Kurses zur Verfügung gestellt. Leider kann man nun nicht einfach mit dem Digitalisieren starten, sondern muss das Urheberrecht beachten, und zwar in Form des gültigen Urheberrechts sowie einzelvertraglicher Regelungen. Ist eine solche Bereitstellung eines digitalen Semesterapparats geplant, sollte man also mit der Bibliothek vorher Rücksprache halten.

Der Webservice RSS

Regelmäßig in den Lieblingsseiten des Webs zu suchen, gehört für viele heute schon der Vergangenheit an. Mit Hilfe von RSS oder anderen Newsfeeds muss der Benutzer nicht mehr nach den Neuerungen in Webseiten suchen, sondern die Webseite informiert den Benutzer, dass sich ihr Inhalt geändert hat. RSS wird auch in Lernplattformen Einzug halten. Der Studierende erhält eine Nachricht, dass der Dozent Inhalte in einem Lernmodul aktualisiert hat oder es trifft die lang gefürchtete News ein, dass die Noten der letzten Online-Klausur nun eingesehen werden können. Der Dozent erfährt per RSS automatisch, dass ihm endlich im Forum ein Studierender widersprochen hat.

Vom Podcast zum Profcast

Podcasts sind über Newsfeeds angebotene Audio- oder Videodateien im Internet, die leicht über Synchronisationssoftware auf tragbare Medienplayer (wie z. B. iPod, von dem der Begriff Pod-

cast herrührt) übertragen werden können. Podcasts können neben vielen anderen Inhalten auch Bildung zum Inhalt haben und schaffen einen neuen Anwendungsbereich im mobilen Lernen. In diesem Zusammenhang ist der Begriff Profcast entstanden, in dem das „Pod“ durch die Abkürzung von Professor, also „Prof“ ersetzt wurde. Der Begriff Profcast ist inzwischen auch zu einem Produktnamen von entsprechender Software geworden. In der MMB-Studie „Learning Delphi für Hochschulen 2006“, in der 52 Hochschul- und E-Learning-Experten aus Deutschland, Österreich und der Schweiz befragt wurden, sehen allerdings nur 20 Experten eine große Bedeutung für die Hochschullehre.³

Lehrevaluation

Software zur Ermittlung der Qualität von Lehre kommt zunehmend auf den Markt. Lernplattformen bieten teilweise bereits integrierte Werkzeuge um die Qualität der Lehre zu bewerten. Andererseits gibt es Spezialsoftware, die versucht sich der Daten der Lernplattformen zu bedienen, um die Datenerhebung zumindest teilweise zu automatisieren. Blubbsoft hat mit dem Produkt Zensus bereits eine Lösung, die Daten aus einigen Lernplattformen herausholen kann. Eine Demoversion von Zensus kann von Peter Ihrler ausgeliehen werden. Einen ganz anderen Weg schlägt die Webplattform <http://www.meinprof.de> ein. Hier geben Studierende ihre Meinung über ihre Professoren – auch die der KU – ab. Die Qualität der Professoren und ihrer Veranstaltungen wird öffentlich, wenn auch mit anzweifelbaren Methoden.

Wissenschaftliches Zitieren aus Wikipedia

Dieses Thema fällt ein bisschen aus der Reihe der bisher behandelten Punkte und dessen Zukunftsträchtigkeit wird hier nicht abschließend bewertet. Darf ein Studierender in seiner Seminararbeit aus Wikipedia zitieren? Gehört diese neue Möglichkeit des Recherchierens inzwischen in den Bereich des wissenschaftlichen Arbeitens? Muss das sogar in unserem Zeitalter nicht so sein, wenn die größte Wissensquelle das Internet ist? Ist ein bestimmter Verlag

3. MMB-Trendmonitor II / 2006, Szenarien für die eUniversity 2011. Experten prognostizieren eine deutliche Zunahme von neuen Computer-Lernformen an Hochschulen (http://www.mmb-institut.de/2004/pages/trendmonitor/Trendmonitor-Downloads/Trendmonitor_II.2006.pdf)

bzw. eine bestimmte Website der Indikator für wissenschaftliche Qualität, oder ist es der Autor oder der Inhalt? Die Problematik sollte in der Lehre thematisiert sein. Bei der Verwendung von Zitaten sollten Studierende wissen, was man tun darf und was nicht und letztlich auch, dass es Software gibt, die Plagiate aufspüren kann (Plagiarism-Finder, Eve2, Übersicht in <http://plagiat.fhtw-berlin.de/html/links/tools.html>), und dass es Lehrende gibt,

die diese auch benutzen. Zum Abschluss noch ein Zitat, das seine Herkunft nicht verschweigt: „Für Internetseiten gilt, was für Bücher auch gilt: Der eine schreibt vom anderen ab. Autoren machen Fehler und begehen Irrtümer, die durch den Blick in eine weitere Veröffentlichung aufgedeckt werden könnten.“ (http://de.wikipedia.org/wiki/Wissenschaftliches_Arbeiten, 5.10.2006).

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Peter Ihrler	Er: eO-004	-1585	peter.ihrler

ILIAS-News

P. Ihrler

Das Universitätsrechenzentrum stellt im Rahmen seiner Multimedia- und E-Learning-Aktivitäten die Lernplattform ILIAS (<http://elearn.ku-eichstaett.de>) als Dienstleistung bereit. Alle lernenden und lehrenden Angehörigen der Universität sowie auch Lehrbeauftragte und Gaststudierende können Inhalte einstellen und benutzen.

Neue Version

Die vorlesungsfreie Zeit wurde genutzt, um ILIAS auf den aktuellen Stand zu bringen. Die neue Version bringt viele Verbesserungen, von denen nur die wichtigsten kurz erwähnt werden sollen:

- ▷ ILIAS ist es gelungen, den Level A für barrierefreies Internet zu erlangen. Barrierefreies Internet soll auch Menschen mit Behinderungen, altersbedingten Einschränkungen etc. die Benutzung des Internet ermöglichen. Die mit ILIAS mitgelieferte Standardoberfläche ist freundlicher als die der älteren Versionen, die oft von Benutzern als trocken und kalt bezeichnet wurden.
- ▷ Ein Schwerpunkt der Neuerungen lag im Ausbau der Möglichkeiten des individuellen Lernens. Es gibt nun Werkzeuge für den Lernfortschritt (vor allem für die akademische Weiterbildung, Fernlehre), die Lernplanung und das Management von Blended Learning (Planung von Präsenzveranstaltungen wie Blockseminare, Anfahrtskizzen, Verbesserung der Teilnehmerlisten, automatisch erzeugte E-Mail-Listen der Teilnehmer an einer Veranstaltung (siehe Abb. 1), Mitglieder-Galerie).
- ▷ Lernmodule können jetzt auch nur teilweise für die Studierenden frei gegeben werden, so dass ein Dozent z. B. während der Vorlesungszeit noch ungehindert den Lernstoff der kommenden Wochen einstellen kann, ohne dafür mehrere kleinere Module machen zu müssen.
- ▷ Besonders für Mathematiker und andere, die viele Formeln verwenden, ist es hilfreich, dass jetzt auch \LaTeX unterstützt wird. Die nächste Version wird außerdem einen Formeleditor beinhalten, so dass dann für Formeln keine \LaTeX -Kenntnisse notwendig sein werden.
- ▷ Kleinere Verbesserungen wurden in den Test- und Übungstools gemacht: bessere Unterstützung von Lückentext, Zufallstest und Feedbackmöglichkeiten, anonyme Tests und Umfragen, Anzeige der restlichen Bearbeitungszeit (siehe Abb. 2).
- ▷ In den Foren ist jetzt mehr Platz für die eigentlichen Diskussionsbeiträge. Foren können nun auch statistisch ausgewertet werden.

Abb. 1: E-Mail an alle Mitglieder einer Veranstaltung

Abb. 2: Anzeige der restlichen Bearbeitungszeit in Übungen

iLEX → eLAIX

eLAIX2.0 ist das Nachfolgeprodukt von iLEX1.0. eLAIX ermöglicht das schnelle Erstellen von Lernmodulen mit einem Textverarbeitungssystem.

Nach Fertigstellung wird die Datei in ILIAS hochgeladen.

Es wurde vor allem die Installationsroutine vereinfacht und die Software läuft stabiler als die

alte Version. Einziger kritischer Punkt ist die durch die Namensänderung erzeugte Begriffsverwirrung. Der Autor wollte lediglich die ursprünglich deutsche Aussprache von iLEX in die englische Aussprache übertragen; man soll eLAIX also „ilex“ aussprechen.

Geht ILIAS auch ohne Internetanschluss?

ILIAS kann mit voller Funktion auf einem lokalen Computer bzw. Notebook installiert werden und man kann so sämtliche Inhalte (Lernmodule, Tests, etc.) entwickeln. Wenn man dann wieder online ist, können die Module in das Online-ILIAS der Universität hochgeladen werden. Zuerst muss XAMPP unter Windows oder Linux installiert werden und dann ILIAS. XAMPP enthält unter anderem einen Apache Webserver, PHP und das Datenbanksystem MySQL. Die Installation von XAMPP geht leider nur mit etwas Glück schnell vonstatten. Mehr Informationen finden Sie unter <http://www.ilias.de/docu/>. Wenn nur Lernmodule offline erstellt werden sollen, kann dafür auch eLAIX benutzt werden.

Lernende können Teile von Kursmaterialien wie Lernmodule und Dateien (pdf, doc, xls, ppt ...) herunterladen (wenn es der Autor erlaubt hat!) und diese offline lesen.

Interne E-Mail umleiten

ILIAS hat ein internes E-Mail-System, das vielfach genutzt werden kann. Es kann z. B. allen Teilnehmern eines Kurses eine E-Mail („Die Vorlesung muss morgen leider entfallen ...“) geschickt werden oder man kann sich optional eine E-Mail schicken lassen, wenn jemand auf einen eingestellten Forumsbeitrag antwortet.

Nachteilig wurde von Benutzern gesehen, dass man in ILIAS nicht so oft die E-Mails liest als in

der normalen E-Mail-Box. Es gab in ILIAS schon immer die Option, sich die internen E-Mails auch an die im persönlichen Profil angegebene Adresse schicken zu lassen. Doch war dies nur wenigen bekannt. In der neuen Version ist jetzt bei allen neu angemeldeten Benutzern die E-Mail automatisch so eingestellt, dass Nachrichten in beide Boxen geschickt werden.

Benutzer, die sich vor dem September 2006 in ILIAS angemeldet haben, erhielten bislang ihre E-Mails nur innerhalb von ILIAS. Seit 5. Oktober erhalten alle Benutzer ihre E-Mails sowohl innerhalb ILIAS als auch unter der von ihnen angegebenen E-Mail-Adresse. Wer das nicht so möchte, kann dies in ILIAS bei den Mail-Einstellungen ändern. Es gibt drei Einstellungsmöglichkeiten: nur innerhalb ILIAS, nur weitergeleitet oder beides („Lokal und Weiterleitung“ = derzeitige Einstellung).

Statistik: Benutzer, Lernmodule

Während des Sommersemesters wurde protokolliert, wie viele BenutzerInnen wann ILIAS-Lernmodule benutzten. Zu beachten ist, dass nicht bei allen Lehrveranstaltungen ILIAS-Lernmodule eingesetzt werden. Es gibt eine Vielzahl anderer Nutzungsmöglichkeiten wie Diskussionsforen, Einstellen von Dateien im pdf- oder Powerpoint-Format (mehr dazu unter http://www1.ku-eichstaett.de/urz/inkuerze/1_06/e-learning.html). Bis Ende des Sommersemesters waren 347 BenutzerInnen registriert. Im Laufe des Sommersemesters haben 234 verschiedene BenutzerInnen (von 347) auf ILIAS-Lernmodule (Verweildauer mind. 300 Sek.) zugegriffen (siehe Abb. 3). Besonders oft wurde gegen Semesterende während der Prüfungsphase auf ILIAS-Module zugegriffen (siehe Abb. 4).

Tracking-Daten	
Suchbegriff(e):	<input type="text"/>
Zeitraum:	2006 ▾ 4 ▾ 1 ▾ - 2006 ▾ 9 ▾ 30 ▾
Anzeigemodus:	Tageszeiten innerhalb des Zeitraums ▾
Zugriffsobjekte:	Lernmodul ILIAS ▾
Benutzersprache:	Alle Sprachen ▾
Daten anzeigen	

Die nachfolgende Zugriffsstatistik bezieht sich auf alle Objekte des Typs 'Lernmodul ILIAS'.

Zugriffsstatistiken: Tageszeiten innerhalb des Zeitraums		
Zeit	Anzahl	
00:00:00 ~ 01:00:00	13	
01:00:00 ~ 02:00:00	10	
02:00:00 ~ 03:00:00	0	
03:00:00 ~ 04:00:00	9	
04:00:00 ~ 05:00:00	0	
05:00:00 ~ 06:00:00	48	
06:00:00 ~ 07:00:00	314	■
07:00:00 ~ 08:00:00	513	■
08:00:00 ~ 09:00:00	810	■
09:00:00 ~ 10:00:00	997	■
10:00:00 ~ 11:00:00	1100	■
11:00:00 ~ 12:00:00	886	■
12:00:00 ~ 13:00:00	1133	■
13:00:00 ~ 14:00:00	821	■
14:00:00 ~ 15:00:00	1122	■
15:00:00 ~ 16:00:00	916	■
16:00:00 ~ 17:00:00	897	■
17:00:00 ~ 18:00:00	696	■
18:00:00 ~ 19:00:00	751	■
19:00:00 ~ 20:00:00	446	■
20:00:00 ~ 21:00:00	502	■
21:00:00 ~ 22:00:00	408	■
22:00:00 ~ 23:00:00	154	■
23:00:00 ~ 24:00:00	91	■

(Eintrag 1 - 24 von 24)

Abb. 3: Aufrufe von Lernmodulen im Sommersemester 2006 nach Tageszeiten

Tracking-Daten	
Suchbegriff(e):	<input type="text"/>
Zeitraum:	2006 ▾ 7 ▾ 13 ▾ - 2006 ▾ 7 ▾ 31 ▾
Anzeigemodus:	Tage innerhalb des Zeitraums ▾
Zugriffsobjekte:	Lernmodul ILIAS ▾
Benutzersprache:	Alle Sprachen ▾
<input type="button" value="Daten anzeigen"/>	

Die nachfolgende Zugriffsstatistik bezieht sich auf alle Objekte des Typs 'Lernmodul ILIAS'.

Zugriffsstatistiken: Tage innerhalb des Zeitraums		
Zeit	Anzahl	
2006-07-13	118	■
2006-07-14	112	■
2006-07-15	8	
2006-07-16	6	
2006-07-17	97	■
2006-07-18	395	■
2006-07-19	325	■
2006-07-20	273	■
2006-07-21	108	■
2006-07-22	17	
2006-07-23	155	■
2006-07-24	126	■
2006-07-25	462	■
2006-07-26	498	■
2006-07-27	50	■
2006-07-28	26	
2006-07-29	12	
2006-07-30	11	
2006-07-31	52	■

(Eintrag 1 - 19 von 19)

Abb. 4: Aufrufe von Lernmodulen gegen Semesterende nach Tagen

Kurse und Benutzertreffen

Im Laufe des Wintersemesters und kurz nach der Vorlesungszeit werden wieder Kurse zu ILIAS und eLAIX (vormals iLEX) angeboten (siehe <http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/kurse.de>). Je nach Bedarf können auch nach Absprache weitere Kurse und Einführungen organisiert werden.

Mitte Oktober fand das erste Benutzertreffen statt, zu dem alle bisherigen ILIAS-Kurs-Teilnehmer eingeladen wurden. Schwerpunkte des Treffens waren die wichtigsten Neuerungen der aktuell an der KU installierten ILIAS-Version und Methoden zur Erstellung anonymer Umfragen (ohne dass man sich in ILIAS registrieren muss) und wie man Lernmodule aus anderen Lernplattformen auf ILIAS migrieren kann.

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Peter Ihrler	EI: eO-004	-1585	peter.ihrler

Virtuelles Angebot für Absolventen der Fakultät für Soziale Arbeit

Prof. Dr. H.-J. Göppner

Die Fakultät für Soziale Arbeit bemüht sich seit Jahren, den Kontakt zu ihren Absolventen zu intensivieren. Bisher bestand über die Website der Fakultät die Möglichkeit, in einer Maske die aktuellen Adressdaten einzutragen. Diese werden in einen Postverteiler aufgenommen, in dem mittlerweile von den über 2.000 Absolventen ca. 1.200 eingetragen und so für die Fakultät postalisch erreichbar sind. Damit bestand die Möglichkeit zu Veranstaltungen, Jubiläen und Ehemaligentreffen einzuladen. Mit Unterstützung des Universitätsrechenzentrums (Herr Ihrler) konnten nun weitere sehr attraktive Angebote eingerichtet werden:

- ▷ Externer Zugriff auf Bibliotheksdatenbanken. Die Absolventen können damit Recherchen zur aktuellen Literatur in ihrem Bereich durchführen.
- ▷ Lebenslange KUEI-E-Mail-Adresse.
- ▷ Forum für Absolventen (und Dozenten). Es besteht die Möglichkeit zu allen aktuellen Themen einen Text einzustellen, so dass sich eine Diskussionsplattform entwickeln kann. Außerdem können auch Informationen und Suchanfragen ausgetauscht werden. Die Fakultät hofft auf eine zahlreiche Inanspruchnahme der angebotenen Dienste.

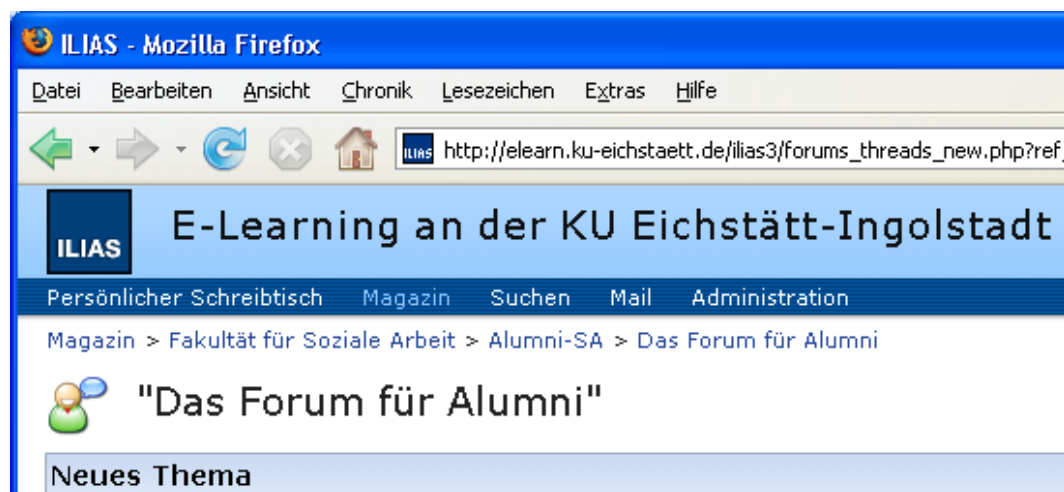


Abb.: Das Forum wurde über die Lernplattform ILIAS realisiert

VoIP: Telefonieren über das Datennetz

Dr. W.A. Slaby

Seit nahezu bei jedem DSL-Anbieter z. B. mit iPhone kostenloses Telefonieren mit Computer und Headset über das Internet ermöglicht wird oder sich mit Skype weltweite Peer-to-Peer-Telefonverbindungen ohne weitere Gesprächsgebühren aufbauen lassen, ist Voice-over-IP (VoIP), das Telefonieren über die weltweiten Datennetze, zumindest im privaten Bereich unaufhaltsam auf dem Vormarsch. Aber eignet sich diese Technologie auch für den Einsatz in einer Universität, wo hunderte von Telefonen als Nebenstellen zu betreiben sind und wichtige Telefoniefunktionen wie z. B. Chef-Sekretär-Funktionen in gewohnter Weise gewährleistet sein müssen? Dies herauszufinden ist Gegenstand eines Pilotprojekts, welches das Universitätsrechenzentrum seit Mitte 2005 durchführt.

VoIP-Server Asterisk

Auf der Basis der OpenSource-Software Asterisk, die auf einem gewöhnlichen Linux-Server aufsetzt, wurde dazu ein VoIP-Telefonserver eingerichtet, an den über das Hochschulnetz der KU inzwischen mehr als 60 IP-Telefone, überwiegend vom Typ Snom360 (siehe Abb. 1), angeschlossen sind. Über ein dem HTTP im WorldWideWeb

vergleichbares Protokoll SIP (*Session Initiation Protocol*) kann zwischen zwei IP-Telefonen über den VoIP-Server eine Verbindung aufgebaut werden, über die anschließend via RTP (*Real-time Transport Protocol*) die digitalisierten Sprachdaten des Telefongesprächs in gewohnter ISDN-Qualität übertragen werden.



Abb. 1: IP-Telefon Snom360

Damit die IP-Telefone im Hochschulnetz der KU aber nicht nur für interne Gespräche untereinander verwendbar sind, sondern darüber hinaus aus dem normalen Telefon-Festnetz und den Mobilnetzen erreichbar sind bzw. zu Telefonen im Festnetz oder in den Mobilnetzen eine Gesprächsverbindung aufbauen können, verfügt der VoIP-Server über eine zusätzliche, von der Fa. Digium, dem Haupt-Entwickler von Asterisk, produzierte Interface-Karte mit zwei in der ISDN-Telefonie

üblichen S_{2M} -Schnittstellen. Über diese beiden S_{2M} -Schnittstellen ist der VoIP-Server mit der Telefon-Nebenstellenanlage Siemens HiPath4000 der KU gekoppelt (siehe Abb. 2), so dass gleichzeitig bis zu 60 ein- oder ausgehende Gespräche mit Teilnehmern innerhalb der KU an Nebenstellen der HiPath4000-Anlage oder außerhalb im Festnetz oder in den Mobilnetzen geführt werden können.

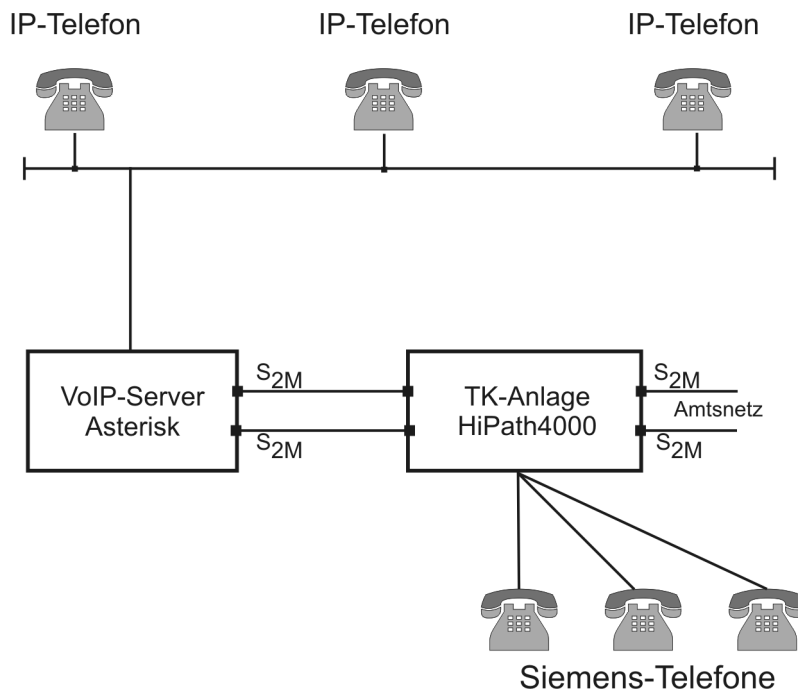


Abb. 2: Kopplung zwischen Asterisk und HiPath4000

Die aus der ISDN-Welt gewohnten Funktionen wie Automatische Weiterleitung, Weiterleitung bei Besetzt oder nach einem Zeitintervall, Anklopfen, Makeln, Konferenzschaltung, etc. stehen selbstverständlich auch an den IP-Telefonen zur Verfügung. Darüber hinaus ist für jeden Teilnehmer an der IP-Telefonie auf dem VoIP-Server eine Sprachbox eingerichtet, in die eine IP-Nebenstelle entweder dauerhaft umgeleitet werden kann bzw. in die automatisch verzweigt wird, wenn sich der Teilnehmer der IP-Nebenstelle nicht innerhalb von 20 Sekunden meldet. Dort kann der Anrufende eine Sprachnachricht (Voice-Mail) aufsprechen, die je nach den vom Besitzer der IP-Nebenstelle vorgegebenen Präferenzen in

der Sprachbox abgelegt und/oder als Anhang einer E-Mail diesem zugestellt wird. Zur Verwaltung der Sprachbox stehen selbstverständlich umfangreiche, über ein Sprachmenü am Telefon auswählbare Funktionen zur Verfügung; eine Übersicht dazu finden Sie unter <http://www.kueichstaett.de/Rechenzentrum/dienstleist/fax>

VoIPbreakout

Hinter der Bezeichnung *VoIPbreakout* verbirgt sich ein neuer, von T-Systems im Auftrag des DFN-Vereins erbrachter Dienst, mit dem allen Hochschulen und Forschungseinrichtungen im Deutschen Forschungsnetz, die über einen VoIP-

Server verfügen, ermöglicht wird, ihren ausgehenden Telefonverkehr nicht vor Ort direkt ins Amtsnetz zu leiten, sondern zunächst über das deutsche Wissenschaftsnetz X-WiN zu einem

zentralen Server der T-Systems in Frankfurt zu senden, der die Weiterleitung in das jeweilige Zielnetz (Festnetz, Mobilnetz) vornimmt.

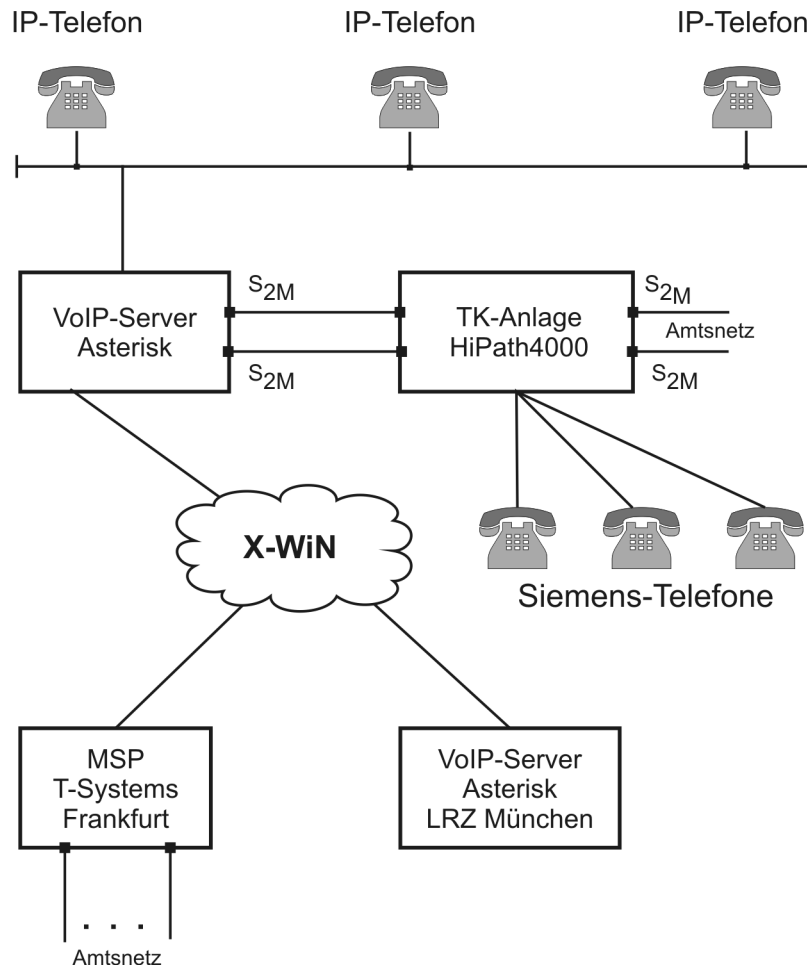


Abb. 3: Einbindung in den Service VoIPbreakout

Neben dem Leibniz-Rechenzentrum München, der Universität Rostock und der Geschäftsstelle des DFN-Vereins in Berlin gehörte das Universitätsrechenzentrum der KU zu den vier Pilot-Anwendern, die diesen neuen Dienst erproben konnten. Inzwischen wird dieser Service VoIPbreakout von uns produktiv genutzt: nicht nur die von IP-Telefonen ins Fest- oder Mobilnetz ausgehenden Telefonate werden statt direkt ins Eichstätter Amtsnetz zunächst zum MSP-System nach Frankfurt geleitet, sondern auch alle von den Nebenstellen an der Siemens HiPath4000-Anlage ausgehenden Gespräche (mit Ausnah-

me von Telefonaten zu gewissen Sondernummern 0800-, 0180-, 0190-, etc.). Neben der Entlastung des Amtsanschlusses der HiPath4000-Anlage lässt sich für die KU als weiterer Vorteil eine Reduzierung der Telefonkosten erzielen, da sämtliche Ferngespräche ins deutsche Festnetz zum rabattierten Ortstarif abgerechnet werden. Darüber hinaus haben wir (siehe Abb. 3) eine direkte Kopplung unseres Asterisk-VoIP-Servers mit dem entsprechenden Asterisk-VoIP-Server des Leibniz-Rechenzentrums München vorgenommen, so dass Telefonate ins Leibniz-

Rechenzentrum oder in die Münchener Universitäten kostenfrei geführt werden können.

Weitere Entwicklungen

In naher Zukunft soll dieser Service VoIPbreakout zu einem Dienst VoIPconnect weiterentwickelt werden, der es zusätzlich gestattet, IP-Telefonanlagen von DFN-Einrichtungen nicht bilateral (wie bei der Kopplung der beiden Asterisk-VoIP-Server von KU und LRZ) sondern über das MSP-Gateway der T-Systems in Frankfurt multilateral miteinander zu verbinden.

Desweiteren streben wir eine Vereinheitlichung im Bereich der Sprachboxen an, die derzeit für IP-Telefonteilnehmer auf dem Asterisk-VoIP-Server, für alle übrigen mit Nebenstellen an der HiPath4000-Anlage aber auf unserem Tobit Fax-/VoiceMail-Server verwaltet werden. Die Umstellung der Sprachboxen für den letztgenannten Nutzerkreis wird noch in diesem Jahr erfolgen, der Umstellungstermin wird rechtzeitig vorher bekanntgegeben. Hierdurch kann der Tobit-Server auf den Faxempfang und -versand beschränkt werden, was zu einer Lizenz- und damit Kostenreduzierung führen wird.

Derzeitige Defizite

Natürlich würden wir auch den Faxempfang und -versand gern über den Asterisk-VoIP-Server ab-

wickeln, um auf diese Weise den Tobit-Server komplett einsparen zu können. Mit dem Fax-/Mail-Gateway *Asterfax*, welches als Software auf Asterisk aufsetzt, haben wir dazu bereits ausgiebige Versuche unternommen. Allerdings ließ sich die für den Fax-Service notwendige Stabilität mit dieser Lösung nicht gewährleisten, was insbesondere daran liegt, dass die übliche Faxübertragung besonders empfindlich gegen die bei der Übertragung von IP-Paketen unvermeidbaren Schwankungen (Delay + Jitter) ist. Hier wird erst die Nutzung des für die Übertragung von Faxdaten in IP-Netzen geeigneteren Protokolls T.38 Abhilfe schaffen können, dessen Implementierung in Asterisk sich allerdings noch im Entwicklungsstadium befindet.

Ein weiteres Problem mit Schwankungen in der Qualität der IP-Telefonie besteht derzeit noch in zwei vom Campus-Netz der KU abgesetzten Bereichen, deren Anbindung an das Hochschulnetz mit einer Übertragungsleistung von nur 2 Mbit/s sich trotz Priorisierung der VoIP-Datenpakete für die erforderliche Qualität und Stabilität von IP-Telefonie als unzureichend erwiesen hat. Dieses Defizit werden wir durch Anbindung der beiden Bereiche mit Richtfunkstrecken einer Übertragungsleistung von 54 Mbit/s in naher Zukunft beseitigen können.

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Dr. Wolfgang A. Slaby	EI: eO-109a	-1214/-1462/-1670	wolfgang.slaby

Und dauernd funkt das Netz

A. Kaltenbacher

Seit geraumer Zeit bietet das URZ den Studierenden und der Mitarbeiterschaft die Möglichkeit, mit einem Notebook in das Internet zu gelangen. Gerne wird das Angebot angenommen, besonders seit es auch möglich ist, an einigen Teilen des Campus sich an einem Funknetz anzumelden. Leider gibt es aber oftmals Hürden, die ein angenehmes Arbeiten behindern oder unterbinden. Im nachfolgenden Artikel will ich auf einige Probleme eingehen und Lösungsansätze beschreiben.

1. Allgemeine Vorgehensweise beim Zugang:

Die nachfolgende Grafik verdeutlicht im Wesentlichen die Verbindungsaufnahme und den Ablauf für einen Zugang ins Internet. Das Ganze gliedert sich in die Phasen

- a) Netzverbindung mit dem Notebook herstellen, danach IP-Adresse beim DHCP-Server anfragen und erhalten,
- b) VPN-Client herunterladen und installieren (dies aber nur einmal),
- c) VPN-Client starten und mit eigener Kennung authentisieren und
- d) die Angebote im Internet wahrnehmen.

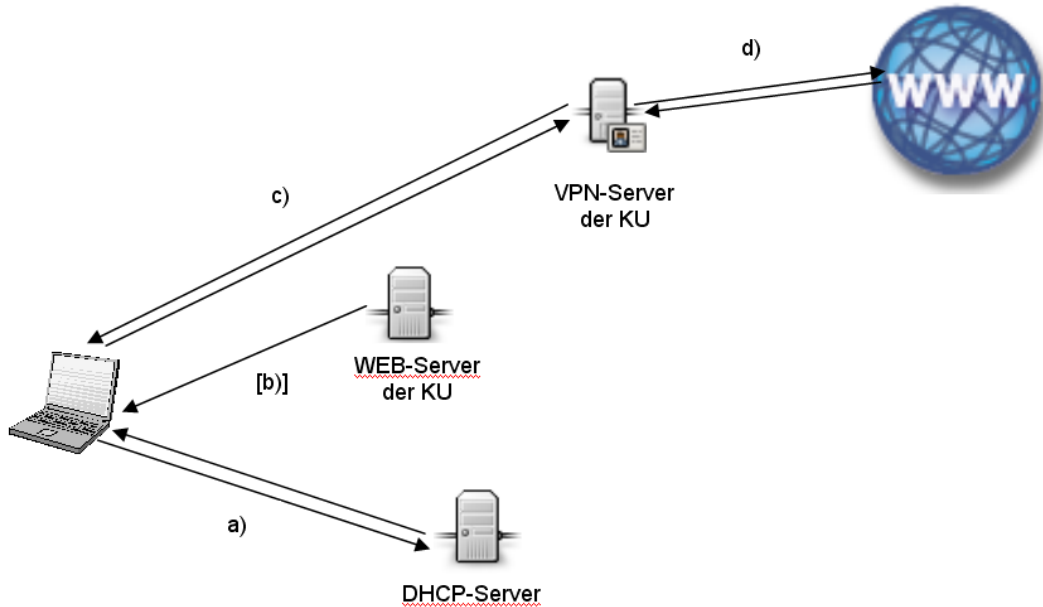


Abb. 1: Schematischer Ablauf für einen Zugang ins Internet

Während der einzelnen Phasen können immer wieder Probleme auftreten, die der Anwender mit etwas Interesse und Neugier selbst leicht identifizieren und in den meisten Fällen beheben kann. „Aber ich kenne mich mit dem Notebook doch gar nicht aus“; das mag zwar stimmen, hilft Ihnen leider aber nicht weiter. Wie beim Kauf eines neuen Produkts (sei es Auto, Fernseher – Verzeihung Plasma-/LCD-TV) wird man das Handbuch eingehend studieren. So ist auch bei Notebooks, hier gibt es – wenn auch dünne – Handbücher, fast immer CDs, in denen zusätzliche Dokumentationen stehen und nach dem Start des Notebooks hat man bei MS Windows über *Start → Hilfe und Support* noch mehr Möglichkeiten, sich mit seinem System bekannt zu machen.

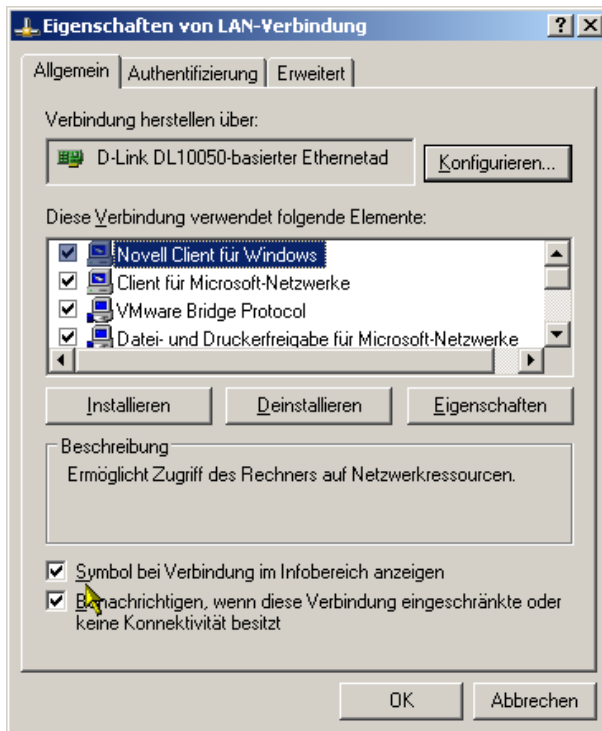
2. Fehlende oder falsche Netzverbindung

Die erste große Hürde ist die Verbindungsaufnahme mit dem lokalen Netz der KU, d. h. entweder Kabel einstecken in den RJ45-Dosen für den öffentlich zugänglichen Bereich oder Einschalten der Funknetz-Karte.

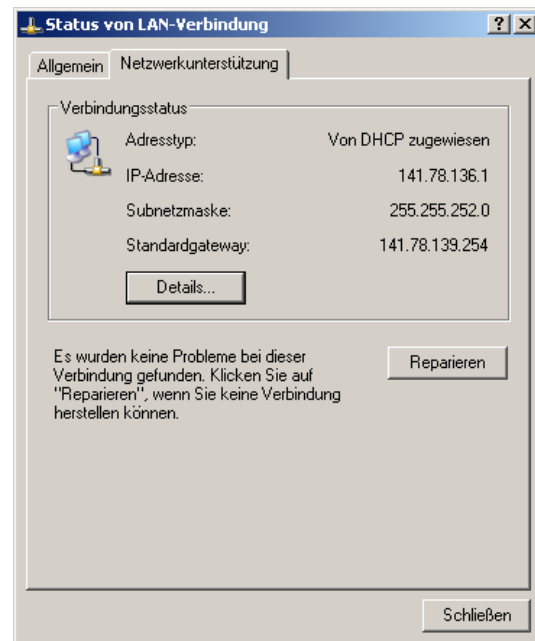
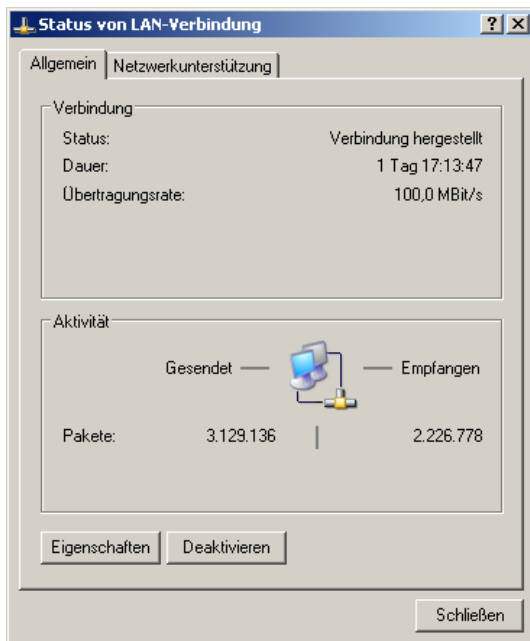
„Wie, ich muss die Funknetz-Karte einschalten?“; unter Umständen ja, aber das hängt vom jeweiligen Notebook und den individuellen Einstellungen ab, die wir nicht kennen, die der Anwender aber leicht jederzeit mit Hilfe seines Handbuches oder den weiteren bekannten Informationsquellen bestimmen kann.

Nachdem nun also die Netzgeräte laufen, wird meist im Systray (rechts unten in der Taskleiste) ein Symbol für die Netzverbindung angezeigt. Wenn dies nicht der Fall ist, kann man dieses Symbol über *Start → Einstellungen → Systemsteuerung → Netzwerk- und Internetverbindungen →*

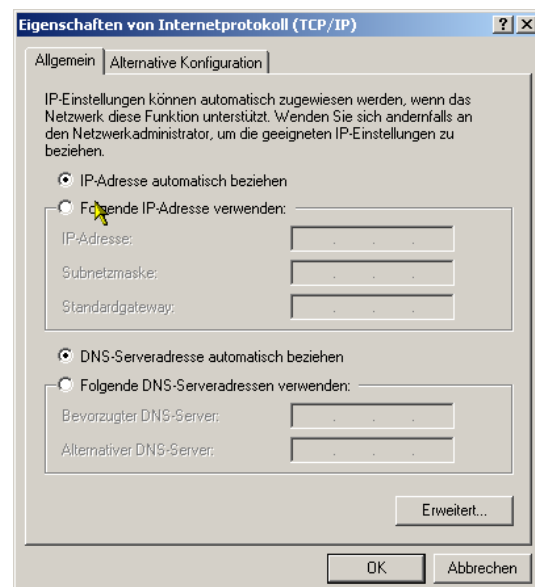
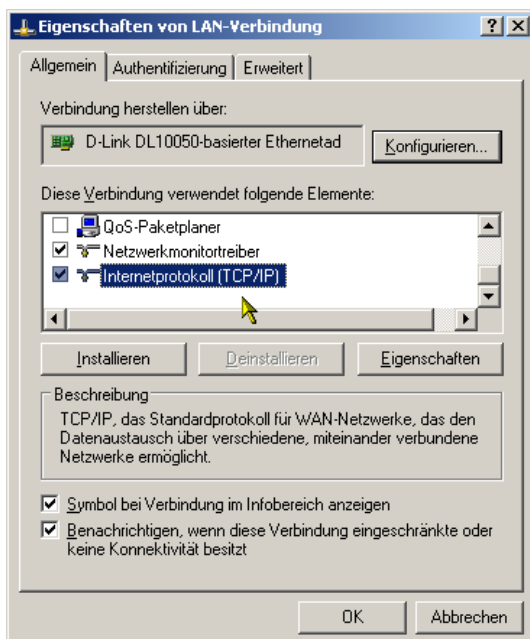
Netzwerkverbindungen oder *Start* → *Verbinden mit* → *Alle Verbindungen anzeigen* danach Auswahl der entsprechenden Netzwerkkarte und mit rechter Maustaste *Eigenschaften* und Aktivierung des Punktes *Symbol bei Verbindung im Infobereich anzeigen* darstellen lassen.



Dieses angezeigte Symbol ist unser erster Ansatz für eine Lösungsmöglichkeit, denn wenn Windows anzeigt, es gäbe eine Verbindung, aber man keine Daten erhält, dann muss ich erst sehen, ob überhaupt Daten fließen. Mit einem Doppelklick auf das Symbol der Netzverbindung: erhält man ein Fenster mit vielfältigen interessanten Informationen über die Register *Allgemein* und *Netzwerkunterstützung*.



Interessant für uns ist zunächst das *Allgemein*-Register, dort muss im Bereich *Empfangen* ein Wert stehen, der größer als Null ist und langsam weiter steigt. Ist dies nicht der Fall schaut man im Register *Netzwerkunterstützung* nach ob eine IP-Adresse ordnungsgemäß zugewiesen wurde. Eine von unseren DHCP-Servern zugewiesene IP-Adresse hat den Aufbau 141.78.x.y, wobei x und y verschiedene Werte annehmen können. Hat man eine andere Adresse, so sind die Einstellungen des Internetprotokolls (TCP/IP) in den Eigenschaften der jeweiligen Netzwerkkarte zu kontrollieren. Wie man die Eigenschaften der jeweiligen Netzwerkkarte aufruft, hat der interessierte Anwender bereits gesehen. In dem Fenster wählt man Bereich *Diese Verbindung verwendet folgende Elemente* das Element *Internetprotokoll (TCP/IP)* und klickt auf *Eigenschaften*.



Im Register *Allgemein* muss bei den beiden Auswahlmöglichkeiten die des automatischen Bezugs von Adressen gewählt werden. Dadurch ist sichergestellt, dass die IP-Adressen aus dem Bereich der KU kommen.

„Aber bei mir muss ein fester Wert stehen, damit ich zu Hause ...“; das kann schon sein, dass bei der Nutzung an anderen Orten feste Adressen eingetragen werden müssen. Will man den Zugang ins Internet vom Campus der KU nutzen, ist wie oben vorzugehen. Die vorhandenen Werte schreibt man sich am besten auf oder speichert sie als Dokument auf dem eigenen Notebook, dann hat man sie immer zur Hand.


Wir haben nun die ersten Voraussetzungen getroffen, um auf den WWW-Server der KU zugreifen zu können. Nun kann man wie in den Installationsanleitungen unter http://www.ku-eichstaett.de/Rechenzentrum/aktuelles/HF_sections/content/ZZhpAv0VjzmoDZ oder <http://www1.ku-eichstaett.de/urz/install/funklan.pdf> beschrieben den Cisco-VPN-Client herunterladen und installieren. Dies ist möglich, weil man ohne VPN-Client einen unverschlüsselten Zugang ausschließlich zum WWW-Server der KU hat¹.

Nachdem der VPN-Client installiert wurde und das Notebook neu gestartet wurde, ist man nun grundsätzlich für den Zugang ins Internet bereit. Das heißt nun, sich nach dem Neustart des Rechners zu überzeugen, dass eine ordnungsgemäße Netzverbindung existiert (wurde oben beschrieben), und den VPN-Client zu starten und sich mit Kennung und Passwort anzumelden.

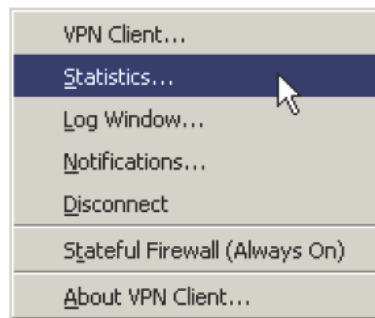
3. Fehlermeldungen vom VPN-Client

Ein Fehler besteht darin, dass die Client-Software beim Punkt *Securing communications channel* stehen bleibt und nicht mehr weiterarbeitet. Das ist in nahezu allen Fällen auf eine installierte und laufende Firewall-Software oder Internet-Security-Software zurückzuführen. Der Cisco-VPN-Client hat intern eine eigene rudimentäre Firewall-Komponente von ZoneLabs. Und da sich die Softwarehersteller nicht in die Karten schauen lassen, ist die reibungslose Zusammenarbeit zwischen VPN-Software und Firewall nicht garantiert. Am einfachsten läuft die Zusammenarbeit mit der Firewall von ZoneLabs (ZoneAlarm). Wenn obiges Problem auftritt, dann muss man vor dem Start des VPN-Client ZoneAlarm deaktivieren und nachdem Aufbau der Verbindung über den VPN-Client wieder aktivieren. Bei anderen Produkten (Norton, Symantec, McAfee usw.) kann es unter Umständen nicht ausreichen, die Software zu deaktivieren, d. h. man muss dann hier diese Software deinstallieren. Ich weiss, dass dies eine unbefriedigende Situation ist, aber zur Zeit gibt es keine bessere Lösung.

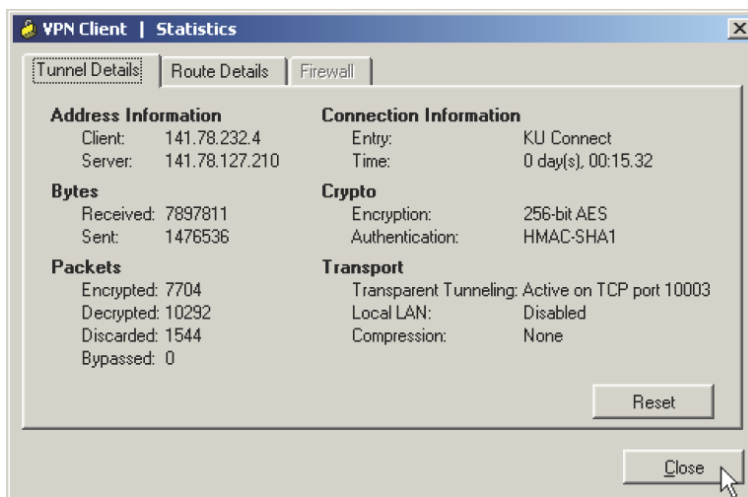
4. Verbindung über VPN aufgebaut, aber kein Internetzugang

Nachdem obige Klippen umschiff sind, kann es noch einen Zustand beim VPN-Client geben, bei dem zwar eine Verbindung zum VPN-Server aufgebaut wurde, aber man nicht in das Internet kommt. Das kann bedeuten, dass die Verbindung ins Internet gestört oder unterbrochen ist, das merkt der Anwender aber sehr schnell, denn auch die 'Mit-Surfer' werden über Zugangsprobleme klagen. In diesem Fall hilft nur warten. Ich meine aber den Fall, dass keine Daten über den VPN-Client empfangen werden. Man stellt das über einen Klick mit der linken Maustaste auf das verschlossene gelbe Schloss  im Systray der Taskleiste fest, indem man daraufhin den Punkt Statistics auswählt:

1. Benutzer eines Macintosh-Notebooks von Apple mögen sich an die am Ende des Artikels genannten zuständigen Personen wenden, damit auf deren Notebooks der VPN-Client installiert wird



Im danach auftauchenden Fenster müssen im Bereich Bytes in den Teilen Received und Sent jeweils Zahlen größer als 1000 stehen, deren Werte sich auch erhöhen. Steht bei Sent 0, dann ist o. g. Problem aufgetreten. Hier hilft meist ein Disconnect und Beenden des VPN-Client, ein paar Minuten warten und ein Neustart des VPN-Client.



Bytes
Received: 7897811
Sent: 1476536

Ich konnte feststellen, dass obiges Phänomen auch auftritt, wenn man sein Notebook nicht herunterfährt sondern nur in den Standby-Modus bringt. Dann 'vergisst' der Rechner nach einiger Zeit, dass er Netzwerkkarten hat. In so einem Fall hilft nur noch Rechner aus- und wieder einschalten.

5. Regelmäßige Verbindungsabbrüche

Ein großes Problem zeigt sich allerdings bei Funknetzkarten des Typs Intel (Pro) Wireless MiniPCI 2100 3B oder 2200BG (zum Teil auch bei Nachfolgemodellen). Das Problem äußert sich darin, dass die Netzwerkverbindung – und damit auch der VPN-Client – regelmäßig (nach 2 bis 15 Minuten) abbricht. Nach langer Suche konnten wir obige Karten als die 'Schuldigen' identifizieren. Schaut man sich die Netzverbindung genauer an, dann beginnt die Netzwerkkarte mit der maximalen Übertragungsgeschwindigkeit, diese vermindert sich dann bis auf 0 Mbit/s und dann bricht die Funknetz-Verbindung ab und es erfolgt eine Neuverbindung, allerdings ist die VPN-Verbindung auch weg.

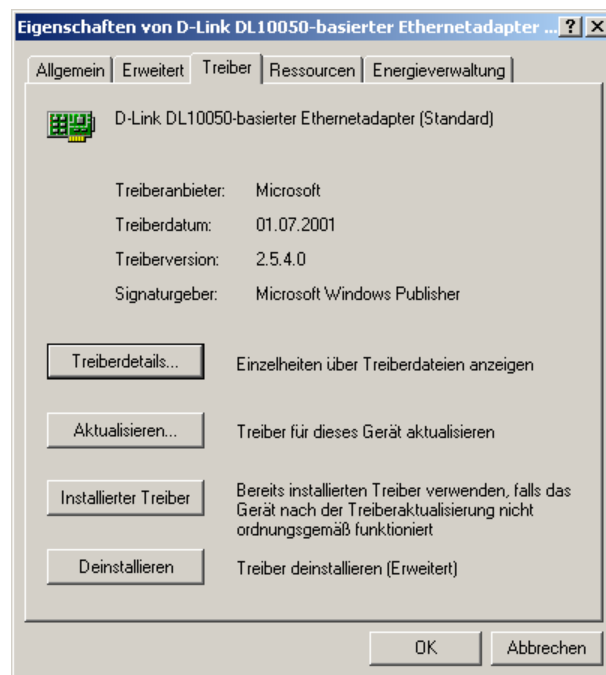
Da jedes Notebook auf unterschiedliche Weise installiert und konfiguriert ist, kann es sein, dass Geräte mit obigen Funknetzkarten einwandfrei funktionieren, während andere nicht laufen. Folgende Lösungsmöglichkeiten bieten sich an:

- ▷ Herunterladen und Installieren der neuesten Treiber von Intel über <http://support.intel.com/support/wireless/wlan/sb/CS-010623.htm>

- ▷ Suchen von weiteren Lösungsmöglichkeiten über eine Suche z. B. Google: Intel 2100 Verbindungsabbrüche oder Intel 2100 connection drops oder Intel 2200 Verbindungsabbrüche oder Intel 2200 connection drops.

Bei allen oben genannten Hinweisen ist peinlichst genau darauf zu achten, dass man sich an alle Angaben hält, vor allem bei der Installation von Treibern.

„*Neue Treiber, ich habe mir das Notebook doch erst vorige Woche gekauft?*“; selbst neu gekaufte Rechner werden selten mit den neuesten Treibern installiert. Welche Treiberversion installiert ist, kann man wieder über die Eigenschaftsseite der Netzwerkkarte erkennen, hier muss man aber auf die Schaltfläche *Konfigurieren* klicken und danach das Register *Treiber* auswählen, es erscheint dann z. B. folgendes Fenster:



Bei den oben angeführten Funknetz Karten von Intel gibt es Treiber von Mitte 2006; diese sollten auch installiert werden.

„*Aber bei mir zu Hause habe ich keine Probleme mit WLAN!*“; wie ich bereits weiter oben erwähnte, tauchen diese Probleme nicht mit jedem Notebook und nicht in jeder Konfiguration auf, so dass eine solche Aussage genauso hilfreich ist wie zu Hause finde ich immer einen Parkplatz, hier aber nicht. Ich selbst habe vier verschiedene Funknetzadapter getestet, nur einer funktionierte überhaupt nicht, aber das lag am Adapter. Die anderen drei (zwei PCMCIA-Karten von Proxim und 3Com und ein USB-Stick von AVM) funktionieren einwandfrei und stundenlang.

Wichtig ist vor allem, dass spezielle Features von manchen Karten, wie etwa ein Zweifach- oder Vierfach-Modus (also 44 Mbit/s oder 108 Mbit/s oder mehr) sofort abgeschaltet werden, denn hier handelt es sich um proprietäre Einstellungen, die nur mit Geräten und Access Points der gleichen Firma arbeiten.

6. Allgemeines

Dem Benutzer wird oftmals in der Werbung weisgemacht, ein FunkLAN wäre die einfachste Sache der Welt und es gäbe nirgendwo Probleme. Das stimmt beinahe, wenn man ein gänzlich ungeschütztes Funknetz betreibt und die sog. SSID auch noch verbreitet, dann kann aber jeder das Netz nutzen.

An der KU haben wir uns daher entschlossen, über eine VPN-Verbindung das Problem des Abhörens zu umgehen und eine anonyme Nutzung des Netzes ausgeschlossen.

„Das ist mir alles zu kompliziert, warum installieren mir die vom URZ das Ganze nicht?“, neue und veränderte Notebooks und Rechner erscheinen beinahe im Wochenrhythmus. Sich in diese neuen Geräte einzeln einzuarbeiten ist eine Sisyphus-Arbeit, denn jeder Rechner hat veränderte Einstellungen durch die werksseitige Erstinstallation und durch Nach-Installation von Software durch den Benutzer und benutzereigene Einstellungen. Deshalb ist es unmöglich allgemeingültige Hinweise zu geben, die eine ordnungsgemäße Funktion garantieren. Und aus diesem Grunde werden wir auch nie für die Anwender System-Software installieren, denn wenn Einstellungen verändert worden sind und/oder das System insgesamt einen ‘Knacks’ bekommt wären wir die Schuldigen, die alles wieder herstellen müssten – und selbst große Systemhäuser weigern sich solche Garantien zu geben für nicht von ihnen installierte Rechner.

„Ja aber bei Firma ... geht das auch, dass die die Software installieren“, das ist richtig für den Fall, dass man sich ganz und gar dem Willen der Firma unterwirft und das heißt, man hat auf seinem Rechner keine Administrator-Rechte mehr, kann keine Software installieren, zum Teil noch nicht einmal einen USB-Stick zum Speichern von Daten anschließen usw. usf.

Ich weiß, meine vorigen Ausführungen erwecken nicht gerade Freudensprünge, aber mit etwas Neugier, gutem Willen und unserer Hilfe (Unterstützung) wird es in vielen Fällen gelingen, ein privates Notebook an das Netz der KU anzuschließen und sei es nur über ein Kabel – das hat bisher noch immer funktioniert.

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Peter Kahoun	EI: eO-107	-1296	<code>peter.kahoun</code>
Alexander Kaltenbacher	IN: HB-203	-1885	<code>alexander.kaltenbacher</code>
Tomasz Partyka	EI: eO-107	-1668	<code>tomasz.partyka</code>

LABS-CHAOS

REALE BEDROHUNG



Cartoon: Dirk Meissner

Sicherer SSL-Zugang zum elektronischen Postfach

B. Brandel

Seit Ende 2004 bietet das Universitätsrechenzentrum seinen Nutzern einen mit SSL verschlüsselten Zugriff auf ihre elektronischen Postfächer an. Die Zugriffsstatistik des dafür notwendigen IMAP-Servers zeigt jedoch, dass dieser abhörsichere Zugang viel zu wenig bekannt ist und statt dessen viele Nutzer Kennung und Passwort im Klartext zum Mailserver übertragen. Besonders riskant ist dies, wenn der Zugriff aus dem unsicheren Internet erfolgt, wo Dritte durchaus diese Daten abgreifen können. Diesen Missstand abzuschaffen ist Ziel dieses Artikels.

Motivation

Über die (Un-)Sicherheit elektronischer Post wurde schon in vielen *INKUERZE*-Ausgaben berichtet. Wer wirklich vertrauliche Daten versenden will, sollte sie digital verschlüsseln und signieren.

Dies ist aber nur ein Aspekt der E-Mail-Sicherheit. Mindestens genauso wichtig ist es, seinen Mail-Client nach der Installation (siehe [1]) sicher zu konfigurieren, damit beim elektronischen Briefgeschäft keine Klartext-Passwörter übers Netz gehen. Denn Ihr E-Mail-Passwort ist gleichzeitig Ihr zentrales Zugangspasswort zum internen Novell-Netz der KU und somit ein sehr kostbares Gut.

Serverseitige Einstellungen beim Posteingang (IMAP-Server)

Seit dem 17. Januar 2005 werden die Posteingangsfächer und E-Mail-Ablagen unserer E-Mail-Service-Kunden ausschließlich auf dem Server `imap.ku-eichstaett.de` verwaltet. Damit der Datenzugriff sicher ist, kann dieser Server den ganzen Datenverkehr zum Mail-Client mittels SSL bzw. TLS verschlüsseln, falls der Client diese Methode ebenfalls unterstützt. TLS ist eine Weiterentwicklung von SSL mit marginalen Unterschieden (siehe [2]).

Da der verschlüsselte Datenkanal bereits beim Verbindungsaufbau hergestellt wird, erfolgt die komplette Authentisierung ebenfalls über diese verschlüsselte Leitung, so dass etwaige Abhörversuche von Daten und Passwörtern chancenlos sind. Außerdem können Sie mit Hilfe des SSL-Zertifikats, das Ihnen der Server beim Verbindungsaufbau zeigt, feststellen, ob am anderen Ende der Leitung wirklich der IMAP-Server der KU ist.

Zum Glück beherrschen heutzutage alle wichtigen Mail-Clients SSL. Serverseitig ist SSL aber noch nicht so verbreitet. Deshalb haben die Software-Hersteller in ihren Client-Produkten (Mozilla Thunderbird, Pegasus Mail, Outlook etc.) SSL meist nicht voreingestellt. Ein solcher Mail-Client versucht daher, eine unverschlüsselte Verbindung zum IMAP-Server aufzubauen, die dieser ebenfalls akzeptiert, mit der Konsequenz, dass sowohl die Authentisierung per Kennung und Passwort als auch die Datenübertragung im Klartext erfolgen, obwohl beide Seiten es besser könnten.

Man mag einwenden, dass die unverschlüsselte Übertragung Ihrer E-Mails „auf den letzten Versandmetern“ eine lässliche Sünde ist, da die Briefe vom Absender bis zu Ihrem IMAP-Postfach sowieso unverschlüsselt übertragen werden und Sie sensitive Mails sowieso immer verschlüsseln und signieren.

Die Klartextübertragung Ihres Intranet-Passworts jedoch sollte Sie ernsthaft beunruhigen – der Gedanke, dass Dritte nicht nur Vollzugriff auf Ihre Mailbox haben, sondern auch noch mit Ihrem Passwort auf Ihre Intranet-Daten zugreifen können, ist mehr als bedenklich. Daher raten wir Ihnen dringend, am Mail-Client grundsätzlich die SSL-Verschlüsselung für den IMAP-Posteingang zu aktivieren. Wie das geht, wird ab dem übernächsten Abschnitt für die wichtigsten Mail-Clients beschrieben. Zuvor möchte ich jedoch noch die Konfiguration unseres Postausgangsservers darstellen.

Serverseitige Einstellungen beim Postausgang (SMTP-Server)

Für den SMTP-Postausgangsserver `smtp.ku-eichstaett.de` gelten andere Regeln als für den Posteingang. Unser SMTP-Server unterstützt momentan weder SSL-Verschlüsselung noch Authentisierung. Er entscheidet stattdessen ausschließlich anhand der IP-Adresse, ob er von Ihrem Client Ausgangspost annimmt oder nicht. Zum Mail-Versand an externe Empfänger muss nämlich Ihr PC eine IP-Adresse aus dem KU-Netz besitzen (141.78.*.*) – ansonsten lehnt der Server den Versand ab. Außerhalb des KU-Netzes müssen Sie deshalb den VPN-Client verwenden, der Ihnen eine IP-Adresse der KU verschafft und Sie so als versendeberechtigt legitimiert. Details dazu finden Sie in der letzten Ausgabe 1/2006 der *INKUERZE*.

Man kann mit diesen Servereinstellungen durchaus leben. Denn erstens muss man beim Postversand keine Passwörter preisgeben und zweitens wird beim Weiterversand der Mails vom Server in die weite Welt sowieso kein verschlüsselter Datenkanal verwendet. Daher sind SMTP-Server,

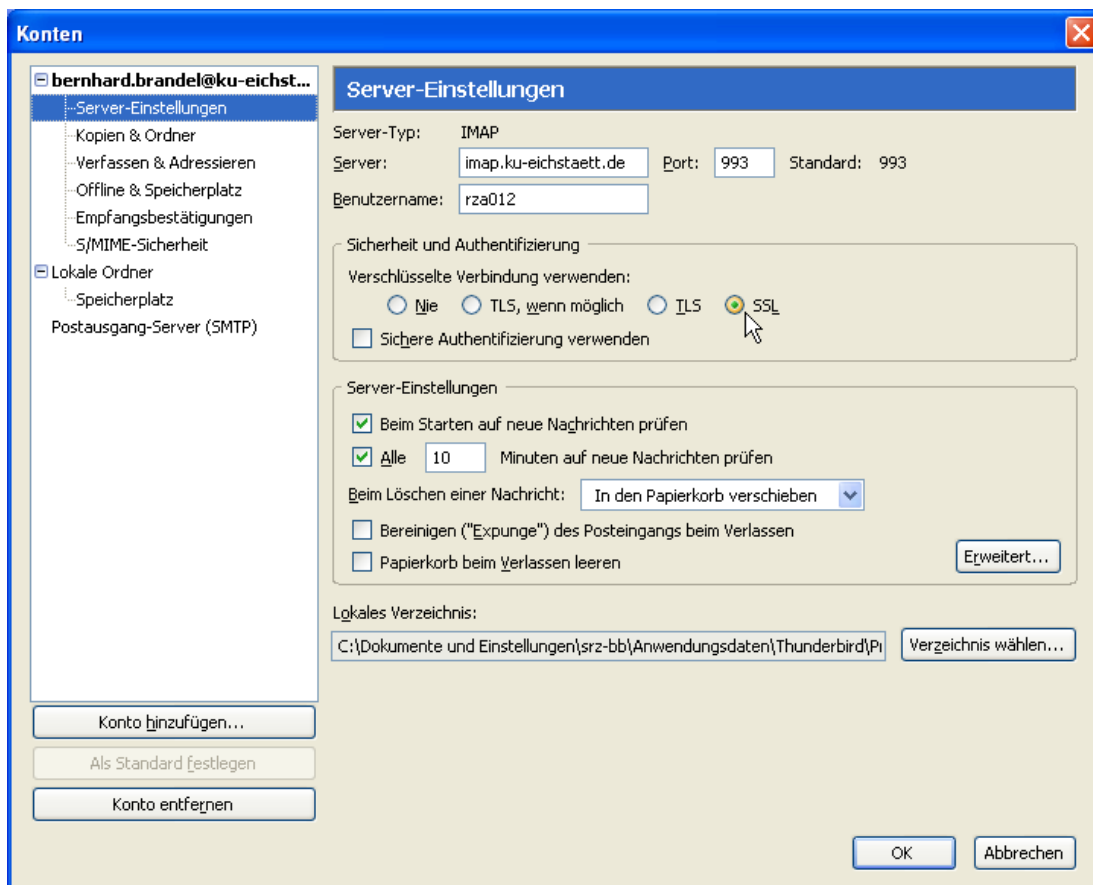
die SSL bzw. TLS unterstützen, noch nicht sehr verbreitet. Es gibt sie gelegentlich, aber noch nicht bei uns.

Deshalb empfiehlt momentan das URZ folgende Einstellungen für alle Mail-Clients am Postausgang:

- ▷ Deaktivieren Sie jegliche Authentisierung.
- ▷ Wählen Sie als Verschlüsselungsmethode „TLS, falls möglich“ oder deaktivieren Sie TLS vorerst ganz.

Einstellungen bei Mozilla Thunderbird

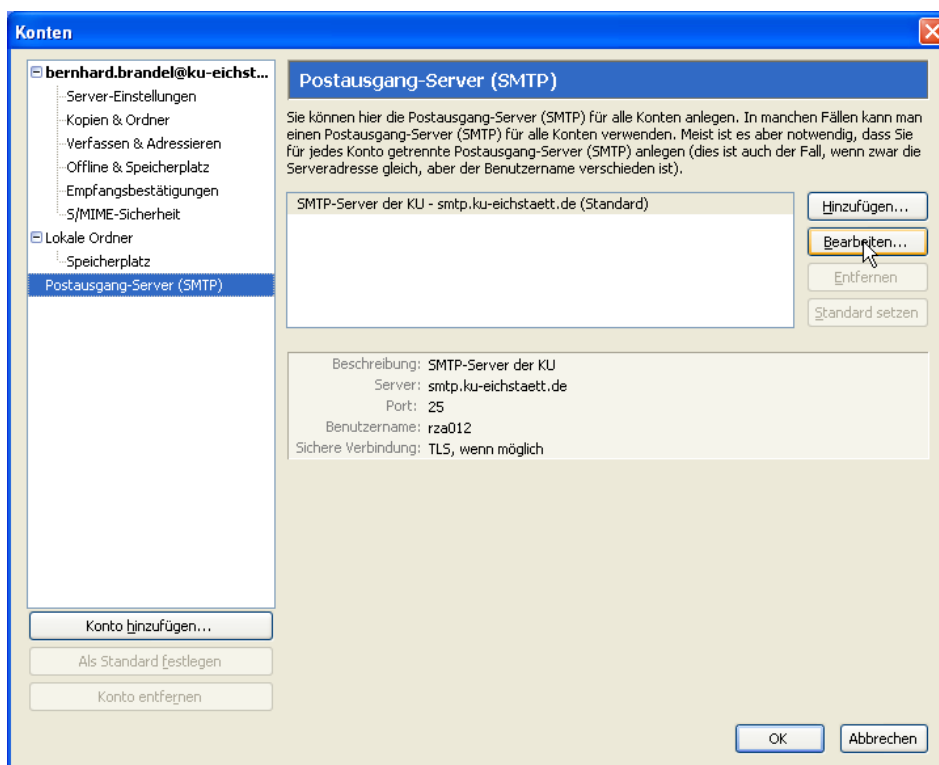
Zuerst konfigurieren wir den Posteingang. Dazu öffnen Sie über *Extras* → *Konten ...* das Kontenmenü von Mozilla Thunderbird. Wählen Sie dann in Ihrem KU-Postfach den Eintrag *Server-Einstellungen* aus. Aktivieren Sie nun unter *Sicherheit und Authentifizierung* die Option SSL, während Sie die Option *Sichere Authentifizierung verwenden* bitte ausschalten.



Diese Deaktivierung bedeutet lediglich, dass Ihr Client sich nicht als Rechner beim Server per SSL authentisiert, denn dazu müsste jeder Client ein eigenes SSL-Zertifikat haben, das dem Server bekannt sein muss. Da Sie sich sowieso bereits beim Server per Kennung/Passwort ausweisen, benötigen wir diese aufwändige Zusatz-Authentisierung nicht.

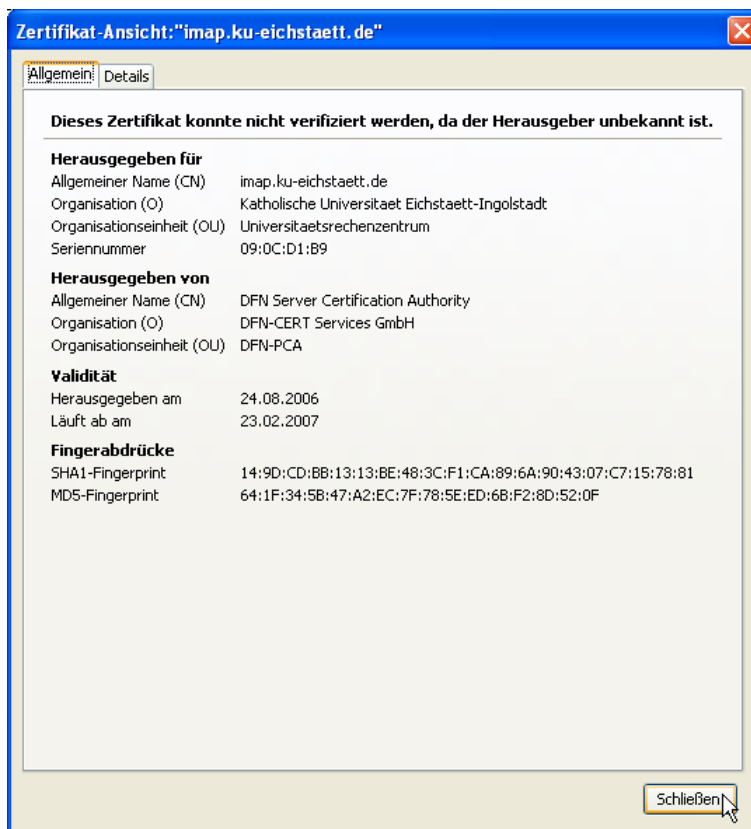
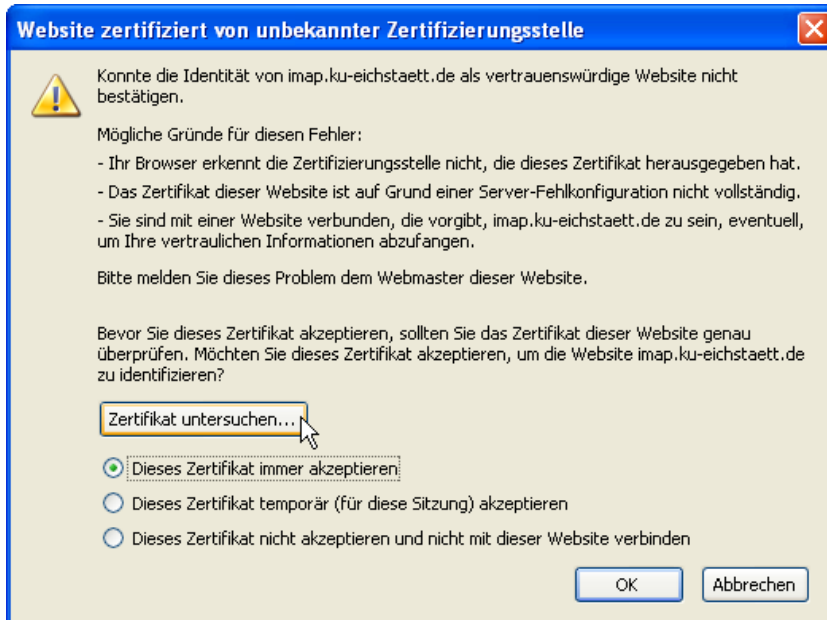
Um den Postausgangsserver zu konfigurieren, wählen Sie nun links den Eintrag *Postausgang-Server (SMTP)* aus und klicken auf *Bearbeiten...* ...:

Im nächsten Fenster deaktivieren Sie bitte die Option *Benutzername und Passwort verwenden*. Zum Schluss aktivieren Sie bitte *TLS, wenn möglich* und schließen mit *OK* alle Konfigurationsfenster.



Beim nächsten Start von „Mozilla Thunderbird“ erscheint das Fenster „Website zertifiziert von unbekannter Zertifizierungsstelle“. Prüfen Sie das Zertifikat, indem Sie auf *Zertifikat untersuchen* ... klicken. Im übernächsten Bild sind die Finger-

abdrücke des aktuellen bis 23.02.2007 gültigen Zertifikats abgebildet. Wenn die Fingerabdrücke des Ihnen präsentierten Zertifikats mit den hier abgedruckten übereinstimmen,



kehren Sie bitte durch Klick auf *Schließen* zum vorigen Fenster zurück. Nun können Sie die Option *Dieses Zertifikat immer akzeptieren* getrost aktivieren und mit *OK* den Vorgang abschließen und sich wie gewohnt Ihrer Mailbox widmen.

Zugang über den Webmailer

Bei der Nutzung des Webmailers Squirrel Mail, den Sie über <https://imap.ku-eichstaett.de/> erreichen, brauchen Sie nichts an Ihren Konfigu-

rationseinstellungen zu ändern. Der Webmailer-Zugang ist von Hause aus SSL-verschlüsselt. Kennung und Passwort werden im verschlüsselten SSL-Tunnel übertragen, Ihre Zugriffe auf Mailbox und Postausgang ebenfalls. Dies können Sie optisch im Browserfenster an den beiden Schlössern im URL und am unteren Fensterrand erkennen, die beide bereits im leeren Loginfenster, also schon vor der Authentisierung, zugesperrt sind:



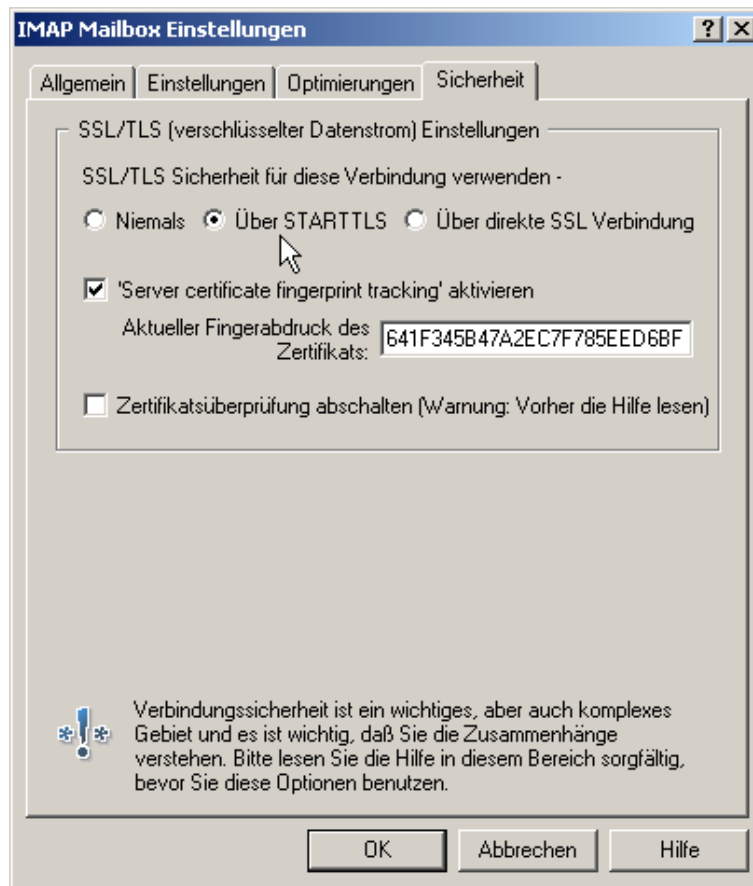
Damit ist der Webmailer ideal als Mailzugang für unterwegs, vorausgesetzt, dass der Rechner, auf

Einstellungen bei Pegasus Mail

Im Mail-Client Pegasus Mail öffnen Sie bitte über *Extras* → *IMAP Profile ...* die Profilverwaltung und klicken dann auf *Bearbeiten*. Ak-

dem Sie den Webmailer aufrufen, keinen Keylogger installiert hat, der Ihr Passwort mitschreibt.

tivieren Sie dann im nachfolgenden Fenster folgende beiden Einstellungen: *Über STARTTLS* und *'Server certificate fingerprint tracking'* aktivieren.



Diese Optionen bedeuten folgendes:

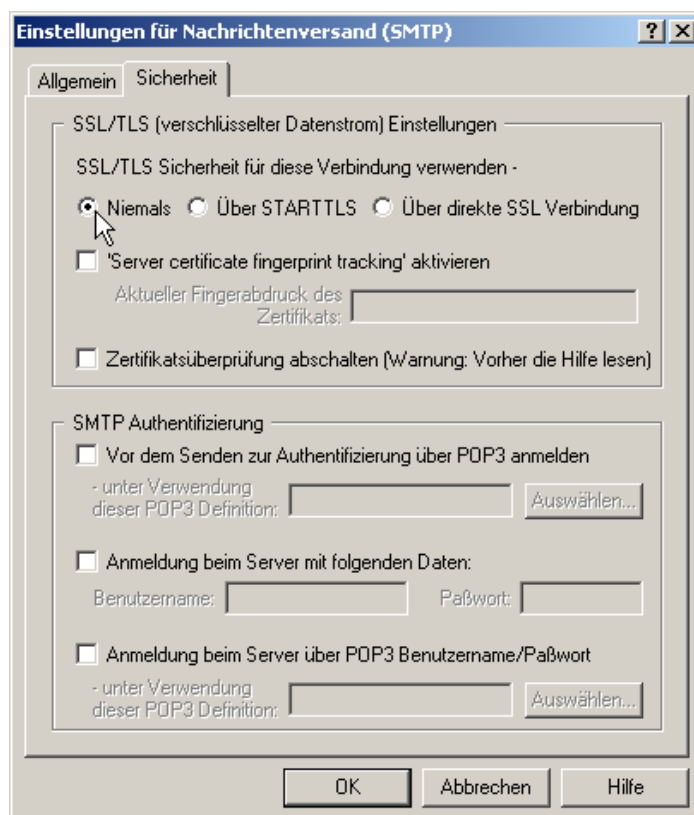
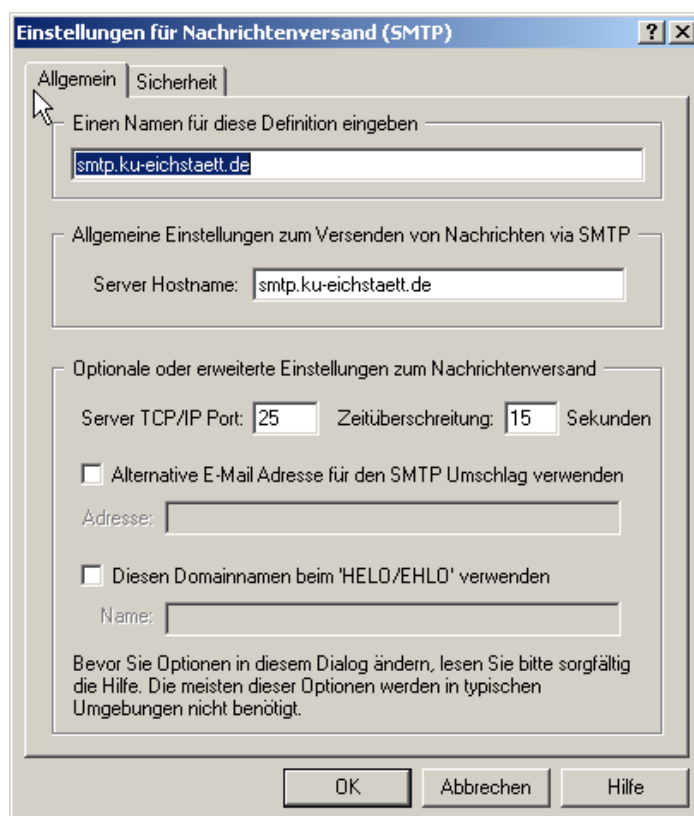
Bei der SSL-Nutzung wird die Verbindung entweder von Anfang an durch einen SSL-Tunnel geleitet oder es wird direkt nach dem Aufbau der Verbindung (also vor der Authentisierung!) per STARTTLS auf SSL gewechselt. Prinzipiell sind beide Methoden gleich sicher. Bei Pegasus Mail empfehlen wir den Weg über STARTTLS. Mit der zweiten Option wird bei jedem Sitzungsaufbau das Serverzertifikat und damit dessen Identität überprüft. Sie brauchen dazu den MD5-Fingerabdruck des Servers bei Erstbenutzung nicht einzugeben, er wird von Pegasus Mail ohne Nachfrage, ob Sie das Zertifikat für echt halten, automatisch für die zukünftigen Logins mit eingetragen. Prüfen Sie daher unbedingt beim nächsten Start von Pegasus Mail,

ob der eingetragene MD5-Fingerabdruck auch korrekt ist, aktuell (gültig bis 23.2.2007) muss er 641F345B47A2EC7F785EED6BF lauten.

Abschließend beenden Sie bitte mit *OK* und *Fertig* die IMAP-Konfiguration.

Zum Schluss müssen Sie noch Ihre SMTP-Einstellungen ändern: Öffnen Sie bitte *Extras* → *Interneteneinstellungen ...* und klicken Sie im folgenden Fenster im Reiter *Senden (SMTP)* auf *Bearbeiten ...*:

Im nächsten Fenster muss beim Reiter *Allgemein* der Server-Hostname `smtp.ku-eichstaett.de` eingetragen sein. Im Reiter *Sicherheit* stellen Sie bitte SSL/TLS auf *Niemals* und deaktivieren alle weiteren Optionen:



Abschließend beenden Sie mit zweifachem OK die SMTP-Konfiguration von Pegasus Mail.

Einstellungen bei Microsoft Outlook

Die Mail-Clients Microsoft Outlook und Outlook Express gehören nicht zu den vom URZ unterstützten Produkten, weil diese regelmäßig mit Sicherheitslücken aufwarten. Wenn Sie partout diese Programme verwenden möchten, können Sie dort analoge Einstellungen vornehmen. Tipps hierzu finden Sie im WWW z. B. unter [3], die Sie dann auf unsere Serverumgebung übertragen müssen.

Zukünftige Planungen

Um Sicherheit und Komfort für Ihren elektronischen Briefverkehr weiter zu erhöhen, gibt es momentan folgende Planungen im URZ:

- ▷ Um unverschlüsselte Passwort-Authentisierungen am IMAP-Server zu verhindern, möchten wir mittelfristig den unverschlüsselten Zugang auf Port 443 deaktivieren und nur noch Verbindungen per SSL/STARTTLS zuzulassen, da praktisch alle E-Mail-Clients SSL/TLS unterstützen.
- ▷ Außerdem planen wir mittelfristig auch eine LDAP-Authentisierung am Postausgangsserver, in Kombination mit einer TLS-Verschlüsselung der Verbindung. Nach kurzer Übergangszeit möchten wir danach den SMTP-Zugriff ohne TLS verbieten. Über diese Änderungen werden wir Sie aber rechtzeitig informieren.
- ▷ Das SSL-Zertifikat unseres IMAP-Servers läuft am 23.02.2007 ab. Wir werden uns rechtzeitig um eine neue Zertifizierung kümmern.

Literatur:

- [1] <http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/install.de>
- [2] http://de.wikipedia.org/wiki/Secure_Sockets_Layer
- [3] http://www.rz.uni-hohenheim.de/kommunikation/app/mail/outlook/outlook_imap.html

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Bernhard Brandel	IN: HB-204	-1888	bernhard.brandel
Tomasz Partyka	EI: eO-107	-1668	tomasz.partyka

Der Umgang mit Malware in der Praxis

B. Brandel

Beim Umgang mit Viren und anderer Malware werden aus Unkenntnis über die genauen Sachverhalte immer wieder verhängnisvolle Fehler gemacht. Dieser Artikel will Sie darüber aufklären und Ihnen helfen, sich in Zukunft besser zu wappnen und im Schadensfall richtig zu verhalten. Für die praktische Anwendung sind zahlreiche Links zu Hintergrundinformationen und Software-Bezugsquellen beigefügt.

Motivation

Mit dem Thema „Malware-Schutz“ wird man als Computer-Nutzer so oft konfrontiert, dass die Versuchung groß ist, das Thema nicht mehr ernst zu nehmen. Vielleicht gerade deshalb schätzt man die wirkliche Situation falsch ein und denkt, sowieso alles im Griff zu haben mit der Gefahr, im Ernstfall das Falsche zu tun.

Im Folgenden möchte ich Sie auf die wichtigsten Irrtümer hinweisen und Ihnen zeigen, wie Sie hartnäckige Malware loswerden können.

Was ist Malware?

Laut Wikipedia ist Malware [1] ein Kofferwort, gebildet aus den beiden englischen Begriffen „malicious“ (boshaft) und „Software“. Als Malware bezeichnet man Computerprogramme, welche – vor dem Benutzer verborgen – unerwünschte (schädliche) Funktionen ausführen.

Mögliche Schadfunktionen sind zum Beispiel Dateimanipulationen oder -löschungen, aber auch die technische Kompromittierung der Sicherheitssoftware (wie z. B. Firewalls und Antivirenprogramme) eines Computers. Es ist bei Malware auch nicht unüblich, dass eine ordnungsgemäße Deinstallation mit den generell gebräuchlichen Mitteln fehlschlägt, so dass zumindest Software-Fragmente im System verbleiben. Diese können möglicherweise auch nach der Deinstallation weiterhin Schaden anrichten.

Die wichtigsten Malware-Typen sind: Computerviren, Computerwürmer, Trojanische Pferde, Spyware (Software zum Ausspionieren Ihres Rechners) und Backdoors (Hintertüren zum späteren Eindringen).

Dialer werden nicht immer als Malware angesehen. Statt die Opfer vor den Tätern zu schützen, spricht man in diesem Zusammenhang gerne euphemistisch von „Einwahlprogrammen auf Mehrwertrufnummern“. Ebenso strittig ist, ob Adware (Software mit lästigen Werbeeinblendungen) [2] automatisch als Spyware und damit auch als Malware gilt.

Wie man sieht, umfasst Malware weit mehr als Computerviren. Ob Software Malware ist oder nicht, wird leider sehr subjektiv gesehen: Insbesondere bei Dialern und Adware ist man sich uneins, ob sie Malware sind oder nicht. Wie schützen Sie sich aber gegen Schädlinge, die Ihre Schutzsoftware vielleicht gar nicht als schädlich ansieht? Eines ist klar: Die nicht ausrottbare Überzeugung, dass man nach einem Malwarebefall schnell mal eben eine Antivirus-Software auf den infizierten Rechner installiert, die dann alles Böse auf dem Computer als böse klassifiziert und danach restlos entfernt, ist somit mehrfach falsch.

In den folgenden Abschnitten wird dargestellt, welche präventiven Maßnahmen Sie treffen können, wie ein sinnvoller Grundschutz gegen Malware aussieht und was Sie im Verdachts- und Schadensfall tun können. Bitte beachten Sie die zahlreichen Links auf weiterführende Seiten im WWW, die Sie bequem per Mausklick in der Online-Ausgabe des Artikels erreichen können.

Präventive Maßnahmen

Der beste Schutz vor Malware-Schäden ist eine durchdachte Prävention:

1. Prävention heißt zuallererst: regelmäßige Datensicherungen

Auch der vorsichtigste PC-Anwender kann sich Malware einfangen, die im schlimmsten Fall all seine Daten zerstört oder eine Neuinstallation erfordert. Sichern Sie daher regelmäßig Ihre Daten – dann ist der GAU kein GAU mehr!

2. Vorsicht beim Öffnen von E-Mail-Attachments und beim Ausführen von Dateien

Vorsicht allein schützt zwar nicht gegen alle Schädlinge. Würmer wie Blaster und Sasser (siehe *INKUERZE* 2/2003 [3] und 1/2004 [4]) konnten sich ohne aktives Zutun des Nutzers über Windows-Sicherheitslücken automatisch übers Netz auf ungepatchte Windows-PCs weiterverbreiten. Ohne gesunde Vorsicht sind aber alle Sicherheitsmaßnahmen umsonst!

3. Entscheiden Sie sich für eine geeignete Antivirus-Software und wägen Sie dabei alle Vor- und Nachteile gründlich ab!

Denn nicht jede Antivirus-Software (AV-Software) ist gleich gut. Dies gilt für die Handhabung, den Ressourcen-Verbrauch, die Viren-Erkennungsrate, die Spyware-Erkennung, die Qualität des Supports im Verdachtsfall, die Flexibilität beim Update und auch für den Preis der Produkte. Hierzu ein paar Erfahrungen, die ich gemacht habe:

Einzelne Dateien lassen sich mit Sophos AV nur sehr umständlich auf Viren prüfen, indem man den OnAccess-Scanner speziell mit dieser einzelnen Datei konfiguriert. Bei Kaspersky AV dagegen können verdächtige Dateien bequem per Rechtsklick auf Viren untersucht werden. Sie können verdächtige Dateien zur Analyse an Ihren AV-Hersteller senden. Bei Sophos AV geschieht das per Hand als Mail-Anhang an den Sophos Support. Nun blockiert aber das

Mailgateway der KU sinnvollerweise den Versand ausführbarer Dateien mit der Meldung „Banned Part“, so dass Sie den Dateianhang erst noch umbenennen und erneut versenden müssen.

Kaspersky AV löst auch diese Situationen intelligenter: Trauen Sie einer Datei nicht, wählen Sie im Menü den Punkt „Datei zur Analyse einschicken“. Davor wird sie offenbar verschlüsselt, so dass sie als Mail-Anhang problemlos übers Mailgateway versandt werden kann.

Bei Kaspersky dauert eine technisch fundierte Antwort nach meiner persönlichen Erfahrung i.d.R. wenige Stunden, von Sophos erhielt ich trotz Nachhakens erst nach mehreren Tagen lediglich eine oberflächliche Antwort.

Im Gegensatz zu Kaspersky AV und fast allen anderen Antiviren-Programmen sind auf Ihrem Notebook bei Sophos AV automatische Updates nicht einmal mit VPN-Client reibungslos möglich, da dieser erst nach dem Update-Prozess startet, welcher dadurch erst einmal fehlschlägt.

Das einzige Argument für die Verwendung von Sophos AV am heimischen PC ist m.E. der Preis: Sophos AV ist für Universitätsangehörige umsonst, Kaspersky kostet pro Jahr ca. 15 Euro.

4. Halten Sie Ihr Wissen immer auf dem neuesten Stand!

Lesen Sie Fachzeitschriften wie c't [5], CHIP [6] und Hakin9 [7].

Besuchen Sie die Security-Kurse des URZ, in denen wir Ihnen auch am eigenen Notebook praktisch zeigen, wie Sie selbiges gegen die Gefahren des Intra- und Internet absichern können. Einen Teil der dort besprochenen Kurs-Themen finden Sie auf unserem Ingolstädter Novellserver unter `I:\kurse\Internet-Security\pc-sicherheit.pdf`.

Grundschutz Ihres Systems

1. Automatische Betriebssystem-Updates (Windows [4], Linux) sind absolute Pflicht.

Würmer nutzen meist als automatisierte Hacker-Angriffe die Sicherheitslücken in Betriebssystem- oder Anwendungs-Software aus. Aber vom „Proof of Concept“ über das manuelle Ausnutzen der Schwachstelle bis zur Serienreife (automatisierte Verbreitung über das Internet als Wurm mit wirkungsvoller Schadensfunktion) ist der Weg auch für Malware-Autoren lang und steinig. Betriebssystem-Patches existieren daher meist schon mehrere Wochen vor dem Virus. Sie helfen gegen manche neuartige Malware, die die AV-Software durchlassen würde.

2. Nutzen Sie den Microsoft Baseline Security Analyzer (MBSA [8])

Damit sollten Sie ergänzend Ihr System auf weitere Windows- und Office-Sicherheitslücken überprüfen.

3. Automatische Viren-Updates sind ebenfalls Pflicht.

Dadurch wird die Zahl der unerkannten Viren stark reduziert, aber leider nicht auf Null. Denn Antivirus-Programme haben leider eine grundsätzliche Schwäche: Der Virus existiert immer vor dem Schutz. So werden nagelneue Viren von Ihrer AV-Software trotz verbesserter heuristischer Methoden oft nicht erkannt, da je nach Hersteller und Virus zwischen Auftauchen des Schädlings und seines Gegenmittels mehrere Tage liegen können. Da sich vor allem Würmer immer rasanter ausbreiten, schlüpfen diese immer häufiger durchs AV-Sicherheitsnetz, auch bei automatischer Aktualisierung des Virenwächters. In Kombination mit den oben beschriebenen automatischen Betriebssystem-Updates bietet die automatische Aktualisierung Ihrer AV-Software aber einen effektiven Schutz vor Viren.

4. Deaktivieren Sie die automatische Desinfektion Ihrer Mailboxen:

Viele Mail-Clients speichern aus Performanzgründen den gesamten Posteingang in einer

einzigsten Datei ab. Wenn nun eine einzige E-Mail im Posteingang Malware enthält, löscht u.U. die AV-Software Ihren gesamten Posteingang! (Beispiel: Mozilla Thunderbird [9]) Speichern Sie im Zweifelsfall statt dessen verdächtige Anhänge auf der Festplatte ab. Ihr Virenwächter schlägt dann ebenfalls rechtzeitig Alarm, löscht das abgespeicherte Attachment und Ihr Posteingang bleibt heil.

5. AV-Software kann, will und muss manchmal irren – oder ist Adware doch Malware?

Ob beispielsweise die Fernsteuerungs-Software oder der Dialer auf Ihrem PC ein (von Ihnen!) gewolltes „Feature“ oder ein Fluch (Malware) ist, ist Ansichtssache. Manche AV-Software ist in diesem Punkt sehr tolerant: Da Sie ja Ihr System selbst administrieren, will man Sie schließlich nicht bevormunden. Es wäre ja extrem unhöflich, Ihnen Ihre schöne Zusatz-Software wegzunehmen, oder? Außerdem haben Sie bei der Adware-Installation deren Lizenzbedingungen sicher akzeptiert, die im Kleingedruckten durchaus den Hinweis auf einen Keylogger, Dialer o.ä. enthielten. Darüber darf sich auch die AV-Software rechtlich nicht ohne weiteres hinwegsetzen. Bei AV-Herstellern wie Kaspersky müssen Sie daher aus rechtlichen Gründen den Schutz vor Adware & Co. selbst im Konfigurationsmenü aktivieren. Tun Sie das! Sophos erkennt momentan relativ wenig Spyware, da es sie als „possibly unwanted software“ einstuft. Angeblich soll es in der kommenden Version besser werden. Warten wir es ab . . .

Da Sie Ihrer AV-Software bezüglich Spyware-Erkennung nicht unbedingt trauen können, empfiehlt sich dringend ein ergänzender Schutz gegen Spyware, beispielsweise durch Spybot Search & Destroy [10], am besten mit residentem Wächter und automatischen Updates und regelmäßigen Systemchecks.

6. Eine Personal Firewall ist keine Wunderwaffe, sie ergänzt lediglich den Malware-schutz.

Die einzige Firewall, die Sie komplett vor Netzbedrohungen schützt, ist ein durchgetrenntes Netzkabel („Berliner Mauer“). Denn jede Personal Firewall lässt Verbindungen auf Port 80 (also ins WWW) zu. Wenn Sie sich also mit administrativen Rechten über den WWW-Browser Malware herunterladen und auf Ihrem Rechner installieren, kann dies die Firewall deshalb i.d.R. nicht verhindern. Sie meldet vielleicht später zusätzlichen Netzverkehr, der von der Schadsoftware aufgebaut wird, aber auch nur dann, wenn die Malware Ihre Firewall-einstellungen nicht schon längst funktionsunfähig gemacht hat.

Nur ein sorgfältiger Umgang mit dem Werkzeug sorgt auch für entsprechenden Schutz. Wer bedenkenlos alle Dialoge bestätigt, kann auch gleich ohne Firewallschutz surfen. Zusätzlicher Schutz durch Antivirus- und Antispyware-Produkte ist daher unabdingbar.

Brauchbare Personal Firewalls sind z. B. Sygate [11], Outpost Firewall [12] und Zone Alarm [13]. Beachten Sie unbedingt die genauen Lizenzbestimmungen, einige Personal Firewalls sind zwar für Privatanwender kostenlos, aber meist nicht für den Dienstgebrauch!

Was tun im Verdachtsfall?

1. Vertrauen Sie im Verdachtsfall nicht einem einzelnen AV-Programm.

Speichern Sie verdächtige E-Mail-Attachments oder andere verdächtige Dateien auf Ihrem PC ab – selbstverständlich ohne sie auszuführen! Öffnen Sie nun in Ihrem WWW-Browser einen der folgenden URLs: [14] oder [15]. Dorthin können Sie die Datei hochladen und von 25 bzw. 14 AV-Engines überprüfen lassen. Die Ergebnisse erscheinen anschließend im Browser. Wenn keines der AV-Programme Ihre Datei als virös erkennt, ist die Chance hoch, dass das tatsächlich so ist.

Umgekehrt kann das Löschen von irrtümlich als virenverseucht eingestuftem Dateien („False Positives“) ebenfalls ihr System instabil machen. Sichern Sie sie daher vor dem Löschen auf einen externen Datenträger.

Verdächtige Dateien können Sie außerdem auch an Ihren AV-Software-Hersteller zur Analyse senden (s. o.).

2. Eine weitere Prüfmöglichkeit, vor allem für Spyware, ist HijackThis.

Dieses Tool können Sie von [16] herunterladen, installieren und ausführen. Den (ziemlich kryptischen) Output kann man dann seit kurzem komfortabel zur Website hochladen und dort prüfen lassen. Die Prüfergebnisse werden dann recht gut interpretierbar dargestellt, zumindest ein fortgeschrittener Computernutzer kommt damit ganz gut klar. Die Gefahr von False Positives besteht aber auch hier. Im Zweifelsfall helfen wir vom URZ gerne weiter.

3. Besonders üble Malware können Sie mit Anti-Rootkit-Programmen aufspüren.

Eine gute vergleichende Übersicht finden Sie unter [17]. Eine ausführliche deutsche Einführung zum momentan mächtigsten, aber auch kompliziertesten dieser Tools IceSword finden Sie dort ebenfalls. IceSword können Sie sich unter [18] herunterladen.

4. Vor der Säuberung müssen Sie die automatische Systemwiederherstellung deaktivieren und alle wichtige Daten sichern!

Wenn klar ist, dass Sie Schädlinge an Bord haben, schalten Sie unbedingt vor der Säuberung die bei den neuesten Windows-Betriebssystemen ab Windows XP vorhandene Systemwiederherstellung aus [19], da sonst die Gefahr besteht, dass der Virus nach einem Neustart des Computers von Windows wiederhergestellt wird.

5. Das automatische Säubern im laufenden Betrieb geht meist schief – auch im abgesicherten Modus!

Trotz früherer gegenteiliger Aussagen seitens des Bundesamts für Sicherheit in der Informationstechnik (BSI) lassen sich selbst im abgesicherten Modus unter Windows nicht alle Malware-Programme entfernen. In dieser Betriebsart lädt Windows nur wenige Treiber, womit die Chance steigt, dass nur saubere Treiber in den Hauptspeicher gelangen und damit die Säuberung ohne Störmanöver der Malware erfolgen kann. Dennoch ist nach meiner Erfahrung eine automatische Desinfektion nach Standardschema (Download der neuesten AV-Signaturen von einem sauberen PC aus auf USB-Stick, dann Start des befallenen Rechners im abgesicherten Modus, dann AV-Update vom Stick und AV-Check) meist nicht möglich, da die Malware sich oft so tief ins System eingeknistet hat, dass sie die AV-Software ständig blockiert oder deaktiviert.

Was tun, wenn der Verdacht sich bestätigt hat?

Zur Malware-Entfernung bleiben daher nur folgende Möglichkeiten:

1. Manuelle Analyse und Desinfektion

Sie analysieren die Malware und ihre Eigenschaften genau und entfernen alle Spuren per Hand mit Windows-Mitteln und Zusatz-Software wie Process Explorer, TCPview, Autoruns und anschließender manueller Registry-Reinigung mit regedit und nachfolgender Prüfung (siehe RWTH Aachen: [20] und c't 21/2006 [21]).

2. Säuberung mit Hilfe eines integren Live-Systems (Knoppicillin, Bart PE)

Sicherer ist es, wenn Sie die befallene Festplatte von einem sauberen Live-System aus prüfen, entweder mit Knoppicillin, dem Notfall-Linux-System mit verschiedenen eingebauten Virenscannern (siehe c't, Heft 21/2006: [22]) oder Sie erstellen sich mit Bart PE [23] ein Windows-Live-System mit diversen AV-Scannern. Vom sauberen System aus können Sie nun ohne Gefahr, dass ein Virus beim Säubern stören kann, die infizierte, aber passive Festplatte mit den AV-Scannern des Live-Systems auf Malwarebefall prüfen und die Schadsoftware von der Platte entfernen lassen. Nachteilig ist natürlich, dass das Live-System langsamer läuft als ein normaler Rechner (Laden von CD/DVD statt von Festplatte) und einen großen Teil des Hauptspeichers für virtuelle Laufwerke benötigt. Daher dauern Scans dieser Art recht lange, Abstürze sind vor allem bei Rechnern mit wenig Hauptspeicher ebenfalls möglich.

3. Anschließende Spyware-Desinfektion

Nach der Virendesinfektion sollten Sie noch mit Antispyware-Software wie Spybot Search

& Destroy (am besten ebenfalls vom Live-System aus, sonst vom teilgesäuberten System) etwaige Spyware ebenfalls löschen. Danach starten Sie wieder das hoffentlich gesäuberte System und prüfen es nochmals auf Viren und auf Spyware. Falls nun immer noch Spuren von Schadsoftware vorhanden sind (z. B. laut Meldungen von Spybot Search & Destroy), notieren Sie die verdächtigen Dateien auf und löschen sie anschließend mit Hilfe des Live-Systems. Eine nochmalige Prüfung des gesäuberten Systems mit HijackThis (s. o.) oder IceSword im laufenden Betrieb schadet ebenfalls nicht. Wenn Sie Glück haben, muss auch die Registry nicht mehr manuell nachbearbeitet werden.

4. Neuinstallation: Der letzte, aber einzig sichere Weg

Aus eigener Erfahrung kann ich nur bestätigen, dass diese forensischen Arbeiten sehr viel Zeit fressen und leider auch nicht immer von Erfolg gekrönt sind. Bei den ersten beiden Ansätzen ist durchaus noch das Risiko vorhanden, dass Sie zwar die Schadsoftware entfernt haben, aber eine etwaige vom Virus aus dem Internet nachinstallierte „Nutzlast“ wie z. B. eine Backdoor ins Internet übersehen zu haben. Daher sollten Sie sich generell fragen, ob nicht eine Neuinstallation mit Ihren bereits dank Ihrer Präventivmaßnahmen gesicherten Daten unaufwändiger und vor allem sicherer ist. Sie schlafen dann garantiert ruhiger! Sonst werden Sie sich auch nach jedem Muckser Ihres Rechners voller Unbehagen fragen: War das Malware oder war es doch bloß Windows?

Literatur:

- [1] <http://de.wikipedia.org/wiki/Malware>
- [2] <http://de.wikipedia.org/wiki/Adware>
- [3] http://www1.ku-eichstaett.de/urz/inkuerze/2_03/viren.html
- [4] http://www1.ku-eichstaett.de/urz/inkuerze/1_04/sicher.html
- [5] <http://www.heise.de/ct/>
- [6] <http://www.chip.de>
- [7] <http://www.hakin9.org/de/>
- [8] <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
- [9] http://www.thunderbird-mail.de/hilfe/dokumentation1.5/problem_antivirus.php
- [10] <http://www.safer-networking.org/de/index.html>
- [11] http://www.chip.de/downloads/c1_downloads_13002710.html
- [12] http://www.chip.de/downloads/c1_downloads_13003329.html
- [13] http://www.chip.de/downloads/c1_downloads_12999416.html
- [14] <http://www.virustotal.com>
- [15] <http://virusscan.jotti.org/>
- [16] <http://www.hijackthis.de>
- [17] <http://c-ko.blogspot.com>
- [18] <http://www.heise.de/security/tools/default.shtml?prg=80>
- [19] <http://www.bsi.bund.de/av/texte/wiederher.htm>
- [20] <http://www.rz.rwth-aachen.de/kommunikation/betrieb/dialup/vireninfo/virenentfernen.php>
- [21] <http://www.heise.de/security/artikel/80369>
- [22] <http://www.heise.de/ct/06/21/168/>
- [23] <http://www.heise.de/ct/ftp/result.xhtml?url=/ct/ftp/projekte/pebuilder/default.shtml&words=Bart>

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Bernhard Brandel	IN: HB-204	-1888	bernhard.brandel
Heribert Zimmermann	EI: eO-003	-1662	heribert.zimmermann
Tomasz Partyka	EI: eO-107	-1668	tomasz.partyka

Mozilla Firefox – unser Standardbrowser

Dr. B. Tewes

In der Vergangenheit haben wir im Universitätsrechenzentrum auf Netscape als Browser und damit als insbesondere aus Sicherheitsgründen vorzuziehende Alternative zum Microsoft Internet Explorer gesetzt. Doch nachdem für dieses Produkt auf Mozilla-Codebasis seit 2003 zumindest keine neue deutschsprachige Version (letzte Version 7.1) mehr herausgebracht wurde und mit dem Mozilla-Produkt Firefox ein schlankeres, nur die Browserkomponente beinhaltendes Produkt auf den Markt kam, haben sich unsere Prioritäten verschoben. Da wir nun schon seit einiger Zeit diese ständig auch in deutscher Sprache aktualisierte Software einsetzen und empfehlen, ist es an der Zeit, sich einmal etwas intensiver in einem INKUERZE-Artikel damit zu beschäftigen.

In der letzten INKUERZE-Ausgabe 1/2006 war in der Rubrik IN aller KUERZE zu lesen, dass es eine neue Version 1.5 des Firefox gebe. Kurz vor Redaktionsschluss der vorliegenden Ausgabe wurde nun die Version 2.0 herausgebracht. Dieser Artikel ist zwar noch auf der Basis der Version 1.5.7 geschrieben worden, Änderungen bei der Version 2.0 finden aber in Anmerkungen Berücksichtigung.

Wie schon angedeutet, ist dieses Produkt ein reiner „Web-Browser“. Wer wie in Netscape einen E-Mail-Client oder den Composer (WYSIWYG-Editor zum Erstellen von Webseiten) sucht, wird hier nicht fündig werden. Er kann aber auf ergänzende Mozilla-Programme ausweichen, nämlich Mozilla Thunderbird bzw. Nvu. Der Vorteil dieser Trennung liegt in einem schnelleren Start und einer geringeren Speicherauslastung.

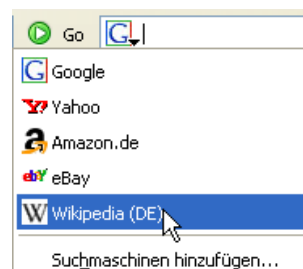
Programmstart

Beim ersten Programmstart startet Firefox eventuell mit einer Meldung, in der angefragt wird, ob für Ihr individuelles Profil die Einstellungen eines anderen Browsers importiert werden sollen. Sollten Sie z.B. im Internet Explorer eine Reihe von *Favoriten* erstellt haben, könnten Sie diese dann durch Auswahl des Internet Explorers in Firefox übernehmen.

Die erste Seite, die aufgerufen wird, ist eine Seite von Mozilla Europe, auf der in deutscher Sprache der Firefox in der aktuellen Version (bei 2.0 derzeit ein Verweis auf die englischsprachigen Release Notes und auf Erweiterungen) vorgestellt wird. Diese Seite erscheint nur beim ersten Start (auch nach einem Update). Ab da entscheiden Sie aufgrund Ihrer Einstellungen, mit welcher Seite der Browser in Zukunft startet.

Im Folgenden werden eine Reihe der Eigenschaften erwähnt, die praktisch jeder moderne Browser besitzt und die somit kein ausschließliches Feature des Mozilla Firefox darstellen. Der Internet Explorer 6 hat diese jedoch in der Regel noch nicht, in der nun auch anstehenden Version 7 (die englischsprachige Version ist bereits erhältlich) sollen sie allerdings dann auch enthalten sein. Hier soll es jedoch darum gehen, wie man diese im Firefox nutzen kann.

Suchfeld



Das Suchfeld oben rechts neben der Adressleiste ermöglicht eine schnelle Suche auf verschiedenartigen Suchseiten. Links sieht man das Symbol der derzeit ausgewählten Suchmaschine (hier *Google*), per Mausklick darauf klappt man ein Menü mit den Alternativen auf, eine Liste, die man mit Hilfe des Eintrag *Suchmaschinen hinzufügen...* ergänzen kann. Die Eingabe eines Suchbegriffs in das Formularfeld wird durch Drücken der Enter-Taste (bei Version 2.0 auch durch Klicken auf das Lupen-Symbol am rechten Rand des Feldes) an die Suchseite übergeben, die die Ergebnisse im aktiven Browserfenster ausgibt.

Die Eingabe des Textes erfolgt mit Vorschlägen zur Autovervollständigung der Historie der bislang eingegebenen Suchbegriffe (bei Version 2.0 optional weitere Vorschläge aus dem Wörter-

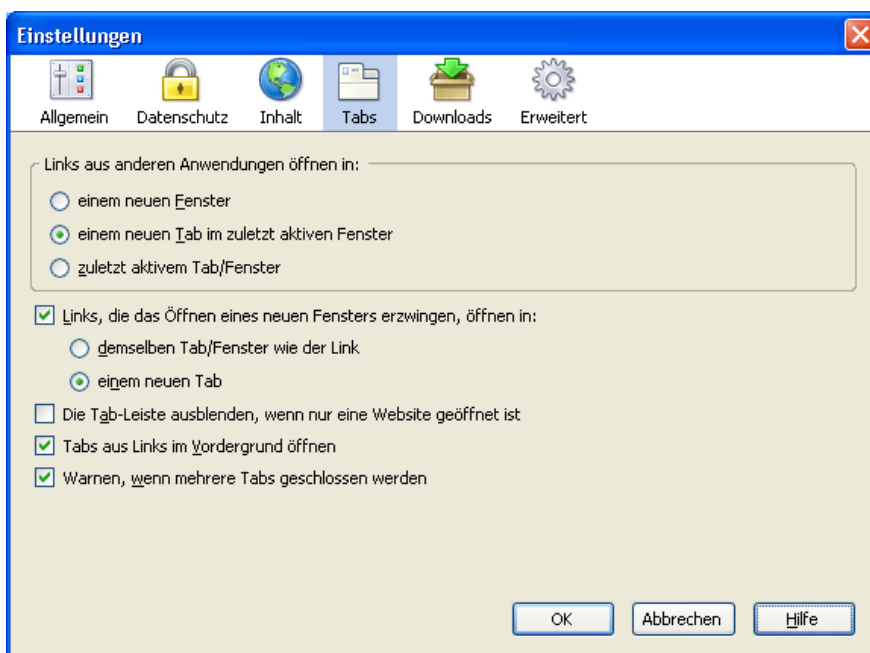
buch), aus denen man per Mausklick auswählen kann. Wenn diese zu lang wird, der kann per Klick mit der rechten Maustaste *Such-Chronik löschen* aus dem Kontext-Menü auswählen.

Tabbed Browsing

Hierunter versteht man, dass innerhalb eines Web-Browsers in sogenannten Tabs (oder Registerkarten) verschiedene Webseiten geöffnet wer-

den können. Da man die entsprechenden Reiter auch der anderen Tabs jederzeit im Blick hat, erhöht dies die Übersichtlichkeit und erleichtert das Wechseln.

Firefox kann bezüglich der Nutzung der Tabs konfiguriert werden. Durch die Menüeinträge *Extras* → *Einstellungen* erhält man ein spezielles Fenster *Einstellungen*. In der Symbolleiste findet man hier den Eintrag *Tabs*.



Ruft man bei bereits geöffnetem Firefox eine Webseite von einer externen Anwendung aus auf, z.B. aus dem E-Mail-Client, so regelt der erste Eintrag mit den drei einander ausschließenden Optionen, wie Firefox hier verfahren soll.

Bei der nächsten Option geht es um die Links, die von der Webseite aus in einem neuen Fenster geöffnet werden sollen. Aktiviert man diese Option nicht, so wird wirklich ein neues Firefox-Fenster geöffnet. Wenn man sich aber aufgrund der *Tabbed Browsing*-Funktionalität dafür entscheidet, diese Option zu wählen, so liegt es nahe, den Link in einem neuen Tab zu öffnen. Alternativ hat man sogar die Möglichkeit, die Vorgabe der Webseite zu ignorieren und den Link im gleichen Tab zu öffnen.

Per Voreinstellung aktiviert ist der Eintrag, die Tab-Leiste auszublenden, wenn lediglich eine Webseite und damit auch nur ein Tab geöffnet ist.

Während der vorletzte Eintrag, der regelt, ob ein per mittlerer Maustaste angeklickter Link in einem neuen Tab im Vordergrund oder Hintergrund geöffnet wird, eher von untergeordneter Bedeutung ist, kann der letzte Eintrag gerade für Neulinge beim Arbeiten mit Tabs sehr sinnvoll sein. Denn schnell ist man dann versucht, eine Webseite mit dem Schließen-Symbol ganz oben rechts statt mit dem gleichen Symbol etwas tiefer in der Tab-Leiste zu schließen, das dann aber das gesamte Browserfenster mit allen Tabs schließt. Hat man diese Option aktiviert, so wird man beim Schließen eines Firefox-Fensters mit mehreren Tabs gewarnt.

Natürlich kann ein neuer Tab auch manuell geöffnet werden, über das Menü (*Datei* → *Neuer Tab*) bzw. die dort angegebene Tastenkombination, aber auch per Kontextmenü, das sich beim Klicken mit der rechten Maustaste auf einen Eintrag in der Tableiste öffnet. Und wenn die Reihenfolge der Tabs nicht passt – schließlich

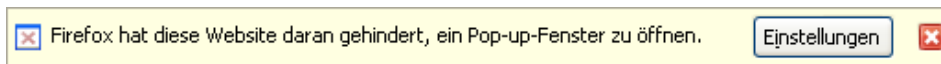
wird ein neuer Tab immer rechts angefügt, was durchaus bei mehreren geöffneten Tabs irritierend sein kann –, der kann diese per Drag & Drop ändern.

Bei der Version 2.0 ist die Gefahr, die Schließen-Symbole für Tabs und das Browser-Fenster zu verwechseln, nicht mehr so groß, da dieses Symbol bei den Tabs in jedem Tab-Reiter selbst untergebracht ist. Es ist weiterhin zu beachten, dass das *Einstellungen*-Fenster hier leicht anders strukturiert ist und z.B. die Funktion, die Vorgabe der Webseite für das Öffnen eines neuen Fensters zu ignorieren, weggefallen ist.

Pop-up-Blocker

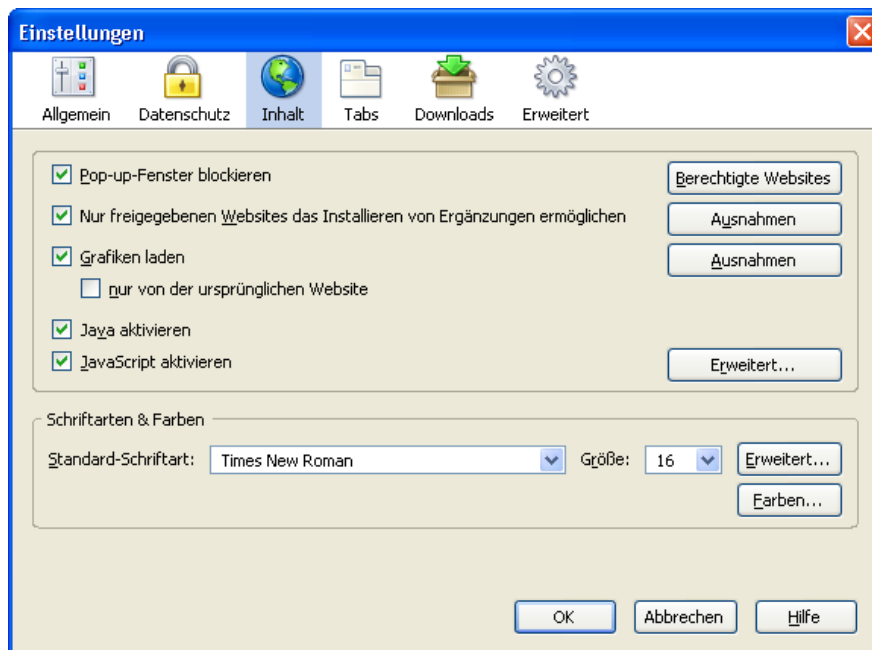
Diese per Voreinstellung aktivierte Funktionalität soll die lästigen kleinen Werbefenster, die häufig aufgehen, wenn man diverse Webseiten besucht, unterbinden helfen. Man darf diese allerdings nicht mit der neueren und aus meiner Sicht noch lästigeren Form verwechseln, bei der Werbeeinblendungen im selben Fenster erfolgen. Mittels CSS-Technik und im Normalfall JavaScript werden Inhaltsbereiche der aktuellen Seite mit Werbung überdeckt, erst ein Klicken auf einen dafür vorgesehenen Bereich ermöglicht es, die Inhalte darunter zu lesen. Gegen diese Technologie, die als Layer-Ads bezeichnet wird, ist der Pop-up-Blocker wirkungslos. Seine eigentliche Aufgabe erledigt er jedoch weitgehend problemlos.

Sollte eine Webseite ein Pop-up-Fenster zu öffnen versuchen, erscheint am oberen Rand des Fenster ein entsprechender Bereich, in dem darüber informiert wird und die Möglichkeit gegeben wird, der Webseite explizit Pop-ups zu erlauben.



Sollte eine Webseite ein Pop-up-Fenster zu öffnen versuchen, erscheint am oberen Rand des Fenster ein entsprechender Bereich, in dem darüber in-

formiert wird und die Möglichkeit gegeben wird, der Webseite explizit Pop-ups zu erlauben.



Im *Einstellungen*-Fenster unter *Inhalt* kann man generell Pop-ups unterbinden und über die Schaltfläche **Berechtigte Websites** einen Blick in die Liste der Websites werfen, die von diesem Verbot ausgenommen sind (Whitelist), sowie diese Liste bearbeiten. Grundsätzlich ist eine solche Whitelist notwendig, da manchmal von durchaus

seriösen Websites Pop-ups für wichtige Angebote in den eigenen Seiten verwendet werden.

Grundsätzlich gilt, dass JavaScript die Basis für das Öffnen möglicher Pop-ups darstellt, wer dies und vielleicht auch andere potentielle Risiken, die mit einem Einsatz solcher Scriptsprachen verbunden sind, ausschalten will, kann Java-

Script vollständig deaktivieren, was übrigens auch gegen die erwähnten LayersAds hilft, oder aber auch nur über Erweitert... einschränken.

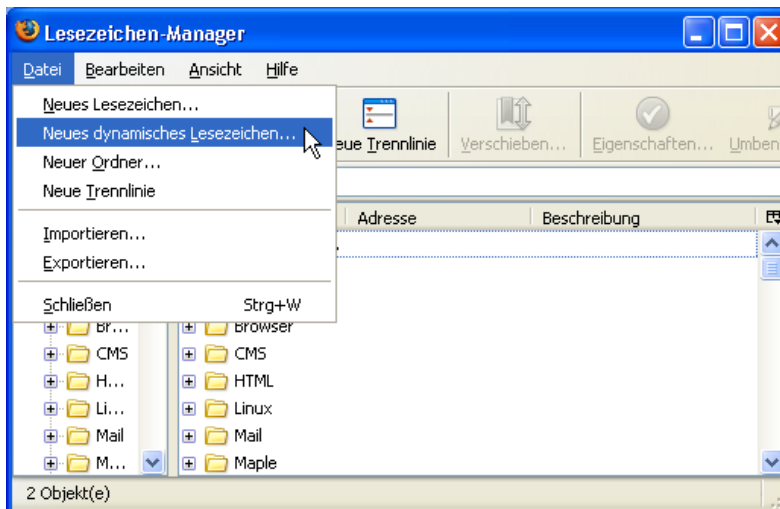
Dynamische Lesezeichen

Lesezeichen oder Bookmarks, im Internet Explorer als Favoriten bezeichnet, sind sicher eine nützliche Sache und schon seit langem Standard in den Browsern. Relativ neu sind noch die sogenannten dynamischen Lesezeichen. Dies bedeutet, dass ein solches Lesezeichen eigene Untermenüpunkte enthält, die selbst letztendlich die

Links zu entsprechenden Seiten darstellen. Diese Untermenüpunkte werden laufend aktualisiert, ohne dass komplette Seiten dafür geladen werden müssen.

In der deutschen Version des Firefox ist als ein sinnvolles Beispiel ein dynamisches Lesezeichen der Tagesschau in die persönliche *Lesezeichen-Symboleiste* eingefügt. Die einzelnen Einträge verweisen auf aktuelle Nachrichten.

Angelegt wird ein dynamisches Lesezeichen über den Lesezeichen-Manager, der über den Menüeintrag *Lesezeichen* aufgerufen werden kann.

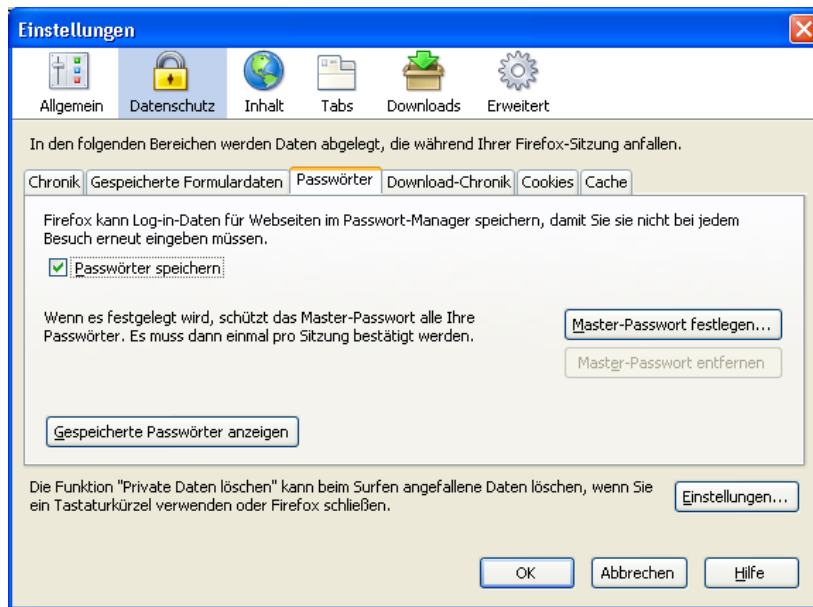


Mit dem Eintrag *Neues dynamisches Lesezeichen...* im *Datei*-Menü öffnet man wiederum ein Dialogfenster, in der neben Name und Beschreibung eine sogenannte *Feed-Adresse* angegeben werden muss. Dies macht deutlich, dass man hier keine URL einer „normalen“ Webseite angeben kann, sondern von Serverseite dies durch ein spezielles Format (RSS-Feeds, verschiedene Endungen wie *.rdf*, *.rss* oder *.xml*) unterstützt werden muss. Solche Dateien findet man inzwischen auf

vielen Seiten, insbesondere solchen, die Nachrichten anbieten (z. B. bei <http://www.spiegel.de> oder <http://www.heise.de>).

Datenschutz

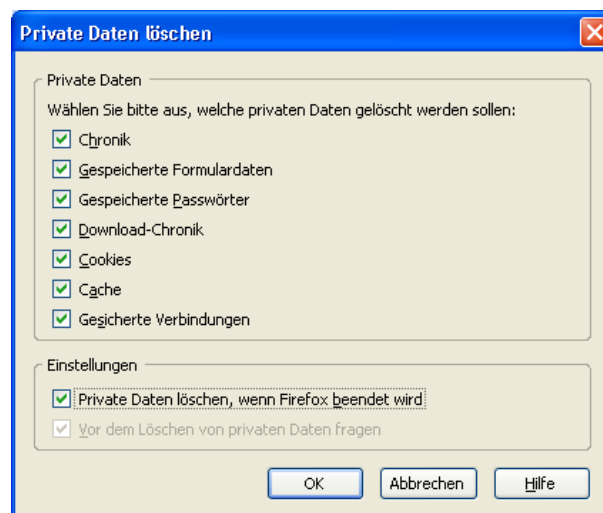
Im *Einstellungen*-Fenster gibt es den Punkt *Datenschutz* als Eintrag in der Symboleiste. Dieser hat wiederum eine Reihe weiterer Untermenüs, die über Reiter angesprochen werden können.



Wichtig werden die hier zu treffenden Einstellungen, bei denen es um persönliche Daten geht, dann, wenn außer Ihnen auch andere Personen mit Ihrem Rechner arbeiten. Zwar gibt es für jeden Windows-Benutzer ein eigenes Firefox-Profil, in dem die Daten abgelegt werden, aber dies ist lediglich eine Hürde, die mit entsprechenden Rechten in Windows kaum eine ernstzunehmende sein dürfte.

Um welche persönlichen Daten es dabei geht, verdeutlichen die Reiter: *Chronik* (zuletzt besuchte Seiten), *Gespeicherte Formulardaten*, *Passwörter*, *Download-Chronik*, *Cookies* und *Cache*. Während es Ihnen vielleicht nur etwas unangenehm wäre, wenn andere Personen genau die

von Ihnen besuchten Seiten und Eingaben nachvollziehen könnten, geht es insbesondere bei den Passwörtern eventuell um wirklich sensible Daten. Haben Sie einen PC nicht ausschließlich für sich zur Verfügung haben, sollten Sie sich gut überlegen, ob Sie ein einzugebendes Passwort von Firefox überhaupt speichern lassen. Wenn Sie es denn tun, könnten Sie diese Daten mit einem einmal pro Sitzung einzugebenden **Master-Passwort** schützen. Sie können sich über **Gespeicherte Passwörter anzeigen** die Webseiten und die verwendeten Benutzernamen anzeigen lassen, auf expliziten Wunsch auch die zugehörigen Passwörter im Klartext!



Wenn Sie nun den Wunsch verspüren, die als private Daten bezeichneten Informationen zu löschen, können Sie über den Button **Einstellungen** unten rechts im Fenster zunächst alle diejenigen Datentypen auswählen, die Sie löschen möchten. Ferner besteht hier auch die durchaus sinnvolle Möglichkeit, die ausgewählten Daten bei jedem Schließen von Firefox löschen zu lassen. Manuell kann man dies über *Extras* → *Private Dateien löschen...* oder eine Tastenkombination erreichen.

In der Version 2.0 ist der Inhalt des *Datenschutz*-Menüs aufgeteilt worden auf *Datenschutz* und *Sicherheit*. Reiter gibt es in diesen beiden Menüs nicht mehr. Die Funktionalitäten bleiben weitgehend unverändert.

Weitere Konfigurationseinstellungen

Bei weitem nicht alle Konfigurationsmöglichkeiten des Mozilla Firefox sind über das *Einstellungen*-Menü möglich. Man hat hier einen Kompromiss zwischen Übersichtlichkeit und Vollständigkeit gewählt. Will man Einstellungen vornehmen, die in diesem Menü keine Berücksichtigung gefunden haben, kann man

`about:config`

in die Adressleiste eingeben. Dann erhält man eine Auflistung mit den Namen der Einstellung, dem Status (*Standard* oder *von Benutzer festgelegt*), dem Typ (*boolean*, *integer*, oder *string*) und dem Wert. Bei Einträgen vom Typ *boolean* führt ein Doppelklick darauf zu einer Veränderung des Wertes – es existieren ja nur die beiden Ausprägungen *false* und *true* –, bei den anderen Datentypen öffnet sich dann ein kleines Dialogfenster zur Eingabe eines neuen Wertes.

Exemplarisch möchte ich hier den Eintrag `browser.cache.check_doc_frequency` betrachten. Dabei handelt es sich um einen *integer*-Datentyp, der die folgenden Werte mit den genannten Bedeutungen annehmen kann:

- 0: Beim jedem Start von Firefox
- 1: Bei jedem Zugriff auf die Seite
- 2: Nie
- 3: Automatisch

3 ist offenbar die Voreinstellung, die bewirkt, dass aufgrund des noch verfügbaren Platzes für Cache-Dateien, des Datums der Aufnahme der Datei in den Cache und der Meta-Informationen im Kopf der HTML-Datei (insbesondere nach dem *expires*-Eintrag) der Cache automatisch verwaltet wird. Dadurch kann es zur Anzeige veralteter Webseiten kommen. So ist es vielfach sinnvoll, nach jedem Start von Firefox bei einem Aufruf einer Seite einen Abgleich von Cache-Seite und Original zu veranlassen, also den Wert 0 zu wählen, sofern man nicht sowieso bei jedem Verlassen von Firefox die *privaten Daten* löschen lässt.

Aufklärung über die Bedeutung dieser Einträge gibt z.B. eine entsprechende Seite im Wiki der deutschsprachigen Website www.firefox-browser.de.

Themes und Erweiterungen

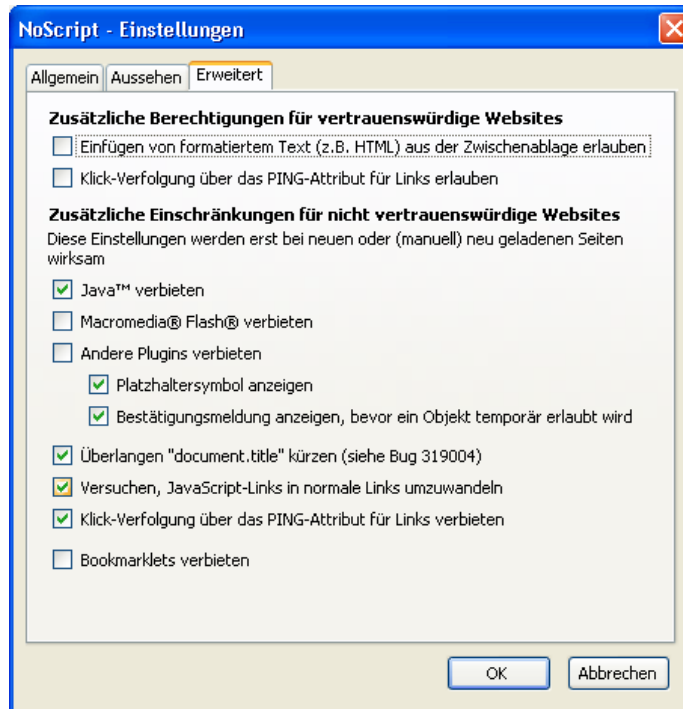
Zum Abschluss will ich noch darauf hinweisen, dass man den Firefox nicht nehmen muss, wie er kommt. Es gibt Möglichkeiten, ihn an den persönlichen Geschmack anzupassen oder ihm neue Funktionalitäten mitzugeben. Im *Extras*-Menü gibt dazu zwei Einträge.



Themes sind eine Möglichkeit, das Aussehen der Oberfläche vom Firefox zu verändern. Dies kann z.B. nur die verwendeten Farben betreffen, es können aber auch alle verwendeten Symbole ausgetauscht werden.

Man kann verschiedene Themes installieren und dann eines davon zur Benutzung auswählen. Grundsätzlich gilt, dass es dabei nur um „op-tisches Tuning“ geht.

Ein „technisches Tuning“ stellen dagegen die *Erweiterungen* dar. Aufgrund des offenen Codes des Mozilla Firefox und klar definierter Schnittstellen haben zahlreiche Personen zusätzliche Funktionalitäten entwickelt. Ein nützliches Beispiel ist *NoScript*. Dieses Tool ermöglicht es, ähnlich wie beim Pop-up-Blocker die Ausführung von JavaScript zunächst allgemein zu verhindern und eine Liste der Websites zu erstellen, die es ausführen dürfen.



NoScript ist konfigurierbar. Über das zugehörige Symbol in der Statusleiste und den Menüeintrag *Einstellungen...* gelangt man in ein Fenster mit mehreren Reitern. Hier kann man die Whitelist der Seiten, die als vertrauenswürdig eingestuft werden, einsehen und bearbeiten oder das Ausse-

hen von *NoScript* im Browser beeinflussen (z.B. ob das Symbol in der Statusleiste des Browsers erscheinen soll). Bei Auswahl des Reiters *Erweitert* sieht man, dass *NoScript* mehr kann als das Ausführen von JavaScript-Code zu verhindern.

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Bernhard Brandel	IN: HB-204	-1888	bernhard.brandel
Dr. Bernward Tewes	EI: eO-106	-1667	bernward.tewes

typokurz – Einige wichtige typografische Regeln*

Ch. Bier

*Dieses kurze Dokument soll einen schnellen Überblick über ein paar aus meiner Sicht wichtige und gleichzeitig leicht einzuhaltende (mikro)typografische Regeln geben, die die Lesbarkeit eines Textes verbessern. Daher spare ich mir lange Erklärungen und das Vorwort. Die Regeln helfen, typografische Fehler zu vermeiden, die mir beim Lesen verschiedenster Texte am häufigsten aufgefallen sind.*¹

Einleitung

Mit den Regeln in `typokurz` sind die typografischen Fehler abgedeckt, die mir beim Lesen verschiedenster Texte am häufigsten aufgefallen sind. Dazu gehören Briefe, Bewerbungen, Vorlesungsskripte, Referate, Hausarbeiten, Diplomarbeiten, aber auch wissenschaftliche Artikel für Journale, die noch nicht vom Verlag/Satzbüro/Lektor korrigiert wurden.

Wer diese Regeln beachtet, erleichtert dem Leser das Erfassen des Inhalts. Mir wird an dieser Stelle immer wieder gerne entgegnet, dass es doch wohl nur auf den Inhalt und nicht auf die Form ankäme. Dies ist einerseits ein Irrtum und andererseits enthalten beispielsweise Satzzeichen selbst inhaltliche Informationen. Es macht nun einmal einen Unterschied, ob an einer Stelle im Text ein Gedankenstrich oder ein Bindestrich steht oder ein Ausrufezeichen oder ein Fragezeichen. Form und Inhalt gehören zusammen; ein roter Klecks ist etwas anderes als ein rotes Herz. Außerdem achten doch die allermeisten sehr genau auf eine korrekte Orthografie. Wer diesbezüglich auf den Duden schwört, findet auch dort Regelungen und Hinweise, wie Anführungszeichen, Gedankenstriche usw. zu setzen sind. Natürlich geht die Typografie weit über diese Dinge hinaus. Doch diese in `typokurz` zu behandeln, würde den Rahmen sprengen. Es geht um für jedermann (und für jede Textverarbeitung!) leicht umsetzbare Regeln. Gerade Letzteres ist auch der Grund, warum `typokurz` systemunabhängig gehalten ist.

Auszeichnung/Hervorhebung von Text

Es gibt verschiedene Möglichkeiten, einzelne Wörter oder Passagen in einem Text auszuzeichnen, die hier genannt und kurz erläutert werden.

Kursive: eigene Schriftform; *integrierte* Auszeichnung, die erst auffällt, wenn man an die entsprechende Stelle kommt; im Normalfall für Auszeichnungen im Text am besten geeignet.

Schräge: Schrägstellung der Aufrechten; keine eigene Schriftform; »Eine [...] elektronisch schräggestellte Schrift ist keine Kursive sondern ein Missverständnis.« (Willberg und Forssman 2001). (Serifenlose Schriften haben häufig keine Kursive.)

zum Vergleich: Kursive *Typografie*
 Schräge *Typografie*

Fette: normalerweise in Textabschnitten zu vermeiden, viel zu aufdringlich (*aktive* Auszeichnung), zieht direkt die Aufmerksamkeit auf sich;² für Überschriften, Bezeichnungen von Tabellen und Abbildungen, für Teile von bestimmten Aufzählungen und Verzeichnissen und Tabellenköpfe geeignet; gelegentlich findet man sie auch für Literaturverweise.

* Mit freundlicher Genehmigung des Autors nachgedruckt aus »Die T_EXnische Komödie«, Heft 3/2006, S. 20–31 (Herausgeber DANTE, Deutschsprachige Anwendervereinigung T_EX e. V.). Der vorliegende Text wurde vom Autor weiterentwickelt und basiert auf Version 1.6.

1. Siehe auch Anmerkungen unter <http://www.zvisionwelt.de/downloads.html>. Dort steht auch die kommentierte L^AT_EX-Präambel des Originaldokuments zur Verfügung.

2. Somit ist die Fette beispielsweise in Nachschlagewerken sinnvoll, in denen man gezielt nach bestimmten Begriffen sucht.

Unterstreichung: unbedingt zu vermeiden; Überbleibsel aus dem Schreibmaschinenzeitalter, als es nur eine Schriftform – die Aufrechte – auf der Schreibmaschine gab.

VERSALIEN: (= Großbuchstaben) nur verwenden, wenn man genau weiß, was man tut, und dann unbedingt leicht sperren (bei vielen Schriften ist eine zusätzliche Verkleinerung sinnvoll; *aktive* Auszeichnung).

zum Vergleich: gesperrt TYPOGRAFIE
 nicht gesperrt TYPOGRAFIE

KAPITÄLCHEN : auch nur verwenden, wenn man weiß, was man tut. Das heißt, man (er)kennt den Unterschied zwischen echten und falschen Kapitälchen; ebenfalls leicht sperren (*integrierte* Auszeichnung).

zum Vergleich: echte TYPOGRAFIE gesperrt TYPOGRAFIE
 falsche TYPOGRAFIE nicht gesperrt TYPOGRAFIE

S p e r r e n: Vergrößerung der Abstände zwischen Buchstaben eines Wortes, wobei nach Tschichold (1960) gesperrte Kleinbuchstaben »immer und überall falsch« sind; Willberg und Forssman (2001) sehen das nicht ganz so streng, sind aber der Meinung, dass Sperren nur etwas für »Typografie-Meister« ist.³

Schriftmischung: die Verwendung einer anderen Schrift; dabei ist zu beachten, dass die verwendeten Schriften zu einander passen. Ist der Text in einer Serifenschrift verfasst, kann eine serifenlose Schrift zur Auszeichnung dienen. Doch Vorsicht: Schriftmischung ist etwas für Experten!

Striche, Auslassungspunkte, Anführungszeichen

Da sich manche der Zeichen in der folgenden Tabelle in einer serifenlosen Schrift nicht so gut unterscheiden lassen, sind diese Zeichen im Zweifelsfall darunter noch in einer Serifenschrift dargestellt.

Bezeichnung	Zeichen	Beispiel	Erläuterung
Trennstrich	-	Silben- trennung	auch <i>Divis</i> genannt; ein kurzer Strich
Bindestrich	-	Bio- und Gentechnologie Öko-Lebensmittel	Das <i>Divis</i> verbindet auch zusammengesetzte Wörter.
Gedankenstrich	–	Ich hoffe sehr – und das meine ich ganz ehrlich –, Sie bald zu treffen.	Halbgeviertstrich, länger als das <i>Divis</i> , steht zwischen zwei Leerzeichen, außer in Verbindung mit Satzzeichen.
Streckenstrich/Bis-Strich	–	Bremen–Hamburg 1–2 Telefonate 25. 9.–28. 12. 25. 9.–28. 12.	Halbgeviertstrich ohne Leerzeichen davor und dahinter; Forssman und de Jong (2004) empfehlen leichte Spationierung (letztes Beispiel).
Minuszeichen	–	6 – 2 = 4	länger als der Bindestrich, gelegentlich dünner als der Gedankenstrich

Fortsetzung ...

3. Ein Beispiel, in dem die Wirkung gesperrter Kleinbuchstaben (»Stolpern«) erwünscht ist: »Hören Sie ruhig Musik in der Badewanne, das entspannt, aber: Elektrogeräte und Badewasser sind eine recht gefährliche Mischung!«

... Fortsetzung

Bezeichnung	Zeichen	Beispiel	Erläuterung
Auslassungsstrich	– —	Der PC kostet 300,—€. 518,89€ 00 300,—€ —	Der Halbgeviertstrich dient im Text auch als Auslassungszeichen; in Tabellen sollte dafür ein Geviertstrich verwendet werden, der die Breite von zwei Nullen hat.
Auslassungspunkte	...	Der Bus fuhr einfach vorbei ... So ein M... aber auch.	Auslassungspunkte sollten etwas gesperrt werden; ⁴ stehen sie am Satzende, wird der Punkt weggelassen (Ausrufe- und Fragezeichen dürfen nicht wegfallen); in vielen Schriften sind sie als einzelnes Zeichen enthalten.
Anführungszeichen (1)	„“ “”	„Es wird noch regnen!“, sagte er.	Nicht zu verwechseln mit den englischen Anführungszeichen (“ ” bzw. “ ”)! Sie dürfen auf keinen Fall durch das Zollzeichen ersetzt werden: "falsch"!
Einfache Anführungszeichen (1)	, ‘ , ‘	„Dann sagte er ‚Es wird noch regnen!‘“, sagte sie.	Kennzeichnung einer Anführung innerhalb einer Anführung
Anführungszeichen (2)	» «	»Es wird noch regnen!«, sagte er.	Guillemets, ebenfalls in Deutschland zulässig; nicht zu verwechseln mit den französischen Anführungszeichen: « vertauscht und spatiiert ».
Einfache Anführungszeichen (2)	› ‹	›Dann sagte er ›Es wird noch regnen!‹«, sagte sie.	Nicht durch die mathematischen Zeichen »kleiner als« und »größer als« ersetzen.
Apostroph	’ ,	Was für ’ne Aufregung!	Nicht mit dem deutschen Abführungszeichen oder dem Fuß- bzw. Minute-Zeichen verwechseln.
Fuß- bzw. Minute-Zeichen	’ , ‘	Höhe: 5’ 49° 13’ 60’’	fünf Fuß neunundvierzig Grad dreizehn Minuten sechzig Sekunden
Sekunden-Zeichen	’’	(siehe oben)	
Schrägstrich	/	WS 2000/2001; und/oder	im Text kein Leerzeichen davor und danach ⁵

Eine Regel zu den richtigen deutschen Anführungszeichen lässt sich besser aus einer Serifenschrift ablesen: „““. Die unteren erinnern in ihrer Form an die Zahl 99 und die oberen an die Zahl 66.⁶

4. Dieser Meinung sind zumindest Willberg und Forssman (2001), es ist so auch im Chicago Manual of Style (Grossman 1998) nachzulesen. Tschichold (1991) und Bringhurst (1997) hingegen lehnen das Sperren von Auslassungspunkten ab.

5. Hier kann es zwar Ausnahmen geben, die in typokurz aber nicht weiter thematisiert werden.

6. Im Englischen ist es umgekehrt und es gibt keine unteren Anführungszeichen: “ ”.

An dieser Stelle sei auch noch etwas zu Leerzeichen vor anderen Satzzeichen gesagt. Vor folgenden Zeichen steht nie ein Leerzeichen:

. , ; : ! ? -) “ ‘

Richtig	Falsch
Dieser Satz, der zur Demonstration ein paar Satzzeichen ... enthält, hat keinen weiteren Sinn – ehrlich! (Dieser Satz auch nicht.)	Dieser Satz , der zur Demonstration ein paar Satzzeichen. . . enthält , hat keinen weiteren Sinn–ehrlich ! (Dieser Satz auch nicht.)

Auslassungszeichen wird dann ein Leerzeichen vorangestellt, wenn sie das Auslassen von Satzteilen markieren; sie werden direkt ohne Leerzeichen an ein Wort angehängt, wenn Teile des Wortes oder daran anschließende Satzzeichen, die ohne Leerzeichen gesetzt werden, ausgelassen werden.

Original	mit Auslassungszeichen
»Wir übergehen die Absicht, eine solche Zeile durch passendes Sperren so lang wie eine bestimmte andere zu machen. Das ist stümperhaft und soll darum hier nicht behandelt werden.« (Tschichold 1960)	»[...] eine [...] Zeile durch passendes Sperren so lang wie eine bestimmte andere zu machen[...] ist stümperhaft [...].« (Tschichold 1960) ⁷

Abkürzungen

Wenn man Abkürzungen verwenden will, sollte man Folgendes beachten: Sparsam und nur übliche Abkürzungen verwenden, keine Abkürzungen am Satzanfang, keine Trennungen von Abkürzungen am Zeilenende und innerhalb von Abkürzungen Verwendung fester Abstände (Dudenredaktion 2004), die kleiner sind als Wortzwischenräume und »auf keinen Fall ganz wegfallen dürfen« (Willberg und Forssman 2001). Ein solcher Abstand wird als *Spatium* bezeichnet. Beispiele finden Sie in der Tabelle. Manche Textverarbeitungen aus Office-Paketen kennen leider kein *Spatium*. In diesem Fall sind wenigstens *feste* Abstände zu verwenden, die man mit einer Trennungssperre verbinden sollte. Dann ist auch sichergestellt, dass innerhalb von Abkürzungen nicht getrennt wird.

Richtig	Falsch	Richtig	Falsch
z. B.	z.B., z. B.	Am Zeilenende dürfen Abkürzungen wie z. B. nicht getrennt werden.	Am Zeilenende dürfen Abkürzungen wie z. B. nicht getrennt werden.

Absatzformatierung

Absätze kann man auf zwei Arten voneinander trennen: *Einzug* oder *Abstand*. Das heißt, entweder ist die erste Zeile eines neuen Absatzes bloß eingezogen, oder aber der Abstand zwischen zwei Absätzen ist erkennbar größer als der Zeilenabstand in den Absätzen. Beide Arten zu kombinieren

7. Hier sei jedoch angemerkt, dass zuviele Auslassungszeichen in einem Zitat an der Kontexttreue zweifeln lassen.

– Absatzabstand und Zeileneinzug – ist überflüssig. Willberg und Forssman (2001) schreiben dazu in Bezug auf wissenschaftliche Dokumente:

Absätze werden durch einen Einzug von ca. 4 mm gekennzeichnet. Abschnitte werden durch einen Abstand von einer Leerzeile gekennzeichnet und zum Unterschied von Absätzen ohne Einzug gesetzt. Das ist die bewährte Regel[. . .].

In diesem Dokument wird zur Kennzeichnung von Absätzen Abstand verwendet.

Eine Zeile sollte nicht mehr als 60–70 Zeichen (einschließlich Satz- und Leerzeichen) enthalten, um die Lesbarkeit nicht unnötig zu erschweren.⁸ Will man den Platz auf einem DIN-A4-Blatt so weit wie möglich nutzen, bietet es sich an, zweispaltig zu setzen.

Die Zeilenlänge wiederum beeinflusst zusammen mit Schriftfamilie, Schriftschnitt und Schriftgröße den *Zeilenabstand*. Leider gibt es aufgrund der vielen involvierten Parameter keine praktikable Faustregel, bei welchen Einstellungen welcher Zeilenabstand geeignet ist; das kann nur das geübte Auge entscheiden. Wenn es eine Faustregel gibt, dann diese: Ein 1,5-facher Zeilenabstand (orientiert an der Bezeichnung in bekannten Textverarbeitungen) ist in normalen Texten immer zuviel!

Flattersatz

Ein gleichmäßiger sogenannter *Grauwert* ist von großer Bedeutung für die Lesbarkeit eines Textes. Zu große und ungleichmäßige Abstände zwischen Wörtern in einer Zeile oder gar zwischen Buchstaben eines Wortes (Sperrung) erschweren die Lesbarkeit eines Textes.

Flattersatz⁹ hat den großen Vorteil, dass die Wortzwischenräume immer gleich groß sind, was positiv für einen gleichmäßigen Grauwert bzw. die Lesbarkeit ist. Andererseits wirkt Flattersatz eher unruhig, vor allem bei schlechtem Zeilenumbruch, und der (meist rechte) Flatterrand hat einen ungleichmäßigen Grauwert.

In Spalten mit weniger als 40 Zeichen kann man kaum gut lesbaren Blocksatz erzeugen, weswegen dort die Verwendung von Flattersatz sinnvoll ist. Allerdings ist guter Flattersatz nicht einfach zu erreichen. Wie beim Blocksatz sind Zeilenlänge, Sprache in der der Text verfasst wird, der Mechanismus der Silbentrennung und des Umbruchalgorithmus' der verwendeten Software von entscheidender Bedeutung.

In Abbildung 1 ist jeweils ein Beispiel für guten und weniger guten Flattersatz dargestellt.

In Spalten mit weniger als 40 Zeichen kann man kaum gut lesbaren Blocksatz erzeugen, weswegen dort die Verwendung von Flattersatz auf jeden Fall sinnvoll ist. Allerdings ist guter Flattersatz nicht einfach zu erreichen. Wie beim Blocksatz sind Zeilenlänge, Sprache in der der Text verfasst wird, der Mechanismus der Silbentrennung und des Umbruchalgorithmus' der verwendeten Software von entscheidender Bedeutung.

In Spalten mit weniger als 40 Zeichen kann man kaum gut lesbaren Blocksatz erzeugen, weswegen dort die Verwendung von Flattersatz auf jeden Fall sinnvoll ist. Allerdings ist guter Flattersatz nicht einfach zu erreichen. Wie beim Blocksatz sind Zeilenlänge, Sprache in der der Text verfasst wird, der Mechanismus der Silbentrennung und des Umbruchalgorithmus' der verwendeten Software von entscheidender Bedeutung.

Abbildung 1: Beispiel für guten und weniger guten Flattersatz

8. Berufsleser haben auch mit längeren Zeilen mit bis zu 90 Zeichen keine Probleme.

9. In Textverarbeitungen als »linksbündig« bzw. »rechtsbündig« bezeichnet.

Blocksatz

Ob man sich für oder gegen Blocksatz entscheidet, ist abhängig von der Zeilenlänge, der Sprache in der der Text verfasst wird, dem Mechanismus der Silbentrennung und dem Umbruchalgorithmus der verwendeten Software. Will man für längere Zeilen Blocksatz verwenden, muss man sicherstellen, dass die verwendete Software gleichmäßige und enge Wortzwischenräume erzeugt; innerhalb einer Zeile sollten die Wortzwischenräume für das Auge gleich groß sein und sich von den Abständen in der vorangehenden und nachfolgenden Zeile nicht deutlich unterscheiden. Denn ein gleichmäßiger Grauwert an den Rändern bringt nichts, wenn ansonsten innerhalb der Zeile zu große Wortzwischenräume auftreten.

[...] eine [...] Zeile durch passendes Sperren so lang wie eine bestimmte andere zu machen[...] ist stümperhaft [...]. (Tschichold 1960).¹⁰

Durch das Aufteilen des Restraums einer Zeile auf die Blocksatz-Zeilenbreite wird die Zeile gesperrt und damit zufällig, ohne jeden inhaltlichen Grund, ausgezeichnet. (Willberg und Forssman 2001)

Zur Verdeutlichung sind in Abbildung 2 ein Absatz mit gleichmäßigem und ein Absatz mit ungleichmäßigem Grauwert bzw. gutem und schlechtem Blocksatz dargestellt.

Ob man sich für oder gegen Blocksatz entscheidet, ist abhängig von der Zeilenlänge, dem Mechanismus der Silbentrennung und dem Umbruchalgorithmus der verwendeten Software. Will man für längere Zeilen Blocksatz verwenden, muss man sicherstellen, dass die verwendete Software gleichmäßige Wortzwischenräume erzeugt; innerhalb einer Zeile sollten die Wortzwischenräume für das Auge gleich groß sein.

Ob man sich für oder gegen Blocksatz entscheidet, ist abhängig von der Zeilenlänge, dem Mechanismus der Silbentrennung und dem Umbruchalgorithmus der verwendeten Software. Will man für längere Zeilen Blocksatz verwenden, muss man sicherstellen, dass die verwendete Software gleichmäßige Wortzwischenräume erzeugt; innerhalb einer Zeile sollten die Wortzwischenräume für das Auge gleich groß sein.

Abbildung 2: Beispiel für gleichmäßigen und ungleichmäßigen Grauwert

Ziffern und Zahlen

Zahlen können sowohl in Ziffern als auch ausgeschrieben werden. Kleine Zahlen sollten immer ausgeschrieben werden (*zehn Personen*).¹¹ Dies gilt nicht, wenn sie den Charakter einer Nummer haben (*auf Seite 8*), mit anderen in Ziffern geschriebenen Zahlen verglichen werden (*von 1,5 auf 2 gestiegen*) oder mit einer abgekürzten Einheit verbunden sind (*5 min*, aber: *fünf Minuten*). Auch große Zahlen sollten ausgeschrieben werden, wenn sie nicht exakte Werte angeben (*rund tausend Zuschauer*).

Ausgeschriebene Zahlen unter einer Million werden klein und zusammen geschrieben (Dudenredaktion 2004). Folgende Regeln zur Formatierung von Zahlen in Ziffern erhöhen die Leserlichkeit und erleichtern das Erfassen der Zahlen (für die Abstände ist das Spatium dem Wortzwischenraum vorzuziehen):

10. Zur Erinnerung: auf Seite 50 steht das komplette Zitat.

11. Leider gehen die Ansichten darüber, wann eine Zahl klein im hier verwendeten Sinn ist, weit auseinander. Häufig werden die Zahlen bis zwölf genannt, in Romanen findet man aber auch dreistellige und sogar Jahreszahlen ausgeschrieben.

Bis zu vier Ziffern solche Zahlen werden ohne Abstände gesetzt¹²

Ab fünf Ziffern solche Zahlen »dürfen durch Abstände strukturiert werden, nicht aber durch Punkte, Apostrophe o. ä.«¹³ (Willberg und Forssman 2001)

Telefonnummern von hinten her Gruppierung in Zweiergruppen mit Abständen, wobei Vorwahl und eigentliche Rufnummer getrennt gezählt werden; Durchwahlnummern werden nicht noch mal unterteilt; es kann auch mit Klammern gegliedert werden.¹⁴ Bei der internationalen Vorwahl werden die zwei Nullen vor dem Länderkürzel durch ein Plus-Zeichen ersetzt.

Kontonummern von hinten her Gruppierung in Dreiergruppen mit Abständen

Bankleitzahlen von vorne Gruppierung in Dreiergruppen mit Abständen

Postleitzahlen werden ohne Abstände gesetzt

Eszett/Das scharfe S

Das scharfe S ist eine Ligatur¹⁵ der Buchstaben s und z, woher auch die Bezeichnung Eszett kommt.¹⁶ *Das scharfe S existiert nur als Kleinbuchstabe!*¹⁷ Bei den Versalien oder Kapitälchen gibt es kein scharfes S. »GROß« ist genauso falsch wie »KLEIn«. Im Versal- oder Kapitälchensatz muss das scharfe S durch »SS« ersetzt werden: GROSS bzw. GROSS. Trägt jemand ein scharfes S in seinem Namen und will dies wegen der Verwechslungsmöglichkeit auf keinen Fall durch »SS« ersetzen, kann er auch auf »SZ« ausweichen. Allerdings wird der Leser, wenn er auf »SZ« stößt, stocken, weil es ungewohnt ist.

Tabellen

Tabellen unterliegen nicht den gleichen typografischen Regeln wie Fließtext. Breite und Höhe werden von der inhaltlichen Struktur bestimmt. Bei Silbentrennungen muss auf die korrekte und sinn gerechte Trennung geachtet werden.¹⁸ Der wichtigste Hinweis neben der korrekten Silbentrennung scheint mir jedoch der auf den Verzicht von vertikalen Linien zu sein. Diese Linien erhöhen keineswegs die Übersichtlichkeit, sondern behindern das Erfassen der Zeilen. Auf die horizontalen Linien kann man auch verzichten, wenn man stattdessen einen geringen Abstand einfügt.

Schriften

Es ist sinnvoll, für längere Texte mit breiten Zeilen eine Schrift mit Serifen und Strichstärkenunterschied zu verwenden. Die Serifen (Endstriche) unterstützen einerseits das Auge bei der Zeilenführung und beim Zeilenrücksprung. Andererseits führt der Strichstärkenunterschied zu eindeutigeren Wortbildern, was das Lesen sehr erleichtert. Serifenlose Schriften – auch Groteskschriften genannt – kann man hingegen in schmalen Spalten (< 40 Zeichen, einschließlich Satz- und Leerzeichen) einsetzen, in denen das Auge die Unterstützung der Serifen nicht unbedingt benötigt. Jedoch muss die Serifenlose

12. Laut Dudenredaktion (2004) können auch vierstellige Zahlen bereits durch einen Festabstand strukturiert werden (9 000).

13. Auch wenn die DIN 5008 die Gliederung mit Punkten empfiehlt ...

14. Folgende Schreibweise ist laut DIN 5008 ebenfalls zulässig, meines Erachtens aber weniger gut leserlich vor allem bei längeren Nummern und/oder mit internationaler Vorwahl: +49 6821 5647008

15. Verschmelzung zweier oder mehrerer Buchstaben, am bekanntesten sind die f-Ligaturen: fi → fi, fl → fl, ff → ff, ffi → ffi, ffl → ffl, ft → ft, fft → fft; finden → finden Aber: FINDEN und nicht fiNDEN

16. In Wirklichkeit handelt es sich um eine Ligatur aus langem S (ſ) und Z; es handelt sich nicht, wie früher diskutiert, um eine Ligatur aus langem S und rundem S (s) (Brekle 2001).

17. Die Einführung eines Versal-ß wurde schon häufiger diskutiert, aktuell unter anderem hier: http://www.signographie.de/cms/signa_9.htm

18. Darauf explizit hinweisen zu müssen, ist dem Tabellensatz bekannter Office-Anwendungen zuzuschreiben.

sorgfältig ausgewählt werden, da ihre Zeichen und die sich ergebenden Wortbilder aufgrund fehlender Strichstärkenunterschiede nicht so eindeutig und unverwechselbar sind wie bei Serifenschriften.¹⁹ Serifenlose Schriften eignen sich auch für Beamer-Präsentationen, weil dort aufgrund der geringen Auflösung (und der unter Umständen großen Entfernung des Betrachters) die Serifen und dünnen Striche nicht gut zu erkennen sind.

Die sehr geringe Bildschirmauflösung (etwa im Bereich 72–105 dpi im Vergleich zu Gedrucktem mit einer Auflösung von mindestens 300 dpi, meist 600 dpi) scheint mir auch der Grund für die mittlerweile sehr weite Verbreitung von serifenlosen Schriften wie Arial²⁰ zu sein. Am Bildschirm sind serifenlose Schriften bzw. solche ohne Strichstärkenunterschied in der Tat häufig besser zu lesen als serifenbehaftete Schriften. Aber denken Sie an den Druck und vergleichen Sie deshalb auf Papier!

Anpassungen für die Schweiz

Anführungszeichen werden in der Schweiz ähnlich den französischen Anführungszeichen gesetzt, jedoch ohne Einschluss von Leerzeichen: «schweizer» Anführungszeichen (« französische » Anführungszeichen). *Telefonnummern* werden von vorne beginnend in eine Dreiergruppe und anschließend in Zweiergruppen gegliedert; die dreistellige Vorwahl wird nicht weiter unterteilt und immer dazugeschrieben, da sie seit 2002 auch immer gewählt werden muss: 076 437 28 66. *Das scharfe S* gibt es in der Schweiz nicht. An seiner Stelle wird immer »SS« bzw. »ss« gesetzt.

Literatur

- BREKLE, Herbert E.: Zur handschriftlichen und typographischen Geschichte der Buchstabenligatur ß aus gotisch-deutschen und humanistisch-italienischen Kontexten. In: *Gutenberg-Jahrbuch*, 2001, S. 67–76
- BRINGHURST, Robert: *The Elements of Typographic Style*. Vancouver : Hartley & Marks, 1997
- DUDENREDAKTION (Hrsg.): *Duden – Die deutsche Rechtschreibung*. Bd. 1. 23. Auflage. Mannheim · Leipzig · Wien · Zürich : Dudenverlag, 2004
- FORSSMAN, Friedrich ; DE JONG, Ralf: *Detailtypografie*. Mainz : Verlag Hermann Schmidt, 2004
- GROSSMAN, John (Hrsg.): *The Chicago Manual of Style*. 14. Auflage. Chicago : University of Chicago Press, 1998
- TSCHICHOLD, Jan: *Erfreuliche Drucksachen durch gute Typographie*. Augsburg : Maro Verlag, 1960
- TSCHICHOLD, Jan: *The Form of the Book: Essays on the Morality of Good Design*. Vancouver : Hartley & Marks, 1991
- WILLBERG, Hans P.: *Wegweiser Schrift. Erste Hilfe für den Umgang mit Schriften*. Mainz : Verlag Hermann Schmidt, 2001
- WILLBERG, Hans P. ; FORSSMAN, Friedrich: *Erste Hilfe in Typografie*. Mainz : Verlag Hermann Schmidt, 2001

19. Es gibt auch serifenlose Schriften mit Strichstärkenunterschied, die aber eher die Ausnahme sind.

20. Willberg (2001) schreibt zur Arial: »[...] Schwer zu beschreiben, da ohne jede Individualität. [...] Sie wird häufig eingesetzt, hinterlässt aber bei mir keinerlei Eindruck.«

T_EXinfo

P. Zimmermann

»Warum kompliziert, wenn es auch einfach geht?« T_EX-Dokumente haben die Eigenschaft, zahlreiche Auszeichnungen und Strukturanweisungen in Form von Kommandos zu beinhalten. Die mit einem »\« beginnenden Zeichenketten der T_EX-Befehle müssen programmgemäß eindeutig sein; falsch geschriebene Direktiven produzieren Fehlermeldungen und führen zu unerwünschten Nebenwirkungen. Bestimmte Textteile wie Tabellen oder Bibliographien schwellen im Verlauf einer längeren Arbeit zu komplexen Gebilden an. Bleibt der Autor hier ohne Hilfe? Nein! Der in unserem Hochschulnetz vielfach eingesetzte Editor WinEdt bietet eine beachtliche Anzahl an nützlichen Erweiterungen an, die – einmal installiert – zu einem nicht mehr wegzudenkenden Hilfsmittel werden.

Nützliche Erweiterungen für WinEdt

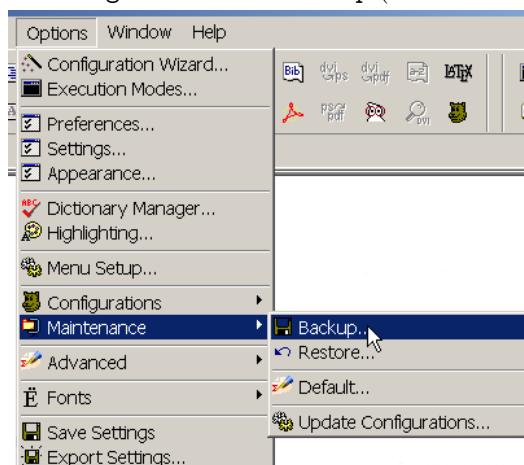
Das zum Editieren für T_EX-Dokumente eingesetzte WinEdt-Programm lässt sich auf vielerlei Weise den eigenen Wünschen und Anforderungen anpassen. Ein großes Reservoir von Zusätzen findet sich im WorldWideWeb unter <http://www.winedt.org>, im Bereich unseres Novell-Netzes unter `i:/Archiv/TeX/TeXEditor/WinEdt/PlugIns`. Die Installation solcher vorgefertigter WinEdt-Zusätze verläuft in zwei Schritten (vorausgesetzt wird eine Version von WinEdt 5.2 oder neuer):

1. den gewünschten Zusatz auspacken und an einen geeigneten Ort kopieren (zumeist WinEdt/PlugIns) und
2. den WinEdt starten und die Installationsroutine aktivieren.

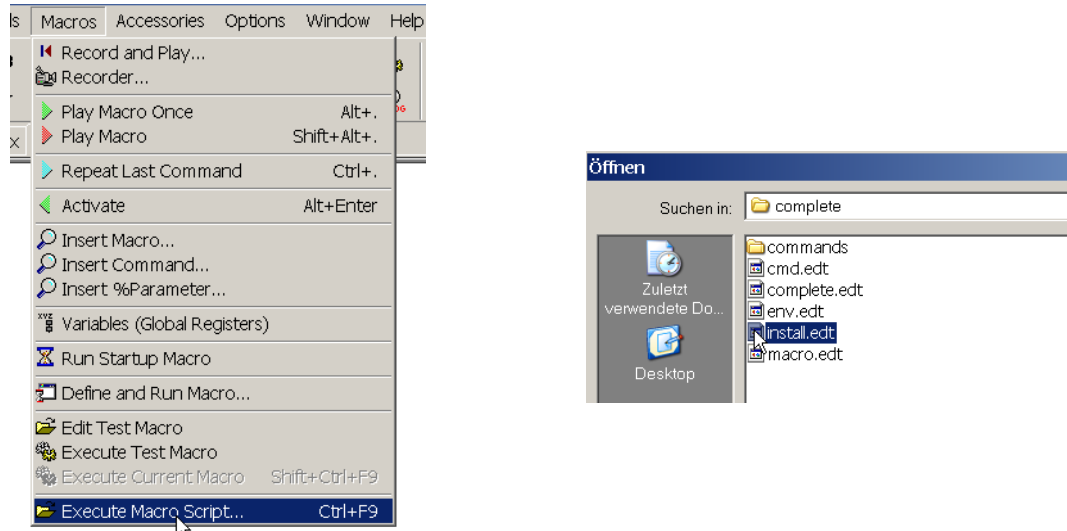
Anschließend stehen die Neuerungen nach einem Neustart von WinEdt bereit.

Als Beispiel sei der »Command Completion Wizard« aus der PlugIns-Sammlung von WinEdt.org angeführt, der auf Tastendruck L^AT_EX-Kommandos und -Umgebungen vervollständigt.

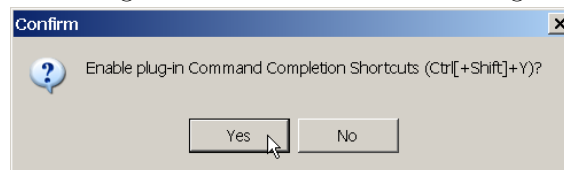
1. In einem ersten Schritt entpackt man die Datei `complete.zip` in ein Unterverzeichnis des WinEdt-Programmverzeichnisses nach `WinEdt/PlugIns/Complete`. Im Netz der KU stehen die entpackten Dateien im Verzeichnis `i:/Archiv/TeX/TeXEditor/WinEdt/PlugIns/Complete`.
2. Nach dem anschließenden Start von WinEdt empfiehlt sich die Sicherung der aktuellen Einstellungen von WinEdt über `Options` → `Maintenance` → `Backup` (für WinEdt 5.4 oder neuer) bzw. `Options` → `Configurations` → `Backup` (für ältere WinEdt-Versionen).



Der Installationsvorgang wird über ein `install.edt` WinEdt-Makro angestoßen, das über den Menüpunkt **Macros** → **Execute Macro Script** geladen wird. Als auszuführendes WinEdt-Makro ist zum Unterverzeichnis `WinEdt/PlugIns/Complete` zu wechseln und die Datei `install.edt` auszuwählen.



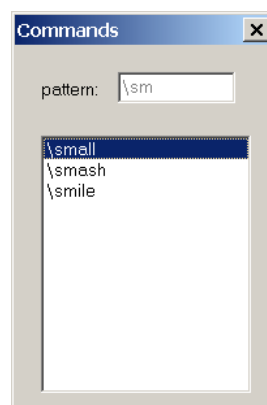
Ein Klick auf **Yes** im Rückfrage-Fenster schließt die Aktivierung des Makros ab.



Fortan komplettiert ein **Strg-Y** jeden angefangenen L^AT_EX-Kommandonamen und jedes **Strg-Shift-Y** jede L^AT_EX-Umgebung. Führt der eingegebene Textteil zu keiner eindeutigen Auflösung des Kommandonamens bzw. der Umgebung, so bietet ein Auswahlmennü mögliche Ergänzungen an.

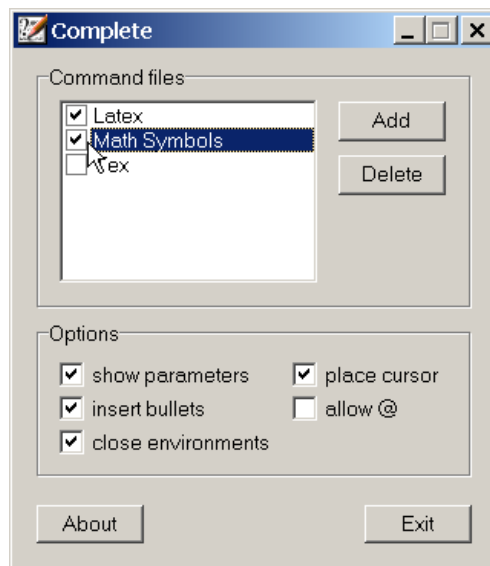
Beispielsweise liefert ein Eintippen von

- ▷ »it« gefolgt von **Strg-Shift-Y** ein `\begin{itemize}` und zwei Zeilen darunter das korrespondierende `\end{itemize}`, die Schreibmarke ist an den Listenanfang positioniert;
- ▷ ein »\sm**Strg-y**« liefert drei Kommandos zur Auswahl:



Ein Klick auf die gewünschte Zeichenkette vervollständigt den Kommandoanfang entsprechend.

Nach einem ersten Aufruf des Command Complete-Makros startet ein zugehöriges `complete`-Programm, das eine Konfiguration des Umfangs der zu ergänzenden Textbausteine erlaubt. Darüberhinaus lassen sich eigene Kommando- und Umgebungslisten einbetten.



Neben zahlreichen Rechtschreibhilfswörterlisten umfasst die Übersicht der WinEdt-Erweiterungen Einträge

- ▷ zur Anpassung der Oberfläche (u. a. BiB_TE_X, internationale Anführungszeichen, Xy-Pic Schablonen),
- ▷ zum leichteren Schreiben von L^AT_EX-Dokumenten (beispielsweise Makros zur bequemeren Eingabe und Verwaltung von Bibliographie-, Index- und Querverweistexten)
- ▷ und Zusatzprogramme, die die Funktionalität von WinEdt durch kleine Programme erweitern (genannt PlugIns; wie etwa das vorgestellte Command Complete oder Hilfsprogramme zur Herstellung von Grafiken und Tabellen).

Neues L^AT_EX-Skript

Das Regionale Rechenzentrum für Niedersachsen/Universität Hannover hat in seine Skriptenreihe eine Einführung in L^AT_EX von THOMAS F. STURM aufgenommen – Titel »L^AT_EX. Einführung in das Textsatzsystem«. In den Sekretariaten des Universitätsrechenzentrums kann das neue L^AT_EX-Skript zum Preis von 6 € bezogen werden.

Das über 300 Seiten starke Werk behandelt reich bebildert die Themen Allgemeine Einführung, Installation, Dokumentenstruktur, Schrift mit Schriftausrichtung, Tabellen, Zähler und Längen, eigene Definitionen, Seitenlayout und mathematische Formeln. Darüberhinaus kommen auch speziellere Fragestellungen zur Sprache: Projektverwaltung, verschiedene Verzeichnisse (Stichwort, Literatur), Kästchen, Graphiken und die Darstellung von Quellcode.

Versehen mit einem umfangreichen Stichwortverzeichnis hilft das Handbuch dem Einsteiger, erste Hürden zu nehmen, dient aber auch dem routinierten Anwender als Nachschlagewerk.

<i>Ansprechpartner im URZ:</i>	<i>Zimmer:</i>	<i>Telefon:</i>	<i>Mail:</i>
Peter Zimmermann	Er: eO-106	-13 51	peter.zimmermann

Mal schnell eine Fernleihe aufgegeben? Oder etwa nicht? Anmerkungen zum aktuellen Gesetzentwurf des Urheberrechts

Dr. M. Löffler

Die Hochschullandschaft ist derzeit reich an Diskussionen, seien es Studiengebühren, sei es der Bologna-Prozess, sei es die Umsetzung des neuen Bayerischen Hochschulgesetzes – ein Thema hingegen scheint dabei nur von Insidern wahrgenommen zu werden, nämlich die zweite Urheberrechtsanpassung. Die allerdings berührt die Informationsversorgung an den Hochschulen sehr deutlich, so dass eine Reihe von Wissenschaftsgesellschaften (z. B. Max-Planck-Gesellschaft), Fachverbände und Hochschulen bzw. Universitätsbibliotheken in öffentlichen Aktionen bereits dagegen protestiert haben¹.

Worum geht es? Die Bundesregierung steht in der Pflicht, die EU-Richtlinie zur Harmonisierung einiger Bereiche des Urheberrechts aus dem Jahr 2001² in deutsches Recht zu überführen. Erste Tatbestände wurden im *Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft* 2003 geregelt. Gegenstand der Kritik ist der Gesetzentwurf der Bundesregierung für einen sogenannten zweiten Korb vom 15. Juni 2006, der bereits auf die Kritik des Bundesrates antwortet. Die erste Lesung fand in der Nacht vom 29. auf den 30. Juni 2006³ statt und machte deutlich, dass entgegen der Mahnung des Bundesjustizministeriums Änderungen im Rahmen der Diskussionen im Rechtsausschuss noch denkbar sind. Dennoch bestehen seitens der Forschungs- und Wissenschaftseinrichtungen Zweifel, ob die Problematiken des gegenwärtigen Gesetzentwurfs von Politikern tatsächlich bereits wahrgenommen worden sind.

Dem Titel des Gesetzes nach geht es um den Schutz geistigen Eigentums, real wird über Formen und Rechte der Verwertung diskutiert, insbesondere vor dem Hintergrund elektronischer Möglichkeiten. Dabei stehen sich die Interessen der Verlage⁴ und diejenigen der Nutzer von Informationseinrichtungen gegenüber⁵. Welche Folgen ergeben sich aus dem Gesetzentwurf für

die Bibliotheken bzw. für die Informationsversorgung des Wissenschaftsbereichs? – Hier zwei Beispiele:

- ▷ Gefährdung der Fernleihe in der bisherigen Form auf Basis von §53 a *Kopienversand auf Bestellung*: Liegt ein Aufsatz durch einen Anbieter im Internet in elektronischer Form vor, so ist keine Fernleihe in der heute üblichen elektronischen Form möglich, sondern nur noch per Fax oder Post. Wichtige Verlage aber verfügen längst über eine elektronische Angebotsplattform, kleinere werden in den nächsten Jahren folgen – die Fernleihe wird für die Mehrzahl aller Aufsätze also unattraktiv, weil für den Nutzer zu langwierig und für Bibliotheken zu aufwendig. Das Fernleihsystem in der heute technisch realisierten Form wäre kaum noch nutzbar. Die Alternative heißt, den Artikel zu kaufen. Was einzelne Artikel kosten, lässt sich heute bereits bei Anbieterplattformen wie IngentaConnect⁶ erkunden – die Preise beginnen bei ca. 20 € in den 'preiswerten', sprich industriefernen Fächern und erreichen durchaus Summen von einigen hundert Euro. Allein für die Zweigbibliothek Ingolstadt wäre 2005 mit

1. Etwa die inzwischen mehr als 5 000 Unterzeichner der *Göttinger Erklärung zum Urheberrecht für Bildung und Wissenschaft vom 05. Juli 2004*: <http://www.urheberrechtsbuendnis.de/index.html.de> <07.11.2006>

2. Richtlinie 2001/29/EG

3. <http://dip.bundestag.de/btd/16/018/1601828.pdf> <07.11.2006>

4. Vgl. dazu die Veröffentlichungen des Börsenvereins des Deutschen Buchhandels:

<http://www.was-verlage-leisten.de/content/category/6/22/44/>

<http://www.was-verlage-leisten.de/images/stories/faqs%20gesamtversion%20061030.pdf> <07.11.2006>

5. Vgl. Anm. 1

6. <http://www.was-verlage-leisten.de/content/category/6/22/44/>

einer Summe von ca. 85 000 € zu rechnen gewesen. Die Schaffung einer Logistik, die eine rasche Bearbeitung und die Verwaltung der gekauften Aufsätze sicherstellt, wird ebenfalls nicht unaufwendig. Gewinnt parallel der Trend zum EBook an Bedeutung, ist auch die Fernleihe von Monographien betroffen⁷.

- ▷ Die Nutzungsmöglichkeit digitalisierter Veröffentlichungen, die nicht bereits in elektronischer Form erworben wurden, wird deutlich eingeschränkt – die Einrichtung eines elektronischen Semesterapparats etwa wird beinahe sinnlos: §52b *Wiedergabe von Werken an elektronischen Leseplätzen in öffentlichen Bibliotheken, Museen und Archiven*. Digitalisierte Informationen aus dem Bestand der Bibliothek dürfen nur in der Zahl zugänglich gemacht werden, in der sie erworben wurden. Eine gleichzeitige Nutzung durch mehrere Personen etwa im Rahmen eines elektronischen Semesterapparats oder eines E-Learning-Programms wäre nicht zulässig. Zusätzlich ist für die Form der Bereitstellung noch eine „angemessene Vergütung“ zu entrich-

ten. Vor allem aber wäre die Nutzungsmöglichkeit eingeschränkt, denn die Bereitstellung darf ausschließlich in den Räumen der Bibliothek „an eigens dafür eingerichteten elektronischen Leseplätzen“ erfolgen. Eine Nutzung über das Netz ist ausgeschlossen.

Ingesamt ist der Gesetzgeber bemüht, die rechtlichen Grauzonen im Umgang mit Informationen auf Basis der neuen technischen Möglichkeiten zu regeln. Der Lösungsansatz allerdings ist unintelligent, denn er symbolisiert keine Lösung zwischen den Interessen von Verlagen und dem Wissenschaftsbereich, ja man ist überrascht, wie ungenau das Kommunikationsverhalten des Wissenschaftsbereichs wahrgenommen wird. Die strukturellen Probleme des Informationsversorgungsbereichs – steigende Kosten bei gleichzeitig wachsendem Medien- und Informationsangebot⁸, sinkenden Etats, aber vermehrtem und differenzierterem Bedarf – werden nicht gelöst, sondern ganz im Gegenteil verschärft. Die Botschaft lautet ‘Kaufen’, Alternativen soll es nur zu nach dem heutigen Entwicklungsstand unakzeptablen Bedingungen geben. Aber das ist für Forschung und Bildung in der Wissenschafts- und Informationsgesellschaft unrealistisch⁹.

7. Vgl. den Hinweis zum EBook-Angebot des Springer-Verlags: „What is Springer’s policy regarding Inter-Library Loan (ILL)? Authorized users are allowed to output print copies of articles for postal or faxed fulfillment of ILL requests for academic, research, or other non-commercial libraries. Digital transmission of articles is not permitted.“ In: <http://springerlink.com/help/default.mpx> <07.11.2006>
8. Zusammenfassend dargestellt in einem fiktiven Briefwechsel in: Franken, Klaus: Die Zeitschriftenkrise. In: <http://www.ub.uni-konstanz.de/kops/volltexte/2004/1155/> <07.11.2006>
9. Weitere Informationen u.a. in: Flechsig, Norbert: Der Zweite Korb zur Verbesserung der Urheber- und Leistungsschutzrechte. In: ZRP 2006, H. 5, S. 145–149 (vgl. auch Beck-Online) Hilty, Reto: Das Urheberrecht und der Wissenschaftler. In: GRURInt 2006, H. 3, S. 179–190 (vgl. auch Beck-Online)

IN aller KUERZE

X-WiN: Verdoppelung der Anschlussgeschwindigkeit

Bereits knapp neun Monate nach Inbetriebnahme der neuen Generation X-WiN des deutschen Wissenschaftsnetzes konnte der DFN-Verein die in die neue Netzkonzeption gesetzten Erwartungen erfüllen und die erzielten Effizienzgewinne in Form einer Verdoppelung der Anschlussgeschwindigkeit bei gleichbleibenden Kosten an seine Nutzer weitergeben. So ist auch die Kath. Universität Eichstätt-Ingolstadt seit dem 12. Oktober 2006 mit der verdoppelten Anschlussgeschwindigkeit von 100 Mbit/s in das deutsche Wissenschaftsnetz X-WiN und damit in das weltweite Internet integriert, ohne dafür einen Euro mehr als bisher zahlen zu müssen.

Erweiterung des Service-Angebotes des URZ

Eifrigen Nutzern des Mail-Systems der KU wird es schon aufgefallen sein: das Universitätsrechenzentrum bietet seit etwa einem halben Jahr seinen Nutzern einen neuen Service an. Jeweils 30 Tage, 10 Tage oder 3 Tage vor Ablauf der Gültigkeit des Passwortes oder der Kennung erhält der Nutzer eine Mail auf sein email-Konto an der KU. In der automatisch erstellten elektronischen Post wird man zum Einen auf den Ablauf des Passwortes (der Kennung) hingewiesen und zum Anderen erhält der Anwender Hinweise, wie das Passwort geändert und somit verlängert werden kann bzw. was man tun kann um die Kennung zu verlängern. Unglücklicherweise nutzen nicht alle, die eine Kennung an der KU haben das hauseigene Mail-System – sei es aus Unkenntnis, obwohl wir in den Einführungskursen explizit darauf hinweisen, sei es aus Unwillen, sich mit weiteren Neuerungen bekannt zu machen – so dass die Hinweise auf dem Mail-Server brach liegen. Wir haben daher die Möglichkeit der Weiterleitung von Mails geschaffen. Dazu gibt man während der üblichen Öffnungszeiten der Sekretariate seine bevorzugte Mail-Adresse an. Es liegt in der Eigenverantwortung des Anwenders dafür zu sorgen, dass die genannte Adresse existiert, solange die Umleitung aktiv ist, und dass die Mailbox nicht voll ist.

Publikation zum Thema Einsatz digitaler Medien an der KU

Im Juni 2005 veranstaltete der Arbeitskreis „Digitale Medien in der Lehre“ einen hochschulweiten Anwendertag „Lehren und Lernen mit Neuen Medien“. Das Ergebnis wurde in einem Tagungsband zusammengefasst und gibt einen Einblick in den Einsatz von rechner- bzw. netzbasierten Medien in der Lehre an der KU. Es werden erprobte und innovative Projekte sowie theoretische Perspektiven in den Bereichen „E-Learning“, virtuelle Lehre und „Blended Learning“ aufgezeigt. Die Beiträge wurden im wesentlichen von Mitgliedern der Fakultäten und des Universitätsrechenzentrums aber auch von externen Autoren verfasst.

Michael Klebl, Michael Köck (Hg.):
Projekte und Perspektiven im Studium Digitale, Neue Medien an der Katholischen Universität Eichstätt-Ingolstadt,
Bd. 3, 2006, 192 S., 16.90 EUR,
ISBN 3-8258-9635-8

Landeslizenz für SPSS

Nachdem die SPSS Software GmbH mit der Version 14 von SPSS eine strenge Auslegung ihrer Lizenzbestimmungen verbunden hat, waren wir im Universitätsrechenzentrum der KU mit unserem Vertrag insbesondere nicht mehr in der Lage, SPSS 14.0 für Windows als Netzlizenz anzubieten und damit z.B. auf allen Pool-PCs. Kulanterweise hat man uns übergangsweise die Weiterverwendung von SPSS 13.0 erlaubt. Nachverhandlungen über Netzlizenzen für SPSS 14.0 haben ergeben, dass wir einen nicht unerheblichen Betrag mehr hätten bezahlen müssen, um den gleichen Standard auch in Zukunft allen Nutzern in unserem LAN zur Verfügung stellen zu können.

Da wir natürlich nicht allein betroffen waren, haben sich die bayerischen Universitätsrechenzentren untereinander abgestimmt und in den Verhandlungen mit der SPSS Software GmbH einen Lizenzvertrag erreicht, bei dem das Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) die Verteilerrolle für alle

interessierten Anderen übernimmt, also so etwas wie eine Landeslizenz.

Dieser neue Vertrag bringt uns unbestrittene Vorteile. Zum einen müssen wir jetzt nur noch etwa die Hälfte von dem bezahlen, was im Rahmen unseres alten Vertrags verlangt wurde. Zum anderen haben wir nun SPSS 14.0 auch als Netzlizenz zur Verfügung, wobei zu den bisher verfügbaren Modulen *Base*, *Regression Models*, *Advanced Models*, *Tables*, *Trends*, *Categories*, *Conjoint* und *Exact Tests* noch *Missing Value Analysis* dazugekommen ist. Auch die Standalone-Produkte *AMOS 6.0*, *AnswerTree 3.1* und *Data Entry 4.0* können wir auf Wunsch zur Verfügung stellen. Neu hinzugekommen ist dabei noch das Produkt *Sample Power 2.0*. Und die Einzelplatzlizenzen, die wir gegen eine Gebühr von derzeit 55 Euro pro Lizenzperiode an Mitarbeiter und Studierende der KU weitergeben dürfen, sind um einige Module erweitert worden. Hier sind nun alle oben erwähnten in SPSS 14.0 integrierten Module sowie auf Wunsch auch AMOS 4.0 enthalten.

Online-Anmeldung an der VHB

Seit August 2006 ist es möglich, dass sich Studierende der KU online an der Virtuellen Hochschule Bayern (www.vhb.org) registrieren können. Das heißt, dass sich jeder eingeschriebene Student, der eine Benutzerkennung im Universitätsrechenzentrum besitzt, über den Link <https://www.vhb.org/kurskatalog/studierende/registrierung/registrieren.asp> an

der VHB anmelden kann. Bei der Anmeldung gibt der Studierende die üblichen persönlichen Daten an und bestätigt durch die Eingabe von Benutzerkennung und Passwort, dass er der KU angehört. Bereits an der VHB angemeldete Studenten brauchen dies jedoch nicht mehr zu tun. Durch diese Lösung entfällt das bislang notwendige Verschicken der Anmeldeunterlagen auf dem Postweg.

Ansprechpartner an der KU: Prof. Dr. Bartosch (Tel. 1264, Ulrich.Bartosch@ku-eichstaett.de)

Tutor e.V.

Der studentische Verein Tutor e.V. (<http://www.tutor-ev.de/ueber.html>), der lehrveranstaltungs begleitende Übungen (sog. Tutorien) zum Lehrstoff der Wirtschaftswissenschaftlichen Fakultät und Veranstaltungen zur Persönlichkeitsbildung für Studierende an der WWF durchführt, hat aus seinen Mitteln dem Universitätsstandort Ingolstadt 2 Accesspoints für den WLAN-Empfang im Obstgarten der WWF und im Aufenthaltsraum EG Neubau (WWF) sowie einen tragbaren Beamer NEC LT 25 (DLP) gespendet. Diese Mittel kommen dadurch allen Studierenden der WWF zugute.

Herzlichen Dank für die großzügige Spende! Danke auch Herrn Schödl und seinem Team, das die schwierige Montage durchgeführt hat und hohe Montagekosten einsparen half!

Veranstaltungen des Universitätsrechenzentrums Sommersemester 2007

Im Sommersemester 2007 werden seitens des Universitätsrechenzentrums die folgenden Veranstaltungen angeboten:

IN EICHSTÄTT:

Für jeden Kurs ist eine Anmeldung im Sekretariat des Universitätsrechenzentrums (Raum: eO-109 mo-do von 9.00–11.30 und 14.00–15.30 Uhr bzw. Tel.: 08421/93-1462) bzw. über WorldWideWeb (<http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/kurse/>) erforderlich.

- 1. E-Learning mit der Lernplattform ILIAS
(speziell für Dozenten)** Ihrler
Ort: eO-112
Zeit: 14.02.2007 8.15–16.00 Uhr
Maximale Teilnehmerzahl: 15

Lernplattformen (Learning Management Systeme) wie ILIAS stellen eine komplette E-Learning-Infrastruktur zur Verfügung. In der Veranstaltung wird ein Überblick über die verschiedenen Möglichkeiten wie Lernmodule (auch eLAIX), Kommunikationswerkzeuge (Forum, Chat, ...), Bereitstellung von Dateien und Medien, Kursverwaltung (Planung, Anmeldung der Studierenden, Zugriffsrechte, ...) gegeben. Der Schwerpunkt wird das Erstellen bzw. Bereitstellen von vorlesungs- und seminarbegleitenden Materialien in ILIAS sein.

- 2. Datenanalyse mit SPSS für Windows
(Blockveranstaltung)** Dr. Tewes
Ort: eO-001
Zeit: 26.–30.03.2007 jeweils 8.15–11.45 und 14.00–16.30 Uhr
Maximale Teilnehmerzahl: 40

SPSS ist ein weitverbreitetes Statistik-Analysesystem, welches an der Kath. Universität in der Version SPSS für Windows zur Verfügung steht. In dieser Veranstaltung werden grundlegende Techniken zur Handhabung von SPSS für Windows vorgestellt. Neben der Dateneingabe und -bearbeitung stehen ausgewählte elementare statistische Prozeduren und Graphiken im Mittelpunkt.

- 3. Einführung in das Programmieren mit C++** P. Zimmermann
Ort: eO-001
Zeit: do 8.15–12.00 Uhr
Beginn: 19.04.2007
Maximale Teilnehmerzahl: 30

Die Programmiersprache C, die von Kernighan und Ritchie in Zusammenhang mit der Entwicklung des Betriebssystems Unix entworfen wurde, verfügt sowohl über assembler-ähnliche Sprachelemente, die ein hardwarenahes Programmieren ermöglichen, als auch über Kontrollstrukturen der modernen blockstrukturierten Sprachen, die ein systematisches, strukturiertes Programmieren unterstützen. Durch ein hohes Maß an Portabilität stehen Compiler für C/C++ auf nahezu allen Rechnertypen

mit den unterschiedlichsten Betriebssystemen zur Verfügung; C und vor allem die Weiterentwicklung C++, eine objektorientierte Programmiersprache, sind heute unentbehrliche Werkzeuge der Softwareentwickler.

In dieser Veranstaltung werden vornehmlich mit dem Borland C++ System (Version 4.5) auf den Windows2000-Workstations die Sprachelemente von C und C++ anhand von konkreten Beispielen vermittelt.

4. Kurzeinführung in SPSS

Dr. Tewes

Ort: eO-112

Zeit: 20.04.2007 8.15–11.45 Uhr

Maximale Teilnehmerzahl: 15

Diese Einführung richtet sich an alle, die im Rahmen einer wissenschaftlichen Arbeit empirisch arbeiten und somit Datenmaterial auswerten müssen. Vermittelt werden die Erfassung der Daten, die man z.B. aus einer Fragebogenaktion erhalten hat, und elementare Methoden zu deren Auswertung.

5. MS-Office-Anwendungen (PowerPoint, Excel, Word, Access)

Woitas

23.04.2007 PowerPoint

24.04.2007 PowerPoint für Fortgeschrittene

21.05.2007 Excel

22.05.2007 Excel für Fortgeschrittene

18.06.2007 Word für Fortgeschrittene

09.07.2007 Access

Ort: eO-001

Zeit: jeweils 8.15–11.30 Uhr

Maximale Teilnehmerzahl: 30

Microsoft PowerPoint ist ein Präsentationsgrafikpaket, mit dem Sie ansprechend formatierte Folienpräsentationen und Folien erstellen können. Es gibt umfangreiche Gestaltungsmöglichkeiten und Präsentationstechniken.

Das Tabellenkalkulationsprogramm Microsoft Excel ist ein Arbeitsmittel zur Planung von Berechnungen und Analyse von Daten. In Tabellen werden Texte, Zahlen und Formeln gespeichert, manipuliert und berechnet. Diese Daten können in Diagrammen schnell und anschaulich dargestellt werden.

MS Word ist das Textverarbeitungssystem von Microsoft. Dieser Kurs richtet sich an alle, die regelmäßig mit MS Word arbeiten und größere Dokumente effizienter gestalten möchten.

MS Access ist das relationale Datenbanksystem von Microsoft. Mit einer Datenbank können Daten erfasst, bearbeitet und nach verschiedenen Kriterien selektiert werden.

6. Erstellung von Web-Dokumenten mit Kontentor/Zope

Dr. Tewes

Ort: eO-112

Zeit: 11.05.2007 8.15–11.45 Uhr

Maximale Teilnehmerzahl: 15

Der Web-Auftritt der Kath. Universität basiert im Wesentlichen auf einem Content Management System. Die technische Basis hierfür stellen Kontentor und Zope dar. Hiermit wird es u.a. ermöglicht, die Seiten direkt im Browser zu bearbeiten oder zu erstellen. Im Rahmen dieser Einführungsveran-

staltung soll das Konzept erläutert werden und exemplarisch der Umgang mit dem System geübt werden.

7. $\text{T}_{\text{E}}\text{X}$ im täglichen Einsatz – Bibliographie P. Zimmermann

Ort: eO-112
Zeit: 29.05.2007 8.15–12.00 Uhr
Maximale Teilnehmerzahl: 15

Bibliographien/Literaturverzeichnisse stellen ein wesentliches Güte- und Bewertungskriterium jeder wissenschaftlichen Arbeit dar. Die im Kurs vorgestellten Komponenten des $\text{T}_{\text{E}}\text{X}$ -Systems bieten Autoren bei der Anfertigung solcher Verzeichnisse Unterstützung auf mehreren Ebenen an: (1) $\text{BibT}_{\text{E}}\text{X}$ liefert eine konsistente Zusammenstellung der Literatureinträge aus einer Datenbank und (2) geeignete Zitierbefehle sorgen für eine logische Stimmigkeit im Text.

8. Präsentationstechniken P. Zimmermann

Ort: eO-112
Zeit: 05.06./12.06./19.06./26.06./03.07.2007 jeweils 8.15–12.00 Uhr
Maximale Teilnehmerzahl: 15

Der Kurs richtet sich an alle, die Informationen effektiv präsentieren möchten. Nach einem Überblick über Präsentationstechniken liegt der Schwerpunkt auf dem Einsatz von computergestützten Medien. Versehen mit den nötigen Grundlagen zur visuellen Kommunikation stellt jeder Kursteilnehmer eine eigene Beamer-Präsentation mit einem Programm der eigenen Wahl – z.B. Microsoft PowerPoint oder $\text{T}_{\text{E}}\text{X}$ – her.

**9. E-Learning mit der Lernplattform ILIAS
(für Studierende und Dozenten)** Ihrler

Ort: eO-112
Zeit: 22./29.06.2007 jeweils 8.15–11.45 Uhr
Maximale Teilnehmerzahl: 15

Lernplattformen (Learning Management Systeme) wie ILIAS stellen eine komplette E-Learning-Infrastruktur zur Verfügung. In der Veranstaltung wird ein Überblick über die verschiedenen Möglichkeiten wie Lernmodule (auch eLAIX), Kommunikationswerkzeuge (Forum, Chat, ...), Bereitstellung von Dateien und Medien, Kursverwaltung (Planung, Anmeldung der Studierenden, Zugriffsrechte, ...) gegeben. Der Schwerpunkt wird das Erstellen bzw. Bereitstellen von vorlesungs- und seminarbegleitenden Materialien in ILIAS sein.

**10. Textverarbeitung und Publikation
wissenschaftlicher Texte mit $\text{T}_{\text{E}}\text{X}$
(Blockveranstaltung)** P. Zimmermann

Ort: eO-112
Zeit: 24.–26.07.2007 jeweils 08.15–12.00 und 14.15–18.00 Uhr
Maximale Teilnehmerzahl: 15

Das Publikationssystem $\text{T}_{\text{E}}\text{X}$ gehört zu den Textverarbeitungssystemen, bei denen der Gesamtprozess der Dokumentenanfertigung in die beiden Schritte Texterfassung und Satz/Umbruch aufgespalten ist. Zur Steuerung des Umbruchs werden bei der Texterfassung bestimmte Kommandos in den Text eingefügt. $\text{T}_{\text{E}}\text{X}$ verfügt über nahezu unbegrenzte Möglichkeiten der Satzgestaltung und bietet eine flexible automatische Handhabung von Fußnoten, Verweisen, Referenzen, Inhaltsverzeichnis

u.Ä. Insbesondere der professionelle Satz von Formeln oder spezieller Textzeichen (Diakritika u.Ä.) und fremder Alphabete (Arabisch, Griechisch, u.v.m.) sind herausragende Merkmale von $\text{T}_{\text{E}}\text{X}$. Neben einer reinen Druckversion kann auch leicht ein PDF- oder HTML-Format generiert werden. Damit eignet sich $\text{T}_{\text{E}}\text{X}$ vorzüglich für die Anfertigung wissenschaftlicher Texte, die in professioneller Satzqualität vorliegen sollen.

IN INGOLSTADT:

Für jeden Kurs ist eine Anmeldung im Sekretariat der Abteilung Ingolstadt des Universitätsrechenzentrums (Raum: HB-202 mo–fr von 8.30–11.00 Uhr bzw. Tel.: 0841/937-1887) bzw. über WorldWideWeb (<http://www.ku-eichstaett.de/Rechenzentrum/dienstleist/kurse/>) erforderlich.

1. Statistische Datenanalyse mit SPSS Brandel

Ort: HB-U03
Zeit: mo 16.00–18.00 Uhr
Beginn: 16.04.2007
Maximale Teilnehmerzahl: 20

SPSS ist ein weitverbreitetes Statistik-Analysesystem, welches an der Kath. Universität in der Version SPSS für Windows zur Verfügung steht. In dieser Veranstaltung werden grundlegende Techniken zur Handhabung von SPSS für Windows vorgestellt. Neben der Dateneingabe und -bearbeitung stehen ausgewählte elementare statistische Prozeduren und Graphiken im Mittelpunkt.

2. Einführung in HTML Brandel

Ort: HB-U03
Zeit: 20.04.2007 8.30–12.00 und 13.00–15.30 Uhr
Maximale Teilnehmerzahl: 20

HTML (Hypertext Markup Language) ist eine Textmarkierungssprache für die Dokumente des WorldWideWeb. Wer im WWW Informationen veröffentlichen will (oder muss), dem schadet es nicht, sich zumindest Grundkenntnisse anzueignen, auch wenn diese speziell für die Pflege des Web-Auftritts der Kath. Universität dank der neuen technischen Basis (Zope) nicht mehr zwingend erforderlich sind. Dieser Kurs will nicht nur die wichtigsten Sprachelemente vermitteln, sondern auch in geeignete Software zur Erstellung von Dokumenten einführen und allgemeine Hilfen zur Gestaltung von Hypertext-Dokumenten geben.

3. Vertiefungskurs Word und Excel Kaltenbacher

Ort: HB-111
Zeit: di 10.15–11.30 Uhr
Beginn: 24.04.2007
Maximale Teilnehmerzahl: 20

Die Grundkenntnisse in den beiden Office-Produkten werden durch weiterführende Themen vertieft, dabei gehe ich vor allem bei WinWord auf die Gestaltung von Briefen und Dokumenten ein (DIN 5008, Verzeichnisse und Indizes, Fuß- und Endnoten, Zentraldokument, Formeln, Makros usw.), bei Excel lege ich den Schwerpunkt auf die Verbreiterung des Wissens bei der Gliederung von Tabellen, Pivot-Tabellen, dem Arbeiten mit Matrizen, Methoden der Datenanalyse, Makros und dem (grundlegenden) Programmieren mit VBA.

Lieber Leser,

wenn Sie **INKUERZE** regelmäßig beziehen wollen, bedienen Sie sich bitte des unten angefügten Abschnitts.

Hat sich Ihre Anschrift geändert oder sind Sie am weiteren Bezug von **INKUERZE** nicht mehr interessiert, dann teilen Sie uns dies bitte auf dem vorbereiteten Abschnitt mit.

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

Vielen Dank!

Redaktion **INKUERZE**

An die
Redaktion
INKUERZE
Rechenzentrum der
Kath. Universität
Eichstätt-Ingolstadt
85071 Eichstätt

Absender:

Name: _____

Fakultät: _____

Straße: _____

Außerhalb der Universität: _____

Bitte deutlich lesbar in Druckschrift ausfüllen!

Ich bitte um Aufnahme in den Verteiler.

Bitte streichen Sie mich aus dem Verteiler.

Meine Anschrift hat sich geändert.

Alte Anschrift: _____

Ich bin damit einverstanden, dass diese Angaben in der **INKUERZE**-Leserdatei gespeichert werden (Art. 4 Abs. 1 Nr. 2 BayDSG).

(Datum)

(Unterschrift)