Mitteilungen des Zentralen Informatikdienstes der Universität Wien
Mitteilungen des Zentralen Informatikdienstes der Universität Wien
1 06/1 06/1 06/1

vienna
university
computer
center

Comment

März 2006

Impressum / Offenlegung gemäß § 25 Mediengesetz:

Herausgeber & Medieninhaber:	Zentraler Informatikdienst der Universität Wien
Redaktion & Gestaltung:	Mag. Michaela Bociurko Katharina Lüthke Elisabeth Zoppoth
Adresse:	Zentraler Informatikdienst der Universität Wien Universitätsstraße 7, A-1010 Wien Tel.: 4277-14001 Fax: 4277-9140 eMail: comment.zid@univie.ac.at online: www.univie.ac.at/comment/
Druck:	Riegelnik, Wien
Grundlegende Richtung:	Mitteilungen des Zentralen Informatikdienstes

Gedruckt auf chlorfrei gebleichtem Papier – Auflage: 3 500 Stk. – ISSN: 1727-6071

Editorial

Liebe Leserin, lieber Leser!

Diesmal wollen wir Ihnen an dieser Stelle eine personelle Veränderung in der Redaktion bekannt geben: Anfang Dezember 2005 ist **Katharina Lüthke**, die bisher im *Supportbüro Neue Medien* des ZID tätig war, zum Redaktionsteam gestoßen. Katharina Lüthke hat ihr Studium der Angewandten Medienwissenschaft an der Technischen Universität Ilmenau (Thüringen) absolviert, ist nach einigen Zwischenstationen in Wien gelandet und hat die vorliegende *Comment*-Ausgabe bereits maßgeblich mitgestaltet. Wir freuen uns sehr, sie bei uns begrüßen zu dürfen. **Michaela Bociurko** bleibt glücklicherweise weiterhin in der Redaktion tätig, wird sich aber zukünftig vermehrt um die PR-Aktivitäten des ZID kümmern (siehe auch die folgende Notiz *Sagen Sie uns Ihre Meinung!*).

Elisabeth Zoppoth

Sagen Sie uns Ihre Meinung!

Evaluierung im Sommersemester 2006 geplant

Liebe LeserInnen,

als Redaktion des Zentralen Informatikdienstes möchten wir Sie stets aktuell und umfassend über unsere Services, Einrichtungen sowie diverse technische Neuerungen informieren. Zu diesem Zweck stellen wir Ihnen auch zahlreiche Dokumentations- und Informationsmaterialien, wie Anleitungen, Folder, Webseiten sowie den *Comment*, kostenlos zur Verfügung. Um dieses Angebot – ganz nach Ihren Wünschen – stetig zu verbessern und zu erweitern, planen wir im Sommersemester 2006 eine entsprechende Evaluierung unter Studierenden durchzuführen. Sollte also in den nächsten Monaten ein freundlicher Mitarbeiter des ZID an Sie herantreten und Sie bitten einen Fragebogen auszufüllen, so nutzen Sie doch diese Gelegenheit zur Mitgestaltung und Partizipation und teilen Sie uns Ihre Meinung mit.

Selbstverständlich freuen wir uns auch jederzeit über Feedback zu unserer Zeitschrift, zu unserem Webangebot und zu diversen anderen Dokumentationen – ob nun postalisch („Leserbrief"), als eMail an `redaktion.zid@univie.ac.at` oder auch als Posting im *Comment*-Board des ZID-Forums (`www.univie.ac.at/ZID/forum/`).

Herzlichen Dank bereits im Voraus für Ihre Mithilfe.

Michaela Bociurko

Inhalt

SPEICHERPLATZ ABSOLUT NOTWENDIG

Storage Area Network (SAN) löst Platzprobleme

Plattenplatz? Bitte warten!

Auf den verschiedenen Servern des Zentralen Informatikdienstes lagern große Mengen an Daten. Die genaue Zahl lässt sich schwer abschätzen; es sind aber sicher mehr als 20 Terabyte, und täglich werden es mehr. Der größte Brocken sind die Fileserver, aber auch die Mailserver beherbergen in Summe mehrere Terabyte an Daten (hauptsächlich Spam). Weitere Services mit großem Platzbedarf sind die Datenbanken der Universitätsverwaltung, die Webservices, die Lernplattform WebCT Vista und noch etliche andere.

Um diese Daten unterzubringen, sind die Server mit leistungsfähigen Platten-Subsystemen ausgerüstet. Allen diesen Plattensystemen ist eines gemeinsam: Sie sind stets zu klein. Ständig werden neue Platten hineingeschraubt, Plattensysteme umkonfiguriert und Daten hin und her geschaufelt. Trotzdem ist die Nachfrage immer größer als das Angebot. Besonders eklatant ist der Platzmangel im Bereich der Fileservices (siehe *Comment 05/1*, Seite 24 bzw. unter `www.univie.ac.at/comment/05-1/051_24.html`). Diese sind erfolgreicher, als uns lieb ist: Ständig werden wir mit – vollkommen verständlichen und legitimen – Wünschen nach Plattenplatz für Projekte konfrontiert, die wir nicht oder nur zum Teil erfüllen können. Es ist nicht abzusehen, dass die Nachfrage je nachlassen wird: Multimedia-Anwendungen werden immer wichtiger, und der Platzbedarf von Bild-, Audio- und Video-Daten kennt keine Grenzen.

Aus diesem Grund hat sich der Zentrale Informatikdienst zu einem radikalen Schritt – und einer Investition von mehreren Millionen Euro – entschlossen: All diese Plattensysteme werden durch ein einziges *Storage Area Network* (kurz SAN) ersetzt. Sobald dieses in Betrieb geht – das wird voraussichtlich im Herbst 2006 der Fall sein – sollte es mit den Platzproblemen für längere Zeit vorbei sein. Diese gute Nachricht ist die Kernaussage des vorliegenden Artikels; im Folgenden sind einige Hintergrundinformationen über Storage-Technologien, die Problematik der Verwaltung großer Datenmengen und die Funktionsweise eines Storage Area Network zu finden.

Massenspeichertechnologien – einst und jetzt

Plattenkapazität

Die Kapazität von Festplatten hat sich in den letzten Jahren durchschnittlich alle 18 Monate verdoppelt. Heute sind bereits Spitzenmodelle zu 500 GB erhältlich, Platten mit 250 GB sind weit verbreitet. Zum Vergleich: In einen IBM-Katalog aus dem Jahr 1998 werden 2,2 GB- und 4,5 GB-Platten angeboten, sowie – zu einem horrenden Preis – das neueste Topmodell mit 9,1 GB. Zehn Jahre davor war am EDV-Zentrum der Uni Wien ein Plattensystem IBM 3380 in Betrieb, das mehrere Schränke füllte. Es bestand aus 8 Platten mit je einem GB und weiteren 8 Platten mit je einem halben GB.

Schnittstellen

Während die prinzipielle Bauweise der Festplatten in praktisch allen Systemen gleich ist, gibt es essentielle Unterschiede bei den Schnittstellen: Diese definieren, auf welche Weise Daten zwischen den Platten und den angeschlossenen Computern ausgetauscht werden.

Im PC-Bereich ist ATA (*Advanced Technology Attachment*) die weitestverbreitete Schnittstelle. Von ATA gibt es mehrere Varianten; eine davon ist auch als IDE (*Integrated Disc Electronics*) bekannt. Im Server-Bereich hingegen wird hauptsächlich SCSI eingesetzt, das *Small Computer System Interface*. Von 1986 (SCSI 1) bis heute (Ultra-320) entstanden sehr viele Varianten des SCSI-Protokolls, wobei die Bandbreite kontinuierlich gesteigert wurde – von ursprünglich 5 MB/s auf 320 MB/s.[1)] Etliche dieser SCSI-Versionen sind nicht miteinander kompatibel, auch werden viele verschiedene Varianten von Steckern und Kabeln eingesetzt.

Sowohl SCSI als auch ATA sind *parallele* Schnittstellen, d.h. die Übertragungsrate wird dadurch erhöht, dass mehrere Bits gleichzeitig über mehrere Leitungen übertragen werden. Das wird allerdings mit wesentlichen Nachteilen erkauft (dickere und damit teurere Kabel, begrenzte Kabellänge), sodass in letzter Zeit wieder *serielle* Architekturen an Bedeutung gewinnen. Von IBM wurde die *Serial Storage Architecture* (SSA) entwickelt, die sich allerdings nicht durchsetzen konnte, sodass IBM die Entwicklung eingestellt hat. Seit einigen Jahren kommen immer mehr Platten mit *Serial ATA*-Schnittstellen (S-ATA) auf den Markt. Trotz des Namens hat S-ATA relativ wenig mit der parallelen Vorgängerversion gemeinsam.

Unter den neueren Entwicklungen sind vor allem zwei zu nennen: *Fibre Channel*, wo der Anschluss über ein Glasfaserkabel erfolgt und Bandbreiten bis zu 4 Gbit/s möglich sind, und *iSCSI*, das SCSI über IP(*Internet Protocol*)-Netze transportiert.

1) Damit ist die Entwicklung von SCSI am Ende angelangt: Der ursprünglich geplante Ultra-640-Standard mit 640 MB/s wird nicht mehr weiterverfolgt.

Zugriffszeiten und Performance

Während die Kapazitäten und die Busgeschwindigkeiten enorm gewachsen sind, gab es bei den Umdrehungsgeschwindigkeiten der Festplatten nur bescheidene Fortschritte. PC-Festplatten rotieren üblicherweise mit 5400 bis 7200 Umdrehungen pro Minute. Im Serverbereich werden auch Platten mit 10000 und 15000 Umdrehungen eingesetzt, letztere sind schon sehr teuer. Allzu große Fortschritte sind hier auch nicht zu erwarten.

Zwei Kenngrößen charakterisieren die Leistungsfähigkeit einer Festplatte: Einerseits die Datenmenge, die pro Sekunde geschrieben bzw. gelesen werden kann („Datendurchsatz"; dieser liegt bei etlichen Megabyte pro Sekunde, Spitzenmodelle bringen es auf 100 MB/s und mehr), andererseits die Zugriffszeit („Latenz"), für welche die Umdrehungsgeschwindigkeit ausschlaggebend ist: Um ein bestimmtes Datenelement zu lesen oder zu schreiben, muss im ungünstigsten Fall eine volle Umdrehung abgewartet werden, bis die entsprechende Position der Festplatte am Lese-/Schreibkopf vorbeikommt. Bei den schnellsten Platten entspricht das vier Millisekunden. Zum Vergleich: Bei Hauptspeicher (RAM) liegen die Zugriffszeiten im Bereich von wenigen Nanosekunden, RAM-Zugriff ist also fast eine Million Mal so schnell.

Um trotz dieser langen Zugriffszeiten eine akzeptable Performance zu erreichen, werden verschiedene Techniken eingesetzt; die wichtigsten davon sind *Caching* und *Striping*. Caching bedeutet, dass Daten nicht sofort auf Platte geschrieben, sondern in wesentlich schnelleren Speichern (*Disk Caches*) zwischengelagert werden; nach einer gewissen Verzögerung werden dann größere Datenmengen auf einmal geschrieben, was wesentlich effizienter ist. Beim Striping werden einzelne Dateien bzw. Filesysteme auf mehrere Platten verteilt, um einen höheren Datendurchsatz zu erreichen.

Haltbarkeit

Die elektronischen Bauteile eines Computers wie CPU und Hauptspeicher sind ziemlich unverwüstlich und werden nur selten defekt – wenn überhaupt, dann meistens als Folgeschäden (z.B. durch Überhitzung infolge eines defekten Lüfters). Die schnell rotierenden Platten sind jedoch hohen mechanischen Belastungen ausgesetzt. Die Lebensdauer von Platten ist begrenzt; in einem Betrieb wie dem ZID, wo mehr als tausend Platten im Einsatz sind, kann man mit Sicherheit damit rechnen, dass von Zeit zu Zeit einige davon den Geist aufgeben.

Es gibt verschiedene Techniken, um Betriebsunterbrechungen und vor allem Datenverlust durch defekte Platten zu vermeiden. Die wichtigste davon ist RAID, *Redundant Array of Inexpensive Disks* (alternativ wird das I manchmal als *Independent* gedeutet). Es gibt verschiedene Varianten (*Level*) von RAID; welche im Einzelfall die beste ist, hängt von den Anforderungen an Datensicherheit und Performance ab, sowie davon, wie viel Bruttokapazität man zu opfern bereit ist. Die am häufigsten verwendeten RAID-Level sind RAID 1 und RAID 5. Bei RAID 1, auch *Mirroring* genannt, werden alle Daten auf zwei physischen Platten gespeichert, sodass der Ausfall einer der beiden Platten mit keinem Datenverlust verbunden ist. Bei RAID 5 werden die Daten auf mehrere Platten (mindestens drei, üblicherweise aber mehr) verteilt und zusätzliche *Paritätsdaten* geschrieben. Mit Hilfe dieser Paritätsinformationen lassen sich die Daten jeder Platte aus den Daten aller anderen Platten des RAID-Set rekonstruieren. Der Ausfall einer Platte führt daher zu keiner Betriebsunterbrechung und zu keinem Datenverlust. Die oben beschriebene Technik des Striping wird manchmal als RAID 0 bezeichnet, trägt aber natürlich nichts zur Datensicherheit bei.

Der Plattenbestand der Server des Zentralen Informatikdienstes

Ein Rundgang durch die Serverräume des ZID gleicht einem Besuch in einem Museum der Storage-Technologien der letzten Jahre: Von den oben beschriebenen Technologien sind dort praktisch alle zu finden. Etliche Jahre lang waren SSA-Platten sehr beliebt, die trotz des höheren Preises gegenüber SCSI deutliche Vorteile hatten. Aber auch verschiedene RAID-Systeme auf SCSI-Basis werden eingesetzt, in letzter Zeit immer mehr RAID-Systeme auf Fibre Channel-Basis sowie für geringere Ansprüche auch IDE-RAID. Praktisch alle Plattensysteme sind redundant ausgelegt – für große Datenmengen wird meistens RAID 5 eingesetzt, besonders wichtige Daten (z.B. die Datenbanken der Universitätsverwaltung) werden gespiegelt (RAID 1). Diese Maßnahmen haben sich bewährt: In den letzten Jahren gab es viele defekte Platten am Zentralen Informatikdienst, wobei die meisten Ausfälle keinerlei Auswirkungen auf den Betrieb hatten. Nur in seltenen Fällen entstanden durch Plattendefekte Betriebsunterbrechungen; Datenverlust durch Hardware-Schäden kam nicht vor. Dennoch wird in Zukunft noch wesentlich mehr in die Vorbeugung von Datenverlust investiert werden, vor allem im Hinblick auf Katastrophenfälle (Brand, Hochwasser usw.).

Es mag überraschen, wie klein die in vielen Server-Systemen eingesetzten Platten sind. Einerseits liegt das daran, dass im Server-Bereich mehr Gewicht auf Verlässlichkeit gelegt wird, sodass neue, größere Plattengenerationen erst später auf den Markt kommen. Andererseits liegt das am Durchschnittsalter der Server: Die Lebensdauer eines Servers beträgt meistens zwischen drei und fünf Jahren, dann ist ein Austausch auf ein leistungsfähigeres System erforderlich. Die alten Server werden üblicherweise nicht sofort verschrottet, sondern für weniger anspruchsvolle Aufgaben, Testsysteme usw. eingesetzt. Beispielsweise dient ein Server, der 1998 für DCE angeschafft wurde, seit 2003 als Applikationsserver für *UNIVIS online* (`www.univie.ac.at/uvo/`). Die Platten älterer Server sind entsprechend kleiner: Der erwähnte Server hat vier Platten zu je 4,5 GB; es sind auch

noch etliche Plattensysteme mit 9 GB- und 18 GB-Platten im Einsatz.

Die derzeitige Massenspeicherausstattung des Zentralen Informatikdienstes hat einige gravierende Nachteile:

- Zu geringe Kapazitäten und chronischer Platzmangel;
- hoher „Verschnitt" durch ungenutzte Kapazitäten auf Servern mit geringerem Platzbedarf;
- Performance-Probleme, speziell auf Servern mit relativ geringem Platzbedarf, aber vielen Lese- und Schreiboperationen, die auf wenige Platten konzentriert sind (z.B. bei manchen Datenbanken);
- hoher Wartungsaufwand und geringe Flexibilität aufgrund der Inkompatibilität der verschiedenen Storage-Systeme.

Was ist ein SAN?

Die Grundidee eines SAN (*Storage Area Network*) ist es, den Massenspeicher physisch von den Servern zu trennen und alle Komponenten über ein Netzwerk – üblicherweise Glasfaser – miteinander zu verbinden.

SAN-Komponenten

- **Ein (oder mehrere) Storage-System(e)**: Die Platten in diesen Systemen beruhen meist auf Fibre Channel-Technologie; für weniger hohe Ansprüche wird auch S-ATA eingesetzt. Große Caches sorgen für entsprechende Performance. Alle Komponenten sind von höchster Qualität (und entsprechend teuer): Prozessoren, Caches, Netzteile usw. sind redundant ausgelegt.
- **Die erforderliche Netzwerk-Infrastruktur**: Diese besteht neben der Glasfaser-Verkabelung aus speziellen Switches; besonders leistungsfähige Switches nennt man *Direktoren*. Ein in sich geschlossener Bereich eines solchen Netzwerks wird als *Fabric* bezeichnet (engl. für „Gewebe").
- Der **Anschluss der Server (Hosts)** an das Storage-Netzwerk erfolgt über so genannte *Host Bus Adapter*.
- Neben der Hardware ist auch die **Software zur Administration** ein wichtiger Bestandteil eines SAN: Diese ermöglicht die Konfiguration von verschiedenen RAID-Sets, die Definition von Teilen eines RAID-Sets als LUNs (*Logical Units* – virtuelle Platten), die Zuweisung von LUNs zu Hosts usw.

Ein Beispiel einer typischen SAN-Konfiguration ist in Abb. 1 zu sehen. Das Netzwerk besteht aus zwei getrennten Fabrics (mittels durchgezogener bzw. gestrichelter Linien dargestellt). Je nach Anforderungen an die Ausfallssicherheit sind Server über eine oder beide Fabrics angeschlossen. Der mit S_1 bezeichnete Server mit seinen Daten in D_1 ist gegen alle Arten von Ausfall gesichert: Nicht nur den Ausfall einer Fabric (z.B. durch eine Fehlkonfiguration oder einen defekten Switch) übersteht er unbeschadet; selbst im Katastrophenfall, wenn einer der beiden Standorte komplett zerstört werden sollte, kommt es zu keiner Unterbrechung – die Daten sind am anderen Standort in D_2 gespiegelt, und der Server S_2 kann automatisch die Aufgaben von S_1 übernehmen.

Vorteile

- **Ausfallsicherheit**: Wie im obigen Beispiel beschrieben, kann ein SAN hoch ausfallsicher konfiguriert werden. Wichtig für die Katastrophenvorsorge ist, dass sich ein solches Storage-Netzwerk auch über große Entfernungen erstrecken kann. Distanzen von einigen Kilometern sind überhaupt kein Problem, mit speziellen Technologien ist auch wesentlich mehr möglich. Beispielsweise haben viele US-amerikanische Firmen ein SAN, das Rechenzentren an der Ost- und der Westküste miteinander verbindet.
- **Performance**: Viele Faktoren tragen zu der hohen Performance bei, die mit SAN-Systemen erreicht werden kann: Schnelle Platten mit bis zu 15000 Umdrehungen pro Minute; bis zu 4 Gbit/s Bandbreite im Netzwerk; sehr große Caches; die Möglichkeit, Lese- und Schreiboperationen auf viele Platten zu verteilen. Durch Kombination von Filesystemen mit hohen Anforderungen (z.B. Datenbanken) und wenig belasteten Filesystemen wie Archiven lässt sich eine gleichmäßige Auslastung erreichen.
- **Flexibilität**: In einem großen Betrieb mit vielen Servern wie dem ZID ändert sich der Massenspeicherbedarf der einzelnen Server ständig. Mit einem SAN können die erforderlichen Anpassungen der Konfiguration wesentlich einfacher, schneller, komfortabler und meistens ohne Hardware-Umbauten durchgeführt werden.
- **Features**: Hochwertige Storage-Systeme haben etliche Funktionen, die weit über das hinausgehen, was z.B. mit preiswerten RAID-Systemen möglich ist. Ein Beispiel sind *Snapsbots*, womit in Sekundenbruchteilen eine „Momentaufnahme" einer (logischen) Platte erstellt werden kann. Solche Snapshots werden unter anderem zur Datensicherung eingesetzt.

Nachteile

- Ein Storage Area Network ist teuer. Auch wenn durch bessere Ausnutzung und das Vermeiden von Verschnitt einiges eingespart werden kann, sind die Kosten pro Terabyte deutlich höher als bei konventionellen Speichersystemen. Berücksichtigt man jedoch auch Nebenkosten wie Personalaufwand usw. (*Total Cost of Ownership* – TCO), so schneidet ein Storage Area Network häufig besser ab.

- Auch wenn es in Summe weniger Aufwand ist, ein einziges großes SAN zu administrieren als viele kleine Einzelsysteme, so ist die Konfiguration und Administration eines solchen Netzwerks keine triviale Aufgabe und erfordert einiges an Know-how.

- Ein solide konzipiertes Storage Area Network vermeidet alle *Single Points of Failure* (SPOFs) und ist daher hoch ausfallsicher; dennoch lassen sich bei keinem System der Welt Ausfälle hundertprozentig ausschließen. Bei stark zentralisierten Storage-Systemen können die Auswirkungen von Hardware-Schäden oder Konfigurationsfehlern gravierender sein als bei mehreren kleineren Einzelsystemen.

Die neue Storage-Lösung des ZID

Die Anschaffung des geplanten Storage-Systems erfolgt über eine EU-weite Ausschreibung, die am 7. Februar 2006 veröffentlicht wurde. Die Angebotseröffnung erfolgt am 31. März 2006. Die Bewertung der Angebote muss spätestens am 30. Juni 2006 abgeschlossen sein; es ist jedoch damit zu rechnen, dass der Zuschlag schon wesentlich früher erfolgen kann.

Im Leistungsverzeichnis der Ausschreibung wurden nur die wichtigsten Eckdaten spezifiziert – die Details bleiben den Anbietern überlassen:

- Das neue Storage-System muss über eine Gesamtkapazität von 200 TB brutto verfügen.

- Das System wird auf zwei getrennte Standorte verteilt. Der primäre Standort ist einer der Systemräume des ZID im Neuen Institutsgebäude; für den sekundären Standort wird ein Raum im Universitäts-Hauptgebäude adaptiert, der früher als Öltank diente.

- Es werden verschiedene Storage-Klassen mit unterschiedlichen Anforderungen an Performance und Ausfallsicherheit definiert. Ein kleiner Teil dient für kritische Daten – beispielsweise die Oracle-Datenbanken der Universitätsverwaltung – und muss hochperformant und ausfallsicher sein (Mirroring über beide Standorte, zwei getrennte Fabrics).

- Das derzeitige Backup-System des ZID (siehe `www.univie.ac.at/ZID/backup/`) stößt bereits an die Grenzen seiner Leistungsfähigkeit und ist für die Sicherung der Daten des neuen Storage-Systems auf jeden Fall zu klein. Deshalb wird auch ein neues Backup-System ausgeschrieben.

Falls Sie für ein Projekt ein Terabyte Platz am Fileserver haben wollen, müssen wir Sie derzeit noch enttäuschen. Wir bitten aber um etwas Geduld: Bis zum nächsten Winter wird sich das ändern.

Peter Marksteiner ■

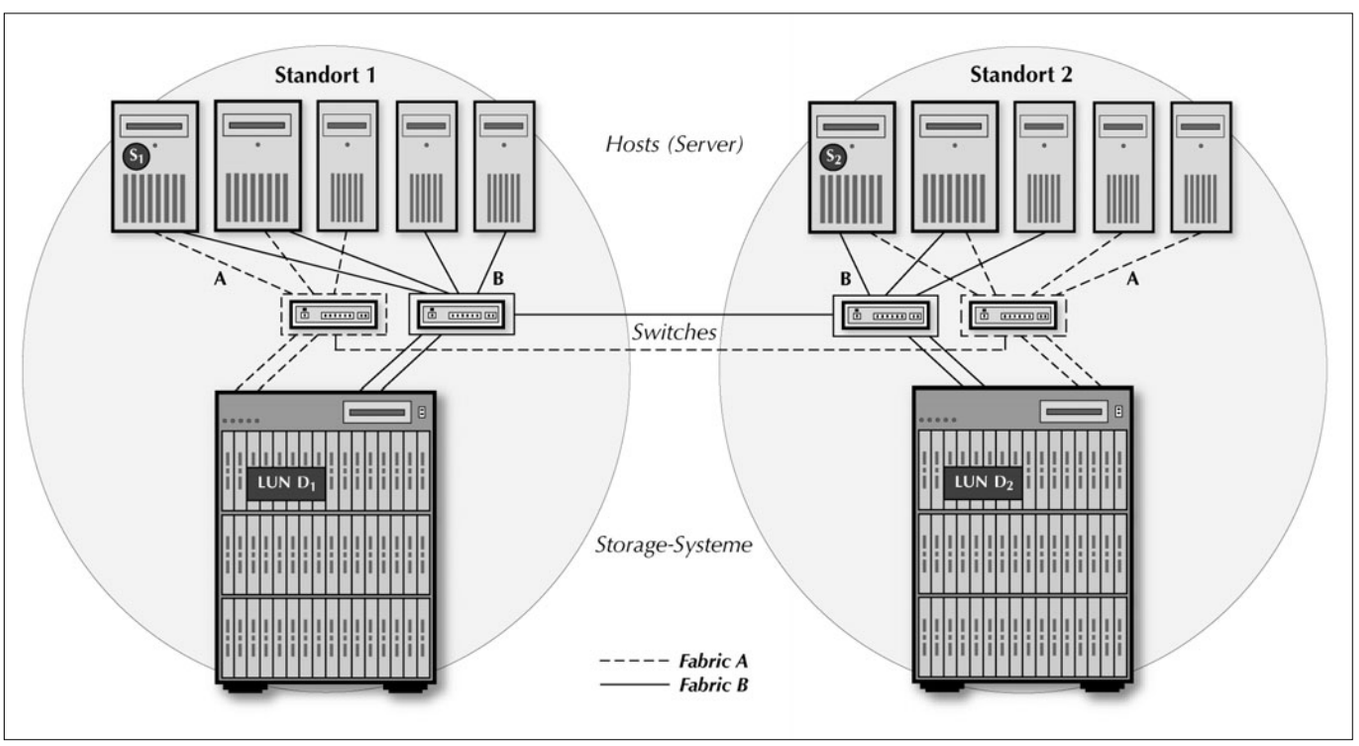


Abb. 1: In diesem Beispiel werden mehrere Maßnahmen zur Ausfallsicherheit illustriert: Zwei getrennte Fabrics; Verteilung auf zwei Standorte; RAID: die zum Server S_1 gehörenden Daten sind über beide Standorte gespiegelt (*Remote Mirroring*); zusätzlich sind die beiden LUNs (*Logical Units*) physisch innerhalb eines Storage-Systems über mehrere Platten verteilt (RAID 5). Die Server S_1 und S_2 bilden gemeinsam einen Cluster, sodass auch der Ausfall eines der beiden Server zu keiner Betriebsunterbrechung führt.

ARTGERECHTE SERVER-HALTUNG
SERVERHOUSING AM ZID

Es war einmal ein kleiner Server, der fristete sein Dasein in einem dunklen, staubigen Winkel eines Institutsbüros. Seine unmittelbaren Nachbarn – eine halb vertrocknete Grünpflanze, einige alte Kartons, zwei Abfalleimer und ein wackeliger Sessel, der meistens unter Ordnern und Papieren begraben war – drängten den armen kleinen Server im Laufe der Zeit immer weiter in die Ecke, bis sein Aufenthaltsort schließlich nur noch demjenigen Menschen bekannt war, der ihm ab und zu ein neues Bauteil zusteckte. Das war jedoch ein seltenes Vergnügen – meistens musste sich der Server mit dem Allernotwendigsten zufrieden geben: Seine Strom-Ration kam aus einer Steckdose, die gleichzeitig auch eine Kaffeemaschine, eine Schreibtischlampe und ein Radio zu versorgen hatte, und sein Netzwerkanschluss war gerade schnell genug, um die Datenpakete zumindest in ruhigen Zeiten einigermaßen pünktlich ausliefern zu können.

Aber nicht genug damit, dass der Server ohne jegliche Zuwendung dahinvegetieren musste, sein Leben steckte auch voller Gefahren: Wenn Besucher kamen, wurden die Papierstapel vom Gästesessel kurzerhand dem Server aufgeladen, der unter dem zusätzlichen Gewicht ächzte. Wenn die Putzfrau kam und den Staub in seinem Winkel aufwirbelte, litt er unter Atembeschwerden. Wenn der Sommer kam, stöhnte er unter den maschinenunwürdigen Temperaturen im Büro. Wenn die Topfpflanze neben ihm gegossen wurde, erhielt mitunter auch der Server eine kleine Dusche. Hin und wieder stolperte jemand über seine Kabel, sodass ihm ganz schwarz vor den Augen wurde. Einmal hatte sich sogar ein Unbekannter heimlich an ihn herangemacht und versucht, ihm einige Teile zu stehlen; das konnte dann aber im letzten Moment von „seinem“ Büromenschen verhindert werden.

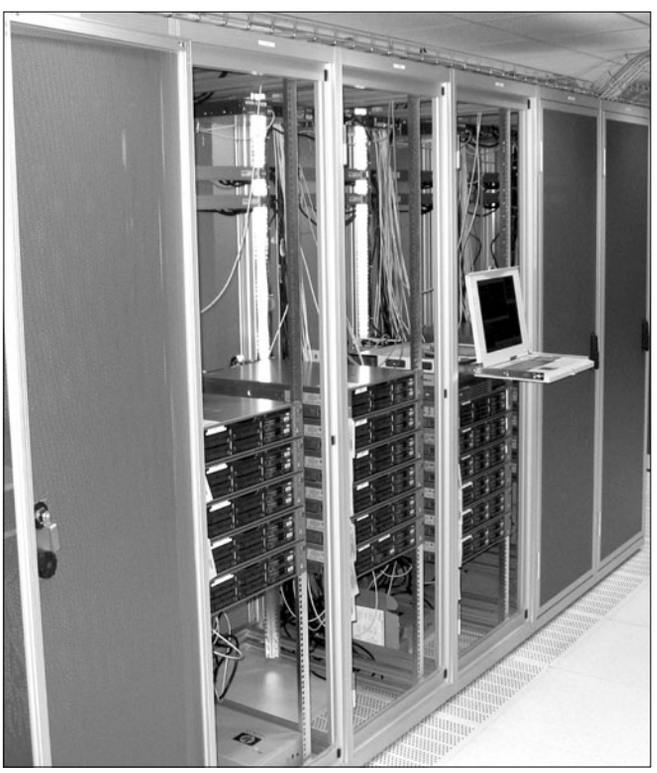
Trotz dieser Widrigkeiten verrichtete der kleine Server seine tägliche Arbeit ohne zu murren, so gut er es eben konnte – bis er eines Tages ohne Vorwarnung vom Netz genommen wurde. Als er wieder zu sich kam, glaubte er zu träumen: Er befand sich nicht länger in seiner gewohnten Ecke, sondern vielmehr in einer Art Schrank in einem großen, hellen Raum. Die Luft war angenehm temperiert und erfüllt von einem sympathischen Rauschen. Als der Server entdeckte, dass dieses Geräusch von Artgenossen stammte, fiel er vor Aufregung fast aus dem Schrank. „Wo bin ich denn hier?“ piepste er schüchtern. „Du bist in einem Serverraum des ZID“, brummte ein dicker Rechner neben ihm. „Ein Serverraum? Nur für uns? Sowas gibt's?“, staunte der kleine Server. „Na klar“, sagte der Dicke. „Du bist wohl auch einer von denen, die bisher nicht viel zu lachen hatten, oder?“ „Kann schon sein“, räumte der kleine Server ein und streckte sich vorsichtig. War sein Netzwerkanschluss tatsächlich gewachsen? Ja wirklich – die Datenpakete flutschten durch die Leitung, dass es eine Freude war. Keine Bit-Staus mehr! „Habt ihr hier zufällig auch eine USV?“, fragte er seinen freundlichen Nachbarn. „Natürlich, was glaubst du denn? Unser Stromnetz ist dreifach abgesichert – das ist schließlich ein Serverraum!“ Der kleine Server konnte sein Glück kaum fassen. Und fortan war er fröhlich und zufrieden bis an sein Lebensende...

2004, an einem Universitätsinstitut: Stellplatz eines Fileservers für ca. 300 BenutzerInnen

Serverhousing?!

Server sollten rund um die Uhr erreichbar und infolgedessen gegen Ausfälle aller Art gut gesichert sein. Das bedeutet einerseits, dass der Zugriff auf einen Server beschränkt werden muss: Niemand außer den AdministratorInnen soll den Ausschaltknopf drücken, den Netzstecker ziehen oder die Konfiguration verändern können. Zum anderen braucht man für einen reibungslosen Betrieb auch eine geeignete technische Infrastruktur – eine Klimaanlage, eine unterbrechungsfreie Stromversorgung (USV) und einen Internetanschluss mit ausreichender Bandbreite – sowie qualifiziertes Personal für die Wartung dieser Infrastruktur. Insgesamt ist der Aufwand für den laufenden Betrieb eines Servers weitaus größer, als allgemein angenommen wird, was natürlich auch finanziell entsprechend zu Buche schlägt: Bei „artgerechter

Haltung“ kostet der Betrieb (berechnet auf einen Zeitraum von drei Jahren, inklusive Strom und Arbeitszeit) inzwischen oft mehr als der Rechner selbst. Begnügt man sich hingegen mit der Minimalvariante der Serverpflege, so riskiert man unerfreuliche Auswirkungen auf Leistungsfähigkeit und Lebensdauer des Rechners – und vor allem auch auf die Servicequalität.



2006, in einem Serverraum des ZID: EDV-Schränke (*Racks*), in denen jeweils mehrere Server untergebracht sind

Einen Ausweg aus diesem Dilemma bietet das so genannte Serverhousing. Dieser Begriff bezeichnet die Unterbringung „fremder“ Server in dedizierten Räumlichkeiten eines professionellen Rechenzentrums. Das Rechenzentrum stellt dabei den Standplatz für die Geräte, die (sicherheits)technische Infrastruktur sowie die Internetanbindung zur Verfügung; für Administration und Wartung der Server sind in der Regel weiterhin die jeweiligen BesitzerInnen zuständig. Diese Lösung hat den Vorteil, dass die Verantwortung für den Betrieb der Infrastruktur in den Händen von SpezialistInnen liegt, was für die Kunden eine erhebliche Entlastung darstellt.

Das ist auch der Hauptgrund dafür, dass der Zentrale Informatikdienst seit Beginn des Jahres 2006 den Universitätsinstituten ein solches Service anbietet. Das einleitende Märchen ist zwar stark überzeichnet, entbehrt aber nicht des berühmten Körnchens Wahrheit: An der Uni Wien existieren neben den „großen“ (d.h. universitätsweit verfügbaren) Mail-, Web-, File- und sonstigen Servern des ZID auch zahlreiche „kleine“ (dezentrale) Server an den Instituten und Dienststellen, die in der Regel deren spezielle Anforderungen abdecken sollen, aber leider nicht immer adäquat untergebracht werden können. Am Zentralen Informatikdienst hingegen sind sowohl die technische Ausstattung als auch das nötige Know-how für eine optimale Betreuung solcher Rechner vorhanden.

Serverhousing am ZID

Das Serverhousing des ZID ist für Institute und Dienststellen der Universität Wien kostenlos verfügbar; der Zentrale Informatikdienst behält sich jedoch vor, Anmeldungen ohne Angabe von Gründen abzulehnen oder zu beschränken.

Geboten werden:

- **Rack-Space:** Der Server erhält einen Stellplatz in einem speziellen EDV-Schrank (*Rack*). Die Racks sind für einbaufähige Serversysteme im 19“-Standard-Format geeignet – Desktop-PCs als Server-Hardware können daher nicht akzeptiert werden. Die in den Serverräumen untergebrachten Geräte müssen darüber hinaus auch bestimmten technischen Anforderungen des ZID genügen. Es empfiehlt sich, die Details möglichst schon vor dem Kauf der Rechner mit dem Zentralen Informatikdienst abzuklären.

- **Infrastruktur:** Für Strom-/USV-Anbindung, Klimatisierung und Brandschutz-Vorkehrungen (Handfeuerlöscher, Brandmelder mit Direktleitung zur Feuerwehr) sorgt der ZID. Alle Arbeiten, die die Infrastruktur der Serverräume betreffen, dürfen ausschließlich von MitarbeiterInnen des Zentralen Informatikdienstes vorgenommen werden.

- **Datennetz-Anbindung:** Standardmäßig werden die Server mit einer Bandbreite von 100 Mbit/s an das Datennetz angeschlossen; bei Bedarf kann diese Bandbreite auf 1 Gbit/s erhöht werden.

- **Zutrittskontrolle:** Die Serverräume verfügen über Sicherheitstüren, Spezialschlösser mit kodierten Schlüsseln und Kamera-Überwachung. Der Zugang ist nur für namentlich bekannte Personen mit schriftlicher Voranmeldung und nur in Begleitung eines ZID-Mitarbeiters möglich.

- **WLAN:** Ein Accesspoint in den Serverräumen ermöglicht bei Bedarf den drahtlosen Internetzugang mittels Notebooks und ähnlichen Geräten.

Lizenzverwaltung und Software-Wartung des Servers liegen vollständig in der Verantwortung des jeweiligen Instituts. Zusätzlich zum regelmäßigen Einspielen von Updates und Patches ist es ratsam, den Server mit entsprechenden softwaremäßigen Zugriffsbeschränkungen zu schützen, da unbefugte Manipulationen durch Dritte trotz aller Sicherheitsvorkehrungen des ZID nicht gänzlich ausgeschlossen werden können.

Die Software-Wartung sollte idealerweise via Datennetz (*remote*) erfolgen, um die Besucherfrequenz in den Serverräumen niedrig zu halten. Ein eigenes Konsolennetzwerk ermöglicht darüber hinaus den Remote-Zugriff auf die Serverkonsole. Sofern der Server Fernwartungsfunktionen – beispielsweise iLO (*integrated Lights-Out*) von HP – unterstützt, können daher auch „Notoperationen" wie z.B. Neustarts über das Netzwerk durchgeführt werden. Eine physische Anwesenheit der AdministratorInnen in den Serverräumen ist in diesem Fall nur mehr bei Hardware-Arbeiten erforderlich.

Die Hardware-Wartung ist ebenfalls Sache des Instituts; bei sicherheitsrelevanten Hardware-Mängeln – z.B. schadhafte Ventilatoren – kann der Zentrale Informatikdienst jedoch das Institut zu einer Behebung derselben auffordern. Wird dieser Aufforderung nicht Folge geleistet oder liegt ein anderer grober Verstoß gegen die Serverhousing-Richtlinien vor, drohen Sanktionen bis hin zur fristlosen Kündigung des Vertrags (im Normalfall beträgt die Kündigungsfrist drei Monate).

Zu guter Letzt sei noch ein kleines, aber nicht unwesentliches Detail erwähnt: Bei der Übersiedelung in die Serverräume wird dem Rechner vom Zentralen Informatikdienst eine IP-Adresse zugewiesen; der Server bleibt jedoch im Subnetz des jeweiligen Instituts. Sofern das Institut über eine Institutsfirewall verfügt, bleibt der Server somit auch hinter dieser Firewall.

Elisabeth Zoppoth ■

Weitere Infos & Kontakt

Genauere Informationen zu diesem neuen Angebot des Zentralen Informatikdienstes sowie die entsprechenden Richtlinien sind unter `www.univie.ac.at/ZID/serverhousing/` zu finden.

Bei Interesse oder bei Fragen wenden Sie sich bitte an die eMail-Adresse `serverhousing.zid@univie.ac.at`.

WER RUFT MICH? INVERSSUCHE MITTELS CTI

Die Möglichkeit, zu einem Namen eine Telefonnummer zu suchen, existiert, seit es Telefonbücher gibt – also seit mehr als hundert Jahren. Die Rückwärts- oder Inverssuche, bei der Namen und sonstige Daten von TeilnehmerInnen anhand der Telefonnummer gefunden werden, gibt es erst seit kurzer Zeit.

Das hat keine technischen, sondern rechtliche Gründe: In Österreich ist die Inverssuche erst seit dem 20. August 2003 gestattet; an diesem Tag trat das Telekommunikationsgesetz 2003 in Kraft. Ausdrücklich erlaubt wird die Inverssuche auch hier nicht, aus der etwas umständlichen Formulierung des § 69 lässt sich allerdings implizit eine solche Erlaubnis entnehmen:

Abb. 1: CTI-Teilnehmerauskunft aus dem Herold-Telefonbuch

§ 69 (5) Sofern dies ein Teilnehmer wünscht, hat die Eintragung der ihn betreffenden Daten in das Teilnehmerverzeichnis ganz oder teilweise zu unterbleiben (Nichteintragung). Dafür darf kein Entgelt verlangt werden. Sofern dies ein Teilnehmer wünscht, hat die Eintragung der ihn betreffenden Daten in ein elektronisches Teilnehmerverzeichnis, das die Suche anhand anderer Daten als anhand des Namens des Teilnehmers ermöglicht, zu unterbleiben.

Mehrere Telekom-Anbieter und Auskunftsdienste bieten in Österreich eine solche Inverssuche an, beispielsweise mittels Mehrwert-SMS.

CTI und Herold – ein starkes Team

Bisher gab es im *Computer Telephone Interface* der Universität Wien (CTI, siehe `www.univie.ac.at/ZID/cti/`) zwei Datenquellen für die angezeigten Namen: Einerseits das Online-Personalverzeichnis (`http://data.univie.ac.at/pers`) und andererseits das persönliche Adressbuch. Durch einen Vertrag mit der Herold Business Data GmbH (`www.herold.at`) konnte im Februar 2006 noch eine dritte Quelle angezapft werden.

Bei Verbindungen mit dem österreichischen Festnetz und mit zahlreichen österreichischen Mobilnetz-TeilnehmerInnen wird daher demnächst in der Anrufliste der entsprechende Eintrag aus dem Datenbestand von Herold erscheinen. Die Daten werden einmal pro Monat aktualisiert werden. Durch diese Neuerung gewinnt das CTI nochmals deutlich an Benutzerfreundlichkeit – in fast allen Fällen ist dann auf einen Blick ersichtlich, mit wem der betreffende Anruf geführt wurde.

Peter Marksteiner ■

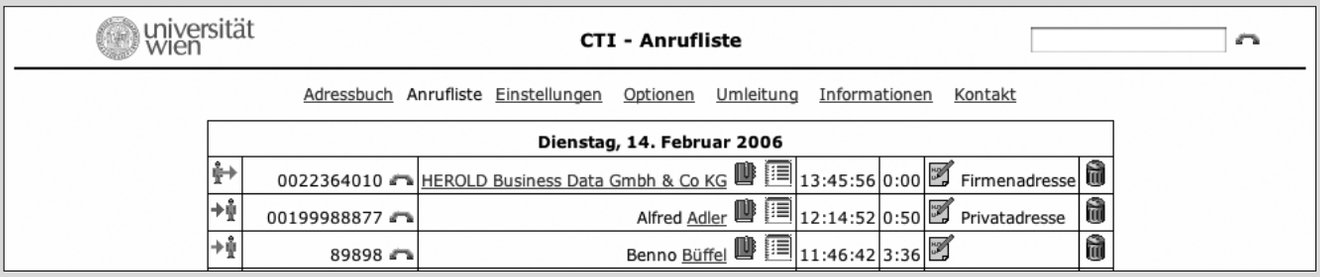


Abb. 2: CTI-Anrufliste mit Namenseinträgen aus dem Herold-Telefonbuch (Beispiel)

Europäischer Computer Führerschein (ECDL)

Jetzt auch am ZID

Der Zentrale Informatikdienst – seit kurzem autorisiertes *ECDL Test Center* – bietet ab dem Sommersemester 2006 allen Studierenden und MitarbeiterInnen der Uni Wien die Möglichkeit, den ECDL (*European Computer Driving Licence* bzw. *Europäischer Computer Führerschein*) zu erwerben. Der ECDL ist ein international anerkanntes und standardisiertes Zertifikat, mit dem EDV-BenutzerInnen ihre grundlegenden und praktischen Fertigkeiten im Umgang mit dem Computer nachweisen können. Er ist für Personen in allen Wirtschaftsbereichen geeignet und gilt als wichtiger Wettbewerbsvorteil am Arbeitsmarkt.

ECDL Core

Die Lehrinhalte des am ZID angebotenen Basispakets *ECDL Core* umfassen im Wesentlichen die allgemeine Benutzung des PCs sowie den Einsatz der typischen Büroanwendungen (Office-Programme) und des Internet. Praxisbezogene, anwendungsrelevante Fertigkeiten sowie das Verständnis der wichtigsten Fachbegriffe stehen im Vordergrund der sieben Module, aus denen sich der *ECDL Core* zusammensetzt:

- **Modul 1**: Grundlagen der Informationstechnologie
- **Modul 2:** Computerbenutzung und Dateimanagement
- **Modul 3**: Textverarbeitung
- **Modul 4**: Tabellenkalkulation
- **Modul 5**: Datenbank
- **Modul 6**: Präsentation
- **Modul 7**: Information und Kommunikation

Die detaillierten Inhalte (*Syllabus*) der einzelnen Module sind unter `www.ecdl.at/syllabus.html` nachzulesen.

Kurse oder Selbststudium?

Die Fertigkeiten zum Erwerb des ECDL können sowohl in den Kursen des ZID als auch im Selbststudium erlernt werden. Für Letzteres stehen empfohlene Skripten und interaktive Medien zur Verfügung. Diese Unterlagen sind von der Oesterreichischen Computer Gesellschaft (OCG, `www.ocg.at`) bzw. der ECDL Foundation (`www.ecdl.com`) auf die inhaltliche Überdeckung mit dem *ECDL Core Syllabus* überprüft worden und eignen sich sehr gut für die Prüfungsvorbereitung. Die vom Zentralen Informatikdienst angebotenen EDV-Kurse decken den ECDL-Syllabus weitgehend ab; fehlende Module müssen im Selbststudium erarbeitet werden. Auf den Webseiten des ZID (`www.univie.ac.at/ZID/kurse/`) sowie in der Informationsbroschüre *EDV-Kurse 2006* (am Helpdesk erhältlich) findet sich bei den betreffenden Schulungen ein Hinweis, welchem ECDL-Modul der jeweilige Kurs entspricht.

Organisatorisches

Als Grundgebühr sind € 47,– an die OCG zu entrichten. Dafür erhält man – quasi als Eintrittskarte – einen Prüfungspass (*SkillsCard*), der dazu berechtigt, Teilprüfungen in allen österreichischen Test Centers abzulegen. Mit der SkillsCard ist es auch jederzeit möglich, die Ergebnisse der absolvierten Teilprüfungen in der ECDL-Datenbank einzusehen.

Am ZID werden nur Studierende und MitarbeiterInnen der Uni Wien zu ECDL-Prüfungen zugelassen. Die SkillsCard ist am Helpdesk (`www.univie.ac.at/ZID/helpdesk/`) erhältlich; dort erfolgt auch die Prüfungsanmeldung zu den einzelnen Modulen. Die Prüfungsgebühr beträgt pro Modul und Antritt € 13,– (nicht inkludiert sind eventuelle Ausbildungskosten, der Erwerb zusätzlicher Schulungsunterlagen und weitere Prüfungsgebühren bei negativen Testergebnissen). Um die Qualität des Zertifikats sicherzustellen, müssen die sieben Teilprüfungen innerhalb von drei Jahren abgelegt werden. Sobald Sie alle Module positiv absolviert haben, werden Ihnen Ihr ECDL-Zertifikat (im A4-Format) und Ihre ECDL-Card (im Scheckkartenformat) auf dem Postweg zugestellt.

Eveline Platzer-Stessl ■

Neues aus dem Kursreferat

Mit Beginn des Sommersemesters 2006 werden im Kursreferat des ZID einige wichtige organisatorische Änderungen wirksam, und auch das Kursangebot wurde wieder ausgeweitet:

Neue Modalitäten für An- und Abmeldung

Die **Anmeldung** wird nun für alle EDV-Kurse eines Semesters gleichzeitig freigegeben: Seit 23. Jänner 2006 ist es möglich, sich für alle Schulungen des Sommersemesters anzumelden. Ist die Teilnehmerzahl am Ende der Anmeldefrist zu gering, wird der Kurs abgesagt. In diesem Fall besteht die Möglichkeit auf Umbuchung oder vollständige Rückzahlung der Kursgebühren.

Achtung – geänderte Storno-Bestimmungen: Bis zum Anmeldeschluss (dieser ist in der Regel ca. eine Woche vor dem Kurstermin) kann man sich wieder abmelden, ohne Stornogebühren zu bezahlen. Bei einer Abmeldung *nach* Ende der Anmeldefrist verfällt jedoch die gesamte Kursgebühr; eine Umbuchung ist ebenfalls nicht möglich.

Neue Mailingliste

Ab sofort steht die Mailingliste *edv-kurse* zur Verfügung, die unter `http://lists.univie.ac.at/mailman/listinfo/edv-kurse` abonniert werden kann. Zweck dieser Mailingliste ist es, einerseits dem Kursreferat die Weitergabe aktueller Informationen (Neuigkeiten, zusätzliche Kurstermine, ECDL-Prüfungstermine, ...) zu ermöglichen und andererseits Interessierten eine Plattform für Wünsche, Verbesserungsvorschläge, Lob, Kritik etc. zu bieten.

Neues Kursmodul

Wie in der letzten *Comment*-Ausgabe berichtet, sind seit Juni 2005 auf allen Webservern des Zentralen Informatikdienstes PHP und MySQL verfügbar (siehe *Comment 05/2*, Seite 36 bzw. unter `www.univie.ac.at/comment/05-2/052_36.html`). Daher wurde auch das Kursangebot des ZID um Vorträge und Workshops zu diesem Thema erweitert: Das Modul *Programmieren mit PHP* besteht aus den drei Vorträgen *Programmieren mit PHP – Teil 1 & Teil 2* und *MySQL-Datenbank mit phpMyAdmin verwalten*, die kostenlos und ohne Anmeldung besucht werden können. Zusätzlich – allerdings nicht mehr gratis – wird der zweitägige Workshop *Programmieren mit PHP und MySQL* angeboten, der auf dem Vortrags-Modul aufbaut und in dem die praktische Umsetzung des Gehörten geübt werden kann. Alle Details entnehmen Sie bitte den Webseiten des ZID (`www.univie.ac.at/ZID/kurse/`).

Neu: ECDL Core

Seit März 2006 ist der ZID ein autorisiertes *Test Center* für den Europäischen Computer Führerschein (ECDL) und bietet Studierenden und MitarbeiterInnen der Uni Wien die Möglichkeit, Teilprüfungen für die Module des *ECDL Core* abzulegen. Nähere Infos dazu finden Sie auf Seite 9.

Eveline Platzer-Stessl ■

Online-Verzeichnisse: aktuell, flexibel und gestylt

Die ersten zehn Jahre

Die Online-Verzeichnisse der Uni Wien (Personal-, Institutsund Vorlesungsverzeichnis, alle drei zu finden unter `http://data.univie.ac.at/pers`) sind schon fast so alt wie der Webauftritt der Universität: Die ersten Versionen stammen aus dem Jahr 1995 und waren noch recht rudimentär. Auch die Datenqualität ließ manchmal zu wünschen übrig. Einerseits lag das an den verschlungenen Wegen, auf denen die Daten von den Datenbanken der Universitätsverwaltung (damals auf der VM-Großrechenanlage) ins Web gelangten, andererseits an den Originaldaten: Was für Verwaltungsabläufe nicht unmittelbar relevant und für niemanden sichtbar war, wurde naturgemäß nicht allzu sorgfältig gepflegt.

Im Lauf der Jahre wurden die Online-Verzeichnisse kontinuierlich weiterentwickelt. 1998 erschien eine neue Version;[1)] seither haben sich Aussehen und Funktionalität nicht wesentlich geändert. Mit der Einstellung der VM-Großrechenanlage und der Inbetriebnahme der Universitätsverwaltungssoftware i3v seit 2001 mussten große Teile umgeschrieben werden, auch wenn von außen nicht viel davon zu bemerken war. Die Datenqualität hat sich ständig verbessert, heute werden die Verzeichnisse täglich aktualisiert. Durch die Einstellung des gedruckten Vorlesungsverzeichnisses, das im Sommersemester 2004 zum letzten Mal erschienen ist, wurde das Online-Vorlesungsverzeichnis weiter aufgewertet. Zwar gab es bis vor kurzem immer wieder punktuelle Verbesserungen und Anpassungen an geänderte Gegebenheiten (z.B. Zuordnung von Lehrveranstal-

tungen zu Studienprogrammleitungen statt zu Instituten, Inhaltsverzeichnis bei den einzelnen Kapiteln im Vorlesungsverzeichnis); manche schon lange gewünschten Erweiterungen ließen sich jedoch nur durch ein komplettes Redesign und Neuschreiben erreichen. Seit Sommer 2005 wurde daran gearbeitet, am 3. März 2006 wurde die neue Version veröffentlicht.

Was ist neu?

Auf den ersten Blick sind die Änderungen nicht allzu auffällig: Das Aussehen hat sich nur leicht geändert, Inhalt und Struktur sind im Wesentlichen gleich geblieben. Alle bisher gültigen URLs funktionieren auch weiterhin; es wurden zwar einige neue Parameter hinzugefügt, aber keine weggelassen. Dass nunmehr ausschließlich syntaktisch korrektes HTML (genauer gesagt, *XHTML 1.0 Strict*) verwendet wird[2], ist zwar nicht unmittelbar sichtbar, aber für eine richtige Anzeige in möglichst vielen Browsern wichtig.

Es gibt jedoch eine Menge neuer Features:

Mehrsprachigkeit

Die neuen Verzeichnisse sind durchgehend zweisprachig (deutsch und englisch) gehalten. Im Prinzip ist die Software für beliebige Sprachen geeignet: Alle Textbausteine stehen in einer Tabelle in einer Datenbank, einem so genannten *Message Catalogue*; wenn ein Baustein in der gewünschten Sprache nicht vorhanden ist, wird stattdessen der deutsche genommen. Da die meisten Daten in i3v nur in Deutsch und Englisch erfasst werden, ist die Anzeige in anderen Sprachen zwar möglich, aber derzeit wenig sinnvoll.

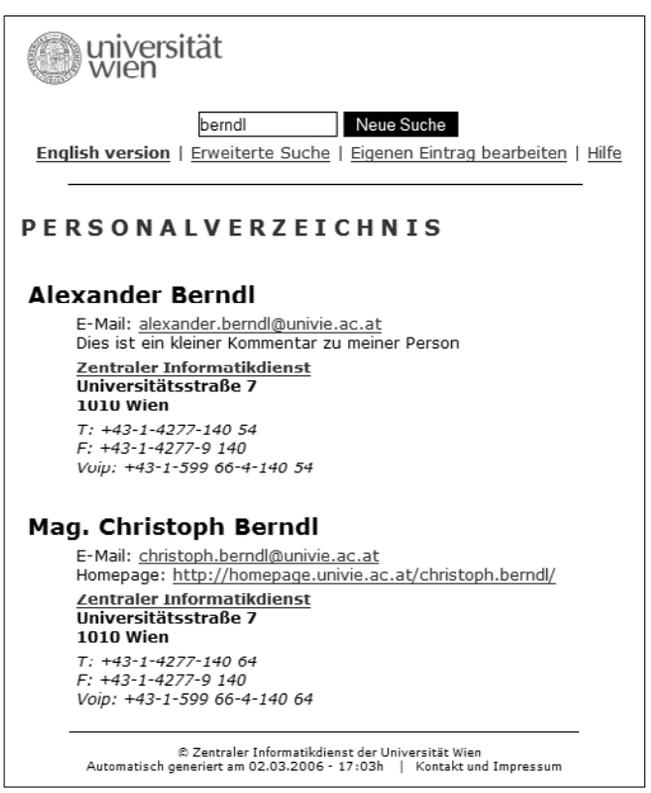
Persönliche Anpassungen

Bisher bestand die Möglichkeit, mittels `http://data.univie.ac.at/homepage` die persönliche Homepage ins Personalverzeichnis einzutragen und mittels `http://data.univie.ac.at/kommentar` einen Kommentar zu einer Lehrveranstaltung zu veröffentlichen. Die Gestaltungsmöglichkeiten des eigenen Eintrags im Online-Personalverzeichnis wurden nun wesentlich erweitert:

- **Kommentar**: ein beliebiger Kommentar zur Person;
- **Zimmernummer** und **Sprechstunden**;
- **aktuelle Meldung**: z.B. für Termine oder Abwesenheiten; der Zeitraum, in dem diese Meldung angezeigt werden soll, ist frei wählbar.
- **Foto**: Es besteht die Möglichkeit, ein Foto am Server abzulegen. Zudem werden in Kürze für Dienstausweise auch Fotos in i3v gespeichert, die auf Wunsch im Online-Personalverzeichnis angezeigt werden können.

Abb. 1 (oben): Eintrag im Personalverzeichnis (Standardansicht)

Abb. 2 (unten): Andere Darstellung dieses Eintrags mittels alternativem Style Sheet und *exclude*-Parameter



1) siehe Artikel *Das neue Online-Vorlesungsverzeichnis: Kommentare erbeten!* in *Comment 98/1*, Seite 32 bzw. unter `www.univie.ac.at/comment/98-1/981_32.html`

2) Ausnahmen sind Kommentare im Online-Vorlesungsverzeichnis mit fehlerhaftem HTML-Code.

Das Eintragen oder Ändern dieser Informationen erfolgt über die Webmaske `http://data.univie.ac.at/pers_edit`, die auch über den Link *Eigenen Eintrag bearbeiten* rechts oben im Online-Personalverzeichnis zu erreichen ist (siehe Abb. 1 & 2 auf Seite 11).

Die Möglichkeit, einen Kommentar ins Online-Vorlesungsverzeichnis einzutragen, besteht nach wie vor. Allerdings bietet seit einiger Zeit i3v selbst die Möglichkeit, Lehrveranstaltungen ausführlich zu kommentieren. Dazu dienen die Felder *Inhalt*, *Methoden*, *Ziele* und *Literatur*, die unter *Weitere Informationen* auch im Web angezeigt werden.

Flexibles Design

Neben den zentralen Online-Verzeichnissen gibt es zahlreiche Personallisten auf Instituts-Homepages, kommentierte Vorlesungsverzeichnisse zu einzelnen Studienrichtungen und Ähnliches mehr. Die Wartung und Pflege solcher Listen ist oft ein beträchtlicher Aufwand, der sich durch die Verwendung der zentralen Verzeichnisse vermeiden ließe. Häufig geschieht das nur deshalb nicht, weil deren Design nicht zu der betreffenden Homepage passt. Aus diesem Grund wurde das Design der neuen Online-Verzeichnisse so flexibel gestaltet, dass es an das *Look & Feel* jeder beliebigen Webpräsenz angepasst werden kann.

Alternative Style Sheets

Die grafische Gestaltung erfolgt ausschließlich über Style Sheets, im HTML-Code selbst sind keinerlei Formatierungs-Informationen enthalten.[3] Mit Hilfe des Parameters `style` kann ein alternativer Style Sheet angegeben werden, womit Farben, Schriftarten usw. nach Wunsch definiert werden können. Jedes Element – Name, eMail-Adresse, Telefonnummer usw. – gehört einer eigenen Klasse an, sodass für jedes dieser Elemente ein eigener Style definiert werden kann (siehe Abb. 2 auf Seite 11).

Selektive Anzeige

Für manche Zwecke ist die Angabe der vollständigen Informationen überflüssig oder unerwünscht: Beispielsweise genügen für ein Telefonverzeichnis Name und Telefonnummer, Lehrveranstaltungen sind hier uninteressant. Mit Hilfe der Parameter `include` und `exclude` kann ausgewählt werden, welche Elemente angezeigt werden sollen und welche nicht.

XML-Schnittstelle

Immer wieder wird der Wunsch nach einem direkten Zugriff auf die Personaldatenbank geäußert, um diese in eigene Webapplikationen einzubauen. Aus verschiedenen Gründen ist ein solcher Zugriff nicht möglich, aber die neu geschaffene XML-Schnittstelle erfüllt eine ähnliche Funktion: Bei Angabe des Parameters `format=xml` wird eine XML-Datei ausgegeben, die alle öffentlich zugänglichen Informationen zu einer Person, einer Einrichtung oder einer Lehrveranstaltung enthält (siehe Abb. 3). Diese XML-Datei ist für automatisierte Verarbeitung geeignet und kann z.B. in CGI-Skripts oder PHP-Programmen ausgewertet werden.

Peter Marksteiner ■

```
<?xml version="1.0" encoding="iso-8859-15" ?>
<personen>
<person aktiv="Ja"
      aktuell_sichtbar="nein"
      email="alexander.berndl@univie.ac.at"
      geschlecht="M"
      kommentar="Dies ist ein kleiner
         Kommentar zu meiner Person"
      photo="jpg"
      pkey="83373"
      sip="+43-1-59966-4-140 54"
      sprechstunden="täglich"
      username="ab"
      vorname="Alexander"
      zimmernummer="B0110"
      zuname="Berndl">
  <info></info>
  <inst name="Zentraler Informatikdienst"
      inum="A140"
      karenziert="Nein"
      link="Ja"
      url="http://www.univie.ac.at/ZID/">
    <abteilung_von name="inum" name1="">
      <inum></inum>
      <name2></name2>
    </abteilung_von>
    <adresse ort="1010 Wien"
        strasse="Universitätsstraße 7">
      <fax>(01) 4277 9140 </fax>
      <telefon>(01) 4277 14054</telefon>
    </adresse>
    <email></email>
    <fakultaet name="Dienstleistungseinrich-
    tungen, Stabstellen, etc." code="0" />
    <funktionen></funktionen>
      <position attribut="Zentralen
        Informatikdienst"
      code="A"
      praeposition="am"
      text="Dienstverhaeltnis" />
  </inst>
  <lv></lv>
  <titel></titel>
  <url></url>
</person>
</personen>
```

Abb. 3: Eintrag im Personalverzeichnis, Ausgabe als XML-Datei

3) siehe Artikel *HTML mit Stil – Teil II: Cascading Style Sheets* in *Comment 03/1*, Seite 30 bzw. unter `www.univie.ac.at/comment/03-1/031_30.html`

OPERATION GELUNGEN, PATIENT WOHLAUF

Umstellung der Unet-Services für Medizin-Studierende

Mit dem Sommersemester 2006 bricht für Studierende der Medizinischen Universität Wien (MUW) eine neue Ära an: Die EDV-Services, die ihnen bisher im Rahmen des Unet-Service vom ZID der Universität Wien zur Verfügung gestellt wurden (eMail, PC-Räume, Fileservices etc.), werden ab März 2006 von der Abteilung ITSC (*IT Systems & Communications*) der Medizinischen Universität angeboten.

Die Unet-Accounts von Medizin-Studierenden bleiben weiterhin gültig und sind bis zu ihrem endgültigen Ablauf uneingeschränkt verwendbar (die Gültigkeitsdauer kann unter `www.univie.ac.at/ZID/account-info/` abgefragt werden). Ab Sommersemester 2006 erhalten jedoch nur mehr jene Studierenden einen neuen PIN-Code zur Verlängerung ihres Unet-Accounts, die an der Uni Wien ebenfalls zum Studium zugelassen sind („MitbelegerInnen"). Der Datenbestand (Mail- und Fileserver-Dateien) aller betroffenen Unet-Accounts wurde am 5. Februar 2006 auf die entsprechenden Server der Medizinischen Universität kopiert. Seither werden die Daten nicht mehr abgeglichen; d.h. alle BenutzerInnen, die sowohl mit ihrem Unet- als auch mit ihrem MUW-Account arbeiten, müssen nun selbst dafür sorgen, dass z.B. neu hinzugekommene Unet-Daten auch auf den MUW-Servern verfügbar sind. Konkret ergeben sich durch die Umstellung folgende Änderungen:

eMail

Für die betroffenen Unet-Mailadressen (a*Matrikelnummer*`@unet.univie.ac.at`) wurden automatische Weiterleitungen zu den entsprechenden MUW-Mailadressen (n*Matrikelnummer*`@students.meduniwien.ac.at`) eingerichtet. Diese Weiterleitungen können auf Wunsch über die Webmaske `https://data.univie.ac.at/forward/` deaktiviert werden. Bereits bestehende Weiterleitungen von Unet- auf externe Mailadressen (z.B. Hotmail, GMX) wurden bei den entsprechenden MUW-Accounts eingetragen. **Achtung:** Seit Februar 2006 werden die eMail-Adressen n*Matrikelnummer*`@students.meduniwien.ac.at` von der MUW verwendet, um wichtige Mitteilungen unter ihren Studierenden zu verbreiten. Die Nachrichten an diese Mailadressen sollten daher regelmäßig gelesen werden, andernfalls könnten wesentliche Informationen versäumt werden.

PC-Räume / Fileservices

Die PC-Räume an Instituten der Medizinischen Universität werden ab Sommersemester 2006 von der Abteilung ITSC betreut und sind nur mehr mit MUW-Accounts verwendbar. Das betrifft die Standorte Währinger Straße 10, 13 und 13a, Schwarzspanierstraße 17 und Neues AKH (6M und – neu – im BT87 Lernzentrum). Die PC-Räume der Uni Wien können mit dem Unet-Account weiterhin benutzt werden; dabei ist aber zu beachten, dass es sich nun um zwei getrennte Systeme handelt und die Dateien auf unterschiedlichen Fileservern gespeichert werden. Wenn die Daten auf beiden Systemen verfügbar sein sollen, muss der Datenabgleich von den BenutzerInnen händisch durchgeführt werden.

Internetzugang von daheim

Bereits seit Dezember 2005 ist muwADSL verfügbar, das Pendant zum uniADSL-Angebot des ZID:

- Wer weiterhin auch an der Universität Wien studiert, derzeit uniADSL verwendet und auf muwADSL umsteigen möchte, muss einen so genannten Providerwechsel durchführen, der bis 31. März 2006 kostenlos ist.
- Studierende, die nur an der Medizinischen Universität zum Studium zugelassen sind, müssen den Providerwechsel bis Ende März 2006 durchführen (keine automatische Umstellung). Der Umstieg auf muwADSL ist unter `www.meduniwien.ac.at/itsc/services/muwadsl-help/uniadsl2muwadsl.php` genau beschrieben. Dabei werden alle uniADSL-Daten übernommen; es muss nur mehr die Kennung (MUW-StudID) und das Passwort geändert werden. Bis zum Ablauf des Unet-Accounts kann mit beiden Kennungen (a*Matrikelnummer*`@adsl.univie.ac.at` und n*Matrikelnummer*`@students.meduniwien.ac.at`) gearbeitet werden, danach nur mehr mit der MUW-StudID.

Alle Infos zu muwADSL sind unter `www.meduniwien.ac.at/itsc/services/muwadsl-help/` zu finden.

Der Internetzugang via StudentConnect (chello), xDSL Uni (inode) und Modem/ISDN wird derzeit noch über den ZID der Uni Wien bzw. den Unet-Account abgewickelt. Entsprechende Angebote der Medizinischen Universität sind in Vorbereitung; Näheres dazu wird in Kürze auf den Webseiten der Abteilung ITSC (`www.meduniwien.ac.at/itsc/studierende/`) veröffentlicht werden.

Infos, Hilfe & Kontakt

Alle Informationen zum EDV-Angebot der Medizinischen Universität Wien und zum aktuellen Stand der Umstellung finden Sie auf den Webseiten der Abteilung ITSC (`www.meduniwien.ac.at/itsc/`). Auch ein Support-Dienst wurde eingerichtet (siehe `www.meduniwien.ac.at/itsc/support.php`). Bitte bedenken Sie, dass der Helpdesk des ZID bei Fragen zu MUW-Services nur sehr eingeschränkt behilflich sein kann, und wenden Sie sich dafür an den **Support der Abteilung ITSC**:

- Öffnungszeiten: Mo – Fr 8:00 – 16:00 Uhr
- Tel.: (+43 1) 40160-21288
- eMail: `stud-helpdesk@meduniwien.ac.at`

Elisabeth Zoppoth ■

VISTA-RUNDSCHAU – WANDERUNG MIT WEITBLICK

Eine Jahresbilanz

Große Veränderungen sind für das Jahr 2005 in Sachen eLearning zu verzeichnen – auf personeller wie auf technischer Ebene. Eine Zäsur in personeller Hinsicht stellte der plötzliche Tod von Herbert Stappler dar, dem langjährigen Leiter der Abteilung *Software & Benutzerbetreuung* des ZID. Ihm sind die ersten eLearning-Bestrebungen am Zentralen Informatikdienst zu verdanken, er hat mit Eveline Platzer-Stessl am ZID entsprechende Infrastrukturen und ein Supportteam aufgebaut, und mit ihm ist uns ein visionärer und über die Maßen der Professionalität hinaus engagierter Pionier des eLearning verloren gegangen. Mehrfach hat sich seitdem der *Support Neue Medien* reorganisieren müssen, durch Aufbau und Stärkung neuer Strukturen sowie durch technische In(ter)vention. Mit Peter Marksteiner hat das eLearning-Team nun einen neuen Leiter, kompetenten Berater und Mitdiskutanten gewonnen.

Wanderung | Wandelung

Neben der Restabilisierung der personellen Strukturen und der Weiterführung mittelfristiger Strategiepläne wurden aufgrund einer höheren Auslastung der Ressourcen auch neue Erfordernisse aktuell. Zeitgleich mit dem Software-Upgrade von WebCT Vista 2.1 auf die leistungsfähigere Version 3.0 wurden in den Sommerferien 2005 alle vorhandenen Daten der Lernplattform von dem bisherigen Einzel-Server auf eine neue Hardware migriert. Mehrere Rechner sind jetzt zu einem Cluster zusammengeschlossen, ein vorgeschalteter Load Balancer verteilt die Anfragen gleichmäßig auf die einzelnen Server.

Der Umstellung ging eine umsichtige Testphase (Probemigration) ohne sichtbare Kollateralschäden voraus, und das Endergebnis wurde sowohl von den beteiligten Lehrenden wie auch von den Studierenden breit akzeptiert: Zählte die Datenbankabfrage im Oktober 2004 noch 154 Lehrveranstaltungen, die mittels WebCT Vista abgewickelt wurden, so waren im darauffolgenden Sommersemester bereits 242 Einträge zu verzeichnen. Per Ende des Wintersemesters 2005 wurden 350 Vista-unterstützte Lehrveranstaltungen angeboten. Tendenz steigend: Die aktuelle Projektphase des Strategieprojekts *Neue Medien in der Lehre* der Universitätsleitung ist der Verankerung des eLearning-Angebots in den neuen Studienplänen und auf fakultärer Ebene gewidmet, sodass mit einem weiteren raschen Zuwachs gerechnet werden kann.

Support revisited

Als Folgeleistung der technischen Neuerungen arbeitete das Supportteam Neue Medien gemeinsam mit dem Projektzentrum Lehrentwicklung ein neues, an WebCT Vista 3.0 angepasstes und in seiner Gesamtstruktur reformiertes Schulungskonzept aus, das didaktische und technische Belange besser zu verbinden sucht. Begleitet wurden die Umstellungen von einem *Vista 3.0 Opening | Tag der Offenen Tür* im September 2005, an dem das Supportteam des ZID und das Projektzentrum Lehrentwicklung den BenutzerInnen mit persönlicher Betreuung und Upgrade-Schulungen zur Verfügung standen. Eine Bereicherung stellt darüber hinaus die Ausweitung der Öffnungszeiten des Supportbüros auf 37 Stunden pro Woche dar (siehe `www.univie.ac.at/ZID/elearning/`).

Wo gehobelt wird, da fallen Späne

Nachdem man eigene Fehler nur mit den Augen der anderen gut sehen kann, wurde auch das eLearning-Team erst durch das heftige Anwachsen der Supportanfragen auf einen Missstand aufmerksam: Das Zusammentreffen einer neuen Java-Klientenversion mit der Umstellung des Load Balancers auf SSL[1)] führte im Oktober 2005 zu Ausfällen der Plattform, Problemen beim Einloggen und Schwierigkeiten bei Features, die Java verwenden (vor allem beim Up-/Download via Dateimanager). Diese Schwierigkeiten konnten vorläufig durch ein Downgrade auf eine ältere Java-Version und eine Rekonfiguration auf das unverschlüsselte HTTP-Protokoll überbrückt werden.

Der Zentrale Informatikdienst hat aber aus den Leiderfahrungen der betroffenen BenutzerInnen Konsequenzen gezogen und zwei neue Load Balancer für den Aufbau getrennter Server-Umgebungen mit WebCT Vista beschafft, die voraussichtlich Mitte April 2006 in Betrieb genommen werden. Dadurch soll eine gezielte Fehlerkontrolle auf einer Test- bzw. Backup-Umgebung ermöglicht werden: Updates werden vor ihrem Einsatz im laufenden Betrieb auf der Testumgebung eingespielt; damit wird es nicht mehr nötig sein, in kurzen Wartungsfenstern Versuche „am lebenden Patienten“ durchzuführen.

Viel Wandern macht bewandert – schöne Aussichten

Neue Horizonte und Gestaltungsmöglichkeiten hat das eLearning-Team durch zwei Projekte gewonnen: Für den administrativ sehr aufwendigen Aufnahmetest der Fakultät für Psychologie wurde ein spezieller Belegscanner mit entsprechender Software beschafft, der von Michael Janousek betreut wird. Eine weitere Zukunftsperspektive in Sachen eLearning liegt im Videostreaming von unterrichtsbeglei-

tendem Material. Nähere Informationen zu diesen beiden Projekten entnehmen Sie bitte dem Artikel *Neue Services bei den Neuen Medien* auf Seite 16.

Ein anderes heißes Thema ist die Entwicklung von Schnittstellen zu bestehenden Datenbanken der Universität Wien. In ausgewählten Lehrveranstaltungen wird bereits die automatisierte Übernahme von Prüfungsergebnissen aus dem *Gradebook* von WebCT Vista in die Universitätsverwaltungssoftware i3v geprobt (Notenexport). Auch die Anmeldung von Lehrveranstaltungen soll stark vereinfacht werden; zu diesem Zweck wird ein neues Anmeldesystem entwickelt, das ebenfalls mit i3v verknüpft ist. Darüber hinaus wird auch die Studierendenverwaltung laufend optimiert, und ein neues System für die Anmeldung zu eLearning-Schulungen befindet sich unmittelbar vor der Fertigstellung.

Neue Einsichten erwarten wir von der diesjährigen *WebCT User Conference*, die Ende Februar 2006 (Anm.: nach Redaktionsschluss dieser *Comment*-Ausgabe) in Edinburgh stattfindet. Die Teilnahme von VertreterInnen des Projektzentrums Lehrentwicklung und des Supportteams Neue Medien an dieser Konferenz soll im Wesentlichen dazu dienen, Entscheidungen zu beschleunigen, weiterführende Kontakte in Sachen WebCT aufzubauen – und nach Möglichkeit zu klären, ob eventuelle Nachrüstungen in Vista 3.0 oder ein Upgrade auf eine noch zu entwickelnde „Fusion"-Version[2] vonnöten sind.

Darüber hinaus versucht das Team in Edinburgh zu erreichen, dass ein lästiger Programmfehler im *User Tracking* beseitigt wird. Für die BenutzerInnen soll sich die gewohnte Bedienung der Plattform nur in dem Maße verändern, wie es zur Optimierung ihrer Funktionen unbedingt notwendig ist. Die Darstellung der Kursliste wurde von der Firma WebCT bereits wesentlich übersichtlicher gestaltet; an weiteren Verbesserungen wird gearbeitet.

Wir blicken auf ein eLearning-Jahr zurück, in dem stabile und verläßliche Strukturen gewachsen sind und in dem wir aus Verlusten gelernt haben. Und da wir noch lange nicht am Ziel aller Wünsche sind, werden wir in nächster Zeit eines wohl kaum vermissen: das Wandern zum Ziel.

Annabell Lorenz ■

1) SSL (*Secure Sockets Layer*) ist ein Netzwerkprotokoll, das eine verschlüsselte Kommunikation zwischen Browser und Webserver ermöglicht.

2) Die beiden führenden Hersteller von Lernplattformen, WebCT und Blackboard, fusionierten im Herbst 2005; welche Auswirkungen dies auf die angebotene eLearning-Software haben wird, ist noch ungewiss.

Personalnachrichten

Im Vergleich zur letzten Ausgabe des *Comment* (bei deren Erscheinen erstmals mehr als 200 Angestellte am Zentralen Informatikdienst zu verzeichnen waren, zumindest wenn man die „geringfügig beschäftigten" PC-Raum-BetreuerInnen mitzählt) sind diesmal nur wenige personelle Veränderungen zu berichten:

In der Abteilung *Datennetze & Infrastruktur* verstärkt seit Dezember 2005 **Günter Paar** unser noch recht kleines Referat *Datenleitungs-Infrastruktur*. Das Leitungsnetz in den zahlreichen Gebäuden der Uni Wien ist Günter Paar nicht unbekannt – er war während der Umstellung des Telefonsystems an der Universität in den Jahren 1997 bis 2002 als Mitarbeiter der Elektroinstallationsfirma Beck maßgeblich an den Verkabelungsarbeiten beteiligt.

In der Abteilung *Zentrale Services & Benutzerbetreuung* sind vor allem im eLearning-Bereich personelle Neuigkeiten zu vermerken: **Eveline Platzer-Stessl**, die gemeinsam mit Herbert Stappler am ZID die entsprechenden Strukturen aufgebaut hat, hat sich nach der erfolgreichen Realisierung des Projekts aus diesem Bereich zurückgezogen, um sich wieder mit voller Kraft ihrem ursprünglichen Aufgabengebiet, unserem Kurswesen, widmen zu können. Auch **Katharina Lüthke** hat den eLearning-Support verlassen: Sie unterstützt seit Anfang Dezember 2005 die *Comment*-Redaktion. Um die Java-Applikationen im eLearning-Bereich kümmert sich anstelle von **Ewald Geschwinde**, der den ZID mit Ende Jänner 2006 verlassen hat, nunmehr **Bernhard Weigl**. Darüber hinaus hat am Helpdesk im Jänner 2006 **Thomas Riener** die Nachfolge von **Nasret Ljesevic** angetreten, der zum Referat *Support Instituts-PCs* wechselte.

Mit der Errichtung des *Center for Integrative Bioinformatics Vienna* (CIBIV) an der Max F. Perutz Laboratories GmbH hat der Zentrale Informatikdienst seine Außenstelle am Vienna Biocenter in der Dr.-Bohr-Gasse endgültig aufgelassen und seine Infrastruktur, insbesondere den österreichischen EMBnet-Knoten, in das neue Zentrum eingebracht. **Martin Grabner**, der seit den Anfängen im Jahr 1992 diese Außenstelle geleitet hat, bleibt der Bioinformatik treu und arbeitet nunmehr am CIBIV.

Seit März 2006 absolviert **Martin Zeitlberger** als Student der Fachhochschule Technikum Wien sein Berufspraktikum im Datawarehouse-Team der Abteilung *Universitätsverwaltung*. **Dejan Vidovic**, der vor eineinhalb Jahren die Leitung des Referats *UNIVIS-Produktionsbetrieb* übernommen und in dieser Funktion ganz entscheidend dazu beigetragen hat, dass die erste Phase des Projekts *Reporting System* mit der Inbetriebnahme des Datawarehouse erfolgreich abgeschlossen werden konnte, verlässt hingegen nach getaner Arbeit die Universität Wien, um sich in der Privatwirtschaft zu bewähren.

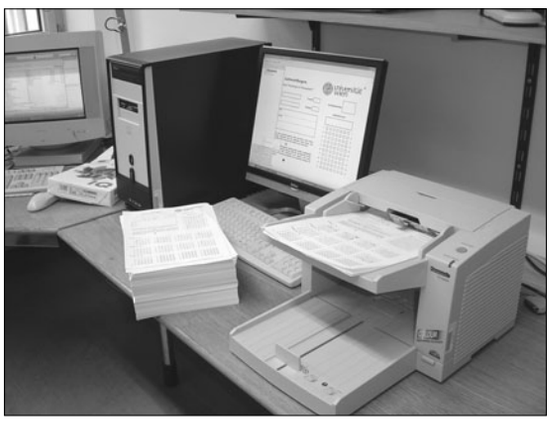
Allen scheidenden Mitarbeitern danken wir sehr herzlich für ihre wertvolle Arbeit am Zentralen Informatikdienst und wünschen ihnen für ihre Zukunft ebenso Freude und Erfolg, wie wir es auch unseren neuen Angestellten am ZID wünschen.

Peter Rastl

Neue Services bei den Neuen Medien

Belegscanner und Video-on-Demand

Im laufenden Universitätsbetrieb ergeben sich immer wieder neue Anforderungen, welche die Möglichkeiten einer modernen EDV-gestützten Bearbeitung ins Auge fassen und somit an den Zentralen Informatikdienst herangetragen werden. In diesem Zusammenhang wurden in jüngster Zeit zwei Projekte angestoßen, die im Supportbüro Neue Medien angesiedelt wurden.



Der neue Belegscanner des ZID, der vom Supportbüro Neue Medien betreut wird

Projekt: Belegscanner

Durch die jährliche Steigerung der Studierendenzahlen sowie die erst im letzten Semester vollzogene Öffnung der österreichischen Universitäten für alle EU-Studierenden kam es erstmalig an vielen Fakultäten zu zahlenmäßigen Beschränkungen bei der Zulassung von Erstsemester-Studierenden. Die Fakultät für Psychologie, die den Ansturm der Studierenden mit einem Einstufungstest zu reglementieren versucht, trat im vergangenen Semester mit folgender Frage an den ZID heran:

Wie kann man 1000 Studierende innerhalb einer Woche mittels standardisierter Fragebögen einem Eignungstest unterziehen und die Ergebnisse zügig bekannt geben, dabei den Arbeitsaufwand jedoch so gering wie möglich halten?

Zur Bewältigung dieser Aufgabe kommt nun ein so genannter Belegscanner inklusive Erfassungssoftware zum Einsatz, ein speziell für Formulare geeignetes Programmpaket, um Fragebögen – wie bei Volkszählungen oder Multiple-Choice-Tests üblich – schnellstens zu erfassen und zu interpretieren.

Funktionsweise des Scanners

Das Ausgangsformular, ein einseitiger Multiple-Choice-Test im A4-Format, enthielt folgende Text- und Grafik-Elemente: Den Header bildeten die Überschrift mit dem Titel der Lehrveranstaltung sowie der Datumsangabe. Dazu kamen die Felder, welche die Studierenden mit Namen und Matrikelnummer selbst auszufüllen hatten. Den Rest bildeten in Fünferblöcken zusammengefasste nummerierte Kästchen, die von den TestteilnehmerInnen entsprechend anzukreuzen waren.

Im ersten Schritt wurde der Fragebogen unausgefüllt in das System eingelesen und anhand dessen beliebige, über die gesamte Seite verteilte Erkennungspunkte mittels Software fixiert. Dadurch wird die spätere Erkennung auch bei verkehrtem oder verzogenem Einzug eines Blattes und bei umgekehrter Seitenausrichtung (*Top down*) sowie die Unterscheidung zwischen Vorder- und Rückseite der Belege erhöht.

Im nächsten Schritt mussten für den Test der Software zahlreiche Bögen ausgefüllt und mit verschiedenen Schreibstilen und Schreibutensilien etliche Male getestet werden, bis die Einstellungen der Software zur Erkennung der Fragebögen zufrieden stellend waren.

Nach Abschluss dieser Prozedur und Einlesen aller Daten erzeugt die Software eine Textdatei, die dann beispielsweise in das Programm SPSS zur weiteren Verarbeitung eingespielt werden kann. Im vorliegenden Fall waren dort alle Testteilnehmer mit den entsprechenden Fragen sowie den dazugehörigen korrekten Antworten gespeichert. Aus SPSS heraus entsteht dann erst die Note, die gemeinsam mit den abgegebenen und den korrekten Antworten des Multiple-Choice-Tests in die Prüfungsverwaltung eingespielt wurden. So konnten die Studierenden nicht nur ihre Note erfahren, sondern auch die abgegebenen Antworten mit den korrekten Ergebnissen vergleichen. Eine persönliche Prüfungseinsicht war so in nur wenigen Fällen notwendig – eine große Arbeitserleichterung für die Fakultät.

Weitere Scanner-Services

Neben der Erfassung von Fragebögen kann mit dem Hochgeschwindigkeitsscanner auch jede andere Art von Einzelblättern einscannt werden. Vollständige Bücher, oder auch nur Teile daraus, sind in Minuten erfasst und in ein PDF-Dokument verwandelt. Und dies nicht nur als Grafik, sondern auf Wunsch auch mit Suchfunktion, Schutz vor Kopie, Druck oder Veränderung bzw. mit Signaturen versehen etc. Selbst ganze Fotostapel lassen sich komfortabel einscannen, weiterverarbeiten oder archivieren.

Erste Anfragen für die weitere Nutzung des Scanners gibt es bereits von Seiten der ÖH, die mit Hilfe dieses kostenlosen Services des ZID die Qualität von Lehrveranstaltungen und der Vortragenden mittels Fragebogen erfassen will. Ferner möchte das Institut für Bildungswissenschaften alte Frakturschriften elektronisch erfassen, keine leichte, aber lösbare Aufgabe.

Die Scanner-Erfassung im Detail

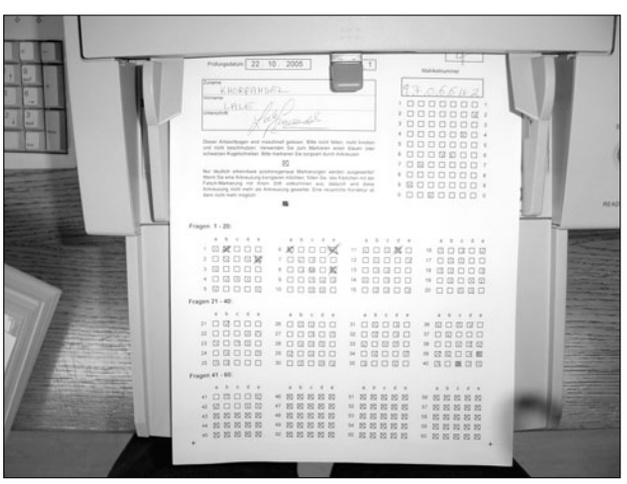
Technische Daten

Scanner: Panasonic KV-S2046CU mit einer Ausgabe von 40 Belegen pro Minute und einer 100-Blatt-Dokumentenzuführung

Software: FORMS 5 von Readsoft in einer Lite Version, die sowohl Papierformulare als auch elektronische Informationen zeitsparend erfassen und verarbeiten kann. Die Software überträgt ferner die Informationen in nachgeordnete Systeme, wie z.B. eine Datenbank. Im Vergleich zum manuellen Erfassen ist die elektronische Formularerfassung bis zu 90% schneller. Die Fehlerrate ist dabei sehr gering. Informationen, die sich nicht eindeutig durch die Software erfassen lassen, werden anschließend noch einmal manuell bearbeitet und überprüft.

Softwareerkennung

Nach Einlesen der Daten mittels Scanner wird die Softwareerkennung gestartet, die vergleichbar mit jeder handelsüblichen OCR (*Optical Character Recognition*) ist – nur, dass sie in diesem Fall wesentlich genauer durchgeführt wird und ganz speziell auf die Struktur von Formularen ausgelegt ist.



Einlesen von Fragebögen in den Belegscanner des ZID

Dazu dienen manuell einstellbare Schwellenwerte, die ein Kästchen ab einem bestimmten Prozentwert an Füllung als leer, nur verschmutzt, angekreuzt bzw. gänzlich ausgestrichen interpretieren. Diese Prozentwerte sind die heikelsten Einstellungen, die über die Menge der späteren Handarbeit entscheiden.

Nach der automatischen Erkennung erfolgt das so genannte *Verify*. Hier gibt der Computer nur die fraglichen Elemente aus, sodass man diese dann mittels menschlicher Urteilskraft einordnen kann. Dazu wird das dazugehörige eingescannte Bild angezeigt, und man vergibt manuell eine 1 (= angekreuzt) oder eine 0 (= nicht angekreuzt).

Trotz sorgfältiger Testphase traten im ersten Prüfungsdurchlauf unvorhergesehene Probleme auf, die durch die sehr unterschiedlichen Schreibgewohnheiten vieler Studierender hervorgerufen wurden. Die Schwierigkeit bei der Erkennung ist nämlich folgende: Erstens bedeutet ein Kreuz innerhalb eines Kästchens, dass diese Antwort richtig ist. Zweitens soll ein ganz ausgefülltes Kästchen zeigen, dass man sich geirrt hat und die Antwort doch falsch ist, also gleichbedeutend mit gar nicht angekreuzt. Viele Studierende hatten jedoch die Angewohnheit, ein Kästchen zu gut anzukreuzen, so dass es schon wieder ausgestrichen war. Dazu kam, dass einige TeilnehmerInnen das Ausstreichen nicht ganz so wörtlich genommen hatten und meinten, dass ein Kreuz mit einem darüber gemalten Plus (also ein Stern) schon ausgestrichen sei.

Ein Mensch ist durchaus in der Lage, solche Kreuze zu erkennen, auch wenn sie über den Rand des Kästchens hinausgehen, die Maschine berechnet jedoch nur den Wert der gefüllten Fläche innerhalb der Umrandung. Dies führte zu etlichen Fehlern bei der Interpretation durch die Software, die weitere Anpassungen notwendig machten. Nach mehreren weiteren Testdurchgängen mit Einlesen, Interpretieren und Auswerten der 1000 Fragebögen konnte die Fehlerrate so weit minimiert werden, dass nur mehr einige Extremfälle von Hand nachgebessert werden mussten.

Für den zweiten Prüfungstest konnte bereits aus den anfänglichen Schwierigkeiten gelernt und entsprechende Vorkehrungen getroffen werden. Hier führten vor allem eine genaue Instruktion der Studierenden sowie die inzwischen sehr guten Einstellungen der Software bereits im ersten Scan-Vorgang zu einem 100-prozentigen Ergebnis, so dass keine händischen Verbesserungen mehr nötig waren. Die Auswertung von knapp 1000 Bögen nahm nunmehr nur vier Stunden in Anspruch und kann somit von nur einer Person betreut werden.

Projekt: eLearning via Video-on-Demand

Der Ansturm auf einzelne Institute zeigt deutlich Grenzen in der herkömmlichen Lehre an der Universität Wien, wenn die Fakultät für Psychologie – so letztes Semester geschehen – sogar Räumlichkeiten wie das Austria Center für den Präsenzunterricht der über 1000 Studierenden anmieten muss. Diese neuen Eindrücke führten zu der Überlegung, die eLearning-Bestrebungen der Universität Wien um ein neues Service zu bereichern.

Vorteile

Für viele Studierende wäre es eine große Erleichterung, wenn sie sich manche Vorlesung von zu Hause aus online ansehen könnten. Gründe hierfür lassen sich viele nennen, und könnten sich in Krankheit, Unabkömmlichkeit oder in der zu großen Entfernung zur Vorlesung äußern. Aber eben auch Massenlehrveranstaltungen und die damit einhergehenden überfüllten Hörsäle stellen einen Ansatzpunkt für Videostreaming-Vorhaben (= Live Video) dar.

Dazu kommt die Möglichkeit, dass man ein Video nicht nur als Livesendung verfolgen, sondern auch aufgezeichnet und somit zeitversetzt betrachten kann. Diese Form des Angebotes und der Rezeption von Filmen nennt sich *Video-on-Demand* (VoD), ein Service, das in Österreich UPC Telekabel und seit Neuestem auch die Telekom Austria via ADSL für Spielfilme anbieten. An der Uni Wien werden bereits seit einiger Zeit Aktivitäten auf diesem Gebiet an einzelnen Organisationseinheiten, u.a. an der Fakultät für Chemie oder am Institut für Publizistik- und Kommunikationswissenschaft, angestrengt.

In Zukunft sollen in dieser Form universitätsweit Lehrveranstaltungen wie auch Vorträge, Symposien, Reden etc. aus den Festsälen der Uni Wien übertragen und angeboten werden. Der Zentrale Informatikdienst hat für dieses Vorhaben ein Pilotprojekt angestoßen, das sich derzeit in der ersten Planungsphase befindet und für das im kommenden Semester bereits erste praktische Erfahrungen gesammelt werden sollen.

Wie geht es weiter?

Folgende Schritte sind bereits angedacht:

- Zwei Teststationen mit je einem Notebook, einem Funkmikrofon für die Vortragenden und einer Videokamera mit Stativ werden ein Semester lang bei verschiedenen Lehrveranstaltungen eingesetzt, um praktische Erfahrungen mit der Video-Aufnahme zu sammeln. Dafür sollen ein oder mehrere TutorInnen zur Bedienung des Equipments ausgebildet werden.

- Die Aufnahmen werden je nach Wunsch des Lehrveranstaltungsleitenden „live“ und/oder „on demand“ zur Verfügung gestellt. Die entsprechenden Links zu den Videos werden über die Lernplattform WebCT Vista angeboten, um sie so nur einem bestimmten, registrierten Nutzerkreis zur Verfügung zu stellen. Fragen, die während einer Lehrveranstaltung auftauchen, können sofort via Chat, später über eMail oder in ein Diskussionsforum gestellt werden, zu dem alle VeranstaltungsteilnehmerInnen Zugang haben und wo auch die Fragen der Kommilitonen eingesehen werden können.

- Entsprechend den Ergebnissen aus diesem Probesemester könnten beispielsweise die nächsten Studieneingangsphasen verschiedener Fakultäten über Videostreaming abgehalten werden. Speziell für Studierende aus dem Ausland, aber auch für die Fakultäten selbst wäre dies eine kostengünstige Variante.

- Im nächsten Schritt sollen bestimmte Hörsäle sowie die Festsäle mit fest installierten Kameras, Mischpulten und Mikrophonen ausgestattet werden. Dies ermöglicht in Zukunft professionelle Aufnahmen in HDTV-Qualität. Videos aus den Festsälen und von offiziellen Events können dann nicht nur von Studierenden angesehen, sondern auch von Presse und Fernsehanstalten entsprechend verwendet werden. Damit rückt die Uni Wien ein Stück mehr in den Fokus der Öffentlichkeit.

Bereits im letzten Semester wurden für das Zentrum für Translationswissenschaft mehrere Videos unterschiedlichster Quellen (TV, DVD, VHS, Internet) konvertiert, in ein einheitliches Format gebracht und auf der eLearning-Plattform direkt den Studierenden zur Verfügung gestellt.

Michael Janousek ■

Lehrveranstaltungen für Video-on-Demand-Projekt gesucht

Für das Sommersemester 2006 sucht der Zentrale Informatikdienst noch Test-Lehrveranstaltungen, die sich am Videostreaming-Projekt beteiligen wollen. Alle Einzelheiten dazu finden Sie im nebenstehenden Artikel.

Lehrveranstaltungsleitende, die Interesse an einer Videoaufzeichnung ihrer Vorlesung haben, setzen sich bitte mit dem ***Supportbüro Neue Medien*** des ZID in Verbindung:

Tel.:	4277-14290	
eMail:	`elearning.zid@univie.ac.at`	
Adresse:	1010 Wien, Universitätsstraße 7 (NIG, Erdgeschoss, bei Stiege III)	
Öffnungszeiten:	Mo, Di, Mi, Fr	9:00 – 16:00 Uhr
	Do	9:00 – 18:00 Uhr

Ihr Linux-Rechner wurde assimiliert – ist Widerstand zwecklos?

ROOTKITS UNTER LINUX

Sie sind eines der beliebtesten Hilfsmittel der Computer-Hacker: Rootkits – die mächtigsten und tückischsten aller Trojaner.[1] *Rootkit* bedeutet soviel wie „Administratorenausrüstung", also eine Art Ausstattung an Softwarewerkzeugen, die von Dritten unrechtmäßig und meist unbemerkt in ein Computersystem eingeschleust werden, um zukünftige Logins des Eindringlings zu verbergen, Prozesse zu verstecken, Daten zu kopieren und Eingaben mitzuverfolgen.

Der Einsatz eines Rootkits erfolgt erst nach einem geglückten Einbruch, indem es seine Existenz verschleiert sowie entsprechend einhergehende Tätigkeiten des Systems vor dem eigentlichen Systemadministrator verbirgt. So sorgt es beispielsweise dafür, dass der Eindringling auch zu einem späteren Zeitpunkt wieder Root-Status (gleichbedeutend mit Administratoren-Status) auf dem System erhält. Dazu eröffnet es dem Hacker so genannte *Backdoors*. Diese „Hintertüren" lassen sich in zwei Varianten unterteilen: Zum einen in lokale Backdoors auf dem System – diese setzen die interaktive Präsenz des Angreifers auf dem geknackten System voraus – und zum anderen in Netzwerk-Hintertüren – z.B. ein offener Port, über den der Hacker von einem anderen Rechner aus privilegiert in das System einsteigen kann. Rootkits sind der ultimative Schrecken eines jeden Systemverantwortlichen.

Während unter Windows Trojaner und Rootkits derzeit zu boomen scheinen (siehe dazu auch Artikel *Ungebetene Gäste: Trojaner am Windows-PC* in *Comment 04/1* bzw. unter `www.univie.ac.at/comment/04-1/041_10.html`), ist es um die Rootkits unter Unix etwas ruhiger geworden – aber der Schein trügt. Erst kürzlich wurden zwei neue Rootkits (Phalanx und eNYeLKM; Näheres dazu im Abschnitt *Schau trau – wem?*) für aktuelle Linux-Versionen veröffentlicht, die selbst von den besten Suchwerkzeugen nicht erkannt werden.

Der Angriffszyklus

Bevor ein Hacker sein Rootkit installieren kann, muss er sich zunächst Root-Rechte auf einem System verschaffen. Der dazu notwendige Einbruch und die folgenden Schritte laufen meist nach einem festen Schema ab: Zunächst wird der Angreifer so viele Informationen wie möglich über das potenzielle Opfer beschaffen. So sucht er zuerst nach Diensten, die vom System angeboten werden. Ein so genannter Port-Scan des Systems zeigt in der Regel rasch, welche dieser Dienste offen sind. Die Scan-Methoden sind dabei je nach Vorlieben der Hacker sehr unterschiedlich: Manche gehen direkt vor, andere setzen lieber Täuschungsmanöver ein, um auch geübte Systemverantwortliche auszutricksen.

Hat der Hacker Schwachstellen gefunden – meist sind dies Systeme mit unzureichender Wartung – führt er seinen Angriff durch. Dabei verwendet er für das jeweilige System und seine Schwachstellen geeignete, hoch spezialisierte Programme, die ihm den Einstieg in das System ermöglichen. Mit der Aneignung der nötigen Rechte ist es nunmehr für den Hacker wichtig, die Spuren des Einbruchs sofort zu verwischen, damit der eigentliche Systemverantwortliche nichts bemerkt. Oft sind in Rootkits bereits entsprechende Werkzeuge zum Bereinigen von Log-Dateien enthalten. Danach richtet sich der Hacker auf dem Rechner häuslich ein und installiert sein Rootkit. Mit diesem Schritt ist er wieder bereit, sein Unwesen an einem neuen Ort zu treiben – denn häufig sind die befallenen Systeme (z.B. die mit schnellem Internetzugang ausgestatteten Rechner an der Universität Wien) nicht selbst das Ziel, sondern nur ein Zwischenwirt für den Hacker zur Verschleierung seiner Spuren.

Fallbeispiel

Das Institut X leistet sich zur lokalen EDV-Unterstützung einen größeren SuSE Linux-Server mit einem lokalen SSH (*Secure Shell*)-Zugang, einem Web-Server sowie einem Windows Fileservice mittels Samba. Der Server steht nicht hinter einer Institutsfirewall, ist aber selbst durch eine IP-Tables Firewall geschützt. Es ist Ferienzeit. Der verantwortliche Administrator, eigentlich Wissenschaftler, ist auf wohlverdientem Urlaub. Während er die freie Zeit genießt, wird ein Sicherheitsproblem bei SuSE publiziert, was dem unbeaufsichtigten Server zum Verhängnis wird. Prompt wird die Lücke im System von einem Hacker entdeckt und genutzt.

Zunächst verschafft sich der Hacker unprivilegierten Zugang zum Server. Das schlecht gewählte Root-Passwort[2] ist durch Probieren rasch geknackt. Beobachtungen des Systems zeigen dem Hacker, dass kein Administrator am System aktiv ist und er in Ruhe schalten und walten kann.

Dazu vernichtet er zuerst jegliche Informationen, die seinen Einbruch enttarnen würden. Dann schließt er die Sicherheitslücke des Webservers – kein zweiter Hacker soll ihm den eroberten Platz streitig machen. Er besorgt sich das Rootkit Adore-ng und installiert es auf dem System. Nur im kurzen Zeitraum des Bootens wären Spuren des Einbruchs

1) Als Trojanische Pferde oder kurz Trojaner bezeichnet man im Computer-Jargon schädigende Programme, die als nützliche Programme getarnt sind oder zusammenhängend mit einem nützlichen Programm verbreitet werden, aber tatsächlich auf dem Computer im Verborgenen unerwünschte Aktionen ausführen können.

2) Tipps zur Wahl eines sicheren Passworts sind unter `www.univie.ac.at/ZID/passwort/` zu finden.

sichtbar – aber da schaut keiner hin. Die Tarnung ist perfekt. Die IP-Tables Firewall wird für einen weiteren Port geöffnet und eine zweite SSH dahinter versteckt. Der Prozess ist unsichtbar, die Log-Dateien, die der zweite `ssh`-Daemon herstellen würde, werden dank Adore-ng nicht geschrieben. Da das System nicht hinter einer Institutsfirewall steht, funktioniert der Zugang zur SSH auch über den neuen, getarnten Port.

Als der Administrator aus dem Urlaub kommt, ist das System in perfektem Wartungszustand. Allerdings ist genau das verdächtig. Ihm bleibt nichts anderes übrig als zu suchen. Tage vergehen – keine Spur. Der Hacker hat perfekt gearbeitet. Panik beim Administrator, der eigentlich eine Tagung vorbereiten müsste. Zerknirscht muss er seinen TeamkollegInnen eingestehen, dass er die Situation nicht im Griff hat.

Während eine weitere Woche vergeht, kopiert der Hacker größere Datenmengen auf den Server und versteckt sie mittels des Rootkits. Daraufhin muss der Administrator feststellen, dass 40% des Plattenplatzes verbraucht sind und das System sehr langsam ist. Allerdings gibt es keinen sichtlichen CPU-Verbrauch.

Nun ist eine genaue Systemanalyse nicht mehr aufzuschieben. Erst bei einer sehr detaillierten Untersuchung treten die Probleme sichtbar hervor. Illegale Videokopien, Musikstücke etc. hat der Hacker auf dem Server abgelegt – und vermutlich weiterverkauft. Eine forensische Analyse der Festplatte zeigt, welche Schritte der Hacker anfangs machte. Das Rootkit wird deaktiviert. Der zweite `ssh`-Daemon wird belassen – es soll herausgefunden werden, von wo der Hacker kommt. Nach dem Start des Rechners läßt dieser auch nicht lange auf sich warten, kommt danach aber nie wieder. Nur die Kunden wollen noch längere Zeit Daten vom System holen. Die Rechnerquelle, von welcher der Hacker kam, liegt irgendwo in Taiwan. Eine Rechtsverfolgung dorthin ist leider unmöglich.

Vorbeugung

Um nicht selbst einen derartigen Eingriff zu erleben und Hackern nicht ahnungslos ausgeliefert zu sein, ist Vorsorge der beste Schutz! Es sollte erst gar nicht soweit kommen, dass ein System von Eindringlingen geentert und übernommen wird. Frei nach Raumschiff Enterprise: Widerstand ist nicht zwecklos! Die besten Waffen hierfür sind:

- **Minimieren der möglichen Angriffsfläche:** Nicht benötigte Services gehören abgeschaltet. Verwenden Sie eine strikte Politik: Nur das ist erlaubt, was wirklich benötigt wird.

- **Eingeschränkter Zugriff auf das System:** Meist muss nicht jeder Dienst aus der ganzen Welt erreichbar sein. Oft ist die Einschränkung auf den Netzwerkbereich der Uni Wien (131.130.0.0/16) und einige externe Internetadressen völlig ausreichend. Dazu hilft Firewalling (Konfigurationstipps hierzu sind unter `www.univie.ac.at/ZID/anleitungen/ip-tables/` zu finden).

- **Das System aktuell halten:** Hier sind vor allem die Dienste angesprochen, die dem Netzwerk zur Verfügung gestellt werden.

- **Das System regelmäßig auf Rootkits überprüfen:** Ist ein System erst einmal geentert worden, kann man sich nur noch durch eine komplette Neuinstallation und ein kritisches Überdenken der angewandten Sicherheitsstrategien verlässlich Ruhe verschaffen.

- **Den Feind kennen lernen:** Das Verhalten von Rootkits, ihre Stärken und Schwächen, lernt man am besten zu verstehen, wenn man sich selbst Rootkits besorgt und sie untersucht.

Jeder, der an einem Linux-Rechner mit Netzwerkanschluss arbeitet bzw. diesen betreut, sollte sich mit Rootkit-Versionen und deren Eigenschaften näher vertraut machen. In welcher Form Rootkits vorgehen und welche Maßnahmen zum Schutz eines Systems getroffen werden können, ist im Folgenden detailliert beschrieben.

Schau trau – wem? Rootkit-Versionen, ihre Vorgehensweise und Gegenmaßnahmen

User Mode-Rootkits

Ist ein Rootkit einmal installiert, hat der Hacker oft leichtes Spiel. Je nach Art des Rootkits werden entweder die Ausgaben der Systemprogramme so modifiziert, dass zu versteckende Dateien oder zu verschleiernde Aktivitäten nicht angezeigt werden, oder es wird im Systemkern deren Ausgabe verhindert. Erstere sind die klassischen Rootkits – die so genannten *User Mode-Rootkits*. Das bedeutet, dass z.B. die Befehle `ls`, `du`, `df` oder `find`, aber auch `ifconfig`, `netstat`, `ps`, `top` etc. einfach falsche Ausgaben anzeigen. Solche Programme laufen – auch unter root – immer im *User Mode*[3] ab, daher ihr Name. So kann zum Beispiel auch das Programm `kill` so modifiziert werden, dass bestimmte Programme nicht ohne weiteres gestoppt werden können, obwohl der Systemadministrator als root den Befehl absetzt. Hintertüren zum Eindringen schafft das Rootkit mit trojanisierten Versionen von `login`, `sshd` oder `xinetd` etc. Etwaige unerwünschte Log-Einträge werden häufig durch einen modifizierten `syslog`-Daemon verhin-

3) In Unix und Unix-ähnlichen Betriebssystemen wie Linux ist der Kernel für alle privilegierten Operationen (Ein- und Ausgabe, Verwalten von Prozessen usw.) zuständig. Solange Prozesse keine solchen privilegierten Operationen brauchen, laufen sie im *User Mode*; wenn ein Prozess z.B. Ein- oder Ausgabeoperationen durchführt, fordert er über genormte Schnittstellen, so genannte *System Calls*, die erforderlichen Dienste vom Kernel an und läuft für die Dauer der Operation im *Kernel Mode*.

dert. Damit ein Hacker seinen Einfluss auf das System und seine Umgebung ausweiten kann, sind zusätzlich häufig auch Netzwerk-Sniffer im User Mode-Rootkit enthalten. Damit lassen sich Username-/Passwort-Kombinationen auf der Ebene des Netzwerkverkehrs ausspähen. Jede Autorisierung, die unverschlüsselt erfolgt, ist davon betroffen.

Da Unix im Allgemeinen ein offenes Betriebssystem ist und viele Teile der Programmquellen ohnehin öffentlich sind, ist die nachträgliche Trojanisierung eines Programms kein Problem. Wichtig für den „Hersteller" eines Rootkits ist nur, dass er dem Systemadministrator eine konsistent falsche Sicht der Vorgänge liefert. Daher muss für User Mode-Rootkits oft eine große Anzahl von Programmen des Betriebssystems modifiziert werden. Wird ein Programm oder ein Shell-Befehl übersehen (gerne z.B. die *Shell-expansion*), so hat der Systemadministrator noch die Möglichkeit, etwas per Zufall zu entdecken (oft hilft `echo *` bei User Mode-Rootkits statt eines `ls`- oder `find`-Befehls). Ein findiger Systemadministrator sollte sich vor dieser Art von Betrug so sichern, dass er ausschließlich eigene Kopien der Originalprogramme verwendet. So sollte er beispielsweise bei der Installation des Systems die Systemprogramme kopieren und auf eine CD brennen. Will er später sichere Programme verwenden, dann kann er mittels eines `mount`-Befehls diese CD an einem geeigneten „Mountpoint" (z.B. in `/mnt/cdrom`) einhängen und mit `chroot /mnt/cdrom` seiner Shell bekannt geben, dass er die Programme von der CD verwenden möchte. Allerdings kann auch `chroot` trojanisiert sein.

User Mode-Rootkits gehen zurück auf das Jahr 1989. Damals beschränkte man sich auf das Modifizieren der System-Logeinträge (`utmp`, `wtmp` und `lastlog`). Damit konnte ein Angreifer mittels der Befehle `who`, `w` oder `last` nicht gesehen werden; allerdings konnte man mittels der Prozessliste `ps` sehr wohl Befehle bei deren Ausführung erkennen. Deswegen sagen viele, dass Rootkits 1994 entstanden sind: Damals wurden außerdem die ersten Werkzeuge so umgeschrieben, dass inkludierte Netzwerk-Sniffer unverschlüsselte Netzwerkdaten unbemerkt analysieren und Username-/Passwort-Kombinationen protokollieren konnten. Das älteste Linux-Rootkit dürfte am 11. Oktober 1994 entstanden sein. Es beinhaltete trojanisierte Versionen der Programme `ps`, `netstat` und `login` – letzteres mit Hintertür zum Anmelden als Administrator. Der Begriff *Rootkit* wurde etwa 1995 geprägt. Zwei sehr bekannte Vertreter der User Mode-Rootkits sind LRK (*Linux RootKit*) und T0rnkit, welches ab März 2001 vom „Lion"-Wurm verwendet wurde.

Kernel Mode-Rootkits

Die andere – modernere, effizientere – Art der Rootkits sind die ***Kernel Mode-Rootkits***. Diese Rootkits modifizieren die Daten vor der Ausgabe auf der Ebene des Systemkerns. Sie filtern ungewünschte Informationen heraus, bevor sie allen User Mode-Programmen zur Verfügung stehen. Mit einem `ls`- oder `find`-Befehl erhält man die versteckte Information nicht, ebenso bekommen Programme wie `ps` oder `top` den versteckten Prozess nicht zu Gesicht. Relevante neue Log-Einträge werden gar nicht an den zuständigen Daemon geliefert. Aber auch Spuren des Einbruchs, sichtbar z.B. in den Logfiles `utmp`, `wtmp` oder in `messages`, können vor dem Systemverantwortlichen geheim gehalten werden. Die Daten stehen zwar auf der Festplatte, können aber nicht angezeigt werden. Die Täuschung eines guten Kernel Mode-Rootkits ist komplett. Kernel Mode-Rootkits können zudem noch mehr: Sie sind in der Lage, die Ausführung von Programmen umzuleiten, sodass anstelle eines Programms ein anderes unbemerkt zur Ausführung gelangt.

Der einfachste Weg, einen Systemkern zu ändern, wird über dynamisch ladbare Module eingeschlagen. Jedes moderne Betriebssystem hat derartige Methoden, um seine Funktionalität während der Laufzeit zu erweitern. Ältere Unix-Systemkerne konnten hingegen nur durch Neuübersetzen und einen Neustart geändert werden.

Das Ziel eines Kernel Mode-Rootkits ist, den trojanisierenden Programmcode im Bereich des Systemkerns unterzubringen, was gleichbedeutend mit einer Funktionsänderung des Betriebssystems ist. Folgende grundsätzliche Methoden stehen dafür zur Verfügung:

- **Ladbare Kernel-Module (LKMs):** LKM-Rootkits ersetzen im Allgemeinen Systemaufrufe des Betriebssystems. Damit werden zum Beispiel die Funktionen zum Anzeigen der Prozessliste, der Liste der Dateien zum Öffnen, Lesen oder Schreiben von Dateien etc. so geändert, dass zu versteckende Informationen herausgefiltert werden. Die neuen Module werden in der so genannten *System Call Table* eingetragen. Dieses Problem haben die Linux-Kernel-Entwickler erkannt und mit den Änderungen zum Kernel 2.6 erheblich erschwert. Ein anderer, modernerer Weg führt über das *Virtual File System* (VFS). Neben dem Laden eigener neuer Kernel-Module ist es auch möglich, existierende, vertrauenswürdige, immer vom System verwendete Kernelmodule zu infizieren. Damit bleibt das Rootkit genauso unsichtbar und wird beim Neustart des Systems immer mit dem anderen Modul mitgeladen. Beispiele für LKM-Rootkits sind Knark, Adore, Adore-ng, KIS und – neu – eNYeLKM.

- **Patchen des laufenden Kernels (Modifikation des Speichers)**: Diese Rootkit-Art basiert auf der Änderung des Kernel-Abbilds (*Image*) im Speicher des Systems, welcher durch `/dev/kmem` repräsentiert wird. Rootkits dieser Art kommen ohne ladbare Kernel-Module aus und funktionieren direkt. Allerdings hat die Entwicklung rund um den Kernel 2.6 Rootkits dieser Art schwer behindert, da `/dev/kmem` nicht mehr zur Verfügung steht. Ein Einfügen eines Rootkits über `/dev/mem` ist erheblich komplizierter. SuckIT, das *Super User Control Kit*, basiert auf einer Änderung in `/dev/kmem` und ist nur noch auf älteren Linux-Kernels funktionstüchtig. Neu seit Herbst 2005 ist das Rootkit mit dem Namen Phalanx, welches auf dem Einfügen des schadhaften Codes direkt in `/dev/mem` basiert. Wegen der Schwierigkeiten

mit `/dev/mem` läuft Phalanx nicht auf allen Linux 2.6-Kernels, wurde aber auf zahlreichen Versionen von Fedora Core 4, Vanilla, Debian Gentoo und Ubuntu eingesetzt.

- **Disk Kernel-Rootkits:** Diese sind weniger elegant, aber nicht minder gefährlich. Sie werden durch Änderung der `/boot/vmlinuz`-Datei in einem Linux-System implementiert. Allerdings werden Disk Kernel-Rootkits erst nach einem Neustart des Systems aktiv, weshalb die Ursachen eines Systemneustarts immer zu hinterfragen sind. Ein Vertreter dieser Rootkit-Spezies ist kpatch.

Die ersten Kernel Mode-Rootkits entstanden 1997. Die seit damals häufigste Methode, ein Rootkit in den Kernel zu bekommen, war mittels ladbarem Kernel-Modul und einer Substitution der Systemaufrufe. Zum Vergleich: Das erste Kernel Mode-Rootkit unter Windows entstand 1999 für Windows NT.

Das Kernel Mode-Rootkit Adore-ng

Während die Rootkits Phalanx und eNYeLKM nicht ganz leicht zu installieren sind, lässt sich Adore-ng extrem einfach verwenden und funktioniert außerdem zuverlässig. Die Gefahr, diesem Rootkit auf einem System mit aktuellem Linux 2.6-Kernel zu begegnen, ist daher besonders hoch. Adore-ng funktioniert aber auch auf Systemen mit Linux 2.4-Kernel. Daher lohnt die Betrachtung dieses Rootkits besonders.

Hat der Eindringling einmal das Rootkit mittels `insmod` in den Kernel gebracht, kann es mittels des mitgebrachten Steuerprogramms `ava` (andere Namen können zur Täuschung durchaus vergeben werden) bedient werden. Der richtige Administrator wird das Rootkit jedenfalls durch ein `lsmod` nicht finden können. Das Rootkit verwendet einen so genannten *Adore-Key*, um das Kernel-Modul und das Steuerprogramm zu tarnen. Wenn nicht der Standardwert `fgjgggfd` verwendet wird, entzieht es sich einfachen Suchen. Weiters verwendet das Rootkit eine spezielle UID/GID-Kombination für Files, die zu verstecken sind. Im Jargon der Hacker sind das die ELITE_UID und ELITE_GID. Typischerweise werden hier große Zahlen genommen, was für das Auffinden von Adore-ng hilfreich sein kann.

Der Hacker kann über zwei Wege in das System kommen: Er installiert sich einen eigenen Netzwerkzugang, oder er kommt als lokaler unprivilegierter Nutzer. Als solcher wird er sehr rasch root. Das Steuerprogramm `ava` ermöglicht es, Befehle als root abzusetzen (welche alle versteckt laufen und sich einer Ansicht durch `ps` oder `top` entziehen). Mittels `ava r /bin/bash` bekommt der Angreifer eine Shell, von der er verdeckt operieren kann (siehe Abb. 1). Es ist einfach, Dateien oder Verzeichnisse vollständig vor dem Zugriff durch den Systemverantwortlichen zu entziehen. Mittels der Option `h` kann jede Datei, jedes Directory oder jeder symbolische Link im Filesystem verborgen werden. Mittels `cd` kann der Angreifer sich ein solchermaßen verstecktes Verzeichnis setzen – man muss nur wissen, wie es heißt. Dort ist alles wieder sichtbar, sofern es nicht noch einmal extra versteckt wird. In Abb. 2 ist dargestellt, wie ein Verzeichnis zum Verschwinden gebracht wird.

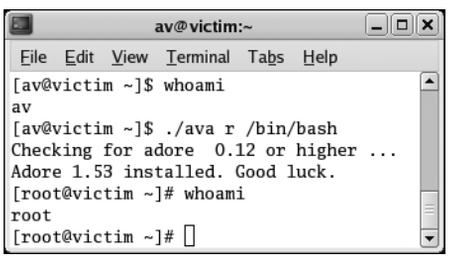


Abb. 1: Versteckte Root-Shell durch Adore-ng Rootkit

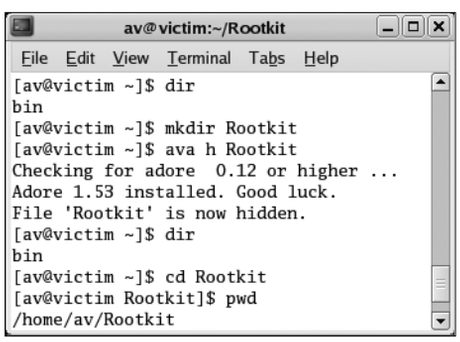


Abb. 2: Verstecken von Verzeichnissen durch Adore-ng Rootkit

Da das Kernel Mode-Rootkit (anders als ein User Mode-Rootkit) die Dateien vollständig verbirgt, ist ein verstecktes Verzeichnis oder eine versteckte Datei durch keines der regulären Systemwerkzeuge aufspürbar. Weder `echo` noch `find` können diese Dateien entdecken. In Abb. 3 ist zu sehen, wie Adore-ng durch das Verstecken eines Verzeichnisses auch die darin enthaltenen Dateien unsichtbar macht.

Die Versteckfunktionen von Adore-ng erstrecken sich nicht nur auf Dateien. Auch Prozesse können versteckt oder wieder sichtbar gemacht werden. Ein von einem versteckten Prozess erzeugter weiterer Prozess – zum Beispiel als Befehl auf einer Shell initiiert – ist ebenfalls unsichtbar. Das Verstecken ist sehr einfach, wenn das Rootkit bereits im Kernel ist. In Abb. 4 ist der Prozess (`bash`) zunächst sichtbar. Er wird anschließend unsichtbar gemacht. Jeder weitere Befehl, der über diesen Prozess abgegeben wird, ist in keinem Prozesslisting auffindbar. Schlimmer noch: Sogar jedes Logging eines versteckten Prozesses in die systemweiten Logfiles wird unterbunden. Damit ist für den Angreifer sichergestellt, dass er keine unbeabsichtigten Logfile-Einträge verursacht. Der ahnungslose Systemadmini-

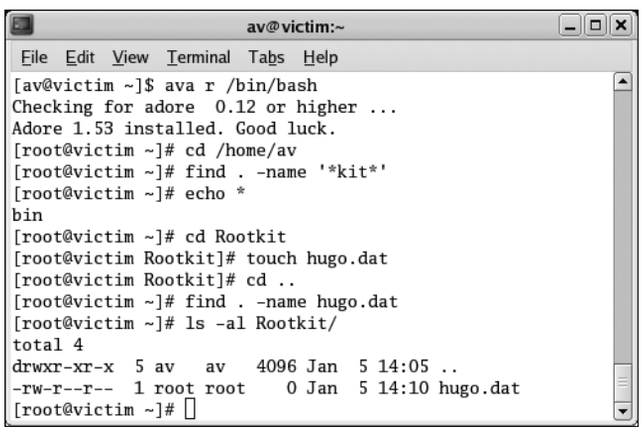


Abb. 3: Unauffindbare Dateien durch Adore-ng Rootkit

strator hat keine Chance, den Eindringling auf diesem Weg zu finden.

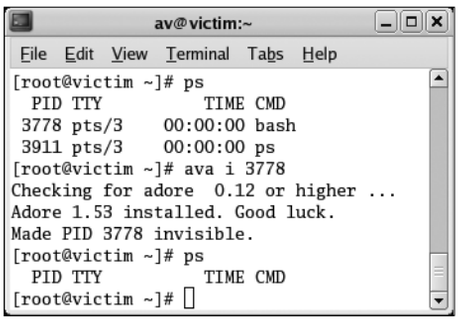


Abb. 4: Verstecken von Prozessen durch Adore-ng Rootkit

Fährtenlesen bei Rootkits

Da Rootkits die moderne Weiterentwicklung des Trojanischen Pferdes sind, ist es grundsätzlich schwierig, Spuren zu finden. Die zentrale Eigenschaft eines Kernel Mode-Rootkits, die Daten *vor* ihrer Verfügbarkeit zu fälschen, macht das erfolgreiche Aufspüren besonders schwer. Es gibt zwar einige Programme zum Suchen von Rootkits, jedoch hat sich im Test gezeigt, dass deren Auskünfte nicht unbedingt zutreffen müssen. Ein Klassiker unter den frei verfügbaren Rootkit-Suchwerkzeugen ist chkrootkit. Ein weiteres, sehr gutes freies Werkzeug zum Aufspüren von Rootkits ist auch der Rootkit Hunter oder kurz rkhunter. Beide finden eine überwiegende Vielzahl von User Mode- als auch Kernel Mode-Rootkits, versagen aber durchaus bei deren modernsten Vertretern. Für beide Suchwerkzeuge gilt: Im Falle von User Mode-Rootkits ist die Verfügbarkeit unverfälschter Originalprogramme für eine verlässliche Suche unumgänglich. Es ist daher sinnvoll, sich nach der Installation eines Linux-Systems die bereits genannten Systemprogramme auf eine CD zu brennen, sodass diese Werkzeuge darauf zugreifen können.

chkrootkit

chkrootkit läuft unter root auf dem System, welches zu untersuchen ist. Die Software ist rasch installiert. Unter `www.chkrootkit.org` kann die neueste Version heruntergeladen werden. Die beigefügte Prüfsumme ist mittels `md5sum` zu verifizieren. Der *Tarball* (die gezippte Tar-Datei) wird mittels `tar xvzf chkrootkit_`*`versionsnummer`*`.tar.gz` entpackt, wobei *`versionsnummer`* die aktuelle Softwareversion von chkrootkit ist. Anschließend wechselt man in das Verzeichnis der neu ausgepackten Software und tippt den Befehl `make sense` ein. Das Programm wird nun erstellt und kann mittels `./chkrootkit` aufgerufen werden. Wer einen sicheren Satz von Systemprogrammen auf CD verfügbar hat, verwendet den Befehl `./chkrootkit -p /mnt/cdrom`, wenn `/mnt/cdrom` der Mountpoint der CD ist. chkrootkit benötigt die Programme `awk`, `cut`, `echo`, `egrep`, `find`, `head`, `id`, `ls`, `netstat`, `ps`, `sed`, `strings` und `uname` und findet derzeit 60 verschiedene Rootkits.

rkhunter

rkhunter, verfügbar unter `www.rootkit.nl`, ist ein etwas komplexeres Werkzeug als chkrootkit. Die Software beschränkt sich nicht nur auf das direkte Suchen, sie ist auch in der Lage, einen Vergleich wichtiger Dateien zur letzten Suche zu ziehen, und prüft auch einige riskante Systemeinstellungen. Anders als chkrootkit wird rkhunter im System installiert. Nach dem Herunterladen des Tarballs wird rkhunter analog zu chkrootkit entpackt. Die Installation geschieht dann im Softwareverzeichnis des entpackten rkhunter mittels `./installer.sh`. Standardmäßig installiert sich die Software unter `/usr/local/rkhunter`. Leider ist dies für Hacker sofort ersichtlich, sodass diese, nachdem sie root-Rechte erhalten haben, die Konfigurationen des rkhunter so abändern können, dass die Ergebnisse eines Suchlaufes nicht mehr stimmen müssen. Deswegen – und weil Prüfsummen wichtiger Dateien dort abgelegt werden – ist zu empfehlen, die Installation von `installer.sh` so abzuändern, dass mittels des Parameters `-installdir` *`Installationsverzeichnis`* ein sicheres Verzeichnis angegeben wird, das nur zum Zeitpunkt des Tests auf dem System gemountet ist. Der USB-Stick des Systemadministrators wäre zum Beispiel ein geeigneter Ort. Nach dem Test sollte der Befehl `umount` und das Abziehen des Sticks nicht vergessen werden. Im Unterschied zu chkrootkit prüft rkhunter auch verdächtige Internetports (siehe Artikel *Firewalls: Schutz vor Gefahren aus dem Internet* in *Comment 02/2*, Seite 14 bzw. unter `www.univie.ac.at/comment/02-2/022_14.html`). So installieren manche Rootkits Netzwerk-Hintertüren, die permanent auf bestimmten Ports auf Verbindungsaufnahme des Hackers warten. Dies ist für die Rootkit-Suche an sich ein Vorteil, da manche Rootkits nur auf diesem Wege gefunden werden können. Allerdings kommt es auch vor, dass rkhunter zu viele Ports verdächtigt (mehr Informationen dazu sind unter dem URL `www.rootkit.nl` zu finden). Der Befehl `rkhunter` hat zahlreiche mögliche Parameter. Ein regulärer Test wäre mittels `rkhunter -c` durchzuführen.

Eigenes Fährtenlesen

Während beide Werkzeuge beim Suchen von User Mode-Rootkits recht erfolgreich sein können, ist ihre Effizienz bei den moderneren Kernel Mode-Rootkits nicht groß. Aktuelle Versionen von Adore-ng, Phalanx oder enYeLKM werden nicht gefunden. Welche Möglichkeiten hat nun der Administrator, um zu erkennen, dass sein System ein Problem hat? Bei nicht allzu großen Servern kann er sich den Netzwerkverkehr näher ansehen. Das ist beispielsweise mit einem Monitoring-Werkzeug wie ethereal möglich, welches in den meisten Linux-Distributionen enthalten ist (siehe z.B. auch `www.ethereal.com`).

Reisen die Benutzer des Systems viel (d.h. kommen sie von vielen unterschiedlichen, nicht vorhersagbaren IP-Adressen), dann kann das schwierig werden. Ein zweiter Nutzen des ethereal-Sniffers ist, dass er – unter root betrieben – die Netzwerkkarte in den so genannten „promiskuitiven Modus“ setzt. Sie empfängt dann auch Datenpakete, die nicht unbedingt an das System adressiert sind, und leitet sie an das Betriebssystem weiter. Damit kann auch der Sniffer Netzwerkverkehr aufnehmen, der nicht direkt für das System bestimmt ist. Ein Rootkit, das beim Befehl `ifconfig` die Anzeige des promiskuitiven Modus unterbindet, um dem Administrator die Tätigkeit des Sniffens nicht anzuzeigen, kann so gefunden werden (bei manchen Linux-

Versionen wird dies allerdings von Haus aus nicht angezeigt). Schaltet der Administrator ethereal ein und ist das Rootkit aktiv und verhindert die Anzeige des promiskuitiven Modus, so weiß der Verantwortliche, dass mit seinem System etwas nicht in Ordnung ist. Das Programm ifpromisc des Suchwerkzeugs chkrootkit bewerkstelligt die verlässliche Anzeige. Dazu ruft man entweder chkrootkit selbst auf und liest die Ergebnisse, oder man startet `ifpromisc` direkt. Wenn ein Programm wie ethereal die Netzwerkkarte in den promiskuitiven Modus versetzt hat, zeigt ifpromisc folgendes an: `eth0: PF_PACKET(/usr/sbin/ethereal)`, wobei der Pfad zu ethereal in der Anzeige wichtig ist: Er sollte mit der Originalplatzierung des Programms ethereal übereinstimmen. Das kann mit dem Befehl `which ethereal` überprüft werden.

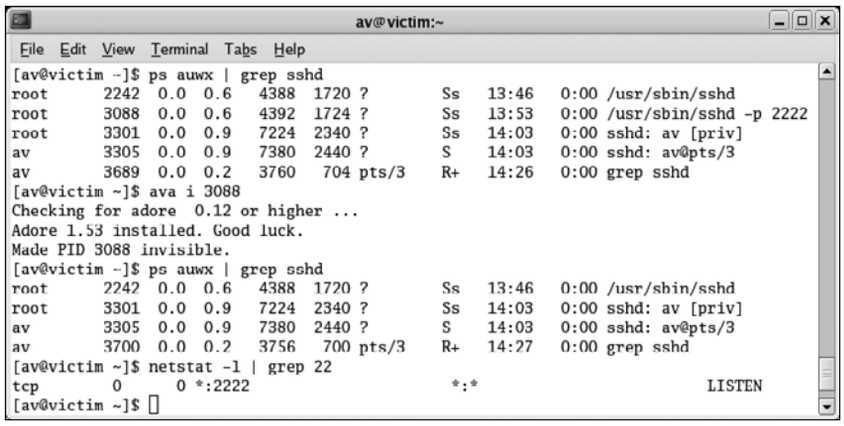


Abb. 5: Versteckt operierender SSH-Daemon auf Port 2222, welcher aufgrund ungeschickter Installation mittels `netstat -l` enttarnt werden kann

Da viele Kernel Mode-Rootkits ELITE_UID/GID-Kombinationen verwenden, die noch dazu aufgrund der Gefahr von Kollision und Entdeckung meist nicht innerhalb des regulären Nutzerbereiches (der Bereich, den der Administrator für die Nutzerkennungen angelegt hat) vergeben werden, lässt sich dies nutzen, um das Vorhandensein dieser Trojaner aufzuspüren. Dazu hilft uns Knoppix (eine komplett von CD oder DVD lauffähige Zusammenstellung von GNU/Linux-Software, zu finden unter `www.knoppix.de`). Durch die Vorgangsweise, Linux von CD zu booten und auf CD zu betreiben, ist Knoppix gegenüber Angriffen sehr sicher: Ein Neustart, und die Standardkonfiguration wird wiederhergestellt. Bootet man Knoppix von der CD, kann man mittels `ls -alR <Dateisystem>` das entsprechende Dateisystem rekursiv, also den gesamten Verzeichnisbaum, auflisten. Auch wenn das Listing sehr lang wird – große UID/GID-Nummern fallen mit Sicherheit auf. Sie sind unter den genannten Voraussetzungen ein nahezu untrügliches Zeichen für das Vorhandensein eines Rootkits. Knoppix kann zudem hilfreich sein, ein „sauberes“ chkrootkit laufen zu lassen.

Im Falle von Adore-ng gibt es für *ScriptKiddies* (Hacker, die vorgefertigte Schadprogramme verwenden, aber eigentlich keine Ahnung haben, was sie machen) allerdings auch Fallen. Installiert der Angreifer beispielsweise eine zweite Secure Shell zur Verbindungsaufnahme auf einem alternativen `ssh`-Netzwerkport (die Ports 2222 und 7350 werden von Adore-ng standardmäßig vorgeschlagen und sollten vor einem Listing durch `netstat -l` versteckt sein), so hat er glücklicherweise viele Möglichkeiten, etwas falsch zu machen, und der Zustand, dass ein Daemon hinter einem dieser Ports lauscht, wird nicht verborgen (siehe Abb. 5). Wie es allerdings richtig geht, wird hier nicht verraten.

Ausblick

Im Anschluss finden Sie den weiterführenden Artikel *Sonys digitaler Hausfriedensbruch*, der sich mit dem Einsatz von Hacker-Methoden durch Firmen beschäftigt. Ferner ist geplant, in einer der nächsten *Comment*-Ausgaben über Rootkits unter Windows zu berichten sowie über ausgefeilte Methoden, um diese Eindringlinge abzuwehren.

Aron Vrtala ■

SONYS DIGITALER HAUSFRIEDENSBRUCH

Wenn Firmen Hacker-Methoden anwenden

Der Musikverlag Sony BMG Music Entertainment hat eine ganze Reihe von CD-Titeln mit einem *Digital Rights Management* (DRM) namens XCP-Aurora versehen. Dieser Kopierschutz der britischen Software-Firma First4Internet (`www.first4internet.com`) greift jedoch unter Windows allzu tief ins System ein: Ende Oktober 2005 entdeckte der Sicherheitsexperte Mark Russinovich von Sysinternals (`www.sysinternals.com`), dass Sony auf den mittels DRM kopiergeschützten CDs ein Rootkit einsetzt, welches sich den Blicken der PC-EigentümerInnen entzieht. Der Kopierschutz installiert u.a. Filtertreiber für Festplatten und CD-ROM-Laufwerke. Damit kontrolliert die Trojaner-Software[1] die Zugriffe auf die Medien und speichert im Verborgenen Nutzungsinformationen. Selbstredend wird diese Software weder in der Software-Liste der Systemsteuerung angezeigt noch lässt sie sich mittels Uninstaller deinstallieren.

1) siehe Artikel *Ungebetene Gäste: Trojaner am Windows-PC* in *Comment 04/1*, Seite 10 bzw. unter `www.univie.ac.at/comment/04-1/041_10.html`

Das XCP-Rootkit (es dürfte in seiner Funktionsweise dem ersten Windows-Rootkit *NT Rootkit* angelehnt sein, das 1999 von Greg Hoglund entwickelt wurde) versteckt die ihm zugehörigen Dateien, Verzeichnisse, Prozesse und Registry-Einträge. Es versteckt alles, dessen Name mit `$sys$` beginnt. Daher kann sich mit Hilfe dieses Kopierschutzes unerwünschte, von HackerInnen stammende Software ebenfalls verbergen. Wenige Tage nach dem Bekanntwerden des Rootkits war bereits der Trojaner *Breplibot* im Umlauf, der `$sys$` als Tarnung verwendet. Ein weiterer solcher Trojaner ist z.B. *Backdoor.IRC.Snyd.A* – er installiert eine Hintertür zum Einstieg in das Windows-System. Wegen dieser Features von XCP wird in einschlägigen Internet-Foren bereits zum Kauf von Sony-CDs geraten.

Für die EntwicklerInnen von Trojanern und Viren ging ein Traum in Erfüllung: XCP-Aurora ist das erste käufliche Rootkit, ironischerweise mit LGPL-Lizenz (siehe `www.gnu.org/copyleft/lesser.html`). Für Sony BMG ging der Schuss nach hinten los: Auch Sonys eigene Spiele können mittels des Rootkits in geknackter Version verwendet werden (eine Musik-CD ist weit billiger als die Spiele).

Für die AnwenderInnen ist das XCP-Rootkit ein doppelter Schaden. Nicht nur, dass es Tür und Tor für Angriffe öffnet, es ist auch schlecht programmiert: Der installierte Treiber fragt jede zweite Sekunde alle laufenden Prozesse nach geöffneten Dateien ab, um sicherzustellen, dass kein Programm unbemerkt zu viele Kopien der geschützten Dateien produziert. Nachdem Programme unter Windows üblicherweise sehr viele Dateien geöffnet haben, bedeutet diese Vorgangsweise einen massiven Performanceverlust für den PC (geprüft wird auch dann, wenn sich gar keine CD im Laufwerk befindet). Darüber hinaus kann das Rootkit in bestimmten Situationen das System zum Absturz bringen und verursacht zusätzlichen Netzwerkverkehr: Es meldet die Verwendung der CDs an die Herstellerfirma und bietet Sony BMG damit die Möglichkeit, Nutzungsprofile zu erstellen.

Sony BMG demonstriert, wie Firmen um jeden Preis industrielle Interessen durchzusetzen versuchen. Mit dem Rootkit konfrontiert, reagierte Sony zunächst sehr unsensibel: *„Ich glaube, die meisten Menschen wissen gar nicht, was ein Rootkit ist, warum sollen sie sich also darum kümmern?“*, meinte Thomas Hesse, Vorsitzender der Abteilung *Global Digital Business* bei Sony BMG. Da die Kritik an Sony trotzdem nicht verstummen wollte, bietet die Firma seit einiger Zeit auf der Webseite `http://cp.sonybmg.com/xcp/` einen Deinstaller (der anfangs selbst eine große Sicherheitslücke in betroffene Windows-Systeme riss) sowie einen CD-Austausch an.

Das Vorgehen von Sony BMG löste eine Menge Fragen und Diskussionen über Gegenwart und Zukunft von Kopierschutzmechanismen aus. Es ist das erste Mal, dass eine Firma zum Schutz geistigen Eigentums und der damit verbundenen Rechte Hackerwerkzeuge einsetzt. Der weltweite Sturm der Entrüstung wird solche Methoden hoffentlich zukünftig verhindern.

Aron Vrtala ■

LAMPORTTAUEPSILONXI

Textverarbeitung und mehr

Hinter diesem kryptischen Namen steckt das in manchen Fachgebieten wohl weltweit am öftesten verwendete, aber auch in der breiten Öffentlichkeit am wenigsten bekannte computergestützte Textverarbeitungssystem: LaTeX. Nahezu jede naturwissenschaftliche Publikation, von Diplomarbeiten über Fachartikel bis hin zu Fachbüchern, wurde mit LaTeX geschrieben. LaTeX ist für alle Betriebssysteme kostenlos erhältlich, die zahlreichen BenutzerInnen und verfügbaren Module machen es zu einem leistungsstarken Werkzeug in der modernen Computerwelt. Der folgende Artikel soll einen ersten Einblick in LaTeX und einige Starthilfen für den Beginn bieten; es wird jedoch bewusst darauf verzichtet, die Leserschaft mit dem „eigentlichen LaTeX“, sprich der Befehlsstruktur, zu quälen. Eine auch nur halbwegs vollständige Anleitung zu LaTeX würde den Rahmen des *Comment* ohnehin bei weitem sprengen.

Die Geschichte von LaTeX reicht zurück bis ins Jahr 1977: Damals begann Donald E. Knuth an der Stanford University ein Textverarbeitungssystem zu entwickeln, das später als **T**au**e**psilon**X**i (TeX) einen weltweiten Siegeszug antrat. Die Zielsetzung war relativ klar umrissen: Die AutorInnen wissenschaftlicher Bücher sollten mit Hilfe eines universalen computergestützten Textverarbeitungssystems mathematische Formeln so editieren können, dass diese exakt so dargestellt wurden wie gewünscht. Die entsprechenden Schriftarten sollten mit METAFONT, einer eigens entwickelten Beschreibungssprache für Vektorschriften (siehe `http://de.wikipedia.org/wiki/Metafont`), definiert werden.

Auch wenn es im Jahr 2006 etwas befremdend klingt: Das Setzen von mathematischen Formeln für den Druck der Fachliteratur war bis vor 20 Jahren fast so langwierig wie das Errechnen der Formeln selbst und nur von Spezialisten des Buchdrucks zu bewerkstelligen, was sich natürlich auf den Preis auswirkte. Auch TeX war anfangs noch relativ unflexibel und gekennzeichnet von vielen Fehlern (die später sukzessive korrigiert wurden – heute ist TeX praktisch fehlerfrei). Deshalb entwickelte Leslie Lamport im Jahr 1982 das La(mport)TeX-System, das durch eine relativ einfache

LaTeX-Linksammlung

Archive & Linkseiten

`www.ctan.org`

Comprehensive TeX Archive Network, der Einstiegspunkt schlechthin – hier findet man so ziemlich alles, was es über LaTeX gibt

`www.dante.de`

Deutschsprachige Anwendervereinigung TeX e.V.

`www.esm.psu.edu/mac-tex/`

alles über LaTeX und Mac OS X

`http://staff.ttu.ee/~alahe/alatex.html`

umfangreichste Linksammlung zum Thema

Einführungen

`www.uni-giessen.de/hrz/tex/cookbook/cookbook.html`

ein Kochbuch für EinsteigerInnen

`www.infosun.fmi.uni-passau.de/infosun/software/latex/latex_tips.html`

jede Menge Tipps und Tricks

`www.weinelt.de/latex/`

alle Befehle, sehr übersichtlich dargestellt

`http://tex.loria.fr/graph-pack/grf/grf.htm`

alles über LaTeX und Grafiken

`http://sites.inka.de/picasso/latex.html`

alles über LaTeX und Grafiken, in Deutsch

`http://latex.tugraz.at/`

LaTeX@TUG, umfangreiches Projekt der Technischen Universität Graz

Editoren

`www.winedt.com`

WinEdt, ein ASCII-Editor für Windows (*„with a strong predisposition towards the creation of [La]TeX documents“*)

`www.lyx.org`

LyX, der erste WYSIWYM-Editor für LaTeX (*What You See Is What You Mean* – dabei wird zwar die logische Textauszeichnung, wie Überschriften oder Listen, am Bildschirm angezeigt, nicht aber die endgültige Formatierung des Textes)

`www.xm1math.net/texmaker/`

Texmaker, ein Editor für alle Betriebssysteme

`www.winshell.de`

WinShell für LaTeX mit vielen Zusatzprogrammen

`www.tex-tools.de/cms/`

WinTeX XP, vor allem für Windows-BenutzerInnen sehr zu empfehlen

Makros & Packages

`www.miktex.org`

MiKTeX, ein komplettes LaTeX-System für fast alle Betriebssysteme

`www.tug.org/texlive/`

TeX Live, eine TeX-Distribution für AIX, Mac OS, IRIX, Linux, Unix, Sun, Windows

`www.tug.org/mactex/`

MacTeX

`www.tug.org/teTeX/`

teTeX, eine vollständige TeX-Distribution für Unix-kompatible Systeme

Werkzeuge

`www.tug.org/yandy/`

Y&Y's Werkzeuge

`www.cs.wisc.edu/~ghost/`

Ghostscript, Ghostview und GSview, die Klassiker

`www.dessci.com/de/`

MathType, ein Formeleditor für MS-Word, der auch LaTeX-Formate ausgeben kann

`http://word2tex.com/`

Word2Tex, verwandelt MS-Word-Dokumente in LaTeX, ganz brauchbar

`http://latex.sehnot.de/`

beliebter LaTeX-Generator, nur für einfache Anwendungen geeignet

Zeichensätze

`http://texcatalogue.sarovar.org/bytopic.html#languages`

vollständige Liste aller unterstützten Zeichensätze

Befehlskette zur Kontrolle der Dokumentstruktur und des Layouts besticht. Mittlerweile ist LaTeX2e(psilon) der verwendete Standard; er basiert auf der aktuellen TeX-Version 3.141592.[1)]

Was ist LaTeX?

Die knochentrockene Definition lautet: TeX ist ein äußerst flexibles, rechnerunabhängiges Satzsystem zum Erstellen von Dokumenten in Buchdruckqualität; LaTeX ist ein integrierter Satz von Ergänzungen (*Makros*) zu TeX, die vorgefertigte Formatierungsanweisungen (*Styles*) enthalten, was das Arbeiten mit TeX wesentlich vereinfacht.

Mit Hilfe von Steuerbefehlen entscheidet LaTeX, wie etwas im Dokument angeordnet bzw. dargestellt wird, und ist daher in etwa mit HTML vergleichbar. Der wesentliche Unterschied: Bei einer HTML-Datei interpretiert der Browser die eingebundenen Steuerbefehle und zeigt die Inhalte des Dokuments dann entsprechend an; das Endergebnis kann jedoch – abhängig von Faktoren wie beispielsweise den am jeweiligen PC installierten Schriftarten oder den verwendeten Spracheinstellungen – recht unterschiedlich ausfallen. Ein LaTeX-Dokument hingegen muss zunächst mit einer speziellen Software übersetzt („kompiliert“) werden; erst die daraus resultierende DVI-Datei[2)] kann mit Hilfe eines weiteren Zusatzprogramms am Bildschirm grafisch angezeigt werden. Im Gegensatz zu HTML ist LaTeX darüber hinaus sehr kompromisslos, was Syntaxfehler anbelangt: Ist der Quellcode der Datei nicht korrekt, wird eine HTML-Datei in den meisten Fällen nur unansehnlich, ein LaTeX-Dokument aber gar nicht kompiliert.

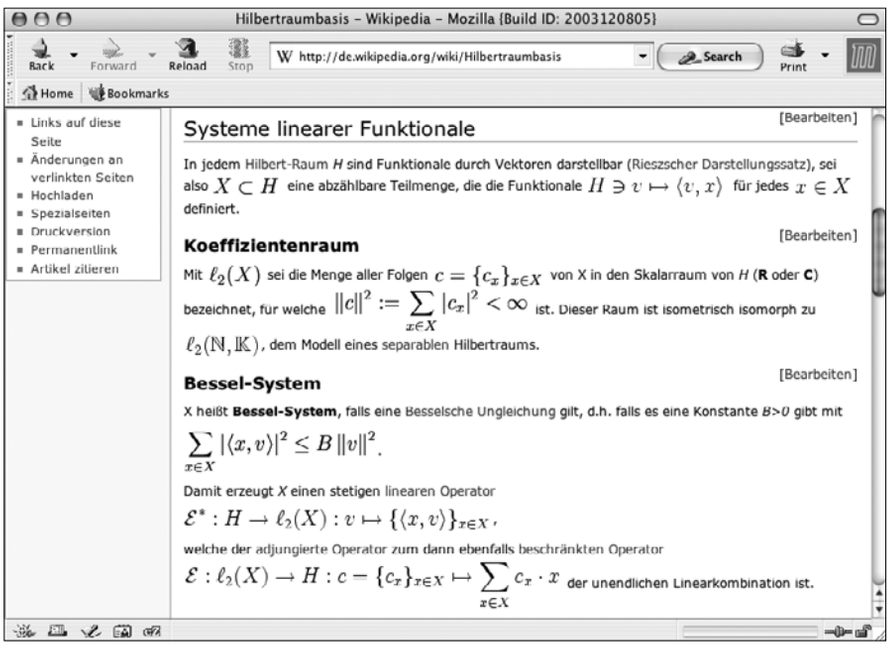
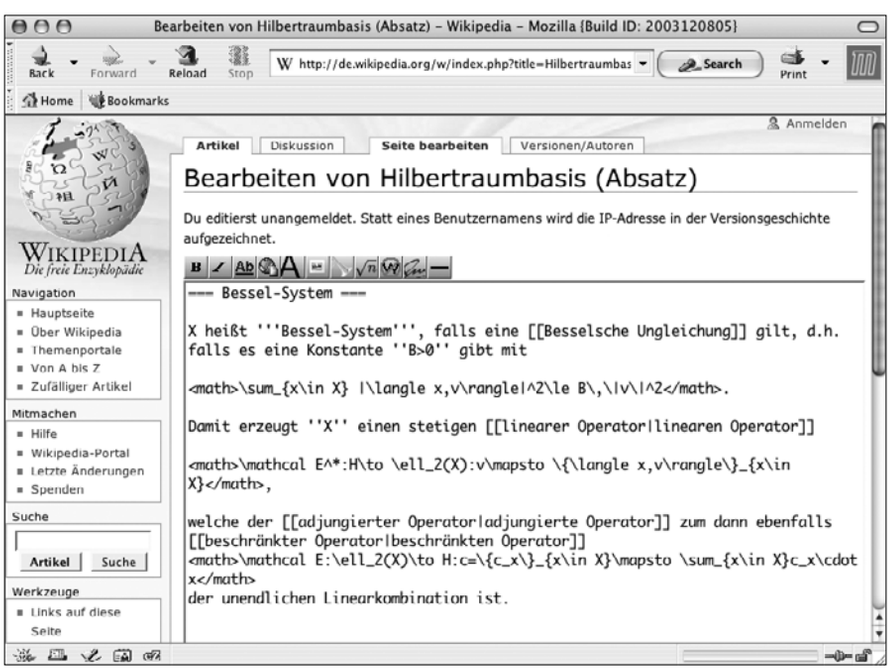


Abb. 1 (oben): Wikipedia-Seite mit LaTeX-Elementen
Abb. 2 (unten): Bearbeiten dieser Seite in Wikipedia



Der große Vorteil von LaTeX liegt darin, dass DVI-Dateien unabhängig von Betriebssystem, Schriftsätzen und Spracheinstellungen auf jedem Computer identisch aussehen – eine Eigenschaft, die der Output der meisten kommerziellen Desktop-Programme nicht besitzt. Im Vergleich mit Textverarbeitungsprogrammen wie MS-Word punktet LaTeX vor allem, wenn mathematische Zeichen gefragt sind: Das Setzen von Formeln aller Art gelingt mit LaTeX um Klassen besser. Abgesehen von der etwas gewöhnungsbedürftigen Bedienung ist LaTeX aber ohnehin mit professionellen Layout-Programmen (z.B. Adobe InDesign, Quark XPress) viel näher verwandt als mit Textverarbeitungen.

Wie bereits erwähnt, ist LaTeX für alle Betriebssysteme kostenlos erhältlich. Die Anzahl der BenutzerInnen weltweit und die Fülle der verfügbaren Werkzeuge sind beachtlich. Egal welche Frage ansteht – für jedes LaTeX-Problem gibt

1) Donald E. Knuth hatte 1977 vorgeschlagen, die transzendente Zahl π als endgültige Versionsnummer für TeX zu verwenden. Das ist die für seinen verschrobenen Humor typische Art anzudeuten, dass es nie eine endgültige Version geben wird: Eine transzendente Zahl hat unendlich viele Stellen nach dem Komma.

2) DVI steht für ***dev**ice **i**ndependent*, also geräteunabhängig.

es bereits eine Lösung, die in den unzähligen Foren und Beschreibungen einfach gefunden werden kann.

Anwendungsbereiche

Natürlich würde niemand seinen Einkaufszettel schnell einmal mit LaTeX schreiben; beim Setzen von mathematischen Formeln ist es aber immer noch der Standard schlechthin. Viele naturwissenschaftliche Fachpublikationen werden von den Verlagen nur als LaTeX-Dokumente akzeptiert, und auch an der Universität Wien sind nahezu alle Diplomarbeiten und Dissertationen in diesem Bereich mit Hilfe von LaTeX entstanden.

Darüber hinaus gibt es auch unzählige AnwenderInnen in anderen Fachgebieten, vor allem in der Linguistik. Dank METAFONT ist LaTeX in Bezug auf Zeichensätze sehr flexibel: Neben allen gängigen afrikanischen, asiatischen, europäischen und indianischen Sprachen sind beispielsweise auch Zeichensätze für die Hieroglyphen und das Olmekische verfügbar. Diese können ganz einfach in jedes Dokument eingebunden werden – ohne zusätzlichen Installationsaufwand und unabhängig von der Sprache des Betriebssystems. Eine vollständige Liste der unterstützten Zeichensätze ist unter `http://texcatalogue.sarovar.org/bytopic.html#languages` zu finden.

Eine sehr nette LaTeX-Anwendung aus der Musikwissenschaft sei hier ebenfalls erwähnt: Mit MusiXTeX (siehe `http://icking-music-archive.org/software/indexmt6.html`) ist es möglich, Noten in einem professionellen Layout darzustellen.

Auch Wikipedia setzt auf LaTeX: Am Beispiel des Wiki-Quellcodes der Webseite `http://de.wikipedia.org/wiki/Hilbertraumbasis` ist erkennbar, wie einfach die MediaWiki-Software das Einbinden von LaTeX in HTML macht (siehe Abb. 1 & 2 auf Seite 27; Näheres zu Wiki-Software finden Sie im Artikel *WIKI – Back to the Future* auf Seite 49).

Mit LaTeX arbeiten

Im *Comprehensive TeX Archive Network* (`www.ctan.org`) – jenem Ort im Internet, wo jede Suche nach „LaTeX-Allerlei" gestartet werden sollte – steht neben zahlreichen Zusatzprogrammen, Dokumentationen, Tutorials etc. auch das LaTeX-Basispaket zum Download bereit. Die Installation gestaltet sich in der Regel völlig problemlos.

Bevor man beginnt, mit LaTeX zu arbeiten, sollte man sich vor Augen führen, dass jedes LaTeX-Dokument grundsätzlich immer gleich und absolut logisch aufgebaut ist:

1. **Vorspann**: Hier wird die globale Struktur des Dokuments festgelegt. Das sind im Allgemeinen das Papierformat, die Textbreite und -höhe, Seitenränder, Seitenkopf und -fuss sowie die einzubindenden Module für Grafiken und Sprachen.

2. **Textteil**: Der Textteil umfasst den gesamten Inhalt des Dokuments – Titelseite, Text, Bilder und verschiedene Verzeichnisse (Inhalt, Tabellen, Bilder).

3. **Bibliografie**: Diese beinhaltet eine Auflistung der im Textteil verwendeten Literatur.

Ist man mit dem LaTeX-Befehlssatz – der, wie eingangs erwähnt, nicht Gegenstand dieses Artikels sein soll – vertraut, so kann man nun mit jedem beliebigen Text-Editor ein LaTeX-Dokument verfassen. In diesem Fall empfiehlt es sich, die Datei hin und wieder zu speichern, zu kompilieren und die DVI-Datei dahingehend zu überprüfen, ob sie dem gewünschten Ergebnis entspricht.

In der Regel wird man jedoch eine bequemere Variante der Bearbeitung wählen. Mittlerweile sind viele LaTeX-Editoren verfügbar (siehe *LaTeX-Linksammlung* auf Seite 26), die in punkto Funktionalität und Bedienung mit HTML-Editoren vergleichbar sind und in den meisten Fällen auch eine integrierte Vorschaufunktion enthalten. Zudem gibt es vorgefertigte „Grundgerüste" für verschiedene Dokumenttypen (z.B. für Fachartikel), sodass man auch ohne Kenntnisse des Befehlssatzes relativ einfach LaTeX-Dateien erstellen kann.

Wie bereits angesprochen, ist eine Datei, die in LaTeX geschrieben wurde, nicht unmittelbar verwendbar. Erst nachdem sie mit einem so genannten LaTeX-Compiler in eine DVI-Datei umgewandelt wurde, kann sie am Bildschirm grafisch dargestellt werden – dann allerdings *device independent*, also unter jedem Betriebssystem in absolut identischer Form. Die dafür benötigten Werkzeuge wie z.B. der Previewer *Yap* sind fester Bestandteil jedes LaTeX-Pakets.

DVI- und LaTeX-Dateien können praktischerweise in viele andere Dateiformate konvertiert werden. Die folgenden Makros sind ebenfalls in den meisten Paketen enthalten (wenn nicht, ist ein Link zur Software angegeben):

- **HTML:** *latex2html* und *dvi2html*
- **PDF:** *latex2pdf* und *dvi2pdf*
- **Postscript:** *dvi2ps*
- **RTF:** *latex2rtf* (`http://latex2rtf.sourceforge.net/`)
- **GIF und PNG:** *Textogif* (`www.fourmilab.ch/webtools/textogif/`)

Im Allgemeinen sollte man sowohl die LaTeX- (bevorzugt) als auch die DVI-Datei in das gewünschte Format umwandeln und die Resultate vergleichen: Vor allem wenn Grafiken eingebunden sind, kann es in seltenen Fällen zu einem unterschiedlichen Ergebnis kommen, weil die Papierformate (zum Beispiel A4 und/oder Letter) nicht immer einheitlich interpretiert werden. Die Umwandlung in eine MS-Word-Datei wird vom klassischen LaTeX-Paket nicht unterstützt, sondern ist nur mit Hilfe „externer" Programme möglich.

Ernst Paunzen ■

NEUE STANDARDSOFTWARE

Neue Produkte (Stand: 1. März 2006)

- Adobe InCopy CS2 1.0 für Win. und Mac
- Apple iLife 06 für Mac
- Apple iWork 06 für Mac
- Corel Draw X3 für Win.
- Corel PaintShop Pro X für Win.
- Endnote 9 für Win. und Mac
- ESRI ArcGIS 9.1 (siehe auch Seite 30)
- FileMaker Pro 8.0 für Win. und Mac
- InfoZoom Prof. 4.0 für Win.
- Macromedia Captivate (Robodemo) 1.01 für Win.
- Macromedia Dreamweaver 8 für Win. und Mac
- Macromedia Fireworks 8 für Win. und Mac
- Macromedia Flash 8 Prof. für Win. und Mac
- MS-AutoRoute Euro 2006 für Win.
- MS-Digital Image Suite 2006 für Win.
- MS-Encarta Premium 2006 für Win.
- MS-Money Deluxe 2006 für Win. (nur englisch)
- MS-Visual Studio Prof. 2005 für Win.
- Nero 7 für Win.
- Omnipage 15 für Win.
- Symantec Antivirus 10.0 für Mac
- Symantec Client Security 3.0 für Win.
- Symantec Norton Ghost 10.0 für Win.
- Symantec Norton Internet Security 2006 für Win.
- Symantec Norton SystemWorks 2006 für Win.
- Symantec PC Anywhere 11.5 für Win.

Updates (Stand: 1. März 2006)

- Exceed 11 2006 für Win. (bisher 10)
- LabVIEW 8.0 für Win., Mac, Linux (bisher – bzw. für Solaris unverändert – 7.1)
- Mathematica 5.2 für Win., Linux, Mac, Unix (bisher 5.1)
- MATLAB 7.0 R14 SP3 für Win. und Unix (bisher 6.5 R13)
- MS-Office 2003 für Win. inkl. ServicePack 2 (bisher ohne ServicePack)
- MS-Virtual Server 2005 R2 (bisher ohne R2)

Alle Informationen zur Standardsoftware finden Sie unter `www.univie.ac.at/ZID/standardsoftware/`

Peter Wienerroither ■

GEOINFORMATIK-SOFTWARE ARCGIS 9

Inklusive kostenloser Lizenzen für Studierende

Der Zentrale Informatikdienst stellt mit Beginn des Sommersemesters 2006 allen Universitäts-MitarbeiterInnen die Software ArcGIS 9 der Firma ESRI, einem der führenden Hersteller im Bereich der Geografischen Informationssysteme (GIS), als Campuslizenz zur Verfügung. Gegen eine geringe jährliche Gebühr (siehe weiter unten) kann jeder Interessent eine Lizenz erwerben, die zudem beliebig viele kostenlose Lizenzen für Studierende enthält. Derzeit wurden bereits Bestellungen von 11 Instituten für insgesamt 200 Lizenzen getätigt sowie 380 Lizenzen für Studierende angemeldet.

Die Software umfasst eine Reihe integrierter Anwendungen und Schnittstellen, mit denen beispielsweise das Erstellen von Karten, raumbezogenen Analysen, Datenbearbeitung und -umwandlung, Visualisierung sowie Geoverarbeitung möglich ist, wobei ArcView für eine umfassende Datennutzung, Kartenerstellung und Analyse geeignet ist. Daneben bietet ArcEditor zusätzliche Funktionen zur raumbezogenen Bearbeitung und Datenerstellung wie Datenmodellierung, Topologie oder Geodatenbanken und ist insbesondere für die Editierung komplexer Datenbestände in Mehrbenutzer-Umgebungen ausgelegt.

In der ArcGIS-Produktfamilie werden die beiden Produkte ArcInfo und ArcView auf eine gemeinsame technologische Basis zusammengeführt. War ArcInfo primär ein vollwertiges GIS auf Unix und ArcView eine reine Visualisierungssoftware auf PC, so hat die technische und anwendungsorientierte Weiterentwicklung zu einem intensiveren Zusammenspiel beider Produkte geführt. Die Software orientiert sich dabei am Bedarf der AnwenderInnen. Neben komplexen Programmen mit umfangreicher Funktionalität werden zunehmend einfach zu bedienende, funktionale Desktop-Programme gewünscht, die durch so genannte *Extensions* individuell erweiterbar sind.

ArcGIS trägt diesem Konzept Rechnung: Die Basisprodukte ArcView, ArcEditor und ArcInfo können sowohl auf einzelnen PCs (Einzelplatz-Lizenz) als auch in einem Netzwerk (Floater-Lizenz) installiert werden. Bei der Floater-Variante besteht zudem der Vorteil, dass die ArcGIS Extensions beliebig kombiniert verwendet werden können, während bei Einzelplatz-Lizenzen nur auf Programme auf diesem spezifizierten Rechner zugegriffen wird.

Der ZID bietet die gesamte ArcGIS-Software in Form von zwei Paketen an (der genaue Inhalt beider Pakete ist unter `www.univie.ac.at/ZID/software-news/` zu finden):

- **Paket 1:** ArcGIS 9 (inkl. ArcGIS Desktop, ArcInfo Workstation, ESRI Data & Maps u.a.)
  Gebühr: € 21,– je Lizenz für ein Jahr
- **Paket 2:** ArcGIS Server
  Gebühr: € 72,– je Lizenz für ein Jahr

Die Software läuft prinzipiell über Lizenzserver. Die für Standalone-Lizenzen – z.B. für Notebooks – benötigten Kopierschutzstecker (*Dongles*) sind in USB- oder Parallelport-Ausführung erhältlich und kosten € 48,– pro Stück.

Aufgrund des großen Umfanges von ArcGIS 9 erhalten LizenzbestellerInnen leihweise eine externe Festplatte mit der gesamten Software, wobei nur die bestellten Pakete freigeschaltet werden. Diese Festplatte darf nicht weitergegeben und die Software nur vom Lizenzinhaber installiert werden. Die Anzahl der Studierendenlizenzen muss dem Zentralen Informatikdienst jeweils zum 1. Februar und 1. September eines Jahres bekannt gegeben werden. Die Ausgabe dieser Lizenzen erfolgt derzeit noch auf einer kostenpflichtigen DVD.

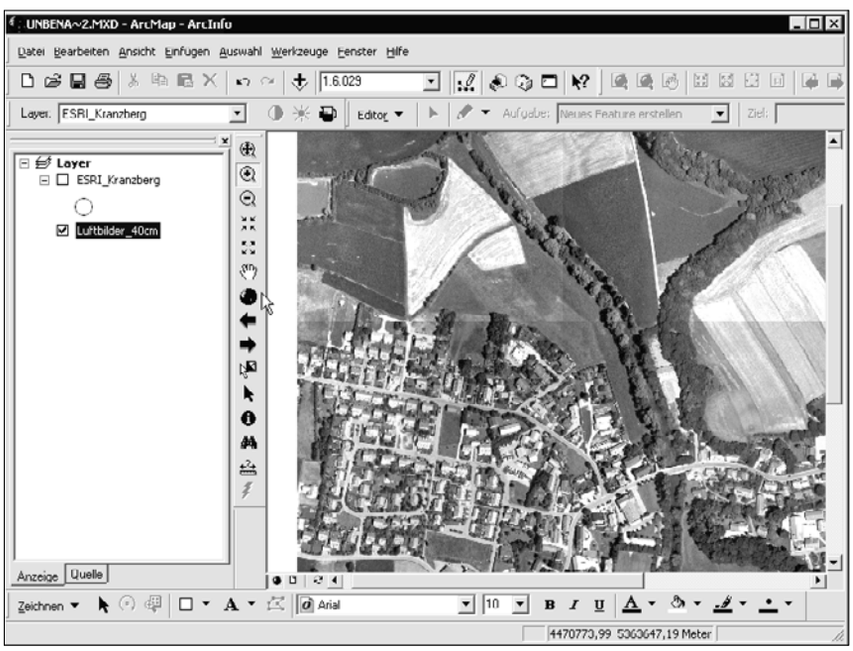


Abb. 1: ArcGIS 9 – Anwendungsbeispiel in ArcMap

Bei Interesse an der ArcGIS 9-Campuslizenz wenden Sie sich bitte per eMail an `software.zid@univie.ac.at`.

Umfassende Informationen zur Software ArcGIS, Demo-Filme zu vielen Features sowie Downloads von Software-Supplements und Dokumentationen finden Sie auf der Webseite der Firma ESRI (`www.esri-germany.de`).

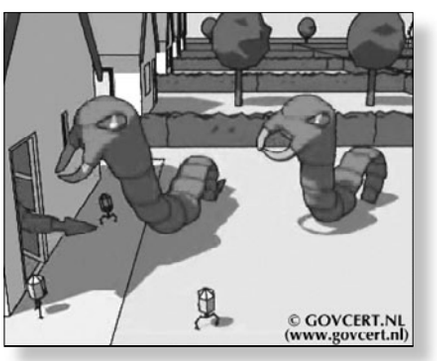
Katharina Lüthke ■

Kammerjäger im Netz: Jetzt geht's den Viren an den Kragen

Vom Scherzkeks zum Security-Problem

Vor wenigen Jahren waren Computerviren[1] noch lustig oder höchstens lästig: Sie spielten zu bestimmten Zeiten eine Melodie, verlangten vom Anwender ein Keks oder löschten im schlimmsten Fall die Festplatte und stellten damit die Wichtigkeit des hoffentlich vorhandenen Backups unter Beweis.

Heute, in der Informationsgesellschaft, sind Computer die Grundlage von Prozessen in allen Lebensbereichen – von Handel über Gesundheitswesen und U-Bahn-Steuerung bis hin zur hoheitlichen Verwaltung. Folgerichtig bleiben Computermanipulationen nicht mehr auf „die Kiste" beschränkt, sondern betreffen das reale Leben. Damit hat sich auch die Virenszene verändert: Computerviren sind keine Spielerei unausgelasteter Technikfreaks mehr, sondern ein Geschäftsmodell. Die aktuellen Viren dienen zwei Zwecken: Möglichst viele Computer und ihren Internetzugang nachhaltig zu bewirtschaften und geldwerte Informationen zu beschaffen. Dieses Business wird so professionell betrieben, dass Viren zum Security-Problem Nummer Eins geworden sind, weit vor Hard- und Softwarefehlern, HackerInnen, unloyalen MitarbeiterInnen etc.



Das größte Rechenzentrum der Welt ...

... ist nicht etwa ein mit High Tech vollgestopftes Gebäude im Silicon Valley, in dem Klimaberechnungen, Crashtest-Simulationen oder dergleichen durchgeführt werden. Die mächtigsten Computercluster sind Zusammenschlüsse von ganz normalen PCs, die sich hinter dem Rücken ihrer BesitzerInnen unter dem Kommando von Viren – bzw. deren UrheberInnen – zu so genannten *Botnets* zusammengerottet haben. Einen Eindruck davon, was das ist und wie es funktioniert, vermittelt auf schauerlich-anschauliche Weise ein englischsprachiger Film des GOVCERT.NL[2], der unter dem URL `www.waarschuwingsdienst.nl/render.html?cid=106` heruntergeladen werden kann und aus dem auch die Illustrationen zu diesem Artikel stammen.

Das Prinzip ist äußerst simpel: Sobald ein Computer befallen wurde, sorgt das moderne Virus für seine Weiterverbreitung, meldet sich bei seinem „Herrn und Meister" und wartet auf weitere Anweisungen, die dann auf Zuruf ausgeführt werden. Den Computer-Besitzer irgendwie zu ärgern, würde zur Entdeckung führen und wird daher tunlichst vermieden.

Wird das Virus aktiv, kann es alles mögliche tun: Spam versenden[3]; Musik und Videos aller Art bis hin zu Kinderpornos downloaden und verbreiten; an einer *Distributed Denial of Service*-Attacke (siehe weiter unten) teilnehmen. Besonders lukrativ ist die Einrichtung einer *Phishing Site*: Hier werden gefälschte Webseiten von Banken, eBay, PayPal etc. angeboten, in der Hoffnung, dass getäuschte AnwenderInnen ihre Passwörter dort eingeben – die dann fleißig missbraucht werden. Der verbrecherischen Phantasie sind kaum Grenzen gesetzt.

Die Vorteile für den Botnet-Meister liegen auf der Hand:

- Keine Unkosten für Hardware, Internetanbindung, Strom und Wartung der Rechner;
- unvorstellbare Ressourcen (ein Botnet aus 100 000 Rechnern kann als klein gelten);
- keine Probleme mit dem Gesetz: Die Täterausforschung endet spätestens beim PC eines ahnungslosen Benutzers.

Die Macht eines solchen Botnet lässt sich leicht am Beispiel einer *Distributed Denial of Service*-Attacke (DDoS) zeigen: Wenn 100 000 Rechner mit z.B. der Bandbreite eines bei uns üblichen Kabelmodem- oder DSL-Anschlusses gleichzeitig auf ein Ziel „losballern", kommen dort gut und gerne 10 Gbit/s an. Das reicht nicht nur aus, um aus einer Serverfarm – bildlich gesprochen – ein Häufchen Asche zu machen, sondern auch, um das gesamte, wahrlich nicht schwachbrüstig angebundene österreichische Wissenschaftsnetz ACOnet mehrfach zu überlasten. Mit einem solchen Druckmittel in der Hand werden beispielsweise Firmen erpresst, die ihre Umsätze mit Online-Diensten machen.

Auch der volle Zugriff auf die Festplatteninhalte der übernommenen Rechner ist nützlich: Mit den dort gespeicherten eMail-Adressen lassen sich die Spamdatenbanken trefflich erweitern. Kreditkartendaten aus Online-Transaktionen sind ohnehin reines Bargeld. Im Mailklienten oder Webbrowser gespeicherte oder auch auf der Tastatur eingetipp-

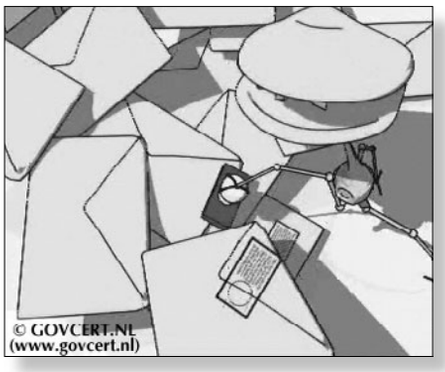
---

1) Die nähere Unterscheidung zwischen Viren, Trojanern, Würmern und anderen Plagegeister-Kategorien ist in diesem Artikel irrelevant. Daher wird hier für alle Arten der landläufige Begriff „Virus" verwendet.

2) GOVCERT.NL ist das *Computer Emergency Response Teams* (CERT) der niederländischen Regierung.

3) Bei Rechnern, die als „Spamschleudern" auffällig werden, ist häufig eine vorangegangene Vireninfektion feststellbar.

te Passwörter sind ebenfalls sehr interessant. Eine beliebte Anwendung dafür ist, zusätzlich zur privaten Homepage des Computer-Besitzers Pornoseiten am Webserver seines Providers unterzubringen. Der Zugriff auf das eMail-Konto des Opfers ermöglicht auch Betrügereien in großem Stil unter fremdem Namen. Gegen all das hilft keine Verschlüsselung und kein noch so sicheres Passwort: Das Virus hat mehr technische Möglichkeiten und kennt (spätestens sobald sie auf der Tastatur eingetippt werden) dieselben Passwörter wie der legitime Anwender.



Um es auf den Punkt zu bringen: Bei Viren geht es um Geld. Mehr noch: um richtig viel Geld. Ein Virus am Rechner ist nicht mehr bloß eine Unannehmlichkeit für den Benutzer, sondern – nicht immer, aber immer öfter – ein kriminelles Werkzeug.

Allzu oft ist doch der Wurm drin

Es gibt wohl niemanden mehr, der noch nie von der Bedrohung eines PCs durch Viren, Würmer und Trojaner gehört hat und nicht weiß, dass ein stets aktueller Virenscanner zumindest auf Windows-Rechnern ein absolutes Muss ist. Für Uni-MitarbeiterInnen steht der Virenscanner von McAfee kostenlos zur Verfügung (siehe `www.univie.ac.at/ZID/gratissoftware/`) – es gibt also wirklich keine Ausrede mehr, wenn kein Wächter den „elektronischen Datenverwurster“ schützt.

Überdies hindern die Virenscanner an den zentralen Mailservern des ZID sowie an vielen Stellen auch noch Firewalls die elektronischen Schädlinge am Zutritt zum Uni-Datennetz. Damit, so sollte man meinen, ist das Virenproblem Geschichte – doch weit gefehlt. Zwar sind die üblichen Maßnahmen ausgesprochen wirksam und wichtig, aber vollständige Sicherheit gibt es auch in diesem Bereich nicht.

- *Virenscanner* haben eine prinzipbedingte Schwachstelle: Trotz aller Bemühungen der Hersteller, jede erdenkliche Intelligenz in die Scanner zu packen, beruhen sie primär auf dem Wiedererkennen bereits bekannter Schädlinge. Neue Viren sind so lange „unsichtbar“, bis die Scanner-Hersteller ein Update zur Verfügung gestellt haben und dieses auch tatsächlich den Virenscanner erreicht hat. In der Praxis muss man oft mit mit einem Zeitraum von mindestens einem Tag zwischen dem Auftauchen eines neuen Schädlings und der Immunisierung des PCs rechnen.

  Die Mail-Virenscanner des ZID schützen zwar – mit der obigen Einschränkung – die zentralen Mailserver der Universität Wien (Unet, Mailbox) vor Virenmails, nicht aber die von Instituten in Eigenregie betriebenen Mailserver, und schon gar nicht verhindern sie den Download einer infizierten Nachricht von außerhalb, etwa von einem Freemail-Account oder von kommerziellen Providern.

- *Firewalls* hingegen bieten einen wirksamen Schutz vor zahlreichen unerwünschten Datenverbindungen und können damit eine Reihe von Angriffen abwehren. Sie verhindern aber nicht die Übertragung von böser Software über prinzipiell zugelassene Kanäle, beispielsweise über eine Webseite.

An dieser Stelle sei auch ein Wort zu so genannten *NAT-Routern* gesagt, die oft irrtümlich als Sicherheitsmaßnahme betrachtet werden: Dadurch, dass alle vermeintlich geschützten Rechner unter derselben IP-Adresse erscheinen, wird im Virenfall der „Feuerwehreinsatz“ zur Schnitzeljagd, da nicht mehr festzustellen ist, welcher Rechner befallen wurde.

Ist die Kiste infiziert, ...

... virt sich's völlig ungeniert: Hat, auf welchem Weg auch immer, ein Virus einmal den Weg in den PC gefunden, ist jede Sicherheit dahin. Es gehört zum Stand der einschlägigen Viren-Technik, im Zuge der Infektion des Rechners allfällige Virenscanner dauerhaft auszuschalten und oft sogar den Zugang zu den Webseiten der Antiviren-Hersteller zu unterbinden.

Firewalls werden häufig nach dem Grundsatz konzipiert, dass der Feind nur außerhalb des eigenen Netzes sein kann, und erlauben ausgehende Verbindungen jeder Art. Damit erlauben sie auch die Kontaktaufnahme eines Virus mit seinem Botnet. Ist ein Rechner aber erst einmal im Botnet angemeldet, ist die Firewall ausgehebelt: All das, woran sie einen Angreifer hindern würde, kann dieser nun vom infizierten Rechner – sozusagen von innen – machen lassen.

Einmal im System, kann sich ein Virus überdies mit Hilfe so genannter *Rootkits* (siehe auch Seite 19) hervorragend vor anderer Software, insbesondere Virenscannern, verstecken. Beispielsweise ist es möglich, dass das Rootkit jedem anderen Programm, das eine Datei liest (etwa einem Virenscanner, der das Vorhandensein eines Virus prüfen soll), deren unangetasteten Originalzustand vorgaukelt, obwohl sie ein Virus enthält.

---

4) Aus lizenzrechtlichen Gründen kann diese CD derzeit leider nicht für Studierende zur Verfügung gestellt werden.

5) siehe auch Notiz *ACOnet-CERT in Betrieb* (*Comment 03/2*, Seite 23 bzw. unter `www.univie.ac.at/comment/03-2/032_23.html`) und Artikel *Freiwillige Feuerwehr im Datennetz: Das ACOnet-CERT* (*Comment 04/1*, Seite 28 bzw. unter `www.univie.ac.at/comment/04-1/041_28a.html`)

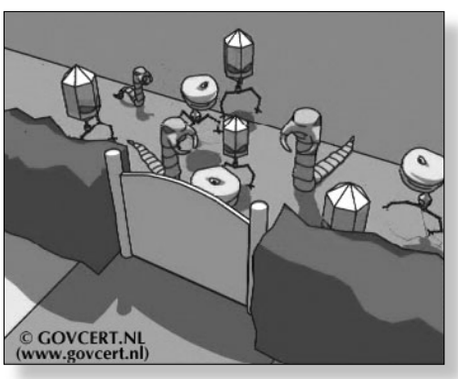
Um ganz sicherzugehen, dass der Virenscanner richtig arbeitet und danach das System wirklich sauber ist, muss man also den Rechner bereits mit einem garantiert sauberen System starten. Hier ist guter Rat gar nicht teuer: Am Helpdesk des Zentralen Informatikdienstes (siehe `www.univie.ac.at/ZID/helpdesk/`) kann von Uni-MitarbeiterInnen[4] eine bootfähige CD mit einem aktuellen Virenscanner gegen einen geringen Kostenersatz erworben werden. Damit diese CD die neuesten Virensignaturen enthält, wird sie stets frisch gebacken – wir bitten daher um Vorbestellung.

Neue Besen für das Netz

Angesichts dieser Bedrohung wurde im Security-Bereich ein Schwerpunkt auf die konsequente Suche nach Viren und deren Entfernung gesetzt. Um eine breitestmögliche Wirkung zu erzielen, finden diese Anstrengungen im Rahmen des von der Uni Wien betriebenen ACOnet-CERT (das *Computer Emergency Response Team* des österreichischen Wissenschaftsnetzes ACOnet; siehe `https://cert.aco.net/`)[5] statt. Wie bei der Feuerwehr bestehen die Sicherheitsaktivitäten eines CERT aus zwei Teilen:

- den Einsätzen mit Blaulicht und Sirene, wenn ein Unglück bereits eingetreten ist (der so genannten *Incident Response*), und
- allen vorbereitenden Maßnahmen wie Vorbeugung, Schulung, PR, Forschung, Einsatzplanung und Einrichtung entsprechender Systeme, um Probleme frühzeitig erkennen zu können.

Um vom ACOnet-CERT überhaupt wahrgenommen und verfolgt zu werden, musste ein von einem Virus befallener Rechner bisher entweder durch ungewöhnliches Verhalten an einer Firewall des ZID auf sich aufmerksam machen oder per eMail an `abuse@univie.ac.at` bzw. `cert@aco.net` gemeldet werden. Automatisierte Community-Services wie MyNetWatchman (Näheres dazu siehe `www.mynetwatchman.com`) haben in dieser Hinsicht sehr wertvolle Dienste geleistet.



Im Rahmen des Antiviren-Schwerpunkts konnten neue Informationsquellen erschlossen und dadurch zahllose Viren entdeckt werden, die bislang gar nicht oder bestenfalls wesentlich später aufgefallen wären. Die erste Maßnahme war, weitere Community-Services auszuwerten und die dort erhältlichen Informationen in einer Datenbank zu speichern. Darüber hinaus wurden die Virenscanner an den zentralen Mailservern des ZID in das System miteinbezogen. Sogar die Nameserver (im Netzwerk verantwortlich für das Übersetzen von Domainnamen wie `www.univie.ac.at` in numerische IP-Adressen) schlagen jetzt bei bestimmten verräterischen Zugriffsmustern Alarm: Das Mytob-Virus etwa versucht, sich an Mailserver mit den eher ungewöhnlichen Namen MXS.*DOMAIN*, GATE.*DOMAIN*, RELAY.*DOMAIN* etc. zu versenden, und kann anhand dieser Kriterien entlarvt werden.

Die so gewonnenen Informationen werden in einer Datenbank gesammelt, im Fall von dynamisch vergebenen Adressen einem Account zugeordnet und täglich zu Berichten zusammengefasst.

Der große Kehraus

Die Interpretation der automatisch generierten und der per eMail empfangenen Berichte stellt eine besondere Herausforderung dar. Werden schwache Indizien zu ernst genommen, besteht die Gefahr, die BenutzerInnen durch irrtümliche Warnungen zu verunsichern und Glaubwürdigkeit einzubüßen. Fatal wäre es aber auch, echte Probleme aus Angst vor Fehldiagnosen zu übergehen.

Wenn ausreichend Grund zu der Annahme besteht, dass ein Problem vorliegt, verständigt das ACOnet-CERT die zuständige Kontaktadresse und ersucht um Prüfung bzw. Behebung (ein Beispiel einer solchen Benachrichtigung finden Sie im Kasten auf Seite 34). Gleichzeitig wird um eine kurze Rückmeldung gebeten – erstens, um den Fall abschließen zu können, und zweitens als Feedback für die weitere Interpretation eintreffender Berichte.

Dieses einfache Modell hat leider zwei Schönheitsfehler. Der eine, seltenere, ist, dass diese Benachrichtigungen mitunter nach dem Motto *„Ich habe ja eh eine Firewall“* oder *„Es geht ja um nix“* ignoriert werden. In solchen Fällen bemüht sich das ACOnet-CERT – nach Abwägung von Gefahrenpotential und dem Wunsch, Härtefälle zu vermeiden – entweder weiter um Kontaktaufnahme oder sieht sich gezwungen, den Rechner oder Zugang zu sperren, nicht zuletzt im Interesse des Benutzers selbst. Der Vollständigkeit halber sei gesagt, dass es in ganz seltenen Ausnahmefällen auch Sperren ohne Vorwarnung geben kann: Wenn wirklich Feuer am Dach ist, oder wenn es sich um IP-Adressen im Datennetz der Universität Wien handelt, die nicht vom ZID vergeben wurden und die keinen DNS-Eintrag aufweisen.

Sollte ein Rechner oder ein bestimmter Dienst im Universitätsdatennetz (beispielsweise das Einwählen mit Modem) gesperrt worden sein, wenden Sie sich bitte an den Helpdesk des Zentralen Informatikdienstes. Dort kann diese Sperre in den meisten Fällen sofort wieder aufgehoben werden. Eines sei noch besonders betont: Derartige Maßnahmen sind keine Strafen, sondern stellen lediglich das Ziehen der „digitalen Notbremse“ dar – besonders auch zu Ihrem eigenen Schutz.

Beispiel für eine Viren-Benachrichtigung des ACOnet-CERT:

```
Date: Sun, 29 Jan 2006 17:56:15 +0100 (CET)
From: "Alexander Talos via RT" <cert@aco.net>
To: alexander.talos@univie.ac.at
Subject: [ACOnet-CERT #13620] Virus (Mydoom): 131.130.2.235 / kling.cc.univie.ac.at

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1


Sehr geehrte Damen und Herren,

Wir haben Berichte (s.u.) erhalten, dass vom Rechner
131.130.2.235 / kling.cc.univie.ac.at
Viren verschickt werden. Vermutlich hat sich ein Virus/Trojaner auf diesem Rechner eingenistet. Ich
bitte um Pruefung/Bereinigung und um eine kurze Rueckmeldung (vorzugsweise auch darueber, ob/welche
Schaedlinge gefunden wurden), damit ich das Ticket schliessen kann. Sollten Sie Hilfe beim
Virenscannen benoetigen, wenden Sie sich bitte an unseren Helpdesk
(http://www.univie.ac.at/ZID/helpdesk/).

Mit freundlichen Gruessen,
Alexander Talos

eMail-Virus (W32/Mydoom.o) k0U8wt9G095747
  Timestamp: 2006-01-28 08:59:04 UTC
  Source:    aconet-cert-mx4.univie.ac.at-2006-01-29
- --
Alexander Talos, ACOnet-CERT
https://cert.aco.net/
Phone: +43 1 4277 14024
Fax: +43 1 4277 9140
Universitätsstrasse 7, A-1010 Vienna

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.2 (FreeBSD
iD8DBQFD3POvvDA926Qg/Y4RAnzlAJ9DQsYk5VqpsiCA7lqN4iFfQLjB6gCgiTGo
bXZdGy1lE0tNyzAVDBccq50=
=vDaK
-----END PGP SIGNATURE-----
```

Anmerkungen:

1. Benachrichtigungen des ACOnet CERT tragen den Absender `cert@aco.net` und sind digital mit folgendem Schlüssel signiert: `1024D/A420FD8E 2005-12-10 [expires: 2007-01-31]`
   Key fingerprint = `8B79 1528 FAD5 20F2 761C B9DD BC30 3DDB A420 FD8E`
   Die GPG-Keys der Team-Mitglieder finden Sie unter `https://cert.aco.net/`
2. Mit dem Siegel `[ACOnet-CERT #13620]` kann der bearbeitete Fall in der Datenbank leicht aufgefunden werden. Bitte führen Sie diese Nummer bei allfälliger Korrespondenz an.
3. In der Regel besteht der Betreff aus drei oder vier Teilen: Kurze Benennung des Problems, IP-Adresse und DNS-Name des betroffenen Rechners, und gegebenenfalls zusätzliche Informationen wie Username bei Dialin-Accounts oder Netzname.
4. genaue Beschreibung des Problems und mögliche Gegenmaßnahmen
5. sofern vorhanden: Logfiles oder sonstige Informationen, die technisch Versierten zusätzliche Aufschlüsse über den Vorfall geben können

Mit dem zweiten Schönheitsfehler ist wesentlich schwieriger umzugehen: Welche ist die zuständige Kontaktadresse? Für den Bereich des ACOnet ist die Sache relativ klar: Der Security-Kontakt des jeweiligen ACOnet-Teilnehmers (das sind u.a. alle Universitäten und Bildungseinrichtungen Österreichs) wird verständigt und ist im eigenen Bereich dafür verantwortlich, alles Weitere zu veranlassen. Beim Kehren vor der eigenen Haustüre – nämlich im Datennetz der Uni Wien – erweist sich die bisherige Praxis des ZID, IP-Adressen so unbürokratisch wie möglich zu vergeben, als Herausforderung:

Allzu oft wurde von den Instituten nicht rückgemeldet, wessen PC an welche Steckdose angeschlossen und welche IP-Adresse aus dem Institutsnetz welchem Rechner zugewiesen wurde. Mitunter kennt der ZID nicht einmal den EDV-Betreuer für ein Institut – sei es, weil es nie einen gab oder weil der ehemals genannte schon lange nicht mehr im Amt ist. Im Zweifelsfall muss der Institutsvorstand, der ja ex lege das Institut nach außen vertritt, mit dem Virenproblem behelligt werden.

Hinsichtlich der Endgeräte-Dokumentation im Universitätsdatennetz hat sich in den letzten Jahren einiges getan. Insbesondere bemühen wir uns, die IP-Datenbank (siehe auch Seite 38) zu vervollständigen.

Hierbei bitten wir um Mithilfe:

Nehmen Sie sich die Zeit, sofern Ihr PC noch nicht erfasst ist, das Webformular unter `www.univie.ac.at/ZID/ipdb/` auszufüllen. So wie es für die Feuerwehr wichtig ist, dass ihre Zufahrt freigehalten wird, hilft es allen Beteiligten, wenn wir Sie im Ernstfall rechtzeitig verständigen können.

Zusammenfassung

Die bisherigen Empfehlungen[6] zum Thema Virenschutz sind zwar nicht mehr ausreichend, aber keineswegs veraltet oder verzichtbar. Eine grundsätzliche Lösung des Problems gibt es nicht. Daher gilt es, den Schaden, wenn er eintritt, möglichst früh zu erkennen und möglichst gering zu halten.

Sie können einiges tun, und zwar vorbeugend:

- Stellen Sie sicher, dass Ihr PC durch einen Virenscanner mit aktueller Signatur-Datenbank[7] sowie durch eine Firewall geschützt ist, und sorgen Sie für regelmäßige Updates Ihres Betriebssystems und Ihrer Software.[8]
- Erwägen Sie die Verwendung eines weniger gängigen Betriebssystems (Apple, Linux, ...).
- Seien Sie skeptisch, bevor Sie Software installieren oder Attachments anklicken.
- Organisieren Sie die zuverlässige Sicherung Ihrer Daten oder verwenden Sie die Fileservices des ZID (siehe `www.univie.ac.at/ZID/fileservices/`) statt Ihrer lokalen Festplatte.
- Bereiten Sie sich auf den Ernstfall vor: Registrieren Sie Ihren PC und die dazugehörigen Kontaktdaten in der IP-Datenbank des ZID (`www.univie.ac.at/ZID/ipdb/`) und halten Sie die Telefonnummer des EDV-Betreuers Ihres Instituts (sofern vorhanden), des Helpdesk etc. griffbereit.

Für den Fall, dass doch etwas passiert:

- Achten Sie auf eMail von `cert@aco.net` (siehe Beispiel auf Seite 34).
- Schalten Sie Ihren Computer ab oder setzen ihn in den Schlafmodus, wenn Sie gerade nicht daran arbeiten:
  - ➠ Es ist besser, wenn Ihr Rechner nur 40 statt 168 Stunden pro Woche Spam und Viren verschickt.
  - ➠ Ihr PC kann nur dann durch ungebührliches Verhalten auffallen, wenn Sie in der Nähe sind – d.h. Sie sind im Ernstfall für uns erreichbar und können sofort Maßnahmen setzen.
  - ➠ Das erhöht die Chancen, dass Sie die Immunisierung vor dem Virus erreicht: Mit etwas Glück erscheinen, während Ihr Computer schläft, die Updates, die das Virus abwehren, das sonst über Nacht eingedrungen wäre.
- Falls nötig, wenden Sie sich an den Helpdesk des ZID (`www.univie.ac.at/ZID/helpdesk/`). Hier wird Ihnen auch telefonisch beim Entfernen von Viren geholfen.
- Ändern Sie nach einem überstandenen Virenbefall Ihre Passwörter: Es könnte sein, dass sie durch das Virus „ausgeplaudert“ wurden.

Der Computer – ein Teufelszeug? Mit Sicherheit nicht, aber ein mächtiges Werkzeug, das alles tut, was ein Programm ihm gebietet. In falschen Händen bedeutet das: Der PC kann innerhalb von kürzester Zeit ungeheuer viel Schaden anrichten. Und deswegen sind Vorbeugung, rasche Diagnose und Schadensbegrenzung hier so wichtig.

Alexander Talos ■

---

6) siehe Artikel *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* (*Comment 04/1*, Seite 16 bzw. unter `www.univie.ac.at/comment/04-1/041_16.html`)

7) siehe Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* (*Comment 04/1*, Seite 21 bzw. unter `www.univie.ac.at/comment/04-1/041_21.html`)

8) siehe Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* (*Comment 04/1*, Seite 18 bzw. unter `www.univie.ac.at/comment/04-1/041_18.html`)

Bildnachweis: Die Bilder sind dem Botnet-Film des GOVCERT.NL (`www.waarschuwingsdienst.nl/render.html?cid=106`) entnommen. Wir danken GOVCERT.NL für die Druck-Erlaubnis.

Webmail: Next Generation

Vor etwa fünf Jahren ging die erste Version eines universitätsweiten Webmail in Betrieb.[1] Binnen kurzer Zeit entwickelte sich dieses Werkzeug zu einem sehr populären Dienst, war es doch so für alle Unet- und Mailbox-BenutzerInnen ganz einfach möglich, nur mit einem Webbrowser – ohne aufwendiges Installieren etwaiger Mailprogramme – von überall an die eigene eMail zu gelangen.

Allerdings machte der technische Fortschritt auch auf diesem Gebiet nicht halt, und so haben sich in den letzten fünf Jahren einige (kommerzielle und nicht-kommerzielle) Projekte rund um das Thema Webmail entwickelt, die im Komfort ausgewachsenen Mailprogrammen kaum noch nachstehen. Es war also an der Zeit, über eine Aktualisierung unseres Webmail-Dienstes nachzudenken.

Das bisherige Webmail der Uni Wien war aufgrund fehlender Alternativen noch eine Eigenentwicklung des ZID; seither sind aber gerade in der Open Source-Welt einige vielversprechende Webmail-Projekte entstanden. Nach einer sorgfältigen Auswahlphase haben wir uns entschlossen, die Open Source-Software SquirrelMail (`www.squirrelmail.org`) als Grundlage des neuen Webmail zu verwenden und entsprechend zu adaptieren.

Warum SquirrelMail?

Das wichtigste Auswahlkriterium bei der Suche nach einem neuen Webmail war Kompatibilität, um eine möglichst große Zahl verschiedener Webbrowser (insbesondere auch ältere) unterstützen zu können. SquirrelMail schien wie für uns geschaffen, da es auf den Einsatz von Java bzw. Javascript weitgehend verzichtet und daher sogar mit jenen Browsern uneingeschränkt verwendbar ist, bei denen diese Technologien nicht vorhanden oder deaktiviert sind. Das Design erfolgt mittels *Cascading Style Sheets* (CSS). Auch hier wurde auf komplexere Features verzichtet, weil diese von den verschiedenen Webbrowsern noch sehr unterschiedlich unterstützt werden. Alle zur Zeit verbreiteten Browser auf allen gängigen Betriebssystemen funktionieren problemlos mit SquirrelMail, insbesondere (getestet) MS-Internet Explorer, Mozilla/Firefox, Netscape, Opera, Konqueror, Safari, aber auch exotischere Browser wie Links, Lynx und w3m.

Eine weitere Anforderung war, dass das gewählte Projekt nicht eines Tages versandet und wichtige technologische Neuerungen nicht mehr umgesetzt werden. Auch hier kann SquirrelMail punkten, denn es ist weit verbreitet und eine große Anhängerschaft kümmert sich um den Fortbestand des Projekts. Nicht zuletzt ist SquirrelMail im Quellcode verfügbar, was umfassende Änderungen überhaupt erst ermöglicht und zudem eine gewisse Investitionssicherheit darstellt.

Von SquirrelMail zum neuen Webmail

Da nun die Wahl auf SquirrelMail gefallen war, galt es, die Software an die besonderen Anforderungen der Universität Wien anzupassen. So waren kleinere Tricks notwendig, um SquirrelMail mit unserem doch relativ komplexen Mailing-System zu „verheiraten“ – z.B. muss das neue Webmail je nachdem, ob beim Login eine Unet- oder eine Mailbox-UserID angegeben wird, zu verschiedenen Mailservern verbinden. Weiters holt sich SquirrelMail die benötigten Informationen über den jeweiligen Benutzer (z.B. Namen und eMail-Adressen) bereits aus dem LDAP-Service, das demnächst universitätsweit angeboten werden soll.[2]

Mehrsprachigkeit

Besonderes Augenmerk wurde auf die Unterstützung mehrerer Sprachen gelegt. BenutzerInnen, deren Muttersprache nicht Deutsch ist, können die Oberfläche von Webmail auch auf Englisch darstellen lassen (hier wurde primär Übersetzungsarbeit geleistet; die entsprechende Einstellung ist unter *Optionen* zu finden). Sollte der Bedarf entstehen, kann Webmail zudem problemlos um andere Sprachen erweitert werden.

Ein besonderes technisches Highlight (und teilweise eine weitere Eigenentwicklung gegenüber dem Standard-SquirrelMail) ist die Verwendung der Zeichenkodierung UTF-8, einer Variante der bekannten Unicode-Zeichenkodierung.[3] Dank UTF-8 kann man mit dem neuen Webmail eMail-Nachrichten in allen erdenklichen Sprachen dieser Welt verfassen und empfangen. Alle modernen Webbrowser unterstützen diese Kodierung, durch die es beispielsweise möglich wird, in einer eMail deutsche, kyrillische, griechische und Hindi-Zeichen zu mischen (siehe Abb. 1).

Neben diesen Modifikationen wurden noch einige kleine Fehler in SquirrelMail gefunden und beseitigt. Im besten Sinne des Open Source-Gedankens werden unsere Verbesserungen, je nach Relevanz, an das SquirrelMail-Projekt zurückfließen.

---

1) siehe Artikel *hotmail@univie.ac.at* in *Comment 01/1*, Seite 34 bzw. unter `www.univie.ac.at/comment/01-1/011_34.html`

2) LDAP (*Lightweight Directory Access Protocol*) ist ein Netzwerkprotokoll, das zur Abfrage von hierarchischen Verzeichnisdiensten entwickelt wurde (die im Falle der Uni Wien z.B. Kontaktdaten von Uni-MitarbeiterInnen und Studierenden beinhalten), aber sehr häufig auch für Authentifizierungszwecke eingesetzt wird. Das im Aufbau befindliche universitätsweite LDAP-Service soll z.B. eine Authentifizierung mittels Unet- bzw. Mailbox-UserIDs auch für Online-Services von Instituten ermöglichen.

3) siehe Artikel *Unicode – Kiss Your ASCII Goodbye?* in *Comment 04/3*, Seite 12 bzw. unter `www.univie.ac.at/comment/04-3/043_12.html`

Abb. 1: Verschiedene Zeichensätze in einer eMail-Nachricht

Was ist neu?

Das neue Webmail, das im Jänner 2006 nach einer mehrwöchigen Testphase in den Echtbetrieb ging, weist eine Vielzahl von Verbesserungen gegenüber der alten Version auf – sowohl in technischer als auch in ergonomischer Hinsicht. Die grundlegende Bedienung lehnt sich stark an die herkömmlicher Mailprogramme an, daher sollen hier nur einige Highlights herausgestrichen werden:

- Auch Unet-BenutzerInnen kommen nun – wie zuvor schon Uni-MitarbeiterInnen mit Mailbox-Account – in den Genuss von IMAP-Ordnern. Wie von den meisten Mailprogrammen gewohnt, sind diese über eine Baumansicht auf der linken Seite des Fensters erreichbar. Versandte Mails werden jetzt im Ordner *Sent* abgelegt und nicht mehr als Kopie direkt in der *Inbox*.

- Nachrichten in der Listenansicht können durch Klick auf den jeweiligen Sortier-Button neben dem Spaltennamen (siehe Abb. 2) sortiert werden, z.B. nach Datum oder Absender. Die Anordnung der Spalten kann in den *Optionen* verändert werden. (Hinweis: Sollten Sie die Sortier-Buttons nicht vorfinden, befindet sich Ihr Postfach noch auf einem älteren Server und wird im Laufe der nächsten Monate umgestellt.)

Abb. 2: Sortier-Button neben dem Spaltennamen

- Zwecks Übersichtlichkeit können Nachrichten nach selbst erstellten Regeln farblich hervorgehoben werden. Möchte man beispielsweise, dass alle eMails von einem bestimmten Absender farbig hinterlegt werden, lässt sich eine entsprechende Regel über *Optionen – Hervorhebung von Nachrichten* definieren. Abb. 3 zeigt das Anlegen, Abb. 4 das Ergebnis dieser Hervorhebung.

- Ein oft geäußerter Wunsch war auch, mehr als ein Attachment pro Nachricht versenden zu können. Dies ist jetzt möglich. Als Maximalgröße pro Datei sind 8 MB konfiguriert. Größere Dateien per eMail zu versenden, ist generell problematisch – speichern Sie diese bitte im `html`-Verzeichnis Ihres Homedirectory (siehe `www.univie.ac.at/ZID/persoenliche-webseiten/`) und versenden Sie nur den URL, unter dem die Dateien abrufbar sind (z.B. `http://www.unet.univie.ac.at/~a1234567/entwurf-diplomarbeit.doc`).

- Ein weiteres wichtiges Feature, um der immer größer werdenden Mailflut Herr zu werden, ist eine ausgereifte Suchfunktion. Auch diese steht jetzt zur Verfügung. Suchanfragen können zudem für die spätere Verwendung gespeichert und jederzeit wieder abgerufen werden.

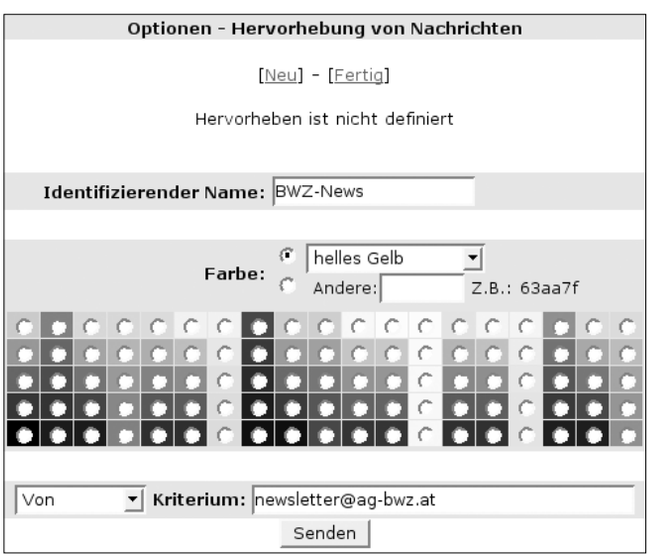


Abb. 3: *Optionen – Hervorhebung von Nachrichten*

Webmail und „POP-User“

Das neue Webmail ist ein vollwertiger IMAP-Klient, kommuniziert also via IMAP-Protokoll mit dem jeweiligen Postfach am Mailserver. Einige wenige BenutzerInnen, die noch das veraltete POP3-Protokoll einsetzen, können deshalb das neue Webmail nicht verwenden.

Es besteht jedoch die Möglichkeit, diese Postfächer auf IMAP umzustellen; wenden Sie sich dazu bitte an den Helpdesk (`www.univie.ac.at/ZID/helpdesk/`). Mehr Informationen zu diesem Thema finden Sie auf den Webseiten des Zentralen Informatikdienstes unter `www.univie.ac.at/ZID/imap/`.

Webmail: Facts & Figures

Zum Abschluss noch einige interessante Kennzahlen zum neuen Webmail der Uni Wien (*Stand Anfang März 2006*):

- BenutzerInnen, die das neue Webmail verwenden: ~25 000
- Webmail-Sessions pro Tag: ~10 000
- Datenvolumen pro Tag: ~2,5 GB
- HTTP-Hits pro Tag: ~400 000

Ausblick

In den nächsten Wochen und Monaten soll das neue Webmail um zusätzliche Features erweitert werden:

- *Adressbuch:* Unter dem Menüpunkt *Adressen* im Webmail, der zur Zeit nur ein Platzhalter ist, wird in Kürze die Möglichkeit geboten, persönliche Adressbücher zu verwalten.
- *Sieve-Schnittstelle:* Mittels Sieve (einer „Programmiersprache“, die speziell für das Filtern von eMail-Nachrichten konzipiert wurde) lassen sich Abläufe erstellen, welche beispielsweise Nachrichten je nach Absender automatisch in unterschiedliche Ordner einsortieren. Solche Abläufe werden auch über Webmail verwaltet werden können.
- *Up- und Download von Attachments in das bzw. aus dem Homedirectory:* Attachments sollen ohne Umwege direkt in das eigene Homedirectory auf dem Unet- bzw. Mailbox-Fileserver gespeichert bzw. von dort ausgewählt werden können.

Viel Spaß mit dem neuen Webmail!

Thomas Wana ■

Abb. 4: Das Ergebnis der Hervorhebung: Unterlegte Nachrichten in der Listenansicht

Neue Features der IP-Datenbank

In Zusammenarbeit mit BenutzerInnen und EDV-BetreuerInnen hat der ZID einige Verbesserungen an den Schnittstellen zur IP-Datenbank (siehe `www.univie.ac.at/ZID/ipdb/`) vorgenommen, die noch im März 2006 in Betrieb gehen sollen:

- SystemadministratorInnen können die von ihnen betreuten Netze in sortierter Form – inklusive der freien Adressen – auflisten lassen. Die Ausgabe ist auch im Template-Format möglich. Zusätzliche Attribute wie Standort, Dose und Beschreibung werden ebenfalls angezeigt.
- Beim Beantragen bzw. Ändern von IP-Adressen wird eine eMail an den beantragenden Benutzer, an den EDV-Betreuer (technischer Kontakt) des Netzes sowie an die Abteilung *Datennetze & Infrastruktur* des ZID versandt.
- Bei Neuanträgen wird automatisch eine freie IP-Adresse vorgeschlagen. Bitte halten Sie trotzdem mit Ihrem EDV-Betreuer Rücksprache – eventuell wird an Ihrem Institut ein anderes Vergabeschema verwendet.

Daniel Schirmer

Wir sind die Kabellosen

Mobiles Arbeiten mit GPRS, UMTS und EDGE

Es gab einmal eine Zeit, da konnte man mit einem Mobiltelefon vor allem eines recht gut, nämlich telefonieren. Dann kamen Short Messages, Multimedia Messages, Downloads von Klingeltönen in allen möglichen Qualitäts- und „Geht mir auf die Nerven"-Stufen, Infrarot, Bluetooth, animierte Hintergrundbilder, MP3-Player, und mittlerweile kann man auf dem Handy auch schon fernsehen (ob es ein wirklicher Genuss ist, sich das Programm des ORF auf einem Mini-Display anzusehen, steht auf einem anderen Blatt).

Kurz gesagt – die technische Entwicklung auf dem Mobilfunk-Sektor hat in den letzten Jahren rasante Fortschritte gemacht, und davon profitieren nicht nur jugendliche Handy-Junkies, sondern auch diejenigen unter uns, die eine mobile Internet-Anbindung für ihre tägliche Arbeit nutzen wollen.

GSM und GPRS

„Mobil ins Internet" ging es auch schon in den seligen GSM-Zeiten (*Global System for Mobile Communications*), als Handys noch Handys waren und keine eierlegenden Wollmilchmediaplayer: Das Handy wurde z.B. via seriellem Kabel oder Infrarot-Schnittstelle mit dem Laptop verbunden und konnte so als Modem verwendet werden – unter der Voraussetzung, dass man a) viel Zeit hatte und b) nur wenige eMail-Nachrichten lesen wollte, denn mit einer maximalen Bandbreite von 9,6 kbit/s kann man allerhöchstens von „Geduldsprobe" sprechen, nicht aber von „entspanntem Surfvergnügen" (vor allem, wenn man ein verwöhnter ADSL-Benutzer ist).

Vodafone Mobile Connect Card

Deutlich interessanter wurde es mit der Einführung der GPRS-Technik (*General Packet Radio Service*), einer Weiterentwicklung von GSM, die in Österreich praktisch flächendeckend zur Verfügung steht und eine Datenübertragungsrate von bis zu 57,6 kbit/s ermöglicht; zumindest auf dem Papier, mit Abstrichen in der Praxis muss man immer rechnen. Damit erreicht man schon annähernd die Geschwindigkeit eines klassischen Modems, wenn auch die so genannte *Latency* bzw. die *Round-Trip-Time* (also die Zeit, die ein Datenpaket von Host A zu Host B und wieder retour braucht) deutlich höher ist als bei kabelgebundenen Internetverbindungen, was vor allem beim interaktiven Arbeiten – beispielsweise via SSH-Login auf einer Shell – ins Gewicht fällt.

UMTS

Der wirkliche Knaller kam allerdings mit der Einführung von UMTS (*Universal Mobile Telecommunications System*, umgangssprachlich auch „3G" genannt, für „die dritte Generation des Mobilfunks"), das nicht nur auf Sprach- und reinen Datenverkehr abzielt, sondern auch Videotelefonie, *Location Based Services* und Ähnliches ermöglichen soll. Die Mobilkom Austria, die im September 2002 das erste nationale UMTS-Netz in Europa in Betrieb nahm, verspricht mit UMTS *„das Fundament für schnelle, mobile Datenübertragung und Multimedia-Services im urbanen Bereich"* – und zumindest im Bereich der Datenübertragung kann man das durchaus unterschreiben.

UMTS ermöglicht Datenraten von bis zu 384 kbit/s, damit rückt das oben erwähnte „entspannte Surfvergnügen" auch im mobilen Einsatz in greifbare Nähe; sogar kleinere Downloads sind damit möglich (wenn auch das Bild aus der Werbung – der Download ist noch vor dem Kaffee fertig – deutlich übertrieben ist).

UMTS ist keine direkte Weiterentwicklung von GPRS bzw. GSM, weshalb die existierenden Mobilfunk-Sender nicht damit kompatibel sind. Darin liegt auch der größte Nachteil von UMTS, nämlich die im Vergleich zu GPRS deutlich geringere Verfügbarkeit: Eine UMTS-Zelle (also der Bereich, der von einem Sender abgedeckt werden kann) ist wesentlich kleiner; es müssten also mehr Sender aufgestellt werden, um die gleiche Flächenabdeckung zu erreichen. Da sich das für die Mobilfunkbetreiber nicht rechnet, funktionieren UMTS-Verbindungen derzeit vor allem im Bereich größerer Städte (ein Plan des A1 UMTS-Netzes findet sich unter `www.a1.net/business/coveragemap/index.php`).

Weiters ist bei der Verwendung einer UMTS-Datenverbindung zu bedenken, dass sich alle NutzerInnen, die sich innerhalb einer UMTS-Zelle befinden, die verfügbare Bandbreite von 384 kbit/s teilen müssen – je mehr aktive UMTS-Verbindungen, desto langsamer wird es.

EDGE

Um der begrenzten Netzabdeckung von UMTS entgegenzuwirken, hat der Mobilfunk-Betreiber A1 im Sommer 2005 mit EDGE (*Enhanced Data Rates for GSM Evolution*) eine weitere Technik eingeführt, die wiederum eine Weiterentwicklung von GSM und GPRS darstellt, sodass die vor-

handenen Sendestationen mit moderatem Aufwand darauf umgestellt werden konnten. EDGE bietet Datenraten von bis zu 200 kbit/s und ist aufgrund der GSM-Kompatibilität auch in ländlichen Gegenden verfügbar – sofern das Handy bereits EDGE unterstützt. Die Abdeckung des A1 EDGE-Netzes findet sich ebenfalls unter dem URL `www.a1.net/business/coveragemap/index.php`.

Mobiles Breitband

Natürlich stellen die Mobilfunk-Betreiber diese mobilen Internetzugänge nicht kostenlos zur Verfügung – die Datenübertragung ist im Vergleich zur Sprachübertragung sogar ziemlich teuer: A1 verrechnet derzeit schamlose € 6,40 / MB für die ersten 10 MB. Das wird für VielnutzerInnen rasch unbezahlbar, weshalb es oft günstiger ist, sich für das Paket *Mobiles Breitband* anzumelden, in dessen Rahmen ein fixes Datenvolumen (500 MB oder 1000 MB) inkludiert ist. Der Vorteil liegt auf der Hand: Sofern man unterhalb des Limits bleibt, fallen keine Mehrkosten an, man erspart sich böse Überraschungen auf der Monatsabrechnung.

Wo es Licht gibt, gibt es bekanntlich auch Schatten – das inkludierte Datenvolumen erkauft man sich mit einer ziemlich hohen Grundgebühr (die jedoch im Vergleich zu den Preisen für einzeln abgerechnete Megabytes sehr günstig ist), mit einer Bindungsfrist von 24 Monaten und einer nicht vorhandenen Roaming-Möglichkeit (das Service wird nur innerhalb Österreichs angeboten, außerhalb gilt der Tarif *Data Roaming*).

Mobiles Breitband für Diensthandys

Das Paket *Mobiles Breitband* ist auch im A1-Network der Universität Wien verfügbar. Es kann sowohl auf die private wie auch auf die dienstliche Abrechnung bestellt werden; für letzteres wird das Einverständnis des Institutsvorstands bzw. Dienststellenleiters benötigt. Bei der Anmeldung für *Mobiles Breitband* besteht die Möglichkeit, eine Vodafone Mobile Connect Card für den Laptop (mehr dazu weiter unten) zu verbilligten Konditionen zu erwerben.

Nähere Informationen dazu finden Sie auf den Webseiten des Zentralen Informatikdienstes unter `www.univie.ac.at/ZID/handy-service/#mb`. Das *Mobile Breitband* ist selbstverständlich auch ohne Mobile Connect Card verwendbar: Etliche Handys – z.B. Nokia 6630 (Auslaufmodell), Nokia N70 oder Sony Ericsson W900i – können auch via Bluetooth oder seriellem Kabel mit einem Rechner verbunden und als UMTS-Modem eingesetzt werden.

Mobile Connect Card

Die Vodafone Mobile Connect Card ist eine normale PC-Card zur Verwendung in Laptops, in die – wie bei einem Handy – eine SIM-Karte geschoben werden muss. Sie ist in mehreren Ausführungen erhältlich; am ZID kamen bisher die Varianten *UMTS/GPRS* und *UMTS/EDGE* zum Einsatz. Abgesehen davon, dass die eine Karte auch EDGE unterstützt und die andere nicht, unterscheiden sie sich kaum – sofern man sie mit einem Windows-Betriebssystem verwendet. BenutzerInnen von Mac OS X oder Open Source-Betriebssystemen wie FreeBSD oder Linux können derzeit nur die *UMTS/GPRS*-Karte einsetzen, da es für die andere Variante noch keine Treiber gibt. Genauere technische Details findet man unter dem URL `www.a1.net/business/vodafonemobileconnectcard`.

Die Installation und die Verwendung der Karte sind denkbar einfach: Zunächst startet man die Installation der mitgelieferten Software (des so genannten *Dashboard*), die sich mit wenigen Klicks erledigen lässt. Nach einem Neustart und dem Einschieben der Mobile Connect Card in den PC-Card-Slot des Laptops ist diese auch schon funktionsfähig – vorausgesetzt, man hat die SIM-Karte nicht vergessen.

Startet man die Dashboard-Software, wird man wie beim normalen Handy nach dem PIN-Code der SIM-Karte gefragt, danach sucht die Mobile Connect Card nach einem geeigneten Netz (UMTS, EDGE oder GPRS). Sobald dieses gefunden wurde, kann man mittels Klick auf *Verbinden* eine Datenverbindung herstellen – voilà, mobiles Internet!

Neben den Funktionen *Verbinden* bzw. *Trennen* einer aktiven Verbindung bietet die Dashboard-Software auch eine SMS-Schnittstelle, um wie mit einem Handy SMS verschicken bzw. empfangen zu können, sowie eine Nutzungs-Übersicht (für den vergangenen und den laufenden Monat), die eine Kontrolle über das verbrauchte Datenvolumen ermöglichen soll. Die Anzeige des Datenvolumens in Dashboard ist allerdings mit Vorsicht zu genießen – unter Umständen kann es vorkommen, dass einige Megabytes nicht korrekt eingerechnet werden. Um sicher festzustellen, wie weit man noch vom Limit entfernt ist, sollte man (direkt von Dashboard aus) eine SMS an die Nummer 421 senden; man erhält dann eine Antwort-SMS, in der das seit der letzten Abrechnung verbrauchte Volumen angeführt ist.

Fazit

Mit Hilfe von UMTS und der Vodafone Mobile Connect Card ist es mittlerweile auf einfachem Weg möglich, alle Angebote des Internet auch unterwegs mit dem Laptop zu verwenden, ohne auf den Komfort eines schnellen Zugangs zu verzichten; das Paket *Mobiles Breitband* ermöglicht dabei eine einfache Kostenkontrolle. Hinsichtlich der Geschwindigkeit ist das Ende der Fahnenstange noch lange nicht erreicht: Die Mobilkom Austria startet derzeit den Betrieb des UMTS-Nachfolgers HSDPA (*High Speed Downlink Packet Access*), welcher eine mobile Bandbreite von bis zu 1,8 Mbit/s verspricht.

Eines steht jedenfalls auch in Zukunft wohl außer Frage: Telefonieren wird man mit einem Handy vermutlich immer können.

Lukas Ertl & Karin Geicsnek ■

„(B)LOGBUCH DES CAPTAINS, STERNZEIT ZWEITAUSENDUNDSECHS …“

Das Thema „Weblogs“ ist gegenwärtig in aller Munde. In einer Auswertung der am häufigsten verwendeten Begriffe in der deutschsprachigen Wirtschaftspresse während des vergangenen Jahres belegte der Begriff sogar den ersten Platz, deutlich vor (in dieser Branche sehr gebräuchlichen) Begriffen wie Risiko- oder Krisenmanagement.[1)] Sowohl Journalisten als auch Medienwissenschaftler und PR-Fachleute publizieren eifrig zu diesem Thema, analysieren, inwieweit Weblogs bisher gebräuchliche Medien beeinflussen, ergänzen oder „revolutionieren“ werden (Stichwort *grassroot journalism*[2)]) beziehungsweise spekulieren über das Potential des neuen Medienformats als Marketing- und PR-Instrumentarium.

Doch: Ist das Phänomen unter Internet-Usern wirklich so bekannt, wie uns dies solche Berichte weismachen wollen? Eine Bestandsaufnahme im Bekanntenkreis bringt ähnliche Ergebnisse zutage wie diverse Umfragen für den deutschsprachigen Raum: Ungeachtet des medialen „Hypes“ ist der Anteil jener, die selbst aktiv ein Weblog betreiben, eher gering (ca. 5%). Im Gegensatz zu jenen BenutzerInnen, denen das Phänomen gänzlich unbekannt ist (etwa 25%), kennt aber der weit größte Teil der User (70%) den Begriff und hat auch schon ein paar Mal Weblogs besucht. *„Weblogs? – Ach ja, Tante Gudrun publiziert dort doch regelmäßig Varianten ihres berühmten Streuselkuchenrezepts und diskutiert diese online mit den Damen ihres Kaffeekränzchens!“* Sie mögen sich nun zu Recht die Frage stellen: *„Und was ist daran so spektakulär?“* (Gut, Sie kennen auch nicht Tante Gudruns Kuchen ;-))

Nun, beispielsweise eignen sich Weblogs (kurz „Blogs“ genannt) auch für zahlreiche Anwendungen in Wissenschaft und Lehre, wie etwa zur Dokumentation von wissenschaftlichen Projekten oder zur Visualisierung von Lernprozessen. Weblog ist eben nicht gleich Weblog. Zwar ist das technische Konstrukt (im Prinzip ein „abgespecktes“ CMS[3)]) überall ähnlich, Blogs finden aber in den unterschiedlichsten Bereichen Anwendung. Das ist in etwa vergleichbar mit einem Buch: Zwar ist es relativ simpel, einem Buch-Unkundigen Struktur und Aufbau eines Buches zu erklären, doch ist eine solche Beschreibung (von zahlreichen mit Zeichen bedruckten und gebundenen Seiten) in der Aussage sehr begrenzt bezüglich der mannigfaltigen Möglichkeiten von Inhalt und Einsatzgebiet eines solchen (Lehrbuch, Bilderbuch, Malbuch, Belletristik, …).

Wir wollen deshalb dem geneigten Leser im Folgenden einen kurzen Überblick darüber geben, worum es sich bei diesem neuen Medienformat handelt, anhand von einigen Beispielen darstellen, in welchen Bereichen es indes Anwendung findet – und natürlich wollen wir Ihnen zu guter Letzt auch nicht vorenthalten, wie Sie bei Interesse selbst ein Weblog einrichten können.

Grundlagen

Was bisweilen fehlt, ist eine allgemeingültige Definition des Begriffes „Weblog“. Als problematisch erweist sich dabei das bereits angesprochene breite Anwendungsspektrum des neuen Medienformats, dessen Inhalte je nach Einsatzort und Funktion stark variieren. Einigkeit herrscht hingegen bezüglich der Etymologie des Begriffs. Die Bezeichnung stammt ursprünglich aus den USA, wo Weblogs bereits während der 90er Verbreitung fanden. Der Begriff setzt sich dabei aus dem auch bei uns längst gängigen Wort *Web* (Synonym für WWW) und dem englischen Begriff *log* (was soviel wie „Tagebuch“ oder „Protokoll“ bedeutet) zusammen.

Ähnlich wie Logbücher bereits seit Jahrhunderten in der Schifffahrt benutzt werden, um bedeutsame nautische Ereignisse chronologisch aufzuzeichnen, besteht ein Weblog aus chronologisch geordneten Einträgen, die im Web publiziert werden. Jedes Mal, wenn das Blog vom Autor – dem „Blogger“ – aktualisiert wird (beispielsweise wenn dieser einen neuen Text oder Bilder hinzufügt), liegt ein so genannter neuer *Eintrag* (oder auch *post*) vor - wobei sich der aktuellste Eintrag stets zuoberst auf der Webseite befindet und erst mit einem neuen Eintrag in der Reihung nach unten wandert. Die älteren Einträge werden zumeist in einem *Archiv* – das in leistungsfähigeren Weblog-Systemen auch mit einer praktischen Suchfunktion ausgestattet ist – aufbewahrt. Zur verbesserten Übersichtlichkeit bieten die meisten Weblog-Systeme eine Möglichkeit, die Einträge mittels sogenannter *Kategorien* thematisch aufzuschlüsseln.

Nun lässt sich einwenden, dass das oben beschriebene Prinzip nicht besonders neuartig erscheint, ähnelt es doch bereits gängigen Medienformaten – wie beispielsweise herkömmlichen Nachrichtentickern. Ein Merkmal unterscheidet Weblogs allerdings von derartigen Systemen: Weblogs sind interaktiv. Für den Leser besteht in der Regel die Möglichkeit, die dort publizierten Einträge zu kommentieren, d.h. einen den Eintrag ergänzenden Beitrag zu verfassen. Üblicherweise werden diese Kommentare mit zusätzlichen Infos versehen wie beispielsweise dem Benutzernamen des Verfassers, Datum und Uhrzeit, wann er den Kommentar erstellt hat, und eventuell einem Link zu dessen Website be-

1) Quelle: *Financial Times Deutschland* vom 05.01.2006 (`www.ftd.de/tm/me/37390.html`)

2) bezeichnet die durch Weblogs initiierte Entstehung eines Journalismus „von unten herauf“

3) CMS = *Content Management System*

ziehungsweise dessen eigenem Weblog. In einigen Weblog-Systemen können in weiterer Folge auch Kommentare kommentiert werden.

Ebenfalls bezeichnend für Weblogs ist deren in der Regel hohe Linkdichte. So sind Weblogs üblicherweise durch zahlreiche Verweise und Kommentare untereinander verbunden. Gefördert wird diese Verlinkung durch diverse Mechanismen wie etwa *Pings* oder *Trackback*. So kann beispielsweise mittels Senden eines so genannten Pings (= „Läuten, Klingeln“) Weblog-Verzeichnissen im WWW mitgeteilt werden, dass ein Weblog aktualisiert wurde. Basierend auf diesen Informationen (also allen eingehenden Pings) werden dann auf diesen Webseiten entsprechende aktuelle Weblog-Listen zusammengestellt. Pings kommen zuweilen auch bei Trackback zum Einsatz, allerdings zu einem völlig anderen Zweck. Um den Nutzen von Trackback zu veranschaulichen, wollen wir ein praktisches Beispiel heranziehen: Anton liest einen Beitrag in Bertas Weblog. Er entschließt sich, in seinem Weblog selbst einen Beitrag zu dem Thema zu verfassen, und bezieht sich dabei auf den Beitrag von Berta. Üblicherweise wird das Blog, auf das verwiesen wird, verlinkt. Nutzt man die Trackback-Funktion, sendet das eigene Blog einen so genannten (Trackback-)Ping in Form eines HTTP POST-Requests an eine bestimmte URL des Ziel-Blogs. In dem anderen Blog werden diese Daten (sofern alles problemlos verläuft) gespeichert (z.B. in einer Datenbank) und anschließend in der Einzelansicht des jeweiligen Eintrags mit Verlinkung zum bezugnehmenden Blog angezeigt, d.h. zu Bertas Beitrag wurde nun auch ein Link auf Antons Beitrag hinzugefügt. Trackback ermöglicht demnach Bloggern festzustellen, ob auf ihren eigenen Eintrag in einem anderen Weblog Bezug genommen wurde. Voraussetzung dafür ist allerdings, dass sowohl Anton als auch Berta ein System benutzen, das Trackback unterstützt.

Viele Weblogs enthalten auch so genannte *Blogrolls*, das sind Linklisten zu anderen Weblogs (oder auch zu Webseiten, Büchern oder anderen Medien). Es handelt sich hier meist um Empfehlungen des Bloggers, bei persönlichen Weblogs oft auch um Listen von Weblogs, die von Freunden betrieben werden (*Friendslists*). Der Umfang der beigepackten Features variiert stark, je nach in Einsatz befindlichem Weblog-System. So beinhalten einige Weblogs beispielsweise zusätzlich einen WYSIWYG-Editor, eine Fotogalerie oder einen Kalender.

Gefördert wird die rasche Verbreitung und der Austausch von Informationen aus Weblogs auch durch sogenannte *RSS-Feeds*. Sind diese im Blog aktiviert, erzeugt die Software automatisch zusätzlich eine maschinenlesbare Version der Einträge im XML-Format, die dann von diversen anderen Medien (z.B. von Newsreadern oder einigen eMail-Programmen) automatisch „aufgelesen“ und angezeigt werden kann. Der große Vorteil für den Leser besteht darin, dass er die entsprechenden Webseiten nicht mehr direkt „ansurfen“ muss. Sein Newsreader oder eMail-Klient holt von abonnierten Weblogs automatisch den aktualisierten Content ab, die Inhalte werden dem Leser konzentriert und übersichtlich in dieser Software dargestellt (für nähere Informationen zum Thema RSS siehe auch Artikel *RSS Enterprise* auf Seite 46).

Anwendungsbereiche

1. Weblogs als „Online-Tagebücher“: Das ganz Private öffentlich gemacht

Vermutlich handelt es sich hierbei um den zahlenmäßig am häufigsten anzutreffenden Typus im WWW, Tendenz steigend. Ähnlich wie vor etlichen Jahren der Trend aufkam, auf einer Personal Homepage persönliche Daten, Hobbies, Fotos u.Ä. zu deponieren und unzählige Privatpersonen entsprechende Webseiten kreierten, so nutzen heutzutage immer mehr User die Möglichkeit, via Weblogs ihre persönlichen Erlebnisse in Büro, Studium, Schule und Freizeit zu publizieren. Das Medium dient dabei zuvorderst der Selbstdarstellung und persönlichen Reflexion, die Inhalte spiegeln die persönlichen Interessen und Befindlichkeiten wieder (weshalb Weblogs oft auch als eine Art „virtuelles Tagebuch“ bezeichnet werden).

Obwohl die Struktur und zuweilen auch die Inhalte an ein Tagebuch erinnern, kann der Begriff irreleiten. Anders als „klassische“ Tagebücher, die in der Regel keinen Empfänger als den Sender selbst kennen, dienen Weblogs eben nicht ausschließlich der persönlichen Reflexion, sondern kommunizieren (mehr oder weniger bewusst) Botschaften an die Umwelt: Wie der Blogger sich der Welt darstellen will und wie sich ihm/ihr die Welt darstellt. Dabei finden sich nicht selten tiefe Einblicke in Privatleben, Einstellungen, politische Überzeugungen und Persönlichkeitsstruktur des Bloggers. Was aber bewegt den Autor, sich derart geistig zu „exhibitionieren“? Wie so oft lässt sich diese Frage wohl nicht monokausal beantworten, die Motivationen hierzu sind sicherlich vielfältig und komplex: Sei es nun einfach die Freude am Schreiben, am Sich-Mitteilen, der Wunsch nach Selbstdarstellung, Profilierung, Anerkennung oder „Schubladenflucht“ – also Klischees abzulegen, die Wahrnehmung seiner Selbst in den Köpfen der Anderen zu formen, auszuweiten (oder einzugrenzen, je nachdem).

In vielen Fällen sind Weblogs oft auch nur ein weiteres Medium, um soziale Kontakte anzubahnen bzw. zu pflegen. Ähnlich wie sich beispielsweise bei Chats und Foren „Communities“ entwickeln, können auch Weblogs als Kommunikationsplattformen für Gleichgesinnte dienen (z.B. um sich über ein gemeinsames Thema oder Hobby auszutauschen). Manche Autoren, die via Weblog kommunizieren, kennen sich auch persönlich (z.B. aus der Schule, dem Büro) – das Bloggen ersetzt dabei nicht die realen Kontakte, sondern ergänzt sie vielmehr. Dabei erlaubt das Medium eben jene Tiefe und Ausführlichkeit, denen sich gewöhnlicher Smalltalk oft entzieht. Die Informationen sind dabei jederzeit abrufbar und somit vom Sender autark. Vorteil für den Blogger:

Der halbstündige Bericht von der Südamerikareise muss somit nicht jedem Kollegen einzeln vorgetragen werden, die Bilder können gleich „dazugepackt" werden. Der Vorteil für den Rezipienten: Er muss dem Bericht nicht am Gang zwischen zwei Meetings lauschen – er kann ihn auch am Abend gemütlich via Weblog nachlesen und kommentieren. Oder eben nicht. Ganz nach Belieben.

2. Weblogs als Medien der Expertenkommunikation

In Technikerkreisen werden Weblogs schon länger genutzt, um Expertise in einzelnen Fachbereichen auszutauschen. Der bloggende Experte kommentiert dabei via Blog die aktuellen Entwicklungen im jeweiligen Gebiet und diskutiert sie mit seinen Lesern. Durch die Einbindung von Links zu Quellen, Literatur, nützlichen Webseiten und Weblogs zu dem Thema stellt der Blogger, aufbauend auf persönliche Erfahrungen, Wissen und Erkenntnisstand, seinen Lesern ein Kompendium an vorselektierten Quellen zur Verfügung, die er für das Thema als nützlich erachtet. Inzwischen haben freilich auch andere Berufsgruppen das Weblog für diesen Zweck entdeckt – ein Beispiel wären hier die sogenannten *Blawgs* (eine Wortsynthese aus *Blog* und *law*), in denen Juristen aktuelle Urteile und Gesetzesentwürfe diskutieren.

Knowledge Blogs für das interne Wissensmanagement

In den USA sind Weblogs bereits fester Bestandteil der Forschungskommunikation. Der unkomplizierte Publikationsmechanismus ermöglicht es dabei, dass wissenschaftliche Forschungsergebnisse sehr rasch veröffentlicht und auch auf internationaler Ebene diskutiert werden können. Zu Recht wird hier allerdings von Kritikern angemerkt, dass eben dieses Charakteristikum auch häufiger die Publikation von „Unfertigem" bedinge, was in der Wissenschaft nicht immer erwünscht sei.

Dem lässt sich freilich entgegenhalten, dass die Dokumentation von Entwicklung und Diskurs, ja des Forschungsprozesses selbst, letztlich wiederum eine unschätzbare Wissensquelle darstellen kann. Dabei müssen sich Blogs nicht zwangsläufig an einen „globalen" Leserkreis wenden. So können interne Blogs (z.B. einer Forschungsgruppe) dazu benutzt werden, um Erfahrungen, Fortschritte, Fachartikel, Tipps etc. weiterzugeben oder um den Verlauf eines Forschungsprojekts sukzessive zu dokumentieren. Das Blog

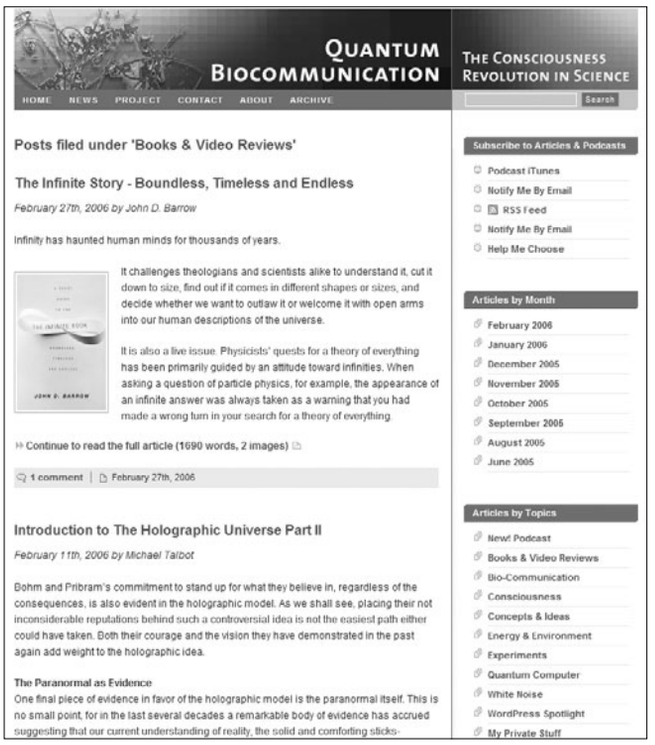


Abb. 1: Anwendungsbeispiel Weblogs (www.quantumbiocommunication.com)

(in diesem Fall ein so genanntes *Knowledge Blog*) unterstützt dabei das persönliche Wissensmanagement.

Vorteile für die Anwendung in Wissenschaft und Lehre ergeben sich auch aus den spezifischen Eigenschaften des Medienformats: So betonen Didaktiker, dass die vielen kleinen Nachrichtenteile fokussierter und verständlicher wären als lange, ausschweifende Abstracts und deshalb stärker die Interaktion (Diskurs, Kritik etc.) fördern würden. Weiters lassen sich mittels *Permalinks*[4] in Weblogs auch kleinere Textteile adressieren – und somit auch referenzieren (im Gegensatz zu Webseiten). Nützlich ist auch die Trackback-Funktion (siehe *Grundlagen*), mit der sich ein (potentiell weltweiter) virtueller Diskussionskontext herstellen lässt.

Anhand von Weblogs Lernprozesse visualisieren

Der bereits zuvor angesprochene prozessorientierte Charakter von Weblogs läßt sich auch im Bildungsbereich sinnträchtig verwerten. Der Bildungstechnologe Dr. Peter Baumgartner betont, dass es immer wichtiger werde, *„Lernende zu befähigen ihren eigenen Lernprozess selbst zu steuern."*[5] Die chronologische Struktur von Weblog-Content und die subjektorientierte Publikationsform eignet sich besonders für ein kontinuierliches, selbstgesteuertes und sozial situiertes Lernen. So würden *„Weblogs mit fortschreitender Dauer der Nutzung die individuelle persönliche Lernkarriere bzw. Erkenntnisgeschichten der jeweiligen WeblogautorInnen dokumentieren. Durch die chronologischen Aufzeichnungen und Diskussionen (Foren, Kommentar und Trackback-Funktion) kann der Prozess der Wissenskonstruktion der jeweiligen WeblogautorInnen verfolgt werden."*[6]

4) Permalinks (also permanente = dauerhafte Links) werden automatisch generiert. Ihr URL ändert sich nicht, auch wenn der Autor später die Struktur des Blogs verändert.

5) Dr. Peter Baumgartner, *Eine neue Lernkultur entwickeln: Kompetenzbasierte Ausbildung mit Blogs und E-Portfolios.* (`http://bt-mac2.fernuni-hagen.de/peter/gems/eportfoliodeutsch.pdf`)

6) ibid.

3. Weblogs als Erweiterung der (politischen) Öffentlichkeit

In den USA betreiben inzwischen zahlreiche etablierte Journalisten Weblogs, um Kommentare und Informationen ohne die redaktionellen Filter klassischer Massenmedien bereitzustellen. Insbesondere während des Irakkrieges gewannen Weblogs enorm an Bedeutung. Von vielen Lesern beziehungsweise Zuschauern wurde die Berichterstattung etablierter US-Medien als unkritisch und patriotisch gefärbt empfunden, weshalb man auf alternative Informationsquellen auswich. Dies spiegelt sich auch in Umfragen wieder, in denen die Mehrheit der Leser den Weblogs (gegenüber offiziellen Medien) „eine größere Ehrlichkeit in der Berichterstattung" einräumt.

Inzwischen haben auch Zeitungen und Nachrichtensender die zunehmende Bedeutung des neuen Medienformats erkannt. Auf BBC News sind die *Reporters' logs* bereits seit längerem fixer Bestandteil des Berichterstattungskonzepts. So berichtet zur Zeit beispielsweise der Reporter David Shukman täglich von seiner Forschungsreise in der Antarktis (`http://news.bbc.co.uk/1/hi/sci/tech/4611712.stm`), ältere Weblogs dokumentierten etwa das Erdbeben in Pakistan oder die Terroranschläge in London. Im deutschsprachigen Raum hält sich die Anzahl der (offiziell) bloggenden Journalisten noch in überschaubaren Grenzen. Einige noch nicht etablierte, freiberufliche Journalisten sehen Weblogs auch als eine Möglichkeit der Selbstvermarktung und hoffen, Redakteure mit ihren Publikationen auf sich aufmerksam zu machen. Neben diesen bloggenden Professionisten gibt es natürlich auch das umgekehrte Phänomen: Laien, die sich im Rahmen ihrer Blogs als Journalisten betätigen. Massiven Zustrom verzeichneten insbesondere Weblogs, in denen Betroffene von Katastrophen berichteten (beispielsweise von den Terroranschlägen am 11. September 2001 oder von der Tsunami-Flutkatastrophe in Südostasien).

Abb. 2: Anwendungsbeispiel Weblogs (http://news.bbc.co.uk/1/hi/sci/tech/4611712.stm)

Parallel zu den Journalisten entdeckten auch politische Akteure das neue Medienformat für ihre Zwecke. Obgleich auch hier der anglo-amerikanische Raum eine klare Vorreiterrolle innehat, setzen sich Weblogs auch hierzulande immer häufiger als Instrument der politischen PR durch – wenn auch zuweilen mit einigen Einschränkungen: So hatte in Deutschland die SPD die Europawahl mit einem Weblog begleitet, das allerdings über keine Kommentarfunktion verfügte (vgl. `www.spd-newslog.de`). In Österreich wurde zu den Landtagswahlen 2005 in Wien, Steiermark und Burgenland ein kollaboratives Gruppen-Blog (zu finden unter `www.wahlblog.at`) betrieben. Das Blog sollte laut Initiatoren als offene, politisch ausgewogene Diskussionsplattform dienen, auf der Blogger aus verschiedenen politischen Lagern ihre persönliche politische Meinung kundtun und Geschehnisse während des Wahlkampfs subjektiv beurteilen konnten.

Eine Studie zum Thema „Weblogs als Mittel der Kommunikation zwischen Politik und Bürgern" fasst allerdings zusammen, dass das neue Medienformat viele Chancen, aber auch diverse Risiken in sich berge: So würden *„Regeln aus der ‚Blogwelt' kollidieren mit Erwartungen und Kommunikationsmustern aus der politischen Kommunikation, die sehr stark auf Kontrolle von öffentlichen Äußerungen setzt und wenig Spielraum für Interaktivität lässt"*; der Autor räumt deshalb ein, dass es *„gut möglich* (sei), *dass sich Politiker-Weblogs als eine Sonderform der Weblogs etablieren, die zwar eine etwas andere Form der Selbstpräsentation von Politikern, aber keine echte Diskussion/Partizipation ermöglichen."* [7)]

4. Weblogs als Online-Marketingplattform von Unternehmen

Auch in der Geschäftswelt entdeckt man zunehmend das „neue" Medium für die kommerzielle Nutzung, z.B. als offizielles Unternehmensblog. Parallel dazu wächst auch die Riege der (mehr oder weniger selbsternannten) „Weblog-ExpertInnen", welche den Firmen beim Einsatz eines Weblogs beratend zur Seite stehen. Trotz der allzu optimistischen Prognosen einzelner Berater liegen noch kaum

7) Christopher Coenen, *Weblogs als Mittel der Kommunikation zwischen Politik und Bürgern – Neue Chancen für E-Demokratie?* (`www.soz.uni-frankfurt.de/K.G/B5_2005_Coenen.pdf`)

brauchbare Einschätzungen bezüglich Potential und Werbewirksamkeit von Weblogs vor. Dass diskursive Medien, in denen KundInnen (oder auch die Konkurrenz) die Möglichkeit haben, Kommentare abzugeben, auch einige Risiken für das jeweilige Unternehmen in sich bergen, liegt nahe. Auch hängt der mögliche Wirkgrad sicherlich in starkem Maße davon ab, inwieweit Medienformat und „Produkt" korrelieren.

Wagt man eine realistische Einschätzung, so wird wohl kaum eine Revolution in der Unternehmenskommunikation bevorstehen, sondern ist eher anzunehmen, dass sich Weblogs als eine zusätzliche Form etablieren, die die herkömmlichen Kommunikationsprozesse ergänzt. Als Beispiel sei hier jenes Marketinginstrumentarium erwähnt, das der Online-Buchhändler Amazon seinen US-Autoren zur Verfügung stellt. So können diese direkt beim Online-Buchhändler ein *Autorenblog* erstellen und auf ihre privaten Blogs verweisen. Die Schriftsteller erhalten mit Hilfe der Blogs die Möglichkeit, ihre Werke selbst online zu vermarkten. Ein neues Programm namens *Amazon Connect* soll dabei die Kommunikation zwischen Autoren und Lesern verbessern helfen.[8)]

Wie komme ich zu meinem persönlichen Weblog?

Wer nun nach dieser Abhandlung „auf den Geschmack gekommen" ist und selbst ein Weblog betreiben möchte, dem stehen dafür zwei Wege offen:

1. Weblog von einem Anbieter

Der unkomplizierteste Weg zu einem eigenen Blog ist der, sich einfach bei einem der zahlreichen Weblog-Anbieter im WWW (z.B. `www.twoday.net` oder `www.blogg.de`) kostenlos ein komplettes Weblog einzurichten. Die Bedienung des Weblogs erfolgt dann via Internet-Browser. Eine Liste von diversen Weblog-Anbietern finden Sie unter `www.plasticthinking.org/wiki/WeblogAnbieter`. Auch die Telekom Austria bietet zur Zeit aon-Kunden auf ihrer neuen Plattform Weblife (`http://community.aon.at/a/awl`) werbefreie und kostenlose Blogs mit bis zu einem Gigabyte Webspace.

2. Weblog selbst installieren

Technisch sehr versierte BenutzerInnen können sich ein Weblog-System auch selbst installieren. Dafür benötigen Sie zunächst einmal Webspace auf einem Server, der die Anbindung an eine Datenbank über eine serverseitige Skriptsprache erlaubt. Weblog-Systeme basieren üblicherweise auf gängigen Skriptsprachen wie Perl oder PHP. Auf den Webservern des Zentralen Informatikdienstes wurde im Zuge der Umstellung der Mailbox- und Unet-Services eine Konfiguration mit PHP- und CGI-Unterstützung geschaffen. Seit Anfang des Jahres 2005 steht PHP somit auch für persönliche Homepages zur Verfügung. Achtung: Beachten Sie bitte, dass PHP hier im Multiuser-Betrieb und im *Safe Mode* läuft, weshalb es bei einigen Applikationen zu Problemen kommen könnte.[9)]

Wenn Sie sich auf die Suche nach einem geeigneten Weblog-System begeben, werden Sie bald feststellen, dass es ein breites Angebot an kostenloser Weblog-Software gibt. Einen guten Überblick vermittelt die Tabelle unter `http://unblogbar.com/software/`. Hier finden Sie eine Vergleichsliste der diversen Features/Funktionen von insgesamt 30 kostenlosen Weblog-Systemen. Unter *Voraussetzungen* können Sie eruieren, welche Skriptsprache (auch Version beachten) vom Server unterstützt werden muss.

Sind die notwendigen Voraussetzungen gegeben, können die Installationsdateien auf den Server übertragen werden. Bei den meisten Weblog-Systemen werden die erforderlichen Einstellungen mit Hilfe eines integrierten Setup-Programms vorgenommen. Es sei aber nochmals darauf hingewiesen, dass die Installation und die Einstellung der Skriptparameter entsprechende technische Kenntnisse voraussetzt. Wer über diese nicht verfügt, sollte lieber erstere Variante wählen.

Michaela Bociurko ■

Weblogs „zum Reinschnuppern"

- Ein schönes Beispiel, wie sich Weblogs im Wissenschaftsbereich sinnvoll einsetzen lassen: `www.quantumbiocommunication.com/`
- „BildungsBlog" ist ein Community-Weblog, in dem jeder registrierte Benutzer Beiträge verfassen und Kommentare schreiben kann. Hier wird zu den Themen Bildung, Lernen, Pädagogik publiziert und diskutiert: `http://bildung.twoday.net/`
- Auch die Bauingenieure der TU Dresden tauschen via Weblog („BauBlog") News und Informationen zu ihrem Fachbereich aus: `http://baublog.twoday.net/`
- Schokotiger finden unter `http://myblog.de/fritziepfoten/1` einen Weblog, der sie garantiert genüsslich zum Schnurren bringt.
- Vom Typus her eher ein *Phlog* (also ein Blog mit vielen Bildern): Liebliches für das Auge und Gemüt finden Sie unter `http://cuteoverload.com/`.

8) Quelle: `http://klauseck.typepad.com/prblogger/`

9) siehe dazu auch den Artikel *Gerda geht in Pension: PHP auf den Webservern des ZID* (*Comment 05/2*, Seite 36 bzw. unter `www.univie.ac.at/comment/05-2/052_36.html`)

RSS Enterprise

Im Internet-Zeitalter besteht die größte Herausforderung nicht mehr darin, an so viel Information wie möglich zu kommen – nein, heute muss man aus der Informationsflut die interessanten Meldungen herauspicken und die Übersicht behalten. Genau dabei unterstützt RSS. Was aber verbirgt sich hinter dieser Abkürzung, die zur Zeit in aller Munde ist und auf zahlreichen Webseiten aufscheint?

Das Kürzel RSS, das eher an einen Flugzeugträger als an ein Internet-Service erinnert, steht je nach Version für unterschiedliche Begriffe (Näheres dazu siehe Kasten *Am Anfang war...*), bezeichnet aber in allen Varianten eine Technik zur Verbreitung so genannter *Newsfeeds*. Dabei handelt es sich um ein Informationsmedium, das sich immer schneller einbürgert und schon jetzt den klassischen *Newsletters* – die aktuelle Infos regelmäßig per eMail verbreiten – ernsthaft Konkurrenz macht. Die Einsatzbereiche für Newsfeeds sind vielfältig: Nachrichten, Weblogs (meist chronologisch geordnete Auflistungen von Anmerkungen, Notizen, kurzen Artikeln usw. – siehe auch Artikel auf Seite 41), Podcasts (Sammlungen von selbst erstellten Audio-Dateien), aber auch kommerzielle Anwendungen wie Jobangebote, Last-Minute-Angebote, Artikellisten, Lagerstände, Wiedergabelisten oder Softwareversionen können auf diese Weise publiziert werden.

In einer RSS-Datei dreht sich alles um den reinen Text. Sie ist relativ einfach aufgebaut und enthält keinerlei Formatierungsangaben wie Abstände, Farben, Schriftgrößen oder Ähnliches. Daher ist es ein Leichtes, diesen Text plattformunabhängig abzurufen und nach eigenem Geschmack darstellen zu lassen. Eine Möglichkeit ist das Einbinden eines fremden Newsfeed in die eigene Webseite in passendem Design. Man kann den Text aber z.B. auch von einem so genannten *Meta-Blog* abholen lassen – das ist ein Newsfeed, der seine Inhalte von anderen Newsfeeds bezieht und auf einer Seite gesammelt anbietet, was man *Content Syndication* nennt.

Am Anfang war...

Die Geschichte von RSS reicht zurück bis ins Jahr 1997, als Dave Winer, der heutige Generaldirektor der Software-Firma Userland, sein Weblog in einem XML-Format veröffentlichte. XML steht für *Extensible Markup Language* und ist ein vom World Wide Web Consortium (kurz W3C, ein Gremium zur Standardisierung von Techniken, die das WWW betreffen [12]) definierter Standard. Dieses einfache, aber sehr flexible Text-Format bildet die Grundlage eines jeden Newsfeed [13].

Richtig los ging es dann 1999 mit der RSS-Version 0.90, welche von der Firma Netscape ins Leben gerufen wurde. Darauf folgten die Versionen 0.91, 0.92, 0.93 und 0.94. In diesem Stadium steht RSS für *Rich Site Summary/Syntax*.

Parallel dazu entwickelte Netscape die anspruchsvollere, auf RDF basiende Version 1.0; RSS heißt hier *RDF Site Summary*. Bei RDF (*Resource Description Framework* – übersetzt in etwa „Quellenbeschreibungssystem" [14]) handelt es sich um die Spezifikation eines Modells zur Repräsentation von Metadaten (das sind in die jeweiligen Dokumente eingebundene Zusatzinformationen über Webseiten und andere Objekte), die erstmals 1999 vom W3C vorgelegt wurde.

Die Weiterentwicklung des ursprünglichen RSS-Erfinders (Version 2.0) heißt *Really Simple Syndication* – eine einfache, aber vielseitige Version, die derzeit am häufigsten genutzt wird. Wie Version 1.0 lässt sich Version 2.0 mit *Namespaces* erweitern [15]. Dabei wird am Beginn der RSS-Datei anhand eines URI (*Uniform Resource Identifier*, eine eindeutige Kennzeichnung für eine Ressource im Netzwerk) ein standardisierter Tag-Bereich definiert, der im XML-Code verwendet werden kann und zusätzliche Informationen enthält. So ist es beispielsweise möglich, in Podcasts Links zu den zugehörigen Audio-/Video-Dateien sowie deren Format direkt im Feed anzugeben, Copyright-Vermerke genauer zu definieren oder festzulegen, wie oft die Seite vom abrufenden Programm aktualisiert werden soll.

Der Aufbau ist bei allen RSS-Versionen glücklicherweise identisch, auch sind höhere Versionen größtenteils abwärtskompatibel.

Die Disharmonie der jeweiligen Versions-AnhängerInnen und die unübersichtliche Entwicklungsgeschichte trugen jedoch nicht gerade zu einem Durchsetzen eines Standards bei. In diese Kerbe schlägt Atom: Es wurde als Gegenpart zur RSS-Versionsvielfalt und als möglicher Nachfolger entwickelt. Atom ist nicht kompatibel zu RSS, kann jedoch in das RSS-Format umgewandelt werden (und vice versa).

Newsfeeds wollen gefunden werden

Woran erkennt man nun, dass eine Webseite einen Newsfeed enthält? Viele Browser zeigen dies mit Hilfe eines Icons in der Adress-Zeile an (in diesem Fall muss die HTML-Datei einen entsprechenden Eintrag enthalten). Oft findet man ein solches Icon auch direkt auf der besuchten Seite. Ein Klick darauf sollte in der Regel genügen, um den Feed zu abonnieren, sprich den URL der XML-Datei in seinen Newsfeed-Reader zu kopieren. Das Standard-Icon für Newsfeeds [1], das von Mozilla und Microsoft beschlossen wurde, sieht folgendermaßen aus:  Daneben kommen aber auch zahlreiche Eigenkreationen der Webseiten-BetreiberInnen zum Einsatz. Meist sind diese Variationen durch ihre *XML*- oder *RSS*-Beschriftung leicht als Newsfeed-Link erkennbar.

Die beliebten Weblogs oder kurz Blogs basieren ebenfalls auf RSS [2]. Daher sind auch die so genannten *Blogrolls* (oder Blogverzeichnisse, Bloglisten) zu den Newsfeeds zu zählen. Diese enthalten keine Artikel, sondern lediglich Verweise auf Weblogs, in denen Artikel stehen [3]. Man kann sich ein solches Blogverzeichnis in etwa wie die Veröffentlichung einer Bookmark-Liste vorstellen. Die Steigerungsform davon sind *Meta-Blogrolls*: Listen, die ausschließlich aus Verweisen auf weitere Listen bestehen – also Seiten, die nur Links zu Blogverzeichnissen enthalten [4].

Wie verwende ich einen Newsfeed?

Es gibt verschiedene Möglichkeiten, einen angebotenen Newsfeed zu nutzen. Die einfachste ist ein im Browser integrierter Newsfeed-Reader, wie ihn z.B. Firefox oder Safari anbieten [5]. Hier genügt ein Klick auf das Feed-Icon in der Adress-Zeile des Browsers – schon ist ein „dynamisches Lesezeichen", das bei jedem Browserstart aktualisiert wird, angelegt und der Feed kann abgerufen werden.

Daneben gibt es auch spezielle Newsfeed-Programme, die den Inhalt der XML-Dateien auslesen und in übersichtlicher Form darstellen; das gewünschte Design kann vom Benutzer gewählt werden. Diese Programme werden meist gratis oder als Shareware im Internet zum Download angeboten. Ein ganz besonderer Vertreter dieser Gattung ist unter `www.univie.ac.at/ZID/gratissoftware/` verfügbar. Hierbei handelt es sich um eine kostenlose „Uni Wien Edition" des exzellenten *FeedReader* für Windows [6] – ein sehr schlankes, übersichtliches und einfach zu bedienendes Programm, welches vom ZID speziell angepasst wurde: mit einer komfortablen Installations-Routine, vollständiger Übersetzung ins Deutsche und bereits abonniertem ZID-Newsfeed (siehe Kasten *Aktuelle Meldungen des ZID via RSS*).

Eine Untergruppe solcher Newsfeed-Programme sind Webbrowser-Plugins, z.B. *Pluck* [6] für Internet Explorer und Firefox. Als Plugin für Outlook steht z.B. *IntraVnews* [6] zur Verfügung (ab der kommenden Outlook-Version 7 ist ein Reader bereits integriert).

Eine weitere Möglichkeit sind entsprechende Online-Reader auf Basis der Programmiersprache Java [7], mit denen sich die Meldungen direkt im Webbrowser übersichtlich darstellen lassen. Ein solches Service wird unter anderem auch von Google angeboten; um es verwenden zu können, muss man sich lediglich registrieren (und im Browser muss Java aktiviert sein).

Wie eine RSS-Datei „in Rohform" aussieht und wie sie vom Browser bzw. vom Newsfeed-Programm angezeigt wird, ist im Kasten *RSS stellt sich dar* auf Seite 48 ersichtlich.

So füttert man seinen eigenen Newsfeed

Will man auf seiner Webseite einen eigenen Newsfeed anbieten, so hat man in der Regel – d.h. sofern man über keine Programmierkenntnisse verfügt – folgende Möglichkeiten:

- Eine Variante ist die Verwendung eines RSS-Generators [8], mit dessen Hilfe sich die Erstellung eines Newsfeed weitestgehend automatisieren lässt.
- Man kann auch eine statische XML-Seite schreiben. Das hat allerdings den Nachteil, dass man die XML-Datei händisch nachbearbeiten muss, wenn sich auf der Webseite etwas ändert.
- Die dritte Möglichkeit besteht darin, auf ein *Content Management System* (CMS) mit integriertem Newsfeed umzusteigen. Der positive Nebeneffekt dabei ist, dass ein CMS die Wartung der gesamten Website wesentlich erleichtert.

Aktuelle Meldungen des ZID via RSS

Ab sofort bietet der Zentrale Informatikdienst einen Newsfeed für seine Aktuell-Meldungen an. Der Dienst ist in den Versionen RSS 2.0 und Atom verfügbar.

Klicken Sie einfach auf das Feed-Symbol in Ihrem (Firefox-)Browser oder fügen Sie einen der folgenden URLs in Ihren Newsfeed-Reader ein:

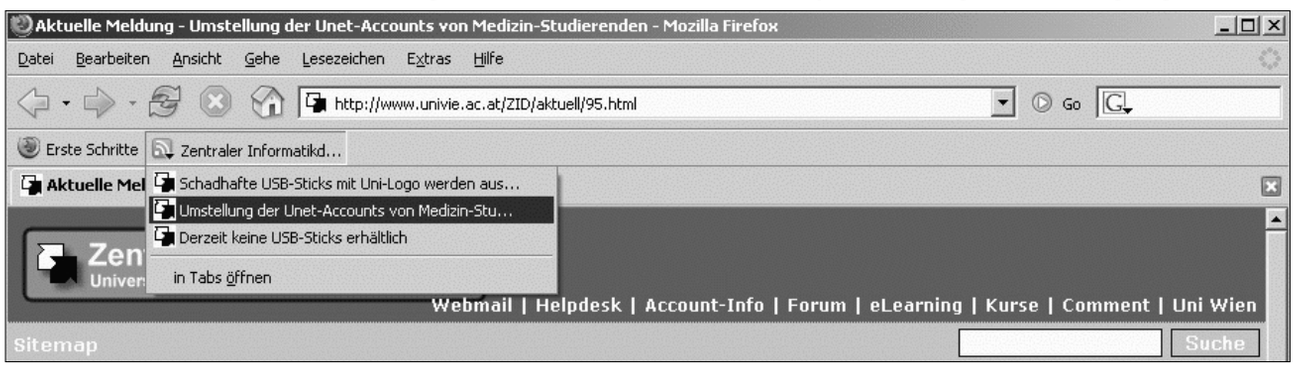
- **RSS 2.0:** `www.univie.ac.at/ZID/aktuell/news.rss`
- **Atom:** `www.univie.ac.at/ZID/aktuell/news.xml`

RSS stellt sich dar

Der Quelltext einer RSS-Datei – hier ein Auszug aus Version 2.0 – hat in etwa das unten gezeigte Aussehen. Um eine richtige und einheitliche Darstellung unter allen Readern zu erreichen, ist es wichtig, die Datei zu validieren, d.h. auf korrekte Syntax überprüfen zu lassen [16].

```
<?xml version="1.0" encoding="ISO-8859-15"?>
<rss version="2.0">
 <channel>
  <title>ZID Aktuell-Meldungen</title>
  <link>http://www.univie.ac.at/ZID/</link>
  <description>Aktuelle Nachrichten des Zentralen Informatikdienstes der Uni Wien
  </description>
  <language>de-at</language>
  <pubDate>Mon, 13 Feb 2006 15:00:00 +0100</pubDate>
  <item>
       <title>Neues RSS-Service auf den Webseiten des ZID</title>
       <pubDate>Mon, 13 Feb 2006 15:00:00 +0100</pubDate>
       <description>Ab sofort bietet der ZID der Uni Wien einen RSS-Newsservice an
       </description>
       <link>http://www.univie.ac.at/ZID/aktuell/100.html</link>
  </item>
 </channel>
</rss>
```

Dieser Code wird von einem Browser mit eingebautem Newsfeed-Reader (hier am Beispiel Firefox) folgendermaßen angezeigt:



In einem klassischen Newsfeed-Programm mit 3-Fenster-Ansicht (hier am Beispiel FeedReader) wird die Datei etwa so dargestellt:

Was die Zukunft bringt

Gerade durch die leichte Erlernbarkeit und die schnelle Verbreitung von XML in vielen Bereichen lässt sich heute schon sagen, dass sich Newsfeeds weiter rasch durchsetzen werden. Nicht zuletzt die ständig wachsenden Ideen und Angebote rund um RSS bestätigen den Stellenwert von Newsfeeds. So tauchen laufend neue, klangvolle Dienste [9] wie *RSS2PDF* (dieses Service wandelt Newsfeed-Dateien in PDF-Dateien um und bietet sie in dieser Form an) oder *RSS2SMS* (damit kann man sich seine Lieblings-Feeds als SMS zuschicken lassen) im Internet auf. Die Konkurrenz zu klassischen Newsletters will man mit einer Kombination aus beiden Services entschärfen. Das nennt sich dann *RSS2MAIL* und bietet dem Benutzer die Möglichkeit, sich die gewünschten Newsfeeds gesammelt per eMail zuschicken zu lassen. Wenn Sie sich mit der „RSS Enterprise“ auf die Reise begeben möchten, starten Sie am besten mit einem Nachrichten-Newsfeed [10]. Auch im Computer-Bereich sind zahlreiche nützliche Newsfeeds verfügbar [11]. Also: Leinen los und viel Vergnügen!

Alexander Berndl ■

Linksammlung

[1] Standard-Feedicon: `www.feedicons.com`

[2] Eigener Weblog: `www.twoday.net`
`www.blogger.com`

[3] Blogrolls: `www.completerss.com`
`www.weblogverzeichnis.de`
`www.rss-scout.de`
`www.rss-nachrichten.de`

[4] Meta-Blogrolls: `www.syndic8.com`

[5] Gratis-Browser mit integriertem Newsreader:
Firefox: `www.mozilla.com`
Safari (Mac OS X): `www.apple.com/macosx/features/safari`

[6] Gratis-Newsfeed-Programme
für Windows:
Feedreader: `www.univie.ac.at/ZID/gratissoftware/`
Plugin für Outlook: `www.intravnews.com`
Plugin für IE6: `www.pluck.com`
für Windows/Linux/Mac: `www.disobey.com/amphetadesk/`

[7] Online-Reader: `www.google.com/reader/`
`www.aggregator.de`
`www.bloglines.com`

[8] RSS-Generator:
`www.softwaregarden.com/products/listgarden/`

[9] RSS2x:
RSS2PDF: `www.rss2pdf.com`
RSS2SMS: `www.rss2sms.de`
RSS2MAIL: `www.feedblitz.com`

[10] Nachrichten-Newsfeeds:
`http://feeds.feedburner.com/reuters/topNews/`
`http://rss.orf.at/news.xml`
`http://derStandard.at?page=rss&ressort=Newsroom`

[11] Computer-Newsfeeds:
`www.heise.de/newsticker/heise.rdf`
`http://rss.orf.at/futurezone.xml`
`http://derStandard.at/?page=rss&ressort=Webstandard`

[12] W3C: `www.w3.org`

[13] XML: `www.w3.org/XML/`

[14] RDF: `www.w3.org/RDF/`

[15] Namespaces:
`www.feedforall.com/directory-namespace.htm`

[16] Feedvalidator: `www.feedvalidator.org`

WIKI – Back to the Future

WIKI – wer oder was ist das? Stellt man diese Frage in den Raum, erntet man in der Regel ein Achselzucken oder die zögerliche Rückfrage, ob das was mit Wikipedia zu tun habe. Um es gleich vorweg zu nehmen – es hat tatsächlich mit Wikipedia zu tun, der freien Enzyklopädie, die in mehr als 100 Sprachen existiert. Wikipedia verwendet eine Wiki-Engine als Basis. Folgt man dem Link `www.wikipedia.org` und wählt als gewünschte Sprache *Deutsch* aus, so erhält man auf der Startseite neben der obligaten Kurzinfo einen Satz, der ganz grob das Wesen der Wiki-Technologie charakterisiert: *„Jeder kann mit seinem Wissen beitragen und die Artikel direkt im Browser bearbeiten.“*

Und was ist jetzt so neu und besonders daran? Die Frage ist leicht zu beantworten – neu ist daran gar nichts, vor allem nicht die verwirklichte Zugriffsmöglichkeit für jedermann. Googelt man ein wenig durchs WWW und liest man in einschlägigen Werken nach, so stellt man fest, dass die Idee der direkten Bearbeitung von jedermann und jederfrau, jederorts und jederzeit ein Grundanliegen an das WorldWideWeb ist – und zwar seit dessen Geburtsstunde: Bereits Anfang der neunziger Jahre schlug Tim Berners-Lee seinem Arbeitgeber CERN ein Projekt vor, das auf dem Prinzip des Hypertext beruhte und den weltweiten Austausch sowie die Aktualisierung von Informationen zwischen Wissenschaftlern vereinfachen sollte – der Grundstein für das WWW, wie es heute existiert, wurde gelegt. Tim Berners-Lee war schon zu Beginn der Ansicht, dass ein Webbrowser eine Kombination aus Viewer und Editor sein sollte.

Die Entwicklung nahm aber einen anderen Verlauf. Webbrowser, wie wir sie heute einsetzen, dienen lediglich als Betrachtungsmedium, während es eine Vielzahl von Softwareprodukten gibt, die für die Erstellung, Wartung und Bearbeitung von Webseiten gedacht sind. Die Komplexität der einzelnen Programme erfordert in der Regel Spezialwissen, und so ist nicht nur die Layouterstellung, sondern auch die Verantwortlichkeit für den Inhalt immer weiter weg vom ursprünglichen Verfasser gerückt – was sich nicht immer als glückliche Lösung entpuppt: Fehlende Aktualität aufgrund mangelnder Ressourcen und zu wenig in die Tiefe gehende Information sind nur einige der Folgeerscheinungen. Auch zahllose lästige Tippfehler auf Webseiten möchte man schnell korrigieren – allein, man darf nicht.

Und mit einem WikiWeb wird man dieser Probleme Herr? Tauchen da nicht neue Probleme auf, wenn jedermann und jederfrau, jederorts, …? Die nachfolgende Beschreibung der Funktionalität von WikiWebs soll einen Einblick in die Materie geben und als Entscheidungshilfe dienen, ob diese Art der Wissensaufbereitung und -vermittlung nicht vielleicht auch im eigenen (Arbeits-)Umfeld sinnvoll einsetzbar ist.

Wiki – was ist das?

Hinter der Bezeichnung Wiki verbirgt sich nicht – wie vielleicht angenommen – eine ellenlange Fachbezeichnung, sondern sie ist schlichtweg die hawaiianische Übersetzung des Wortes „schnell“ (wenn man es ganz genau nimmt, müsste es allerdings *wikiwiki* heißen).

Die erste WikiEngine stammt von Ward Cunningham, einem amerikanischen Softwareentwickler, dessen Idee es war, die *„simplest online database that could possibly work“* zu programmieren. Verwirklicht hat er seine Idee im Jahr 1995, indem er in der Programmiersprache Perl ein Programm schrieb, das es ermöglichte, in einzelnen Dateien gespeicherte Textinhalte mit Hilfe von Formularen direkt im Browser zu bearbeiten und zu veröffentlichen, und das auch Dritten gestattete, diese Dateien zu ändern oder zu ergänzen.

Mittlerweile ist eine Vielzahl solcher WikiEngines verfügbar, in unterschiedlichen Programmiersprachen und mit unterschiedlichen Features: Neben der von Wikipedia verwendeten WikiEngine *MediaWiki* gibt es auch *DocuWiki*, *TWiki*, *TikiWiki*, *MoinMoin*, *PhpWiki* und andere mehr. Abgesehen von der wohl prominentesten Nutzung als Lexikon werden Wikis beispielsweise eingesetzt, um Projekte zu koordinieren und zu dokumentieren, um Anleitungen und Hilfestellung für Software zu bieten oder um die gemeinschaftliche Produktion wissenschaftlicher Werke zu erleichtern.

Wer sich erstmalig mit dem Thema beschäftigt, sei einerseits auf die *Spielwiese* von Wikipedia verwiesen (zu finden unter `http://de.wikipedia.org/wiki/Wikipedia:Spielwiese`), wo die Funktionalität eines WikiWeb ausgetestet werden kann, und andererseits auf die Seite `www.c2.com/cgi/wiki?WikiEngines`, die eine Auflistung zahlreicher WikiEngines bietet, gegliedert nach der verwendeten Programmiersprache. Als sehr informativ und sehr hilfreich für die Entscheidungsfindung, welche WikiEngine für die jeweiligen Bedürfnisse am besten geeignet ist, erweist sich die *WikiMatrix*, die unter `www.wikimatrix.org` zu finden ist.

… und wie funktioniert ein WikiWeb?

Anhand des wohl prominentesten Vertreters der WikiWebs, der Wikipedia, werden nachfolgend die wichtigsten Bestandteile einer ausgereiften WikiEngine kurz erläutert. Um das Beschriebene nachzuvollziehen, kann man sich der bereits erwähnten Wikipedia-Spielwiese bedienen.

Die wichtigste Voraussetzung für das Funktionieren eines WikiWeb ist das verantwortungsbewusste Verhalten jedes einzelnen Benutzers, da die Seiten in der Regel von allen BenutzerInnen ohne spezielle Software-Erfordernisse und -Kenntnisse verändert, ergänzt oder auch gelöscht werden können. Nachdem es keine übergeordnete Qualitätskontrolle für verfasste Beiträge gibt, sind die BenutzerInnen gefordert, sich gegenseitig zu kontrollieren, miteinander zu diskutieren und im Bedarfsfall auch Inhalte zu korrigieren.

Neben dem Verhalten der BenutzerInnen spielen aber auch die technischen Voraussetzungen eine nicht unbedeutende Rolle. Die nachfolgenden Grundfunktionen sollte eine WikiEngine auf jeden Fall abdecken, damit ein funktionierendes WikiWeb aufgebaut werden kann:

- **Einfache Markups:** Für das Editieren bzw. Formatieren von Texten sind keine HTML-Kenntnisse notwendig. Damit werden fehlerhafte Ergebnisse weitgehend hintan gehalten.

- **Linksetzung:** Bei Eingabe von Bildnamen, Webadressen oder Seitennamen (bzw. auf Basis spezieller Kennzeichnungen) sorgt die WikiEngine für die automatische Verlinkung auf weitere Seiten innerhalb des WikiWeb.

- **Automatisierte Seitenerstellung:** Das Anlegen von neuen Seiten im WikiWeb erfolgt ebenfalls automatisch, sobald ein Link zu einer Seite gesetzt wird, die als solche noch nicht existiert.

- **RecentChanges-Funktion:** Wer hat wann welche Seite geändert? Eine chronologische Auflistung beantwortet diese Frage und ermöglicht in der Regel auch ein Zurücksetzen auf vorhergehende Versionen.

- **Differenz-Funktion:** Optische Hervorhebungen zeigen dem Benutzer auf den ersten Blick, welche Bestandteile einer Seite korrigiert, gelöscht oder ergänzt wurden.

- **BackLink-Funktion:** Diese bietet eine Auflistung aller Seiten, die auf die aktuelle Seite verweisen, um rasch auf damit in Verbindung stehenden Informationen zugreifen zu können.

- **Volltextsuche:** Was tun, wenn man nicht mehr weiß, wo man etwas gelesen oder geschrieben hat? Die Volltextsuche hilft dabei, durch Eingabe eines Stichworts Texte wiederzufinden.

- **Seitenarchiv:** Etwas versehentlich gelöscht? Kein Problem – da jeder Schritt aufgezeichnet wird, ist ein Zurücksetzen jederzeit möglich.

Die meisten WikiEngines bieten noch eine Vielzahl weiterer Features, die den Komfort und die Sicherheit verbessern, hier aber nicht detailliert zur Sprache kommen.

… und wie arbeitet man mit einem WikiWeb?

Bearbeitungsmodus und Textgestaltung

Was alle WikiWebs gemeinsam haben, ist die direkte Bearbeitungsmöglichkeit, sobald die Seite im Browserfenster erscheint. Mitunter kommt es vor, dass Seiten für die Bearbeitung gesperrt sind; dies betrifft meist Startseiten oder Seiten, die Anleitungen zur Bedienung des WikiWeb enthalten, wo eine Änderung nicht gewünscht ist. Manche WikiWebs ermöglichen auch Zugriffsbeschränkungen auf bestimmte Benutzerkreise, was mitunter von Vorteil sein kann, dem Grundsatz der freien Bearbeitung aber widerspricht.

Gibt es keine solche Einschränkungen, kann jeder Benutzer mittels *Bearbeiten*- oder *Edit*-Schaltfläche die gewünschten Änderungen durchführen, wobei es in der Regel keinen Unterschied macht, ob sich der Benutzer innerhalb des WikiWeb registriert hat oder nicht.

Klickt man die *Bearbeiten*-Schaltfläche an (siehe Abb. 1), so gelangt man zu einem Formular, in dem der Quelltext der gewählten Seite angezeigt wird. Hierbei handelt es sich in den seltensten Fällen um HTML-Code, sondern vielmehr um einen Wiki-spezifischen Code, der es dem Benutzer ermöglichen soll, ohne spezielle Vorkenntnisse rasch und einfach Änderungen durchzuführen. Jedes WikiWeb stellt dem Benutzer einige Formatierungsmöglichkeiten zur Verfügung, mit denen sich der erfasste Text auch optisch ansprechend gestalten lässt.

Beispielsweise ist im Wikipedia-Handbuch unter *Wiki-Syntax* nachzulesen, dass Überschriften durch je zwei Ist-Gleich-Zeichen am Anfang und am Ende zu kennzeichnen sind (`== Überschrift ==`) oder fett geschriebene Textstellen zwischen je drei Hochkommas eingeschlossen werden müssen (`'''fett'''`). Dieser Formatierungscode kann händisch eingetippt werden, ist aber auch über eine Symbolleiste mit Schaltflächen für z.B. *Fett* oder *Kursiv* verfügbar (siehe Abb. 2 auf Seite 52).

Nach erfolgter Textbearbeitung und -gestaltung muss die Seite gespeichert werden. Damit man zuvor nochmals überprüfen kann, ob die vorgenommenen Änderungen auch wirklich so durchgeführt werden wie beabsichtigt, bieten viele WikiEngines eine Voransicht des Artikels. Ist diese Vorschau zufriedenstellend, steht dem Speichern – über eine eigene Schaltfläche – nichts mehr im Wege.

Interne Verlinkung

Die meisten WikiEngines sind in der Lage, Bildnamen, Webadressen und Seitentitel automatisch zu verlinken. Immer wieder stößt man dabei auf den Begriff *CamelCase*. Damit bezeichnet man die an Kamelhöcker erinnernde, gemischte Groß- und Kleinschreibung von Begriffen – z.B. *PublicDomain* oder *WikiEngine*. In dieser Form geschriebene Begriffe werden automatisch als „verlinkungswürdig" erkannt und führen den Benutzer bei Anklicken auf die jeweilige Seite zu diesem Thema. Da es aber in vielen Fällen nicht sinnvoll ist, alle verlinkungswürdigen Begriffe in CamelCase-Form zu schreiben, existieren in den meisten WikiWebs parallel dazu so genannte freie Links, die wiederum durch bestimmte Sonderzeichen (beispielsweise eckige Klammern) eigens zu markieren sind. Falls die entsprechende Seite zu einem Link innerhalb des WikiWeb noch nicht existiert, kann diese nach dem Speichern durch einen einfachen Mausklick auf den Link bzw. auf ein dahinter stehendes Fragezeichen kreiert werden.

Abb. 1: *Bearbeiten*-Schaltfläche in Wikipedia

Abb. 2: Textformatierung in Wikipedia

BackLink-Funktion

In vielen WikiWebs ist der Titel jeder einzelnen Seite mit einem Suchbefehl verbunden, der alle Seiten auflistet, die einen Link auf die aktuelle Seite enthalten. Wikipedia verwendet einen eigenen Menüpunkt namens *Links auf diese Seite*, der eine Spezialseite mit einer Auflistung aller Seiten aufruft, die mit der aktuell gewählten Seite verknüpft sind. Die für die BackLink-Funktion benötigten Daten werden je nach WikiEngine entweder per Volltextsuche gesucht und gesammelt präsentiert oder aber in einer eigens dafür eingerichteten Datenbank gespeichert.

Was gibt es Neues?

Kein WikiWeb ohne RecentChanges-Liste: Hier sieht der Benutzer auf einen Blick, was sich in letzter Zeit getan hat. Neben wesentlichen Änderungen – z.B. neuen Beiträgen – werden auch kleinere Modifikationen wie die Korrektur von Rechtschreibfehlern oder Layout-Änderungen dokumentiert. Wikipedia zeigt zu sämtlichen Änderungen Datum, Uhrzeit und den Benutzernamen an (sofern es sich um angemeldete Benutzer handelt, ansonsten die IP-Adresse). Damit die Liste nicht überdimensional anwächst, wird die Anzahl der aufgelisteten Änderungen standardmäßig auf einen bestimmten Wert beschränkt, wobei der Benutzer in der Regel die Möglichkeit hat, die Anzahl nach Bedarf zu wählen bzw. anhand von Datumseingaben einzuschränken.

Ein zusätzliches Feature innerhalb der RecentChanges-Liste ist der Versionsvergleich, der genauestens darüber Auskunft gibt, wie ein Beitrag mit der Zeit „gewachsen“ ist, und damit einen detaillierten Überblick über durchgeführte Änderungen ermöglicht (siehe Abb. 3). Mit Hilfe der Differenzfunktion wird hinzugefügter oder gelöschter Text je nach WikiEngine entweder farblich und/oder mit Hilfe der Symbole + und – hervorgehoben. Durch das Archivieren von Vorgängerversionen ist es auch sehr rasch und einfach möglich, ein *Rollback* durchzuführen (sprich eine alte Version wiederherzustellen) und damit mutwilliger Zerstörung Einhalt zu gebieten.

Häufig haben angemeldete BenutzerInnen die Möglichkeit, ihre Korrekturen als „unbedeutend“ zu kennzeichnen; solche Änderungen scheinen dann meist nicht in der Recent-Changes-Liste auf. Daraus ergibt sich die Gefahr, dass umfangreiche Umarbeitungen eines Beitrags als unbedeutende Korrekturen tituliert und von niemandem bemerkt werden. Wenn Verwarnungen nicht helfen, kann solchem Missbrauch nur durch Deaktivieren dieses Features entgegengewirkt werden.

Last but not least bietet die RecentChanges-Liste den BenutzerInnen meist auch die Möglichkeit, über Änderungen zu diskutieren, damit Beiträge, die irrtümlich als nicht korrekt eingestuft werden, nicht voreilig überschrieben werden. Mittlerweile etabliert sich sogar eine Art Benutzerverwaltung: BenutzerInnen müssen sich mit ihren Daten anmelden, um Zugang zu bestimmten (meist internen) Bereichen zu erhalten.

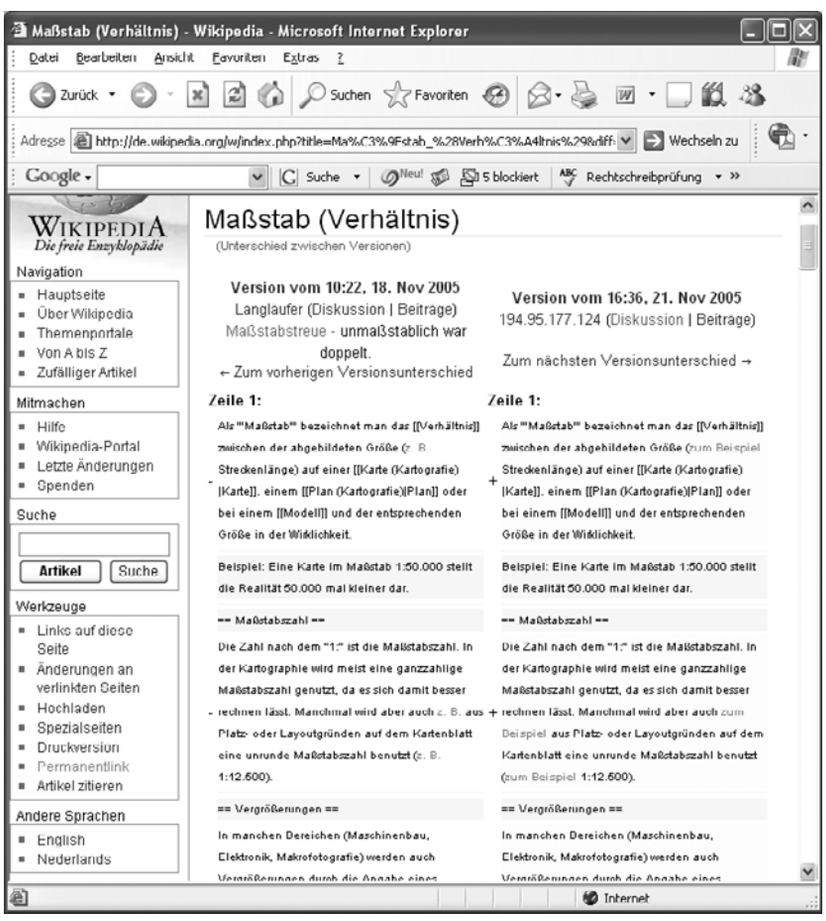


Abb. 3: Kennzeichnung von Änderungen im Versionsvergleich

Gesucht – Gefunden

Zu einem ausgereiften WikiWeb gehört auch eine ausgereifte und vor allem rasch zum Ziel führende Volltextsuche – auch wenn die Implementierung einer Volltextsuche nicht ganz unproblematisch ist, weil sie erhebliche Ressourcen benötigt. Bei einer solchen Volltextsuche wird entweder tatsächlich der Text aller Seiten gelesen und durchsucht, oder es wird ein Index aller Stichworte in einer Datenbank mitgeführt und bei jeder Seitenänderung aktualisiert.

… und die Probleme?

Mit zunehmendem Bekanntheitsgrad der WikiWebs steigt auch die Gefahr der mutwilligen Zerstörung solcher Systeme. Nachdem das Löschen einer Seite dank der Versionssicherung rasch und einfach wieder rückgängig gemacht werden kann, erfreut sich vor allem das Einschleusen fehlerhafter Aussagen zunehmender Beliebtheit. Wie fatal das für eine Enzyklopädie wie Wikipedia sein kann, ist wohl nicht schwer vorstellbar. Hier kann man nur auf die Qualitätssicherung durch andere „Wikianer“ hoffen, die solche Fehler entdecken und korrigieren.

Ebenso ist Spamming innerhalb von WikiWebs ein Thema. Automatisiert übermittelte Beiträge überfordern durch ihre Masse zunehmend die redaktionellen Kapazitäten der WikiBenutzerInnen. Als Gegenmittel kommen hier allerdings nur technische Barrieren in Frage, z.B. die Anforderung einer Bestätigung (wie es teilweise im Mailing-Bereich gehandhabt wird) oder das Sperren bestimmter IP-Adressen.

… und wie sieht die Zukunft aus?

Mit der zunehmenden Verbreitung von WikiWebs wird auch deren Weiterentwicklung in verschiedene Richtungen forciert. Dies betrifft vor allem die etwas umständliche textbasierte Formatierung, die über kurz oder lang durch geeignete WYSIWYG-Editoren abgelöst werden wird. In diesem Zusammenhang ist zu hoffen, dass eine einheitliche Formatierungssyntax entwickelt wird, da die Datenmigration zwischen den einzelnen WikiEngines und der Import/Export von Daten derzeit nicht leicht zu bewerkstelligen sind. Ebenso wird auch der optischen Gestaltung zukünftig mehr Aufmerksamkeit gewidmet werden, was sich bei einigen WikiEngines bereits in Form von Template-Systemen ankündigt. Und nicht zuletzt wird eine Reihe weiterer WikiWebs als Informationsquelle auf uns zukommen – z.B. das Projekt *Wiktionary* (zu finden unter `http://de.wiktionary.org/`), das seit seiner Gründung vor eineinhalb Jahren als frei verwendbares, mehrsprachiges Wörterbuch für den Wortschatz aller Sprachen zur Verfügung steht und bereits mehr als 15 000 Einträge in deutscher Sprache aufweist.

Eva Birnbacher ■

EDUCATION ROAMING

Freier WLAN-Zugang für Uni-Angehörige im eduroam-Verbund

Seit Oktober 2005 ist das österreichische Wissenschaftsnetz ACOnet Teil des eduroam-Verbundes. eduroam steht für *Education Roaming*; es handelt sich dabei um ein Projekt von TERENA (dem Dachverband der europäischen Wissenschaftsnetze, siehe `www.terena.nl`), das es den Angehörigen der angeschlossenen Institutionen ermöglicht, sich mit den Zugangsdaten ihres Heimat-Netzwerks auch im WLAN (*Wireless Local Area Network*) einer anderen teilnehmenden Einrichtung anzumelden. Das bedeutet, dass z.B. Angehörige der Uni Wien mit ihrer Unet- bzw. Mailbox-UserID den Internetzugang an Bildungs- und Forschungseinrichtungen in derzeit 21 europäischen Staaten sowie in Australien und Taiwan nutzen können.

Alle Informationen zum eduroam-Projekt – auch eine Liste aller teilnehmenden nationalen Wissenschaftsnetze – erhalten Sie unter `www.eduroam.org`. Eine Übersichtsseite der beteiligten österreichischen Institutionen ist unter `www.aco.net/eduroam/` im Entstehen. Auf der Webseite `http://eduroam.univie.ac.at/` finden Sie die Zugangsmöglichkeiten (d.h. die Standorte der *Public Network Services*) im Bereich der Universität Wien.

Die Überprüfung der Zugangsberechtigungen innerhalb von eduroam erfolgt über hierarchisch organisierte Server, wobei die von TERENA betriebenen Toplevel-Server die Anfragen an die Authentifizierungsserver der teilnehmenden nationalen Netzbetreiber weiterleiten. Diese wiederum verteilen die Anfragen an die zuständigen Server der jeweiligen Mitgliedsinstitutionen. Zu beachten ist, dass die eduroam-Infrastruktur nur dann genutzt werden kann, wenn das Heimat- und das Gastgeber-Netzwerk dieselbe(n) Zugangstechnologie(n) unterstützen.

Die Nutzung von eduroam wird für drei verschiedene Zugangstechnologien ermöglicht:

- **802.1X** – ein Standard-Protokoll zur Authentifizierung in Funknetzen
- **Captive Portal** – Authentifizierung über eine Webseite, zu der jede Anfrage umgeleitet wird
- **VPN** (*Virtual Private Network*) – Verbindung zum heimischen VPN-Gateway ➠

An der Universität Wien existiert derzeit erst der Zugang über 802.1X; die SSID[1] dieses Netzes ist `eduroam`. Die Zugänge über Captive Portal und VPN werden in naher Zukunft folgen.

Kurt Bauer ■

1) Als *Service Set Identifier* (SSID) bezeichnet man die Kennung eines Funknetzwerks: Jedes Wireless LAN, das auf IEEE 802.11 basiert, besitzt eine konfigurierbare SSID oder ESSID (*Extended Service Set Identifier*), um das Funknetz eindeutig identifizieren zu können. Die SSID stellt also den Namen des Netzes dar und wird daher auch *Network Name* genannt.

DATENTANKSTELLE802.1X

Ein verschlüsseltes Funknetz für die Uni Wien

Parallel zur eduroam-Vernetzung (siehe Seite 53) wurde unter dem Namen *Datentankstelle802.1X* an der Universität Wien ein eigenes, sicheres Funknetz realisiert, dessen Zugangsmöglichkeiten unter `www.univie.ac.at/ZID/pns-standorte/` aufgelistet sind.

Es bietet 128 Bit-WEP-Verschlüsselung, wodurch Mithören sowie andere Attacken deutlich erschwert bzw. unmöglich gemacht werden. Die Authentifizierung erfolgt nicht mehr wie bei den „normalen" Datentankstellen über eine Webseite (Captive Portal), sondern wird direkt beim Verbindungsaufbau über das 802.1X-Protokoll durchgeführt. Benutzername und Passwort werden dabei in einem verschlüsselten Tunnel zum RADIUS-Server der Universität Wien übertragen (Näheres siehe Kasten *802.1X – Technischer Hintergrund*). Neben der Verschlüsselung bietet das 802.1X-Protokoll noch einen weiteren Vorteil: Da das Zugangspasswort gecacht bzw. auf dem Rechner abgespeichert werden kann, müssen die Login-Daten nicht mehr bei jedem Verbindungsaufbau eingegeben werden. Durch das Passwort-Caching wird die Verbindung zudem automatisch wiederhergestellt, wenn der Computer aus dem Ruhezustand wieder „aufgeweckt" wird.

Viele aktuelle Betriebssysteme – z.B. Windows XP SP2 oder Mac OS X 10.4 – unterstützen 802.1X nativ, d.h. man braucht keine zusätzliche Software von Drittanbietern. Sofern das verwendete System keine solche Unterstützung bietet, können diverse 802.1X-Klientenprogramme diese Funktionalität übernehmen:

- *Xsupplicant* (`http://open1x.sourceforge.net/`): kostenloser Open Source-Klient für Linux
- *Odyssey* (`www.funk.com`): kostenpflichtiger Windows-Klient, als Trial-Version erhältlich
- *Aegis* (`www.mtghouse.com`): kostenpflichtiger Klient für Windows, Mac OS X, Solaris, RedHat etc., als Trial-Version erhältlich

Die benötigten Zugangsdaten sind die eigene eMail-Adresse in der Form

- *`Mailbox-UserID`*`@univie.ac.at` (z.B. `musterm9@univie.ac.at`) für Uni-MitarbeiterInnen bzw.
- a*`Matrikelnummer`*`@unet.univie.ac.at` (z.B. `a1234567@unet.univie.ac.at`) für Studierende

sowie das dazugehörige, selbst gewählte Passwort.

Genaue Anleitungen für die Konfiguration des Zugangs zur Datentankstelle802.1X unter Windows XP bzw. unter Mac OS X sind unter dem URL `www.univie.ac.at/ZID/anleitungen/` zu finden.

Daniel Schirmer ■

802.1X – Technischer Hintergrund

Für technisch Interessierte bzw. als Hilfe zum Selbstkonfigurieren (z.B. für Linux): 802.1X basiert auf dem Client-Server-Protokoll RADIUS (*Remote Authentication Dial-In User Service*), welches zur Authentifizierung und Autorisierung von BenutzerInnen bei Einwahlverbindungen, beispielsweise über WLAN, in Computernetzwerke dient.

802.1X (bzw. RADIUS) verwendet diverse EAP-Methoden (*Extensible Authentication Protocol*). An der Universität Wien werden drei davon angeboten:

- PEAP (*Protected EAP*) – sicherer Tunnel, wird als einziges Verfahren von Windows unterstützt
- TTLS (*Tunneled Transport Layer Security*) – ähnlich PEAP
- LEAP (*Lightweight EAP*) – nicht so sicher, sollte nur verwendet werden, wenn kein anderes Verfahren möglich ist

Über eines dieser Verfahren wird die mittels MS-CHAPv2 kryptisierte Benutzername-/Passwort-Kombination übertragen. Andere Verschlüsselungstypen (z.B. TLS, MD5) bzw. Benutzerdaten-Verschlüsselungen wie MS-CHAP sowie Klartext-Passworte werden derzeit nicht unterstützt.

WebCT Vista: Schulungen für Lehrende

In Kooperation mit dem Projektzentrum Lehrentwicklung bietet der ZID kostenlose Schulungen für alle Lehrenden, TutorInnen und PC-Raum-BetreuerInnen, die die Lernplattform WebCT Vista verwenden möchten. Alle Informationen dazu finden Sie unter **www.univie.ac.at/ZID/elearning-schulungen/**.

Einführung: eLearning mit WebCT Vista

Termin	Zeit	Ort
17.03.2006	09:00 – 17:00 h	LE / Kursraum A
05.04.2006	09:00 – 17:00 h	LE / Kursraum A
28.04.2006	09:00 – 17:00 h	LE / Kursraum B
08.06.2006	09:00 – 17:00 h	LE / Kursraum A

Didaktischer Aufbaukurs: Blended Learning

Termin	Zeit	Ort
24.03.2006	09:00 – 12:00 h	Lehrentwicklung
19.04.2006	09:00 – 12:00 h	Lehrentwicklung
10.05.2006	09:00 – 12:00 h	Lehrentwicklung
22.06.2006	09:00 – 12:00 h	Lehrentwicklung

Workshop: Meine Lehrveranstaltung mit WebCT Vista

Termin	Zeit	Ort
15.03.2006	09:00 – 13:00 h	Lehrentwicklung
29.03.2006	09:00 – 13:00 h	Lehrentwicklung
26.04.2006	09:00 – 13:00 h	Lehrentwicklung
17.05.2006	09:00 – 13:00 h	Lehrentwicklung
28.06.2006	09:00 – 13:00 h	Lehrentwicklung

Workshop: Erfahrungsaustausch und Optimierung

Termin	Zeit	Ort
29.06.2006	09:00 – 12:00 h	Lehrentwicklung

WebCT Vista: Schulung für Studierende

Um den Studierenden den Einstieg in die eLearning-Lehrveranstaltungen zu erleichtern, bietet das *Supportbüro Neue Medien* am

Freitag, 17.03.2006, 15:00 – 16:00 Uhr
im **Hörsaal 3 des NIG**
(1010 Wien, Universitätsstraße 7, Erdgeschoss)

eine kostenlose WebCT Vista-Schulung an, die ohne Anmeldung besucht werden kann.

KURSE BIS JUNI 2006

Im Folgenden finden Sie alle Termine der von Mitte März bis Ende Juni 2006 geplanten EDV-Kurse des ZID. Genauere Informationen (An-/Abmeldung, Voraussetzungen, Inhalte, Preise usw.) finden Sie unter

www.univie.ac.at/ZID/kurse/

bzw. in der Broschüre *EDV-Kurse 2006*, die am Helpdesk erhältlich ist (Kontaktadresse siehe Seite 60). Die aktuellen Kursbelegungen (freie Plätze) können unter

www.univie.ac.at/ZID/kursbelegung/

abgerufen werden. Alle Vorträge (*HTML 1 – 3*, *Programmieren mit PHP 1 – 3*) finden im Hörsaal 3 des NIG (1010 Wien, Universitätsstraße 7, Erdgeschoss) statt und sind ohne Anmeldung kostenlos zugänglich. **Bitte beachten Sie auch die Artikel zum *Europäischen Computer Führerschein* (ECDL) sowie zu den organisatorischen Änderungen im Kurswesen des ZID auf den Seiten 9 und 10.**

Betriebssysteme

Windows – Einführung

Termin	Zeit	Anmeldefrist
27.03.2006	09:00 – 16:00 h	23.01.06 – 20.03.06
30.05.2006	09:00 – 16:00 h	23.01.06 – 23.05.06

MS Office-Programme

Word – Einführung

Termin	Zeit	Anmeldefrist
28.03.2006	09:00 – 16:00 h	23.01.06 – 21.03.06
02.05.2006	09:00 – 16:00 h	23.01.06 – 25.04.06
09.06.2006	09:00 – 16:00 h	23.01.06 – 02.06.06

Word – Fortsetzung

Termin	Zeit	Anmeldefrist
03.04.2006	09:00 – 16:00 h	23.01.06 – 27.03.06
04.05.2006	09:00 – 16:00 h	23.01.06 – 27.04.06
12.06.2006	09:00 – 16:00 h	23.01.06 – 05.06.06

Word – Wissenschaftliches Arbeiten

Termin	Zeit	Anmeldefrist
24.04.2006	09:00 – 16:00 h	23.01.06 – 14.04.06
24.05.2006	09:00 – 16:00 h	23.01.06 – 18.05.06
19.06.2006	09:00 – 16:00 h	23.01.06 – 12.06.06

Excel – Einführung

Termin	Zeit	Anmeldefrist
15.05.2006	09:00 – 16:00 h	23.01.06 – 08.05.06

Excel – Fortsetzung

Termin	Zeit	Anmeldefrist
17.05.2006	09:00 – 16:00 h	23.01.06 – 10.05.06

PowerPoint – Einführung

Termin	Zeit	Anmeldefrist
20.03.2006	09:00 – 16:00 h	23.01.06 – 13.03.06
10.05.2006	09:00 – 16:00 h	23.01.06 – 03.05.06

PowerPoint – Fortsetzung

Termin	Zeit	Anmeldefrist
22.03.2006	09:00 – 16:00 h	23.01.06 – 15.03.06
29.05.2006	09:00 – 16:00 h	23.01.06 – 22.05.06

Access – Einführung

Termin	Zeit	Anmeldefrist
22.05. – 23.05.06	09:00 – 16:00 h	23.01.06 – 15.05.06

Access – Fortsetzung

Termin	Zeit	Anmeldefrist
20.06. – 21.06.06	09:00 – 16:00 h	23.01.06 – 13.06.06

Diverse Software

SPSS – Einführung

Termin	Zeit	Anmeldefrist
18.05. – 19.05.06	09:00 – 16:00 h	23.01.06 – 11.05.06
22.06. – 23.06.06	09:00 – 16:00 h	23.01.06 – 14.06.06

Acrobat – Arbeiten mit PDF-Dateien

Termin	Zeit	Anmeldefrist
11.05.2006	09:00 – 16:00 h	23.01.06 – 04.05.06

Photoshop – Einführung

Termin	Zeit	Anmeldefrist
29.03.2006	09:00 – 16:00 h	23.01.06 – 22.03.06
03.05.2006	09:00 – 16:00 h	23.01.06 – 26.04.06

Photoshop & ImageReady – Erstellen von Webgrafiken

Termin	Zeit	Anmeldefrist
25.04.2006	09:00 – 16:00 h	23.01.06 – 18.04.06
02.06.2006	09:00 – 16:00 h	23.01.06 – 26.05.06

Internet

HTML 1 – Erstellen von Webseiten

Termin	Zeit	Anmeldung
10.03.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

HTML 2 – Erstellen von Webseiten

Termin	Zeit	Anmeldung
17.03.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

HTML 3 – Cascading Style Sheets (CSS)

Termin	Zeit	Anmeldung
24.03.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

HTML-Workshop – Erstellen von Webseiten

Termin	Zeit	Anmeldefrist
22.03.2006	09:00 – 16:00 h	23.01.06 – 15.03.06
29.05.2006	09:00 – 16:00 h	23.01.06 – 22.05.06
12.06.2006	09:00 – 16:00 h	23.01.06 – 05.06.06

Webdesign – Konzeption und Gestaltung

Termin	Zeit	Anmeldefrist
30.03. – 31.03.06	09:00 – 16:00 h	23.01.06 – 23.03.06
13.06. – 14.06.06	09:00 – 16:00 h	23.01.06 – 06.06.06

Dreamweaver – Einführung

Termin	Zeit	Anmeldefrist
01.06.2006	09:00 – 16:00 h	23.01.06 – 24.05.06

Flash – Einführung

Termin	Zeit	Anmeldefrist
23.03.2006	09:00 – 16:00 h	23.01.06 – 16.03.06
04.04.2006	09:00 – 16:00 h	23.01.06 – 28.03.06

Systembetreuung

Netzwerk – Grundlagen

Termin	Zeit	Anmeldefrist
09.05.2006	09:00 – 16:00 h	23.01.06 – 02.05.06

Linux – Grundlagen

Termin	Zeit	Anmeldefrist
26.04. – 27.04.06	09:00 – 16:00 h	23.01.06 – 19.04.06

Programmierung

Programmieren mit PHP – Teil 1

Termin	Zeit	Anmeldung
31.03.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

Programmieren mit PHP – Teil 2

Termin	Zeit	Anmeldung
07.04.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

MySQL-Datenbank mit phpMyAdmin verwalten – Teil 3

Termin	Zeit	Anmeldung
28.04.2006	12:30 – 15:00 h	keine (NIG/Hörsaal 3)

Workshop – Programmieren mit PHP und MySQL

Termin	Zeit	Anmeldefrist
15.05. – 16.05.06	09:00 – 16:00 h	23.01.06 – 08.05.06

ÖFFNUNGSZEITEN

Helpdesk des ZID

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

Mo – Fr **9:00 – 18:00**

Support Neue Medien

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

Mo, Di, Mi, Fr **9:00 – 16:00**
Do **9:00 – 18:00**

PC-Räume des ZID

NIG, AAKH, UZA:

Mo – Fr 7:30 – 21:30 / Sa 7:30 – 13:00

PC-Raum-Betreuung für diese Standorte:

Mo – Fr 9:00 – 20:00

Details bzw. weitere Standorte finden Sie unter
www.univie.ac.at/ZID/pc-raeume/

HANDBÜCHER

(Stand: 1. März 2006)

Die unten angeführten Handbücher des *Regionalen Rechenzentrums Niedersachsen* (RRZN) können am **Helpdesk** des ZID (siehe Seite 60) gegen **Barzahlung** erworben werden. Neben den nachfolgend aufgelisteten Titeln sind auch einige Restexemplare zu älteren Programmversionen erhältlich – bitte erkundigen Sie sich daher am Helpdesk, wenn Sie ein bestimmtes Handbuch benötigen.

RRZN-Handbücher dürfen nur an **Studierende und MitarbeiterInnen der Universität Wien** verkauft werden! Eine Weitergabe an sonstige Privatpersonen, Schulen, Firmen usw. ist ausdrücklich untersagt. Solche InteressentInnen können wir nur auf die Literatur im Buchhandel verweisen, insbesondere auf die des Herdt-Verlags (www.herdt.de).

Access 2003 – Grundlagen für Datenbank-Entwickler	EUR 5,50
Access 2003 – Fortgeschrittene Techniken für Datenbank-Entwickler	EUR 5,50
Acrobat 5.0 – PDF-Dateien erstellen und publizieren	EUR 4,00
Excel 2003 – Grundlagen der Tabellenkalkulation	EUR 5,50
Excel 2002 – Fortgeschrittene Anwendungen	EUR 5,50
Excel 2002 – Automatisierung – Programmierung	EUR 5,50
Frontpage 2002 – Grundlagen	EUR 5,00
Image Ready 3.0 – Bildbearbeitung für Web-Seiten	EUR 5,50
Linux – Nutzung mit der grafischen Oberfläche KDE	EUR 5,50
Netzwerke – Grundlagen	EUR 5,00
Photoshop 7.0 – Grundlagen	EUR 5,50
PowerPoint 2002 – Grundlagen	EUR 5,50
PowerPoint 2002 – Fortgeschrittene Anwendungen	EUR 5,50
Publizieren im World Wide Web – Eine Einführung	EUR 5,00
SPSS für Windows – Einführung anhand der Version 11	EUR 4,00
UNIX – Eine Einführung in die Benutzung	EUR 4,00
VBA-Programmierung – Integrierte Lösungen in Office XP	EUR 5,00
Windows XP – Grundlagen	EUR 5,50
Word 2002 – Fortgeschrittene Anwendungen	EUR 5,00
Word 2003 – Grundlagen	EUR 5,00
Word 2003 – Berichte und wissenschaftliche Arbeiten	EUR 5,00

Personal- & Telefonverzeichnis

Sekretariat	4277-14001	
Fax	4277-9140	

Direktion

Rastl Peter *(Direktor)*	4277-14011	Zi.B0112
Buchner Claudia	4277-14015	Zi.B0116
Deusch Maria	4277-14016	Zi.B0113
Griehsler Ulrich	4277-14012	Zi.B0116
Haumer Claudia	4277-14018	Zi.B0113

Abteilung Zentrale Services & Benutzerbetreuung

Marksteiner Peter *(Leiter)*	4277-14055	Zi.B0111
Adam Achim	4277-14273	AAKH, Hof 1
Berndl Alexander	4277-14054	Zi.B0110
Berndl Christoph	4277-14064	Zi.C0102A
Birnbacher Eva	4277-14087	Zi.C0102B
Bociurko Michaela	4277-14072	Zi.B0110
Breyha Wolfgang	4277-14157	Zi.B0117
Dempf Stefan	4277-14151	AAKH/2HEG29
Ekker Heinz	4277-14278	AAKH, Hof 1
Englisch Holger	4277-14270	AAKH, Hof 1
Ertl Lukas	4277-14073	Zi.B0117
Fischl Michael	4277-14186	Univ.str. 11/5a
Führer Heinz	4277-14059	Zi.B0117
Giefing-Meisinger Eva	4277-14295	Zi.C0028
Gonter Gerhard	4277-14158	Zi.B0117
Grünauer Marcel	4277-14272	AAKH, Hof 1
Heimhilcher Markus	4277-14274	AAKH, Hof 1
Helmberger Florian	4277-14276	AAKH, Hof 1
Hofstetter Mark	4277-14275	AAKH, Hof 1
Hurka Franz	4277-14067	AAKH/2HEG31
Janousek Michael	4277-14294	Zi.C0028
Kaider Thomas	4277-14066	Zi.C0102A
Kaltenbrunner Franz	4277-14061	Zi.C0102
Köberl Dieter	4277-14058	AAKH/2HEG33
Kriszta Susanne	4277-14163	Zi.C0102
Kunitzky Walter	4277-14086	Zi.C0102
Lorenz Annabell	4277-14293	Zi.C0028
Lüthke Katharina	4277-14088	Zi.B0110
Mayer Andreas	4277-14271	AAKH, Hof 1
Mislik Heinrich	4277-14056	Zi.B0117
Muharemagic Mirza	4277-14082	Univ.str. 11/5a
Neuwirth Ernst	4277-14052	Zi.D0113
Papst Andreas	4277-14036	AAKH, Hof 1
Plansky Christian	4277-14065	Zi.B0120
Platzer-Stessl Eveline	4277-14071	Zi.C0102B
Riener Thomas	4277-14062	Zi.B0120
Riesing Martin	4277-14162	Zi.B0120
Rode Richard	4277-14291	Zi.C0028
Scherzer Horst	4277-14053	Zi.D0113
Schober Peter	4277-14155	Zi.B0117
Schöllhammer Gudrun	4277-14156	Zi.B0117
Schreiner Willibald	4277-14076	AAKH/2HEG31
Stadlmann Uwe	4277-14037	AAKH/2HEG33
Szabo August	4277-14085	AAKH/2HEG29
Wana Thomas	4277-14057	Zi.B0117
Weigl Bernhard	4277-14185	Univ.str. 11/5a
Winkler Gerhard	4277-14035	AAKH, Hof 1
Zens Birgit	4277-14292	Zi.C0028
Zoppoth Elisabeth	4277-14074	Zi.B0110

Abteilung Datennetze & Infrastruktur

Steinringer Hermann *(Leiter)*	4277-14021	Zi.B0108
Ankner Markus	4277-14077	Zi.B0107
Bauer Kurt	4277-14070	Zi.D0105
Bogad Manfred	4277-14029	Zi.B0104
Dworak Christine	4277-14077	Zi.B0107
Faustin Christian	4277-14092	Zi.B0107
Fischer Martin	4277-14034	Zi.D0107
Geicsnek Karin	4277-14245	Zi.D0114
Gruber Hildegard	4277-14079	Zi.D0105
Gruber Manfred	4277-14241	Zi.D0115
Haitzinger Robert	4277-14023	Zi.B0104
Hartwig Günther	4277-14243	Zi.D0117
Hennerbichler Wolfgang	4277-14031	Zi.D0105
Hof Markus	4277-14248	Zi.D0115
Kiermayr Ulrich	4277-14020	Zi.B0106
Kind Mario	4277-14101	Physik/Zi.3227
Michl Harald	4277-14078	Zi.D0105
Paar Günter	4277-14093	Zi.B0107
Panigl Christian	4277-14032	Zi.D0105
Parcalaboiu Paul	4277-14246	Zi.D0114
Perzi Michael	4277-14083	Zi.D0105
Regius Rene	4277-14242	Zi.D0117
Rosenwirth Thomas	4277-14025	Zi.B0104
Schaidl Christian	4277-14026	Zi.B0107
Schirmer Daniel	4277-14028	Zi.B0104
Schneider Monika	4277-14027	Zi.B0104
Szvasztics René	4277-14091	Zi.B0107

Talos Alexander	4277-14024	Zi.B0106
Wöber Wilfried	4277-14033	Zi.D0107
Zettl Friedrich	4277-14041	Zi.D0114

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

Drnek Jeanette	4277-14313
Engel Herbert	4277-14315
Erasmus Karl	4277-14311
Feigl Gabriele	4277-14317
Kammerer Jürgen	4277-14316
Krnjeta Danijel	4277-14312
Mayr Karl	4277-14314
Sylla-Widon Margaretha	4277-14318
Waba Theodor	4277-14312

Abteilung PC-Systeme & Fakultätsunterstützung

Marzluf Christian *(Leiter)*	4277-14120	Zi.D0111
Balazova Jana	4277-14286	Univ.str. 11/5a
Brabec Erich	4277-14075	Zi.B0105
Brugger Nikolaus	4277-14069	Zi.D0106
Cikan Edwin	4277-14142	Zi.D0109
Domschitz Eduard	4277-14133	Univ.str. 11/5a
Doppelhofer Johann	4277-14152	Zi.D0112
Egger Jörg	4277-14135	Zi.B0101
Filz Michael	4277-14134	Zi.D0108
Fuchs Alexander	4277-14288	Univ.str. 11/5a
Gaberscik Martin	4277-14287	Univ.str. 11/5a
Glaser Walter	4277-14145	VBC/Zi.6108
Hönigsperger Helmuth	4277-14114	AAKH/2HEG35
Jantscher Rainer	4277-14137	Zi.B0101
Just Stefan	4277-14281	Univ.str. 11/5a
Karlsreiter Peter	4277-14131	Zi.D0108
Ljesevic Nasret	4277-14146	Zi.B0101
Nierlich Birgit	4277-14127	Zi.D0110
Nunner Reinhard	4277-14147	Zi.B0101
Osmanovic Richard	4277-14132	AAKH/2HEG25
Paunzen Ernst	4277-14111	Zi.D0112
Pavelic Florian	4277-14284	Zi.D0106
Payer Markus	4277-14129	AAKH/2HEG25
Pechter Karl	4277-14068	AAKH/2HEG35
Pytlik Andreas	4277-14282	Univ.str. 11/5a
Römer Alfred	4277-14139	AAKH/2HEG25
Stampfer Dieter	4277-14063	Zi.B0105
Staudigl Ralph	4277-14224	Zi.D0106
Strieder Martin	4277-14285	Zi.D0109
Vogler Martin	4277-14113	UZAII/Zi.2Z306
Vrtala Aron	4277-14102	Zi.D0110
Wienerroither Peter	4277-14138	Zi.D0110

Abteilung Universitätsverwaltung

(1010 Wien, Universitätsstraße 11/2/5-7; Fax: 4277-9142)

Riedel-Taschner Harald *(Leiter)*	4277-14211	Zi.OG2-18
Anderlik Christopher	4277-14202	Zi.OG2-26
Aschauer Johann	4277-14213	Zi.OG2-13
Bitschnau Martin	4277-14203	Zi.OG2-27
Cella Michael-Alexander	4277-14252	Zi.OG2-13
Cutura Wolfgang	4277-14236	Zi.OG2-37
Dreiseitel Thomas	4277-14216	Zi.OG2-22
Eich Hartmut	4277-14237	Zi.OG2-38
Fink Birgit	4277-14228	Zi.OG2-10
Guttenbrunner Mark	4277-14235	Zi.OG2-37
Kauer Josef	4277-14210	Zi.OG2-22
Klünger Gerhard	4277-14219	Zi.OG2-22
Koller Markus	4277-14212	Zi.OG2-38
Kößlbacher Eva	4277-14214	Zi.OG2-28
Kübler Evelyn	4277-14207	Zi.OG2-10
Lackner Herbert	4277-14217	Zi.OG2-22
Linhart Leopold	4277-14221	Zi.OG2-13
Lohner Gertraud	4277-14222	Zi.OG2-14
Pauer-Faulmann Barbara	4277-14227	Zi.OG2-20
Pallik Stefan	4277-14255	Zi.OG2-13
Plattner Dieter	4277-14232	Zi.OG2-23
Polaschek Martin	4277-14200	Zi.OG2-21
Pröll Michaela	4277-14205	Zi.OG2-27
Redl Karin	4277-14223	Zi.OG2-10
Rosenauer Alexander	4277-14229	Zi.OG2-27
Schöller Robert	4277-14230	Zi.OG2-37
Stark Mario	4277-14239	Zi.OG2-37
Trifonoff Philipp	4277-14238	Zi.OG2-38
Url Clemens	4277-14220	Zi.OG2-37
Vinek Elisabeth	4277-14258	Zi.OG2-27
Wandler Alexander	4277-14215	Zi.OG2-15
Zalcmann Erich	4277-14226	Zi.OG2-15
Zeiner Andreas	4277-14208	Zi.OG2-38
Zeitlberger Martin	4277-14233	Zi.OG2-27

Mailadressen der ZID-MitarbeiterInnen

Die MitarbeiterInnen des Zentralen Informatikdienstes sind unter eMail-Adressen der Form

***vorname.nachname*@univie.ac.at**

erreichbar. Ausnahmen:
Lukas Ertl = `l.ertl@univie.ac.at`
Martin Fischer = `m.fischer@univie.ac.at`
Markus Koller = `markus.p.koller@univie.ac.at`
Andreas Mayer = `andy.mayer@univie.ac.at`

Umlaute bitte mit zwei Buchstaben schreiben (ö = oe).

AnsprechpartnerInnen

In grundsätzlichen Angelegenheiten wenden Sie sich bitte an den Direktor des Zentralen Informatikdienstes oder an die Abteilungsleiter (siehe *Personal- & Telefonverzeichnis*, Seite 58).

Helpdesk

Als erste Anlaufstelle bei EDV-Problemen und technischen Schwierigkeiten,

für **Vermittlung zu AnsprechpartnerInnen** bei speziellen Problemen,

bei **Störungen** im Datennetz und im Telefonsystem der Universität Wien oder an einem Rechnersystem des ZID,

für Vergabe von **Benutzungsberechtigungen** (UserIDs) für die Rechnersysteme und das Backup-Service,

für alle Anliegen hinsichtlich Benutzungsberechtigungen – insbesondere Änderung vergessener **Passwörter**,

für Vermittlung von externen Technikern zur **Unterstützung bei Software-Problemen** (kostenpflichtig!),

bei Problemen mit dem **Internetzugang von daheim** (*uniADSL, StudentConnect, xDSL Uni*, Wählleitungszugänge der Uni Wien),

für **Kursanmeldungen**,

für Ausgabe und Entgegennahme aller **Formulare** des ZID (Formularspender bzw. Briefkasten vor dem Helpdesk),

für **Verkauf von Handbüchern, Netzwerkkarten und Netzwerkkabeln**:

eMail: **helpdesk.zid@univie.ac.at**
Telefon: **4277-14060**
Öffnungszeiten: **Mo – Fr 9:00 – 18:00 Uhr**
NIG (1010 Wien, Universitätsstraße 7), Stg. II, 1. Stock, links

bei technischen Fragen zum Thema eLearning (www.univie.ac.at/ZID/elearning/):

elearning.zid@univie.ac.at
Telefon: 4277-14290

bei Fragen zum Telefonsystem der Uni Wien:

telefon.zid@univie.ac.at
handy.zid@univie.ac.at

bei EDV-Problemen im Bereich der Universitätsverwaltung:

uvpc.support.zid@univie.ac.at

bei Fragen zu bzw. Problemen mit i3v:

support.univis@univie.ac.at

bei Fragen zum Linux-Cluster Schrödinger III:

schroedinger@univie.ac.at
Marksteiner Peter 4277-14055

für Netzwerkplanung & Gebäudeverkabelung:

Steinringer Hermann 4277-14021

bei Fragen zum Datennetz der Uni Wien:

netzwerk.zid@univie.ac.at
Telefon: 4277-14042

bei Fragen zur Fakultätsunterstützung:

fu.zid@univie.ac.at
Telefon: 4277-14140

bei Fragen zur Standardsoftware:

software.zid@univie.ac.at
Wienerroither Peter 4277-14138

für Öffentlichkeitsarbeit:

Comment-Redaktion:	Bociurko Michaela	4277-14072
	Lüthke Katharina	4277-14088
	Zoppoth Elisabeth	4277-14074
Webredaktion:	Berndl Alexander	4277-14054

Wählleitungszugänge

Unet- und Mailbox-Wählleitungszugang

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

Uni-interner Wählleitungszugang

14333	von einer Uni-Nebenstelle (Tel. 4277)
88-14333	von einer AKH-Nebenstelle (Tel. 40400)
90-14333	vom A1 NetWork-Diensthandy (€ 0,16/min.)

Österreichische Post AG Info.Mail Entgelt bezahlt
Bei Unzustellbarkeit bitte retournieren an:
Zentraler Informatikdienst der Universität Wien, 1010 Wien, Universitätsstraße 7

COMMENT-ABO

Der *Comment* erscheint zwei- bis dreimal im Jahr und ist online im HTML- oder PDF-Format verfügbar. MitarbeiterInnen und Studierenden der Uni Wien wird die gedruckte Ausgabe kostenlos zugeschickt; alle anderen interessierten LeserInnen erhalten auf Wunsch eine Verständigung per eMail, sobald eine aktuelle Ausgabe vorliegt (**e-Abo**), und können diese dann online abrufen (**`www.univie.ac.at/comment/`**). Ein Teil der gedruckten Ausgabe liegt am Helpdesk des Zentralen Informatikdienstes bzw. vor den PC-Räumen im NIG (1010 Wien, Universitätsstraße 7, 1. Stock) zur freien Entnahme auf.

- **e-Abo:** Unter `www.univie.ac.at/comment/abo.html` finden Sie einen Link, unter dem Sie Ihr e-Abo an- bzw. abmelden können.

- **Abo für Universitätsangehörige:** MitarbeiterInnen und Studierende der Universität Wien können unter `www.univie.ac.at/comment/abo.html` (nach Login mit Mailbox- bzw. Unet-UserID) die Druckausgabe des *Comment* anfordern, abbestellen oder ihre geänderten Daten eingeben.

Wenn Sie keine Mailbox- bzw. Unet-UserID besitzen und Ihr bestehendes *Comment*-Abo abmelden wollen oder eine Datenänderung bekanntgeben möchten (geben Sie dabei bitte auch Ihre bisherigen Daten an!), kontaktieren Sie uns per eMail an **`comment.zid@univie.ac.at`**. Bitte richten Sie Fragen zum Abo-System ebenfalls an diese Adresse.