Mitteilungen des Zentralen Informatikdienstes der Universität Wien 03/1

vienna
university
computer
center

# Comment

*März 2003*

## IPv6

## Forever Spam!?

## Design in InDesign

## Cascading Style Sheets

## Der Spam-Filter der Uni Wien

**Postgebühr bar bezahlt** – Bei Unzustellbarkeit bitte retournieren an:
Zentraler Informatikdienst der Uni Wien, 1010 Wien, Universitätsstraße 7

## Impressum / Offenlegung gemäß § 25 Mediengesetz:


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

*Gedruckt auf chlorfrei gebleichtem Papier – Auflage 5500 Stk.*

# Editorial

Liebe Leserin, lieber Leser!

Zunächst ein Hinweis in eigener Sache: Durch die Abschaltung der VM-Rechenanlage (siehe Seite 15) mußte auch die *Comment*-Abonnentenverwaltung migriert und überarbeitet werden. Dabei wurde entschieden, daß es ab März 2003 nur mehr für Mitarbeiter/innen und Studierende der Universität Wien möglich sein wird, die gedruckte Ausgabe des *Comment* zu abonnieren. Alle anderen interessierten Leser/innen können ein sogenanntes *e-Abo* beziehen, d.h. sie werden per eMail informiert, wenn eine neue *Comment*-Ausgabe erschienen ist, und können diese dann online abrufen (in einer HTML- und einer PDF-Version, siehe `http://www.univie.ac.at/comment/`). Selbstverständlich wird wie bisher der komplette Inhalt jeder Ausgabe im WWW zur Verfügung stehen und ein Teil der gedruckten Auflage im Service- und Beratungszentrum des ZID bzw. vor den PC-Räumen im NIG zur freien Entnahme aufgelegt. Wir hoffen, mit dieser Regelung einen Weg gefunden zu haben, einerseits Kosten zu sparen und andererseits unsere Zeitschrift für alle Interessenten einfach zugänglich zu machen. Einzelheiten zur neuen Abo-Verwaltung finden Sie auf der hinteren Umschlagseite dieser Ausgabe bzw. unter `http://www.univie.ac.at/comment/abo.html`. Bei Fragen wenden Sie sich bitte an die eMail-Adresse `comment.zid@univie.ac.at`.

Doch nun zur vorliegenden Ausgabe: Abgesehen davon, daß Sie diesmal ein „Schwergewicht" in Händen halten, ist auch der Inhalt äußerst gewichtig – vor allem für alle jene, die wie die *Comment*-Redaktion unter der stetig wachsenden Spam-Flut leiden. Nachdem diese mittlerweile für viele Uni-Angehörige eine ernstzunehmende Behinderung bei ihrer Arbeit darstellt, hat der ZID nun einen Spam-Filter für die zentralen Mailserver der Uni Wien entwickelt. Falls Sie sich fragen, warum dies nicht schon viel früher geschehen ist, sollten Sie die Artikel *Forever Spam!?* (Seite 2) und *Spammer vs. Blacklists: Ein ewiges Wettrüsten* (Seite 37) lesen: Darin wird ausführlich beschrieben, warum es keine einfache Lösung für dieses lästige Problem gibt. Wenn Sie lediglich wissen möchten, wie der neue Spam-Filter arbeitet, können Sie dies im Beitrag *101 – Der Spam-Filter der Uni Wien* (Seite 40) in Erfahrung bringen. Und falls Sie die Sache lieber selbst in die Hand nehmen möchten, finden Sie im Artikel *Spam-Bekämpfung auf eigene Faust* (Seite 45) eine kurze Beschreibung einiger Antispam-Programme für PCs.

Die anderen „Schmankerln" dieser Ausgabe müssen Sie – Platznot im Editorial – selbst entdecken. Viel Vergnügen dabei wünscht

die *Comment*-Redaktion

# Inhalt

## Aktuelles


**2** Forever Spam!?
Warum Spam nicht schon längst abgeschafft wurde

**13** Schrödinger II

**14** Billig, aber gut: Handbücher des RRZN

**14** Personalnachrichten

**15** Notizen

**16** Neuer Newsserver – auch für die Uni Wien

**16** Internetzugang von daheim: Änderungen & Neues


## PCs & Workstations


**17** Vom Prototyp zur Serienreife –
Seriendruck mit Word XP

**22** Desktops in der Ferne: Windows-Terminalservices

**25** Design in InDesign –
Ein Layoutprogramm unter der Lupe

**27** Go! Create a Webgallery!

**29** Neue Standardsoftware


## Netzwerk- & Infodienste


**30** HTML mit Stil – Teil II: Cascading Style Sheets

**35** IPv6 – Das Internetprotokoll der nächsten Generation

**37** Spammer vs. Blacklists: Ein ewiges Wettrüsten

**40** 101 – Der Spam-Filter der Uni Wien

**45** Spam-Bekämpfung auf eigene Faust


## Anhang


**47** Kurse bis Juli 2003

**53** Informationsveranstaltungen

**54** Personal- & Telefonverzeichnis

**55** Öffnungszeiten

**56** Ansprechpartner

**56** Wählleitungszugänge & eMail-Adressen

# FOREVER SPAM!?

## Warum Spam nicht schon längst abgeschafft wurde

*„Wieso bekomme ich so viel Werbung für Porno-Seiten?“ – „Kann man denn nichts gegen die vielen Junkmails unternehmen?“ – „Wieso blockiert ihr den Spam nicht einfach?“*

Die Reaktionen aus der Benutzergemeinde auf die ständig wachsende Flut unerwünschter elektronischer Post reichen vom verzweifelten Stoßseufzer bis hin zu regelrechten Vorwürfen. In dieser Angelegenheit ist guter Rat allerdings nicht einmal teuer, sondern fast überhaupt nicht zu erhalten. Der folgende Artikel gibt einen Überblick über die Spam-Problematik sowie über die landläufig angewendeten rechtlichen und technischen Mittel und die daraus resultierenden Probleme, wobei ausschließlich auf eMail-Spam eingegangen wird. Die vom Zentralen Informatikdienst eingesetzten Gegenmittel sind auf Seite 40 beschrieben.

## Was ist Spam?

Mit dem Begriff Spam bezeichnet man unerwünschte, massenweise verschickte eMail-Nachrichten und Newsgruppen-Artikel. Im Detail wird unterschieden zwischen

- UBE (*unsolicited bulk email*): nicht ausdrücklich bestellte, in großen Mengen versandte eMail;
- UCE (*unsolicited commercial email*): nicht ausdrücklich bestellte, kommerzielle Werbung per eMail;
- ECP (*excessive crosspost*): in unangebracht vielen Newsgruppen veröffentlichter („geposteter“) Artikel;
- EMP (e*xcessive multipost*): in unangebrachter Anzahl gepostete, gleichlautende Artikel in einer oder mehreren Newsgruppen.

Leider lassen sich aus dieser Klassifizierung keine allgemeingültigen Kriterien ableiten, anhand derer Spam eindeutig identifiziert werden könnte. Der Ansatz, Spam als Massenmail zu charakterisieren, hat den Makel, daß er nicht auf der Wahrnehmung der Betroffenen basiert: Der Empfänger erhält schlicht und einfach Mail, die ihn nicht interessiert; daß auch tausende andere mit denselben Nachrichten bombardiert werden, tut für ihn nichts zur Sache. Aus Empfängersicht – und diese muß bei allen Betrachtungen über Gegenmaßnahmen ein zentraler Gesichtspunkt sein – ist also „unerwünscht“ das typische Merkmal von Spam. Dabei handelt es sich allerdings um ein subjektives, der elektronischen Datenverarbeitung nicht zugängliches Kriterium. Aus diesem Grund ist auch der Versuch, Spam über seinen Inhalt zu definieren, zum Scheitern verurteilt: Nachrichten, die für manche Empfänger unerwünscht sind, können für andere durchaus nützlich und willkommen sein. Vielfach werden etwa Werbematerial, Produktinformationen oder Preislisten völlig bewußt und aus freien Stücken bei Geschäftspartnern angefordert und sollen auf Wunsch des Empfängers regelmäßig übermittelt werden.

Das ist auch schon die Achillesferse aller Antispam-Aktivitäten: Selbst bei Einsatz der höchstentwickelten künstlichen oder gar menschlichen Intelligenz (und wer will schon, daß seine eMail vor der Zustellung probegelesen wird?) ist es nicht möglich, zweifelsfrei zu beurteilen, ob eine Nachricht erwünscht ist oder nicht. Deshalb gibt es auch bis heute keinen Konsens über eine gleichzeitig präzise und sinnvolle Definition von Spam: Letztendlich kann darüber nur der Empfänger entscheiden.

## Welchen Spam gibt es, und woher kommt er?

In der Mehrzahl der Fälle handelt es sich bei Spam um kommerzielle Werbung. Davon entfällt der Löwenanteil auf Werbung für Sex-Seiten bzw. Hilfsmittel im einschlägigen Dunstkreis (*Get Viagra now*, *Enlarge your Penis with HGH*) – häufig mit eingebetteten Bildern, die nicht nur Konvulsionen in der Magengegend des Betrachters induzieren,

SPAM ist außerdem ein Produkt und eingetragenes Markenzeichen der US-Firma Hormel, steht in diesem Zusammenhang aber für *spiced pork and ham* (eine Fleischkonserve) und hat mit Spam im Sinne von unerwünschter eMail nichts zu tun.


Über die Etymologie des Begriffs Spam existieren unterschiedliche Meinungen. Eine weitverbreitete Version lautet, daß zu der Zeit, als Spam-Mail zu einem ernstzunehmenden Problem wurde, ein Sketch von Monty Python populär war, in dem das Wort *Spam* innerhalb weniger Minuten unzählige Male wiederholt wird – die Assoziation mit Massenmail lag also nahe. Eine andere Interpretation (die auf der offiziellen Webseite von SPAM nicht aufgegriffen wird) geht davon aus, daß es sich sowohl bei der Dosennahrung als auch bei Spam-Mail um etwas Undefinierbares und Unerwünschtes handelt, das aber allgegenwärtig ist: *„Ich weiß zwar nicht, was es ist, aber ich erkenne es, wenn ich es sehe.“*

sondern auch eine besonders schiefe Optik erzeugen, wenn just in diesem Moment die Chefin/der Chef oder die Freundin/der Freund das Zimmer betritt. Eine weitere wichtige Kategorie wird MMF (*Make Money Fast*) genannt. Hierbei handelt es sich in der Regel um Pyramidenspiele, die in vielen Ländern überdies verboten sind. Zynischerweise werden sogar die Dienste von Spammern bzw. CDs mit vielen Millionen Adressen von angeblich werbehungrigen Konsumenten per eMail feilgeboten.

Die meisten Spam-Nachrichten haben eine handfeste Gewinnabsicht als Motiv. Die einfache Rechnung *Wenn ich mit einer Investition von zehn Euro 10 000 000 eMail-Nachrichten verschicke und nur an jedem zehntausendsten Empfänger wenigstens einen Euro verdiene, habe ich mein Kapital bereits verhundertfacht* geht offensichtlich auf. Augenfällig wird das beim sogenannten *Nigeria*-Spam (der übrigens auch als Briefpost an Unternehmer in der ganzen Welt verschickt wird): Hier werden in betrügerischer Weise von angeblich hochstehenden, regierungsnahen Personen Partner für angeblich lukrative Geschäfte in Millionenhöhe gesucht. Allem Anschein nach gibt es genug Dumme, die darauf hereinfallen – Berichten zufolge wird in den Flugzeugen nach Nigeria sogar schon per Durchsage vor der Betrugsmasche gewarnt, und es sollen auch immer wieder Personen mit Anzug und Köfferchen daraufhin zaghaft fragen, ob sie im Flugzeug sitzenbleiben und gleich zurückfliegen dürfen. Jedenfalls warnt das Department of State der USA bereits bei seinen Reisetips (`http://travel.state.gov/nigeria.html`) vor solchen Geschäften: *Such scams may involve U.S. citizens in illegal activity, resulting in arrest, extortion or bodily harm.*

Auch mit Mehrwertdiensten – erkennbar an Telefonnummern mit der Vorwahl 09xxx[1)] (oder 0190 in Deutschland), bei denen teilweise mehrere Euro pro Minute verrechnet und über die Telefonrechnung eingehoben werden – läßt sich trefflich Geld verdienen. Dazu wird im Spam schnelleres Surfen oder der Gratis-Zugriff auf pornografische Inhalte und/oder Raubkopien nach Installation eines Zugangsprogramms versprochen. Diese Programme werden als *Dialer* bezeichnet: Einmal aktiviert, ändern sie die Wählleitungskonfiguration des PCs derart, daß die Einwahl nicht mehr über den normalen Provider, sondern über eine Mehrwertnummer erfolgt – bis zum teuren Erwachen bei der nächsten Telefonrechnung. Es gibt nichts, was es nicht gibt: Sogar mehr oder weniger schlüsselfertige Pakete zur Realisierung dieser zweifelhaften Geschäftsidee werden feilgeboten.[2)]

Wer die Spammer sind, ist naturgemäß nur teilweise bekannt. Eine der schillerndsten Figuren der Branche ist Alan Ralsky, der den Journalisten Mike Wendland sogar zum Interview eingeladen hat – in seine neue „bescheidene Hütte“, von der aus er über seine eigene T1-Anbindung seine Spam-Server in aller Welt steuert, die täglich mehrere Millionen Spam-Nachrichten versenden. Wendlands Kolumne ist unter `http://www.freep.com/money/tech/mwend22_20021122.htm` online verfügbar und gibt einen interessanten Einblick in dieses offenbar sehr einträgliche Business. Einen guten Überblick bietet auch das *Register Of Known Spam Operations* (ROKSO) unter `http://spamhaus.org/`.

Selbstverständlich ist nicht jeder Spam-Absender ein skrupelloser Verbrecher – es gibt tatsächlich unerfahrene Geschäftsleute, die den Versprechungen glauben, die Adressen von Zillionen kauffreudigen potentiellen Kunden, die sich über jede Art von Werbung freuen, auf einer CD kaufen zu können. Auch völlig unkommerzielle Sendungsbewußte, die die Kunde vom nahenden Weltuntergang oder der nahenden Erlösung einem größeren Publikum nahebringen zu müssen vermeinen, werden mitunter zu Spammern. Und wer weiß, vielleicht wird auch ein stadtbekannter Wiener Zettelditcher einmal seine Poesie nicht nur zum Pflücken, per Telefon und Fax, sondern auch per eMail verbreiten...

Fallweise werden auch die diversen *Wichtig! Unbedingt an möglichst viele Leute weiterleiten!*-Kettenbriefe (z.B. Aufrufe zur Knochenmarkspende, Warnungen vor einem neuen Übervirus, *Taliban Women*) zu Spam gezählt. Allerdings zeichnen sich diese Kettenbriefe, obwohl sie massenhaft und unverlangt verschickt werden, durch das fehlende Unrechtsbewußtsein des Absenders aus: Für nicht besonders mißtrauische Menschen ist kaum ersichtlich, daß diese Nachrichten (die teilweise seit vielen Jahren im Netz kursieren) inhaltlich groben Unfug darstellen. Infolgedessen sind die Absender dieser Kettenbriefe ehrlich davon überzeugt, der Welt etwas Gutes zu tun, wenn sie eine vermeintlich wichtige Nachricht an ihr gesamtes Adreßbuch weiterleiten.

Eine prominente Sparte von Massenmail fehlt noch in diesem Überblick – Computerviren, genauer: Würmer. Daß sich diese selbsttätig zu verbreiten versuchen, indem sie sich ohne Wissen des Absenders in großer Zahl per eMail verteilen, ist spätestens seit *Melissa* kein Geheimnis mehr. Um den Empfänger dazu zu bringen, das infizierte Attachment auszuführen, müssen sich Mailwürmer ähnlicher Verlockungen bedienen wie Spammer: Beispielsweise versprach *VBSWG* ein Bild von Anna Kournikova, und die von *Yaha* versandten Nachrichten waren regelrechte Spam-Emulationen (*This e-Mail is never sent unsolicited. If you need to unsubscribe, follow the instructions at the bottom of the message*). Einige der Spam-Beschwerden, die wir erhalten, sind auch folgerichtig auf einen Mailwurm zurückzuführen. Glücklicherweise ist es jedoch – sowohl vom Aufwand als auch von den erforderlichen Fachkenntnissen – wesentlich schwieriger, Computerviren zu programmieren, als Spam zu versenden. Deshalb können Virenscanner gut mit der Entwicklung schritthalten, und die Virenproblematik im Mailverkehr der Uni Wien hat sich mit der Einführung der Virenscanner (siehe *Comment 01/1*, Seite 28 bzw. `http://www.univie.ac.at/comment/01-1/011_28.html`) fast vollständig gelöst.

1) Der *Nummerierungsplan für öffentliches Telefonnetz und ISDN gemäß ITU-T Empfehlung E.165 entsprechend BGBl. II Nr. 416/1977* ist als PDF-Datei unter `http://www.bmvit.gv.at/sixcms_upload/media/74/np_e164.pdf` verfügbar.

2) siehe `http://www.0190service.de/`

## Woher haben die meine Adresse?

Zur Frage, wie die Spammer zu den eMail-Adressen der Menschen gelangen, die von ihnen beglückt werden, gibt es mehrere Antworten:

- Aus Artikeln, die in Newsgruppen und öffentlich zugänglichen Mailinglisten gepostet wurden.
- Aus Webseiten, die Kontaktadressen oder überhaupt ganze eMail-Verzeichnisse (z.B. des gesamten Instituts) enthalten. Insbesondere Mailadressen, die mit Suchmaschinen wie Google zu finden sind, stehen auch Spammern zur Verfügung.
- Eintragung der eMail-Adresse bei Online-Gewinnspielen, Freemailern usw.: Es gibt immer wieder Berichte, wonach Spam an Adressen geschickt worden sein soll, die nur bei solchen Anlässen verwendet wurden.
- Auch Verzeichnisdienste mit LDAP, Whois-Datenbanken usw. gelten als Adreßquellen für Spammer.
- Es ist zwar bisher kein derartiger Fall dokumentiert, aber sicher nur eine Frage der Zeit, bis auch eMail-Würmer programmiert werden, die sich nicht nur verbreiten, sondern auch gleich eine Kopie des Adreßbuchs des befallenen Rechners an Spam-Firmen versenden.
- HTML-Nachrichten können durch Einbettung von Framesets und Bildern (*Webbugs*) den Mailklienten veranlassen, zur Darstellung einer Nachricht auf den Webserver des Spammers zuzugreifen. Zunehmend werden dafür numerierte URLs verwendet, anhand derer der Spammer feststellen kann, wer seinen Spam im Mailklienten geöffnet hat. Klarerweise ist die Infomation, daß eine bestimmte Mailadresse tatsächlich aktiv ist, für den Spammer bares Geld wert.

Richtiges Spammen ist aber keineswegs nur Experten wie Ralsky & Co vorbehalten – auch Endanwender können, beispielsweise von Spam-Firmen, eigens dafür entwickelte Hilfsprogramme erwerben. Im Segment der Adressensammler glänzt der *Advanced Email Extractor* (`http://www.mailutilities.com/aee/`) mit automatischem Zugriff auf über 330 Suchmaschinen, einem LDAP-Plugin und vielem mehr. Vom *Atomic Harvester* (`http://www.desktopserver.com/ah.html`) gibt es sogar eine Demo-Version zum Download. Natürlich darf spekuliert werden, ob diese Programme die gefundenen Adressen auch an ihre Hersteller weiterleiten, um in einem Aufwaschen auch deren Datenbank zu verbessern...

## Das gehört doch verboten!

Spam ist in vielen Ländern – auch in Österreich – ohnehin verboten. § 101 des österreichischen Telekommunikationsgesetzes lautet:

> *(...) Die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken bedarf der vorherigen – jederzeit widerruflichen – Zustimmung des Empfängers.*

In Europa verbieten außerdem noch Dänemark, Deutschland, Finnland, Griechenland, Italien und Norwegen das Versenden unverlangter kommerzieller eMail (UCE).

In manchen Ländern ist Spam erlaubt, bis der Empfänger widerspricht. Dieses sogenannte *Opt-Out*-Verfahren zeugt von einem besonderen Realitätsbezug der entsprechenden Gesetzgeber: Wie soll man jemandem, von dem man im vorhinein nichts weiß und der sich meist im nachhinein kaum finden läßt (mehr dazu später), die Zusendung von Werbung verbieten? Zudem geht es nicht um einen oder zehn Absender, sondern um tausende. Diese Art der Regelung ist daher völlig wirkungslos.

In einigen Ländern wird noch geprüft und beraten, allerdings gibt die EU-Richtlinie *2002/58/EC* vom 31. Juli 2002 Anlaß zur Hoffnung:

> *Artikel 13*
> *Unerbetene Nachrichten*
> *1. Die Verwendung von automatischen Anrufsystemen ohne menschlichen Eingriff (automatische Anrufmaschinen), Faxgeräten oder elektronischer Post für die Zwecke der Direktwerbung darf nur bei vorheriger Einwilligung der Teilnehmer gestattet werden.*

Zur Umsetzung dieser Richtlinie haben die Mitgliedstaaten jedoch bis 31. Oktober 2003 Zeit. Einen Überblick über die derzeitige Rechtslage in den einzelnen europäischen Staaten findet man im WWW unter `http://www.euro.cauce.org/en/lchaos.html`.

In den USA gibt es keine einheitliche Regelung; allerdings haben zahlreiche Bundesstaaten Maßnahmen ergriffen (siehe `http://www.spamlaws.com/state/summary.html`):

- In Kalifornien muß UCE Instruktionen für das Opt-Out sowie – unter gewissen Voraussetzungen – die Kennzeichnung *ADV:* oder *ADV:ADLT* im Subject enthalten.
  *(g) In the case of e-mail that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, the subject line of each and every message shall include „ADV:" as the first four characters. If these messages contain information that consists of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit, that may only be viewed, purchased, rented, leased, or held in possession by an individual 18 years of age and older, the subject line of each and every message shall include „ADV:ADLT" as the first eight characters.*
- In Florida gibt es keine speziellen Bestimmungen über Spam; Anwälte, die durch unverlangte Mail werben, müssen jedoch *legal advertisement* ins Subject schreiben.

- Louisianas Gesetzgeber waren besonders kreativ: Dort ist es verboten, unverlangte kommerzielle Mail an mehr als 1000 Empfänger zu senden, wenn die Nachricht gefälschte Routing-Informationen (`Received:`-Header) enthält oder der Versand unter Verstoß gegen die Benutzungsbedingungen des jeweiligen Providers erfolgt (Strafrahmen: 5000 USD).

- In Washington darf man kommerzielle eMail versenden, sofern sie nicht den Domainnamen Dritter ohne Genehmigung verwendet, gefälschte Routing-Informationen enthält oder ein falsches oder mißverständliches Subject aufweist.

In Japan besteht eine Regelung, derzufolge eMail-Werbung als solche deklariert werden sowie Opt-Out-Instruktionen enthalten muß.

Fazit: Nicht nur in Bananenrepubliken ist Spammen erlaubt oder höchstens ein bisserl verboten.

## Warum unternimmt denn keiner was?

Wir sind gewohnt, daß Fehlverhalten, das der Gesellschaft schadet und gegen die guten Sitten verstößt, geahndet wird, und ärgern uns, wenn der Bösewicht ungestraft davonkommt. Wieso also legt niemand den Spammern das Handwerk?

Einer der Gründe wurde oben beschrieben: Um einen Spam-Versender mit juristischen Mitteln belangen zu können, muß sein Tun zuerst einmal verboten sein. Gerade im Internet schlägt aber die Globalisierung zu: Auch wenn wir noch so heftig mit unserem § 101 TKG wedeln, wird das den Absender in China nicht kümmern (lediglich in der EU gilt das Prinzip, daß das Recht des Empfängerlandes anzuwenden ist). Auch der günstige Fall, daß Spam im Land des Absenders ebenfalls verboten ist, bedeutet noch lange nicht, daß mit vertretbarem Aufwand gegen diesen vorgegangen werden kann: Der Staatsanwalt (oder welche Behörde auch immer zuständig sein mag) eines anderen Landes wird sich von unsereinem kaum dazu zwingen lassen, aktiv zu werden. Aus dem Spam-Verbot ist ohnehin kein subjektives Recht des Empfängers auf Bestrafung des Täters abzuleiten; daher ist es auch nicht möglich, selbst ein derartiges Verfahren zu betreiben. Dasselbe gilt, falls der Spam-Versender gegen die Benutzungsbedingungen seines Providers verstoßen hat: Dem Empfänger entstehen daraus keinerlei Rechte – er ist ja nicht Vertragspartner.

Wie sieht es nun im eigenen Land aus? Es herrscht allgemein Einigkeit darüber, daß Spam aus Österreich außergewöhnlich selten anzutreffen ist. In einschlägigen Newsgruppen wird jedoch immer wieder berichtet, daß die für die Spam-Problematik zuständige Behörde, das Fernmeldebüro, keine oder kaum erkennbare Tätigkeit entfaltet. Die Frage, ob § 101 TKG in Österreich nicht ebenso totes Recht ist wie das Hupverbot, bleibt mangels veröffentlichter Statistiken leider offen.

Neben dem (Verwaltungs-)Strafrecht gibt es aber natürlich noch das Zivilrecht:

- Eine Variante ist, die *Unterlassung* weiterer Zusendungen zu erstreiten. Das bedeutet aber für das Spam-Opfer einen immensen Aufwand und ein nicht unbeträchtliches finanzielles Prozeßrisiko. Diesem steht selbst im Erfolgsfall ein relativ geringer Nutzen gegenüber, da man vom selben Absender (zumindest erkenn- und nachweisbar) ohnehin nur im Ausnahmefall mehrmals Spam bekommt. Ein generalpräventiver Effekt – in dem Sinn, daß der Spammer oder gar andere Spammer von weiteren derartigen Aktivitäten abgeschreckt würden – folgt daraus leider nicht.

- Anders sieht die Sache aus, wenn ein Konkurrent Spam versendet: Hier kann man mit der Keule des *Unlauteren Wettbewerbs* vorgehen. Da vermutlich nicht allzu viele *Comment*-Leser/innen auf diese Weise gegen die zahlreichen Porno- und Viagra-Spams aktiv werden wollen, wird dieser Aspekt hier nicht näher beleuchtet.

- Auch Klagen auf *Schadenersatz* sind prinzipiell möglich und bereits erfolgreich praktiziert worden. Wie bei der Unterlassungsklage gilt auch hier, daß das Prozeßrisiko einem nur geringen Schadenersatz-Betrag gegenübersteht. Große Firmen/Institutionen, die vom selben Absender eine große Menge Spam erhalten haben, könnten zwar den entstandenen Aufwand für Serverbelastung und eventuell Wartung sowie die entgangene Arbeitszeit in Rechnung stellen. Gerade in diesen Fällen wird eine Verfolgung aber in der Regel ausbleiben: Die Rechtsabteilungen großer Organisationen haben oft weder die Kapazität noch den sportlichen Ehrgeiz zur Spam-Bekämpfung.

Im Zusammenhang mit dem Internet – der angeblichen einzigen funktionierenden Anarchie – wird gern das Schlagwort „Selbstregulierung“ ins Treffen geführt. Internet-Provider können tatsächlich einiges dagegen unternehmen, daß ihre Kunden Spam versenden. Zwar gibt es genügend Provider, die keinerlei Bedenken gegen gut zahlende Spammer in ihrem Kundenkreis haben; der Großteil verbietet Fehlverhalten aber mehr oder weniger ausdrücklich (z.B. durch Verweis auf die Netiquette) in einem entsprechenden Passus der Allgemeinen Geschäftsbedingungen. Leider bleibt ein Verstoß dagegen oft folgenlos: Die attraktive Möglichkeit, Konventionalstrafen vorzusehen (wie z.B. bei `http://trafficspace.de/agb.htm`), wird kaum wahrgenommen – die meisten Provider behalten sich lediglich das Recht vor, im Falle eines Mißbrauchs den Zugang des Bösewichts zu sperren. Allerdings ist in einschlägigen Mailinglisten immer wieder zu lesen, daß Provider angesichts einer drohenden Schadenersatzklage des Zugangsinhabers davor zurückschrecken, die angekündigten Konsequenzen in die Realität umzusetzen.

# Crashkurs: Wie funktioniert eMail?

Was passiert, nachdem Sie in Ihrem Mailklienten auf *Senden* gedrückt haben, ist im Prinzip sehr einfach und sei hier an einem Beispiel illustriert, in dem Stefan Sender von seinem PC mit der Adresse PCSTEFAN.IHW.UNIVIE.AC.AT eine Nachricht an seinen Freund Emil Empfänger schickt.[3)]

### 1. Vorbereitung der Nachricht

Der Mailklient erzeugt eine einfache Textdatei (oder eine äquivalente Datenstruktur in seinem Speicher), die aus zwei lediglich durch eine Leerzeile voneinander getrennten Teilen besteht:

- Der Briefkopf, *Header* genannt:

```
From: Stefan.Sender@kubim.univie.ac.at
To: Emil.Empfaenger@aldebam.sal.at
Date: Mon, 24 Feb 2003 09:55:27 +0100
Subject: Hallo, wie geht's?
```

- Der Text, *Body* genannt:[4)]

```
Servus Emil,
hast Du Lust, mit uns am nächsten Samstag
ins Kino zu gehen?
Herzlichst, Stefan
```

### 2. Ab in den Briefkasten

Die vorbereitete Nachricht wird in ein adressiertes Kuvert gesteckt und bei einem Mailserver eingeworfen. Dazu baut der Mailklient mit dem als *Outgoing SMTP Server* konfigurierten Rechner eine Verbindung auf, über die etwa folgender Dialog[5)] abläuft (> Mailserver spricht; < Mailklient spricht):

```
[01] > 220 mailbox.univie.ac.at ESMTP Service ready
[02] < HELO pcstefan.ihw.univie.ac.at
[03] > 250 mailbox.univie.ac.at Hello pcstefan.ihw.univie.ac.at [131.130.2.235]
[04] < MAIL FROM: <Stefan.Sender@kubim.univie.ac.at>
[05] > 250 2.1.0 <Stefan.Sender@kubim.univie.ac.at>... Sender ok
[06] < RCPT TO: <Emil.Empfaenger@aldebam.sal.at>
[07] > 250 2.1.5 <Emil.Empfaenger@aldebam.sal.at>... Recipient ok
[08] < DATA
[09] > 354 Enter mail, end with "." on a line by itself
[10] < From: Stefan.Sender@kubim.univie.ac.at
[11] < To: Emil.Empfaenger@aldebam.sal.at
[12] < Date: Mon, 24 Feb 2003 09:55:27 +0100
[13] < Subject: Hallo, wie geht's?
[14] <
[15] < Servus Emil,
[16] < hast Du Lust, mit uns am nächsten Samstag ins Kino zu gehen?
[17] < Herzlichst, Stefan
[18] < .
[19] > 250 2.0.0 f9JCrv9170694 Message accepted for delivery
[20] < QUIT
[21] > 221 2.0.0 mailbox.univie.ac.at closing connection
```

Die Absender- und Empfängerangaben in `[04]` und `[06]` bilden die sogenannte *Envelope* – das Kuvert. Der Inhalt des `RCPT TO:`-Befehls `[06]` bestimmt, wohin die Nachricht geschickt wird; bei mehreren `RCPT TO:`-Befehlen geht sie eben an mehrere Empfänger. Der `MAIL FROM:`-Befehl `[04]` legt fest, wohin Fehlermeldungen im Fall der Unzustellbarkeit (z.B. Adressat übersiedelt/unbekannt) gesendet werden. Der eigentliche Brief, von `[10]` bis `[17]`, wird vom Briefträger nicht weiter beachtet oder gar gelesen. Die übrigen Zeilen entsprechen dem Quietschen und Klappern der Briefkastentür.

### 3. Weiterleitung zum nächsten Postamt

Bei eMail bilden Briefkasten, Briefträger und Postamt eine Einheit, den Mailserver. Dieser vermerkt – stark abweichend von der Briefpost-Analogie – den Eingang der Nachricht am Anfang des Briefkopfs (also nicht auf der Envelope, sondern im Brief vor `[10]`). Gibt es bereits einen oder mehrere solche Vermerke, wird der neue Eintrag den bestehenden vorangestellt. Dadurch kann der Empfänger genau nachvollziehen, wann die Nachricht welche Mailserver passiert hat. Bei der Software sendmail sieht dieser Vermerk folgendermaßen aus:

```
Received: from pcstefan.ihw.univie.ac.at (pcstefan.ihw.univie.ac.at [131.130.2.235])
          by mailbox.univie.ac.at (8.11.2/8.11.2) with ESMTP id f9JCrv9170694
          for <Emil.Empfaenger@aldebam.sal.at>; Mon, 24 Feb 2003 09:55:29 +0100
```

Anschließend versucht der Mailserver, dem Mailserver des Empfängers (oder zumindest einem dem Ziel nahe gelegenen Mailserver) die Nachricht zuzustellen. Dabei wird verfahren wie in Punkt 2, wobei natürlich alle vorhandenen `Received:`-Header mitgeschickt werden.

### 4. Zustellung

Hat die Nachricht den Mailserver des Empfängers erreicht, wird sie in ein Postfach einsortiert, aus dem sie der Mailklient des Empfängers z.B. mittels POP oder IMAP abholen kann.

Rein rechtlich ist also nicht viel Unterstützung im Kampf gegen den Spam zu erwarten – und dabei wurde noch gar nicht auf den Gesichtspunkt eingegangen, daß der tatsächliche Absender einer Spam-Nachricht nur in seltenen Fällen überhaupt entlarvt werden kann.

## Über Fälschungen und Tätersuche

Es mag angesichts der allgegenwärtigen Paßwortabfragen verblüffend sein und scheinbar der oft zitierten Tatsache widersprechen, daß man auch im Internet nicht anonym ist und stets eine Datenspur hinterläßt – dennoch stimmt es: In den meisten Fällen ist es schlicht unmöglich, den Absender von Spam-Mail auszuforschen. Der folgende Abschnitt soll die Frage beleuchten, warum das so ist und warum das nicht zu ändern ist.

Da dies letztlich eine technische Frage ist, wird auch die Antwort ein wenig ins Technische gehen. Zum Trost: Die Briefkasten-Analogie hilft weitestgehend, die Vorgänge beim Mailing zu verstehen. Electronic Mail funktioniert, sieht man von der fehlenden Briefmarke ab, fast bis ins kleinste Detail ebenso wie die klassische Briefpost: Es gibt Kuverts, Absender und Empfänger (darunter auch solche, die einfach eine neue Adresse auf das Kuvert schreiben und den Brief wieder in den Postkasten werfen) – nur daß Bits die Rolle von Papier/Tinte und Programme die Rolle des Briefträgers spielen.

Zurück zum Ausforschen: Denken Sie daran, daß die Entarnung des Briefbombenattentäters Franz Fuchs – allen Bemühungen in diesem spektakulären Fall zum Trotz – fast vier Jahre dauerte. Vermutlich sind auch Ihnen damals Überlegungen durch den Kopf gegangen wie *„Weil man sich vor dem Briefkasten nicht ausweisen muß, haben die kaum eine Chance, den zu finden…“* Bei eMail ist es ebenso: Wie soll ein Mailserver prüfen, ob der Absender wirklich der ist, der er zu sein vorgibt? Der naheliegende Gedanke *„Per Paßwort natürlich!“* funktioniert leider nicht zufriedenstellend. Zwar könnten die Mailserver des ZID theoretisch (und mit erheblichem Aufwand) die Paßwörter der Benutzer des ZID zwecks Identitätskontrolle abfragen – zumindest sofern sie `univie`-Adressen und nicht etwa GMX- oder Hotmail-Adressen verwenden. Gegen Spam, der von außerhalb der Universität Wien stammt, ist das aber nutzlos: Wir können weder das Paßwort von `spammer@spamhaus.com` prüfen noch können wir wissen, ob der versendende Mailserver vertrauenswürdig ist und seinerseits Paßwort-Abfragen vorgenommen hat (es gibt einfach zu viele davon – unsere Mailserver haben täglich mit über 20 000 anderen Kontakt, und das sind keineswegs jeden Tag dieselben).

Schlußfolgerung: Solange es irgendwo auf der Welt Postämter gibt, die die Identität des Absenders nicht per Ausweis kontrollieren, ist jede Überprüfung dieser Art sinnlos. Bei eMail ist es nicht anders – die Richtigkeit der Absenderadresse läßt sich nicht garantieren.

### Großmutter, warum hast du so viele Köpfe?

Die Beispiel-Nachricht im Kasten *Crashkurs: Wie funktioniert eMail?* (siehe Seite 6) zeigt den korrekten Gebrauch von Electronic Mail: Alle Header sind sinnvoll und schlüssig ausgefüllt. Im Normalfall sorgt der eMail-Klient dafür, daß alles stimmt. Der im Beispiel geschilderte Dialog läßt sich aber problemlos auch mit relativ einfachen Skripts oder mit Dienstprogrammen wie Telnet abwickeln – und in diesem Fall kann der Absender hineinschreiben, was er will.

Was kann nun ein übelwollender Absender fälschen, ohne daß der Mailserver streikt? Mit zwei Ausnahmen alles!

Wie bei der Briefpost muß eine Angabe stimmen: Die Empfängeradresse(n) auf der Envelope – sonst kommt die Nachricht nicht an. Normalerweise nimmt der Mailklient diese Adressen aus den `To:`-, `Cc:`- und `Bcc:`-Feldern sowie gegebenenfalls fest konfigurierten *Kopie senden An*-Adressen. Bei „Handarbeit“ müssen die `RCPT TO:`-Adressen der Envelope nichts mit diesen Headerzeilen gemeinsam haben – der Briefkopf wird ja vom Mailserver nicht beachtet.[6)]

Was ebenfalls nicht gefälscht werden kann, ist die IP-Adresse des absendenden Rechners,[7)] die im `Received:`-Header vermerkt wurde:

```
Received: from pcstefan.ihw.univie.ac.at
(pcstefan.ihw.univie.ac.at [131.130.2.235])
```

Dies gilt allerdings nur für die IP-Adresse – den Rechnernamen, der im `Received:`-Header gleich zweimal vorkommt, darf man wiederum nicht für bare Münze nehmen:

3) Das Beispiel funktioniert tatsächlich so wie beschrieben und stellt das Prinzip wahrheitsgetreu dar. In der Praxis kommen jedoch zahlreiche Details und Erweiterungen hinzu, die zusammen mit hier sorgsam verschwiegenen Fragen (etwa: *Woher weiß der Mailserver, welcher andere Server näher am Ziel ist?*) aus eMail eine äußerst komplexe Materie machen.

4) Auch Attachments, die absolut kein Text zu sein brauchen, werden so verpackt, daß sie für den Mailtransport als „Text“ gelten – sie sind ebenfalls Bestandteil des Body. Der Aufbau einer eMail-Nachricht ist im Dokument *Internet Message Format* (RFC 2822, `ftp://ftp.univie.ac.at/netinfo/rfc/rfc2822.txt`) genau definiert; Erweiterungen für Umlaute, Attachments usw. sind in den *Multipurpose Internet Mail Extensions* (MIME) festgelegt (RFC 2045 – 2049).

5) Das Protokoll, nach dem dieser Dialog abgewickelt wird, ist das *Simple Mail Transfer Protocol* (SMTP), siehe RFC 2821 (`ftp://ftp.univie.ac.at/netinfo/rfc/rfc2821.txt`).

6) siehe `http://www.univie.ac.at/ZID/faq/mail_nicht_an_mich_adressiert.html`

7) Diese Wahrheit gilt nicht ohne Einschränkungen: Einerseits ist es in der Regel kein Problem, die Adresse eines anderen Rechners im eigenen Netz zu übernehmen, solange dieser nicht eingeschaltet ist. In Zusammenhang mit Spam ist das jedoch kein Thema, weil den Spam-Versendern damit noch nicht gedient ist. Andererseits kann ein Absender mittels *Sequence Number Prediction* (erstmals 1985 in `http://www.pdos.lcs.mit.edu/~rtm/papers/117-abstract.html` beschrieben und seither in verschiedenen Variationen immer wieder aktuell geworden) gegenüber alten Servern eine falsche Identität vortäuschen. Diese Möglichkeit ist aber offenbar zu selten zielführend und zu kompliziert, als daß Spammer darauf zurückgreifen würden.

Die erste Nennung gibt das wieder, was der Absender (im Beispiel bei `[02] HELO`) als Name angegeben hat, ist also durch diesen fälschbar. Der in der Klammer vermerkte Name ist der aus der IP-Adresse über das *Domain Name System* erschlossene Hostname. Dieser kann zumindest vom Eigentümer der jeweiligen IP-Adresse weggelassen bzw. manipuliert werden. Mit diesen Angaben läßt sich also prächtig Verwirrung stiften – tatsächlich werden immer wieder Beschwerdebriefe an die (oft völlig unbeteiligten) Betreiber der im `Received:`-Header genannten Domain gerichtet.

Da jeder Mailserver seinen `Received:`-Header an den Beginn der Headerzeilen scheibt, zeigen diese in umgekehrt chronologischer Folge den Weg, den die Nachricht gegangen ist. Die in vielen Antispam-Ratgebern empfohlene Faustregel, die IP-Adresse in der chronologisch ersten (also untersten) `Received:`-Zeile als die des vom Bösewicht verwendeten Rechners zu betrachten, ist aber schon seit geraumer Zeit nicht mehr gültig: Gängige Praxis bei Spammern ist es, dem eigenen Spam frei erfundene `Received:`-Zeilen anzufügen und so den Eindruck zu erwecken, als hätte der tatsächliche Spam-Versender die Nachricht selbst nur von einem anderen Absender erhalten und ordnungsgemäß weitergeleitet. Beschwerden bei der „ersten“ IP-Adresse gehen ins Leere, da diese der Phantasie des Spammers entspringt. Fälschungen in diesem Bereich zu erkennnen, gelingt selbst Experten nicht immer mit hundertprozentiger Sicherheit.

Als wäre die Rückverfolgung noch nicht kompliziert genug, kommen noch mindestens drei Schwierigkeiten hinzu:

- Die `Received:`-Zeilen mancher Mailserver sind unbrauchbar. Wenn es einem Spammer gelingt, einen Mailserver ausfindig zu machen, der die IP-Adresse nicht im Header vermerkt, kann er nicht mehr ausgeforscht werden – es sei denn, der zuständige Administrator sucht die IP-Adresse des Absenders aus seinen Log-Dateien heraus. Gerade solche Server sind aber üblicherweise nicht gewartet, ein Postmaster ist in der Regel nicht aufzutreiben und eine Log-Datei ohnehin nicht vorhanden.

- Die Nachricht wurde nicht direkt vom Absender generiert, sondern dieser hat z.B. ein nicht gesichertes Web-Formular benutzt. FormMail hat in dieser Hinsicht traurige Berühmtheit erlangt (mehr dazu im Artikel *Spammer vs. Blacklists: Ein ewiges Wettrüsten* auf Seite 37).

- Durch die zunehmend populäre Verwendung von ungeschützten Proxies (siehe Artikel auf Seite 37) kann der Spam-Versender völlig unerkannt bleiben, da hierbei lediglich die IP-Adresse des Proxies vermerkt wird.

### Es ist nicht alles Gold, was glänzt

Angenommen, es gelingt trotz aller Widrigkeiten, die IP-Adresse des Absenders zu ermitteln, ergibt sich daraus noch nicht zwangsläufig ein Täter. Zumindest in folgenden Fällen enden die Ermittlungen in einer Sackgasse:

- Die IP-Adresse führt zu einem öffentlich zugänglichen Gerät (in einem Internet-Cafe, bei Messen, Ausstellungen usw.), wo die Benutzer nicht erfaßt werden und Maßnahmen gegen Mißbrauch – sofern überhaupt vorhanden – umgangen wurden.

- Die IP-Adresse gehört zu Modem-Einwahlverbindungen, und der Spammer hat sich mit erschlichenen oder gefälschten Zugangsdaten eingewählt.

- Die IP-Adresse führt zu einer ungesicherten Netzwerksteckdose, die z.B. mit einem Laptop benutzt wurde (nicht ganz zufällig ist etwa das Hörsaal-Netzwerk der Uni Wien nur mit Paßwort verwendbar).

- Die IP-Adresse gehört einer völlig unbeteiligten Institution, die eines der überaus zahlreichen ungeschützten Funk-LANs[8] betreibt, die – z.B. von der Straße aus – von jedermann mit Laptop und WaveLAN-Karte einfach mitbenutzt werden können.

In den meisten Fällen wird die Absender-Ausforschung außerdem die Kooperation jener Institution erfordern, die das Netzwerk betreibt, von dem aus der Spam versendet wurde. Aus Datenschutzgründen wird dafür in der Regel ein Gerichtsbeschluß verlangt werden. Wie das Procedere bei der Spam-Verfolgung im Ausland genau aussieht, will man sich lieber gar nicht erst vorzustellen versuchen.

Auf den Punkt gebracht bedeutet das: Bestenfalls läßt sich eine IP-Adresse eruieren, doch selbst diese bringt einen oft nicht ans Ziel.

## Wo geht’s hier zum Salzamt?

Trotz aller Widrigkeiten ist es selbstverständlich sinnvoll, sich zu beschweren. Beispielsweise wird der Administrator eines mißbrauchten Rechners sehr daran interessiert sein, von seinem Problem zu erfahren. Ebenso sind Provider bzw. sonstige Institutionen meist auf ihren guten Ruf bedacht und dankbar, wenn sie auf Mißbrauch durch ihre Benutzer aufmerksam gemacht werden.

Bevor Sie erwägen, eine Beschwerde zu schreiben: Bedenken Sie, daß Ihre Header-Analyse möglicherweise Irrtümer enthält, daß der Empfänger der Beschwerde möglicherweise tausende ähnliche (womöglich irrtümliche) Beschwerden erhalten hat und daß für die Behandlung des Falls exakte Informationen über den Vorfall – also die Nachricht einschließlich aller Headerzeilen – unbedingt erforderlich sind. Das Beschweren ist also eher nichts für den Laien.

Guten Gewissens kann aber Spamcop (`http://spamcop.net/`) empfohlen werden. Dahinter verbirgt sich ein Mail-

8) Mehr über den Versuch, in der Tradition der Gaunerzinken eine Kreidezeichen-Subkultur für WaveLANs zu gründen, erfahren Sie unter `http://www.warchalking.org/`.

headeranalyse- und Beschwerdegenerierungssystem, das mit recht guter Treffsicherheit die richtigen Adressen zum Beschweren herausfindet. Das wissen auch die Administratoren von Mailservern, sodaß sie eine Spamcop-Beschwerde eher ernst nehmen als einen handgenerierten Sermon, der womöglich zwar *Traceroutes* und *Whois*-Einträge (die der Administrator, da es seine eigenen sind, ohnehin kennt), aber keine brauchbaren Informationen wie beispielsweise die vollständigen Mailheader enthält.

Die Wirkung Ihrer Beschwerde wird, falls sie einer Überprüfung standhält und der Netzbetreiber seriös ist, in der Regel zumindest eine Verwarnung des Übeltäters sein, oft sogar die Sperre des Zugangs. (Eine Rückmeldung werden Sie dennoch nur selten erhalten, schon allein deshalb, weil der zuständige Administrator lieber das nächste Problem bearbeitet als tausende gleichartige Beschwerden zu beantworten.) Aus der Sicht des geplagten Spam-Empfängers ist das Ergebnis – selbst wenn der Zugang gesperrt wurde – eher entmutigend: Der gesperrte Spammer zählt das Geld, das er in der Zwischenzeit bereits verdient hat, zuckt mit den Schultern und eröffnet anderswo bzw. unter anderem Namen einen neuen Account.

Im Zusammenhang mit dem Thema, wie – außer mit Löschen – zweckmäßigerweise auf den Erhalt einer Spam-Mail zu reagieren ist, seien noch drei häufig leider nicht gestellte Fragen beantwortet:

- **Soll ich antworten und dem Absender meine Meinung sagen?**
- **Soll ich an die Remove-Adresse schreiben?**
  Auf keinen Fall! Fast immer ist die Absenderadresse gefälscht. Falls Ihre Antwort überhaupt irgendwo ankommt, ist es mit höchster Wahrscheinlichkeit die Mailbox einer völlig unbeteiligten Person, die aus tausenden Spam-Reaktionen die wirklich an sie gerichteten Nachrichten mühsam heraussuchen muß (vielleicht war auch gerade das die Absicht des Spams – so etwas nennt sich im Jargon *Joe Job*)[9]. Insbesondere wenn Sie den Anweisungen zum Abbestellen wie *Unsubscribe, Remove-Me* usw. folgen (egal ob es sich um Webseiten oder bestimmte eMail-Nachrichten an bestimmte Adressen handelt), besteht zusätzlich die Gefahr, daß Ihre Adresse nicht nur nicht aus der Adressenliste gelöscht wird, sondern im Gegenteil als besonders wertvoll – weil nachweislich in Gebrauch befindlich – betrachtet und mit noch mehr Spam beglückt wird.

  Um Mißverständnisse zu vermeiden: Es ist nicht alles Spam, was abbestellt werden kann. Bei legitimen Mailinglisten, die Sie selbst subskribiert haben, ist ein *unsubscribe* durchaus wirksam – nicht aber (oder nur ausnahmsweise) bei unverlangt zugestellten Nachrichten.

- **Soll ich den Spam an meinen Webmaster/Postmaster weiterleiten?**
  Da wir immer wieder Spam-Beschwerden an die Adresse `webmaster@univie.ac.at` erhalten: Der Webmaster ist für die Webseiten zuständig, nicht für eMail. Ihr Postmaster kann in der Regel ebenfalls nichts für Sie tun – immerhin ist es ja die Aufgabe Ihres Mailservers, an Sie gerichtete Nachrichten zuzustellen. In besonders krassen Fällen, die z.B. eine Einschaltung der Gerichte erforderlich machen, können wir jedoch versuchen, bei der Ausforschung des Absenders behilflich zu sein. Ebenso werden wir aktiv, wenn ein Mailserver innerhalb des Uni-Netzes zum Absenden oder unbefugten Relayen von Spam mißbraucht wird. In solchen Fällen wenden Sie sich bitte an die Mailadresse `abuse@univie.ac.at`.

## Strategien gegen Spam

Spam ist ein soziales Problem: Skrupellose Geschäftemacher verdienen Geld auf eine Art und Weise, die der Gesellschaft zumindest auf die Nerven geht. Mit technischen Mitteln zu versuchen, soziale Probleme zu lösen, ist methodisch der falsche Ansatz und kann daher nicht perfekt gelingen. Da eine zivile Lösung mit rechtsstaatlichen Mitteln vorerst nicht in Sicht ist, bleibt aber derzeit keine andere Wahl, als sich die Möglichkeiten der EDV – so gut es eben geht – zunutze zu machen. Dabei gibt es zwei verschiedene Ansätze: Den Weg des Spams zum Empfänger zu blockieren, oder empfangene Nachrichten als Spam zu erkennen und zu entsorgen.

### Spam unterwegs blockieren

**Schwarze Listen**

Ein naheliegender Gedanke ist, von Spammern einfach keine Mail mehr entgegenzunehmen. Viele Benutzer haben bereits versucht, die Adressen, von denen sie Spam erhalten haben, mit den Filtermechanismen ihrer Mailklienten einfach auszusperren. Da Spammer immer wieder neue Absenderadressen verwenden, ist dieser Weg jedoch nicht zielführend.

Der Mailserver besitzt aber eine Information, die dem Mailklienten nicht zur Verfügung steht und die sich nicht fälschen läßt: Die IP-Adresse des Rechners, der die Nachricht abliefert. Ein Administrator kann also versuchen, an seinem Server die Mailserver der Spammer – und damit den Spam – zu blockieren, indem er deren IP-Adresse in eine Sperrliste einträgt. Die manuelle Wartung einer solchen Sperrliste durch jeden einzelnen Postmaster ist aber zu mühsam und zu ineffizient, um zielführend zu sein. Es wurden also automatisch abfragbare, zentral anhand der Spam-Berichte aus der Netzgemeinde befüllte Datenbanken mit den IP-Adressen Spam-versendender Rechner angelegt: Die *Blacklists*. Damit wurde es möglich, durch einmalige Konfiguration des Mailservers das Sperren von Mailservern an die Betreiber der Blacklists zu delegieren.

Blacklists werden folgendermaßen verwendet: Sobald eine Verbindung zu einem durch Blacklists geschützten Mailserver aufgebaut wird, überprüft dieser, ob die Adresse der Gegenstelle in der Blacklist aufscheint. Ist dies der Fall, wird

9) siehe `http://www.cotse.com/11022000.html`

die Nachricht abgewiesen. Leider haben die Spam-Versender bisher aber immer wieder Methoden gefunden, um die Blacklists zu unterwandern – hauptsächlich durch unfreiwillige Mithilfe anderer Server im Internet. Das Resultat ist eine Unzahl von Blacklists mit unterschiedlicher Semantik: Spam-Hosts, Open Relays und viele andere (einen Überblick gibt der Artikel *Spammer vs. Blacklists: Ein ewiges Wettrüsten* auf Seite 37).

Blacklists haben – rein statistisch gesehen – durchaus eine gute Aussagekraft; ihre Verwendung birgt jedoch auch ein großes Risiko: Wenn man sich zur Verwendung von Blacklists entschließt, gibt man (das ist ja der Zweck der Übung) die Entscheidungsgewalt darüber, mit wem man kommuniziert, an eine fremde Instanz ab. Das setzt ein gehöriges Maß an Vertrauen voraus, dessen Berechtigung kaum zu überprüfen ist.[10] Aber selbst die bestgeführten Blacklists leiden unter einem systemimmanenten Mangel: Da statt Spam-Nachrichten nur IP-Adressen geblockt werden, trifft die Sperre auch alle anderen Benutzer des betreffenden Servers. Es ist etwa so, als würde man allen Bewohnern eines Häuserblocks den Führerschein entziehen, sobald einer von ihnen einen Unfall verursacht. Zwar hebt eine solche Maßnahme sicher nachweislich die Verkehrssicherheit, aber spätestens an dem Tag, an dem es einen selbst oder gute Freunde trifft, wird klar, daß die „Mitgefangen-Mitgehangen"-Methode vielleicht etwas überzogen ist. Deshalb hat der ZID nie nach Blacklists gefiltert, sondern lediglich – primär für die Betreiber von Instituts-Mailservern – allfällige Blacklist-Informationen in Form des `X-Spam-Flags:`-Headers in der Nachricht vermerkt (siehe `http://www.univie.ac.at/ZID/faq/spam-rbl.html`).

**Geheimhaltung der Mailadresse**

Ein anderer Ansatz, den Weg vom Spammer zum Empfänger zu unterbrechen, ist, die eMail-Adresse geheimzuhalten – oder besser, keine zu haben. Dieser etwas radikalen Grundidee folgend, wurden mehrere Vorgangsweisen entwickelt, die das Kind nicht gleich mit dem Bade ausschütten.

Eine vor allem in Newsgruppen häufig gebrauchte Methode ist *Address Munging*. Dabei werden Adressen wie `Emil.Empfaenger@REMOVETHIS.aldebam.sal.at` verwendet. Die Idee: Sollte jemand antworten wollen, wird ihm hoffentlich auffallen, daß das Wörtchen `REMOVETHIS` aus der Adresse händisch zu entfernen ist, wozu Spam-Programme mangels Intelligenz nicht in der Lage sind. In der Praxis sieht es aber so aus, als würde der gegenteilige Effekt erzielt: Aufgrund der Intelligenz ihrer Programmierer agieren Spam-Programme so, daß sie zumindest die gängigen dieser Füllwörter erkennen und entfernen. Humanoide hingegen interessieren sich nicht besonders für die Mailadresse, sondern verlassen sich darauf, daß diese beim Klick auf *Reply* ohnehin richtig eingesetzt wurde – und scheitern.

Bei Webseiten besteht die Möglichkeit, statt der Adresse im Klartext oder gar als anklickbarem Link eine Grafik anzuzeigen. Diese Methode ist allerdings nicht zu empfehlen: Dadurch bleibt neben Spammern auch ein nicht unbeträchtlicher Teil der Bevölkerung ausgeschlossen – nämlich Blinde, die mit Braille-Zeile oder Sprachausgabegeräten arbeiten.[11] Abgesehen davon haben auch mit Adleraugen gesegnete Mitmenschen meistens keine Freude daran, eMail-Adressen (fehlerfrei!) abtippen zu müssen.

Ein einigermaßen brauchbarer Ausweg, zumindest für stark exponierte Adressen wie beim Posten in Newsgruppen, ist die Verwendung von temporären Mailadressen: Sobald eine Adresse stark spamverseucht ist, verwendet man einfach eine andere und läßt die alte nur mehr für eine Übergangszeit gelten. Dieses Verfahren ist auch äußerst vorteilhaft, wenn man Spam-Traps auslegen möchte (dazu später mehr).

## Spam empfangen und entsorgen

**Content Filter**

*Ich kann zwar nicht definieren, was es ist, aber ich erkenne es, wenn ich es sehe* ist ein Charakteristikum von Spam. Content Filter versuchen genau das: Spam-Mail anhand ihres Inhalts zu identifizieren. Zum Teil funktioniert das recht gut (*Viagra prescriptions* und *Hot asian teens* werden mit ziemlicher Sicherheit erkannt), hin und wieder müssen Content Filter aber auch vernichtende Niederlagen einstecken:

- Todsichere Spam-Schlüsselwörter gibt es nicht – beispielsweise ist *Viagra* für Pharmavertreter, Ärzte und vermutlich auch einige Uni-Angehörige (z.B. Autoren von Artikeln über Spam) ein notwendiges Element ihrer eMail-Korrespondenz. Gerade bei einer so breitgefächerten Benutzerschaft wie an der Uni Wien lassen sich für alle „sicheren" Kriterien auch Gegenbeispiele finden.

- Beim Versuch, natürliche Sprache mit den vergleichsweise plumpen Mitteln der EDV zu behandeln, tauchen nicht selten peinliche Artefakte allzu einfacher Lösungen auf: Microsofts „Adult Content Filter" hat z.B. eine Ausgabe des Microsoft-Newsletter *MSDN Flash* geblockt,[12] weil im Text *Plus, VSLive! San Francisco provides over*

10) Der Betreiber von ORBS (einer auf Non-Profit-Basis betriebenen, sehr effizienten und beliebten Blacklist) mußte, nachdem er ein Gerichtsverfahren verloren hatte, in dem ihm ungerechtfertigte Listings vorgeworfen wurden, den Betrieb einstellen und ein Eingeständnis veröffentlichen. Nach der vorherrschenden Meinung in der Antispam-Gemeinschaft liegt dies jedoch daran, daß der Betreiber den Prozeß nicht finanzieren konnte; folgerichtig wird die faktische Richtigkeit der Vorwürfe weithin angezweifelt.

11) Ein Besuch von `http://www.cast.org/bobby/` sollte ohnehin für jeden Webdesigner verpflichtend sein.

12) `http://catless.ncl.ac.uk/Risks/21.90.html#subj3`

13) Diese beruhen darauf, das Vorkommen bestimmter Wörter als Hypothese dafür zu betrachten, daß die Nachricht Spam oder eben kein Spam ist. Die Richtigkeit der Hypothese wird an einer größeren Menge Mail getestet, die durch den Anwender in Spam und Nichtspam klassifiziert wurde („der Filter wird trainiert"); daraus werden Koeffizienten berechnet, die den einzelnen Wörtern zugeordnet werden. Zur Prüfung einer Nachricht werden die Koeffizienten aller darin enthaltenen Wörter zu einem Spam-/Nichtspam-Verhältnis zusammengerechnet (siehe auch `http://www.paulgraham.com/spam.html`).

*180 hours of (...)* die Zeichenkette *over 18* enthalten ist, was ja eindeutig auf zweideutige Angebote hinweist.

- Statistische Methoden[13] sind bei Anwendung im persönlichen Umfeld (zumindest solange Spam und sonstige Korrespondenz in derselben Sprache abgefaßt sind) zwar sehr vielversprechend, bei einer größeren Benutzergruppe läßt die Treffsicherheit aber nach. Der an sich hervorragende SpamAssassin blockte zum Beispiel – offenbar weil viele Benutzer vom Klez-Wurm versendete eMail als Spam klassifiziert hatten – eine Ausgabe der *Risks*-Mailingliste: Darin wurde dieser Mailwurm diskutiert, und deshalb kam das „böse" Wort *Klez* zu oft vor...

**Massenmail wiedererkennen**

Da Spam die Eigenschaft hat, als gleichlautender Text massenhaft aufzutreten, ist es naheliegend, am Server einlangende Nachrichten dahingehend zu überprüfen, ob ihr Inhalt identisch ist. Die Idee, einfach mitzuzählen und eine Nachricht als Spam zu klassifizieren, wenn sie z.B. zum hundertsten Mal entgegengenommen wurde, ist verlockend – aber so einfach ist das auch wieder nicht:

- Die Methode hat den Nachteil, daß die ersten Empfänger der Nachricht ungeschützt bleiben, weil ja der Zählerstand noch nicht erreicht ist.

- Spammer variieren zunehmend den verschickten Text. Teilweise wird in einer Art von Begrüßung ein wechselnder Name eingefügt, mitunter finden sich einfach nur wirre Zeichenketten im Text, oder es werden in HTML-Mail zufällige HTML-Kommentare eingefügt, die für den Betrachter unsichtbar bleiben.

- Die Mailserver des ZID bearbeiten täglich etwa 150 000 Nachrichten. Um jede einzelne davon mit jenen der letzten 24 Stunden zu vergleichen, wären 22 500 000 000 Vergleiche notwendig – so geht das natürlich nicht. Praktisch anwendbar ist aber die Methode, die Rhyolite mit dem *Distributed Checksum Clearinghouse* (DCC)[14] verfolgt: DCC bildet beim Mailempfang eine Prüfsumme über den Mail-Inhalt und zählt in einer weltweiten Datenbank, wie oft diese Prüfsumme errechnet wurde. Um trotz verschiedener Variationen prinzipiell identische Nachrichten erkennen zu können, werden zusätzlich noch zwei „fuzzy" Prüfsummen berechnet und verglichen. Da die öffentliche DCC-Datenbank von zahlreichen Servern auf der ganzen Welt befüllt wird, kann dieses System Massenmail mit guter Trennschärfe identifizieren. Allerdings birgt der kooperative Charakter der weltweiten DCC-Datenbank auch eine theoretische Mißbrauchsgefahr, da jeder – wenn auch erst nach Anmeldung – Prüfsummen zur Datenbank senden kann. Darüber hinaus ist nicht auszuschließen, daß es durch schlichten Irrtum bzw. falsche Konfiguration zu Fehldiagnosen kommt.

- Massenmail ist nicht unbedingt Spam: Auch subskribierte Mailinglisten und abonnierte Newsletters sind Massensendungen. Sie müssen ausdrücklich von dieser Filtermethode ausgenommen werden.

**Spam-Traps**

Eine ausgezeichnete Möglichkeit zur Spam-Erkennung bieten sogenannte *Spam-Traps* oder *Honeypots* – das sind Mailadressen, die nie benutzt oder vor langer Zeit aufgelassen wurden. Sobald eine Nachricht bei einer Spam-Trap-Adresse einlangt, wird z.B. ihre Prüfsumme mit DCC gespeichert; kommt derselbe Text danach nochmals vor, kann man mit Sicherheit davon ausgehen, daß es sich um Spam handelt. Doch auch hier gibt es Haken:

- Die verräterische Nachricht an die Spam-Trap-Adresse kommt meist zu spät – zumindest für jene, die „ihr" Spam-Exemplar bereits erhalten haben.

- Es ist nicht so einfach, eine nie verwendete Mailadresse in den Datenbanken der Spammer unterzubringen.[15]

**URL-Analyse**

Wurden früher bei Spam-Nachrichten als Kontaktmöglichkeit oft Telefonnummern angegeben, so enthalten sie jetzt meist schon URLs von Webseiten oder (besonders bei pornografischem Spam) in HTML-Mail eingebettete Links auf Bilder, die bei Betrachtung der Nachricht von einem Webserver geladen werden.

Da im Gegensatz zu Absenderadressen die IP-Adressen, die für solche Webserver benutzt werden können, auch für Spammer nicht in beliebiger Zahl zur Verfügung stehen, stellen URLs eine Achillesferse der Spammer dar. Es gibt bereits ein Verzeichnis von Adreßbereichen, die für das Hosting von Spammer-Webseiten verwendet werden; ein real existierender Spam-Filter, der auf diese Weise arbeitet, ist allerdings bisher nicht bekannt.

## Die Gefahr der False Positives

Spam zu erkennen, ist eine interessante Herausforderung, für die es auch zahlreiche gute Werkzeuge gibt. Ein Spam-Filter muß aber auch noch einem anderen Kriterium genügen: Er darf legitime, erwünschte Nachrichten nicht fälschlich abweisen. Angenommen, ein Spam-Filter würde nur 0,01% (ein hervorragender Wert!) der Mail irrtümlicherweise als Spam ausscheiden, wären das an der Uni Wien immer noch 15 Nachrichten täglich.

Eine legitime Nachricht, die irrtümlich als Spam klassifiziert wurde, wird als *False Positive* bezeichnet. Da die Auswir-

14) siehe `http://www.rhyolite.com/anti-spam/`

15) Scheinbar schlucken Spammer nicht jeden ausgelegten Köder: Der Autor dieser Zeilen postet schon lange regelmäßig mit markierten Adressen in Newsgruppen und erhält dennoch nur ca. 200 Spam-Nachrichten pro Tag an diese Adressen. Es wäre denkbar, daß die heiß diskutierten Postings von `klautzi05@hotmail.com`, der/die gebrauchte Zahn- und Klobürsten feilbietet, oder die berüchtigten Postings der *Hürbine von Pleuselspink* gerade dazu dienen sollen, Spam-Trap-Adressen attraktiv zu machen.

kungen einer nicht zugestellten wichtigen Nachricht wesentlich gravierender sind als die von „durchgerutschtem" Spam, muß dieser Problematik besonderes Augenmerk gewidmet werden. Es gibt mehrere Möglichkeiten, diese Gefahr zumindest zu verringern.

### Whitelists

Ein Werkzeug zur Vermeidung von False Positives sind *Whitelists*, in denen Absender vermerkt werden, die generell vom Spam-Filter ausgenommen werden sollen. Diese Listen sollte jeder Empfänger selbst verwalten können – beispielsweise um subskribierte Mailinglisten darin aufzunehmen.

Gerade bei großen Mailinglisten gibt es allerdings im Zusammenhang mit Spam-Filtern ein Problem, für das derzeit keine zufriedenstellende Lösung existiert: Listserver senden regelmäßig sogenannte *Probes* an die Abonnenten aller Listen, um Karteileichen auszusortieren – kommt eine Fehlermeldung zurück, ist die getestete Adresse nicht mehr aktiv und wird von der Mailingliste gestrichen. Diese Testnachrichten werden aber mit einer speziellen (also nicht der sonst verwendeten) Absenderadresse verschickt, sodaß es geschehen kann, daß sie von der Whitelist nicht erfaßt und eventuell abgewiesen werden – mit dem Effekt, daß die getestete, an sich gültige Adresse aus der Mailingliste ausgetragen wird. Der einzige Ausweg ist hier, die gesamte Domain, aus der die Mailingliste verschickt wird, in die Whitelist aufzunehmen.

Ein weiteres Problem liegt in der Notwendigkeit, die Whitelist aktuell zu halten. Man könnte zwar alle Mailadressen automatisch in die Whitelist aufnehmen, an die man selbst Nachrichten geschickt hat; das hilft aber leider nicht, wenn die Antwort von einer anderen Adresse kommt (z.B. wenn bei einer Anfrage an eine Service-Mailadresse der zuständige Bearbeiter unter seiner persönlichen Mailadresse antwortet). Ein solches automatisches Whitelisting könnte sogar generell für die ganze Universität eingeführt werden: Es ist sicher vernünftig, anzunehmen, daß jede Adresse, an die ein Uni-Angehöriger schreibt, auch für alle anderen akzeptabel ist. Diese Vorgangsweise birgt jedoch die Gefahr, daß damit z.B. auch die Adressen von Spammern weißgewaschen werden, denen genervte Empfänger, die diesen Artikel nicht gelesen haben, eine grobe Antwort zukommen lassen.

Abgesehen davon ist es nur eine Frage der Zeit, bis auch Spammer das tun, was im Bereich der Mailwürmer bereits *State of the Art* ist, nämlich eine Absenderadresse verwenden, die aus derselben Domain wie die Empfängeradresse stammt: Diese ist mit hoher Wahrscheinlichkeit bereits in der Whitelist enthalten.

### Signierte Mail

Da es für Spammer aufgrund der leichten Wiedererkennbarkeit nicht sinnvoll ist, Spam zu signieren, und folgerichtig bisher noch kein Spam mit einer elektronischen Signatur gesichtet wurde, wäre es ein gutes Kriterium, Nachrichten, die eine überprüfbare[16)] elektronische Unterschrift aufweisen, auf jeden Fall zuzustellen. Allerdings werden elektronische Signaturen heutzutage noch recht selten verwendet, sodaß diese Maßnahme derzeit nicht besonders effizient erscheint.

### Spam-Folder

Um die Konsequenzen von Fehlentscheidungen des Spam-Filters zu lindern, besteht die Möglichkeit, alle als Spam erkannten Nachrichten automatisch in einem eigenen Spam-Folder ablegen zu lassen. Irrtümlich als Spam eingestufte Mail kann somit vom Empfänger bei der Kontrolle seines Spam-Folders wieder herausgefischt werden. Das setzt allerdings voraus, daß der Spam-Folder regelmäßig überprüft – und geleert! – wird. Nachdem für den einzelnen Benutzer False Positives aber relativ selten sind, ist damit zu rechnen, daß die Kontrollfreudigkeit schnell abnimmt und der Spam-Folder mehrheitlich unbeachtet bleibt. In diesem Fall ist mit einem Spam-Folder niemandem gedient: Der Empfänger bekommt die Nachricht nie zu Gesicht, und der Absender kann nur rätseln, warum er keine Antwort erhält.

Die alternative Methode – die Nachricht abzuweisen und den Absender mit einer Fehlermeldung davon zu verständigen – hat jedoch gleich zwei positive Effekte: Einerseits erfährt der Absender frühzeitig, daß seine Nachricht nicht angekommen ist, und kann sich gegebenenfalls auf anderem Weg mit dem Empfänger in Verbindung setzen. Andererseits ergibt eine unzustellbare Fehlermeldung einen weiteren Indikator für den Spam-Filter – wer sonst setzt schon eine unzustellbare Adresse als Absender ein?

## Conclusio

Auch wenn sein Auftreten im digitalen Medium eMail darüber hinwegtäuschen mag: Spam ist ein Problem der Gesellschaft – es handelt sich um rüpelhaftes Verhalten und skrupellose Geschäftemacherei. Die sonst in solchen Fällen üblichen Methoden, insbesondere juristische Maßnahmen, greifen (noch) nicht, müssen aber weiter umgesetzt und ausgebaut werden. Interimistisch kann man versuchen, mit technischen Mitteln die Folgen zu bekämpfen, also Spam-Filter einzusetzen. Es gibt aber (schon allein, weil Spam sich durch die böse Absicht des Absenders und die Wahrnehmung des Empfängers definiert) keine absolut zuverlässige Methode, sich vor unerwünschter eMail zu schützen – zumindest nicht, ohne daß dabei auch erwünschte Mail geopfert wird.

Für das Design des auf Seite 40 vorgestellten Spam-Filters der Uni Wien ergaben sich daraus zwei Anforderungen: Erstens durch Kombination mehrerer Methoden eine höchstmögliche Treffsicherheit anzustreben und zweitens die Entscheidung für oder gegen seinen Einsatz jedem Benutzer selbst zu überlassen.

*Alexander Talos* ■

16) Etwa GPG/PGP-Signaturen, deren Schlüssel (*Keys*) auf `http://www.keyserver.net/` hinterlegt sind oder von einer Zertifizierungsinstanz ausgestellt wurden.

# SCHRÖDINGER II

*Wer nicht täglich einen Schritt nach vorne geht, bleibt täglich einen Schritt zurück.* – Nirgends gilt dieses Sprichwort so sehr wie in der Informationstechnologie, wo der technische Fortschritt sehr viel schneller ist als in fast allen anderen Bereichen. Beispielsweise hat der Supercomputer der Uni Wien, Schrödinger I (siehe *Comment 02/1*, Seite 2 bzw. `http://www.univie.ac.at/comment/02-1/021_2.html`), im Februar 2002 beim Linpack-Test 204,5 GFlops erzielt: Im November 2001 hätte er damit Platz 147 der Weltrangliste der 500 schnellsten Supercomputer (`http://www.top500.org/`) erreicht, im Juni 2002 belegte er Platz 264, und im November 2002 war er auf Platz 370 zurückgefallen.

Bereits bei der Planung des auf vier Jahre befristeten Supercomputing-Projekts wurde berücksichtigt, daß ein Supercomputer nach vier Jahren hoffnungslos veraltet ist, und Budgetmittel für mindestens zwei Ausbaustufen vorgesehen. Die Planung der ersten Ausbaustufe begann im November 2002; Mitte März 2003 sollen die Umbauten abgeschlossen sein.

Bei allen Komponenten des Supercomputers wurde genau untersucht, wie sie erweitert oder durch leistungsfähigere ersetzt werden sollten:

- **Prozessor:** Im ewigen Wettlauf zwischen Intel und AMD um den schnellsten Prozessor hat Intel gerade die Nase vorne (in einigen Wochen kann sich das wieder ändern): Bei Benchmark-Tests war der Pentium 4-Prozessor mit 2,4 GHz von Intel meistens mehr als doppelt so schnell wie der AMD Athlon XP 1700+, der bisher in Schrödinger I eingesetzt wurde.

- **Hauptspeicher:** Für einen Supercomputer ist schneller Speicher mit hoher Bandbreite mindestens genauso wichtig wie leistungsfähige Prozessoren. Bei den Benchmark-Tests konnten durch schnelleren Rambus-Speicher (siehe `http://www.rambus.com/`) in fast allen Fällen erhebliche Performance-Gewinne gegenüber dem bisher verwendeten DDR RAM erzielt werden – in manchen Fällen mehr als 100%. Trotz des beträchtlichen Preises war die Entscheidung zugunsten von Rambus schon fast gefallen, als von Intel der neue Chipset E7205 (siehe `http://www.intel.com/design/chipsets/e7205/`) vorgestellt wurde, der mit DDR RAM eine ebenso hohe Bandbreite erreichen sollte wie die bisherigen Chipsets mit Rambus. In der Praxis stellte sich heraus, daß Rambus immer noch um einige Prozent schneller ist; das Preis-/Leistungsverhältnis ist jedoch bei DDR RAM mit dem neuen Chipset wesentlich besser.

- **Vernetzung:** Der Anteil an parallelen Programmen, die eine leistungsfähige Netzwerk-Verbindung der Knoten untereinander benötigen, wird immer größer. Bisher waren 96 Knoten mit Fast Ethernet und 64 Knoten mit Gigabit Ethernet ausgerüstet. Für eine noch schnellere Verbindung als Gigabit Ethernet (z.B. Myrinet) besteht wenig Bedarf, Fast Ethernet ist aber eindeutig zu wenig.

- **Massenspeicher:** Mehr Plattenplatz ist dringend notwendig – der Fileserver ist chronisch überfüllt.

Nach einer eingehenden Analyse des Bedarfs, der vorhandenen Budgetmittel und der am Markt verfügbaren Komponenten wurde folgende Ausbau-Variante gewählt:

- Austausch sämtlicher Motherboards und Prozessoren durch Asus P4G8X Deluxe Motherboards (siehe `http://www.asus.com/mb/socket478/p4g8x-d/overview.htm`) mit dem E7205-Chipset und einem Intel Pentium 4-Prozessor mit 2,53 GHz. Der bisherige Hauptspeicher (1 GB DDR RAM pro Knoten) wird weiterverwendet.
- Vernetzung des gesamten Clusters mit Gigabit Ethernet. Die Motherboards haben bereits einen Gigabit-Anschluß, sodaß keine zusätzlichen Gigabit-Karten erforderlich sind. Die bisher verwendeten Ethernet-Switches von HP werden durch einen einzigen Cisco 4500-Switch ersetzt.
- Der Plattenspeicher wird ausgebaut und auf zwei Fileserver verteilt. Beide Fileserver gemeinsam verfügen über eine Plattenkapazität von etwa 1,5 TB, das ist ungefähr das Sechsfache des bisherigen Speicherplatzes.
- Der Cluster wird um 32 zusätzliche Knoten erweitert und hat somit insgesamt 192 Knoten.
- Für einzelne Applikationen mit hohem Speicherbedarf (insbesondere Gaussian 98) wären mehr als 1 GB Hauptspeicher pro Knoten wünschenswert. Vorerst wird versucht, dieses Problem durch Parallelisierung zu lösen; falls das nicht ausreicht, werden einige Knoten mit 2 GB Hauptspeicher ausgerüstet.
- Neben der Parallelisierung von Gaussian wird es noch einige Verbesserungen beim Software-Angebot geben: Das Softwarepaket *Amber 7* (Molekulardynamik für Biomoleküle) steht seit einiger Zeit zur Verfügung und wird ebenfalls parallelisiert. Das bisher verwendete Batchsystem PBS soll durch die modernere und leistungsfähigere Sun ONE Grid Engine (`http://www.sun.com/software/gridware/`) ersetzt werden.

In Summe ist das eher ein Austausch als ein Ausbau: Außer den Gehäusen bleibt von Schrödinger I wenig übrig. Naheliegenderweise erhält der neue Cluster den Namen Schrödinger II. Selbstverständlich erfolgt der Ausbau nicht, um einen guten Platz in der Liste der Top 500 zu erreichen, sondern um ausreichend Rechenleistung für Spitzenforschung zur Verfügung zu stellen. Dennoch ist zu hoffen, daß Schrödinger II die 500 GFlops-Marke zumindest annähernd erreicht und damit die Position vom Juni 2002 halten oder sogar verbessern kann.

*Peter Marksteiner* ■

# Billig, aber gut: Handbücher des RRZN

Dieser Artikel ist für all jene gedacht, die sich über die informativen und äußerst günstigen Handbücher des Regionalen Rechenzentrums Niedersachsen (RRZN) an der Universität Hannover, die auch am ZID der Uni Wien erhältlich sind, nicht nur freuen, sondern auch ein wenig über deren Ursprung und Hintergrund in Erfahrung bringen möchten.

## Es war einmal …

… ein Rechenzentrum in Niedersachsen, das sich zum Ziel gesetzt hatte, die Dokumentation gängiger Softwareprodukte einfacher zu gestalten. Zu diesem Zweck wurde eine Zusammenarbeit mehrerer EDV-Zentren unterschiedlicher Universitäten angestrebt. Anfangs war dieses Unternehmen allerdings eine Einbahnstraße, da das RRZN die Vorleistung (Erstellung und Abgabe der Handbücher an die anderen Rechenzentren in beliebig hohen Stückzahlen) erbrachte, ohne eine sofortige Gegenleistung in Form von Arbeitskraft zu fordern – und demgemäß die Last alleine trug. Mittlerweile hat sich jedoch aus diesem Projekt eine fruchtbare Kooperation im wahrsten Sinne des Wortes entwickelt, an der sich 130 Hoch- und Fachhochschulen in Deutschland und Österreich beteiligen: Die Kooperationspartner – auch der ZID der Uni Wien gehört dazu – beziehen wie bisher regelmäßig größere Stückzahlen zahlreicher Handbücher vom RRZN, um sie an ihre Studierenden und Mitarbeiter weiterzugeben. Im Gegenzug begutachten sie Texte und liefern Korrekturvorschläge, entwickeln Teiltexte zu neuen Publikationen oder überlassen selbst erstellte Schriften dem RRZN zum Druck und zur Verbreitung.

## Kooperation erbeten

Da die Handbücher des RRZN nicht nur sehr gut ausgearbeitet, sondern auch extrem günstig sind, kommt es häufig vor, daß auch „universitätsfremde" Personen sie erwerben möchten. Die Abgabe ist jedoch aufgrund der vertraglichen Vereinbarungen mit dem RRZN und dem Herdt-Verlag ausnahmslos nur an Studierende und Mitarbeiter der kooperierenden Unis möglich. Der Verkauf an Privatpersonen, Schulen, Firmen etc. ist ausdrücklich untersagt. Solche Interessenten können wir nur auf die zahlreiche Fachliteratur im Buchhandel verweisen – besonders auf den Herdt-Verlag selbst.

Weiters wird gebeten, von direkten Anfragen an das RRZN bezüglich der Handbücher abzusehen, da die zuständigen Mitarbeiter mit der Erstellung und dem Vertrieb genug zu tun haben und deshalb nicht zusätzlich belastet werden sollen. Bei Fragen zu Verfügbarkeit, Preis usw. steht das Service- und Beratungszentrum des ZID (Tel.: 4277-14060, eMail: `helpdesk.zid@univie.ac.at`) zur Verfügung. Aus organisatorischen Gründen können wir nicht alle vom RRZN angebotenen Handbücher vertreiben und bitten Sie daher, unsere Publikationsliste im WWW (`http://www.univie.ac.at/ZID/publi.html`) zu beachten.

*Vera Potuzak* ■

## Personalnachrichten

Mit Freude kann ich diesmal berichten, daß sich der Mitarbeiterstand am ZID um einen „guten alten Bekannten" vermehrt hat: **Markus Reicher**, der bereits in den Jahren 1998/99 erfolgreich in unserer Unix-Gruppe gearbeitet hat, ist Anfang 2003 wieder zu uns zurückgekehrt. Sein reiches Systemwissen und sein Engagement wird dem weiteren Ausbau unserer diversen Unix- und Netzwerk-Services sehr zugute kommen.

Auch **Eva Kößlbacher** ist an der Uni Wien keine Unbekannte: Seit Anfang 2000 leitete sie die Presse- und Öffentlichkeitsarbeit der Universität, hat sich aber auch in EDV-nahen Bereichen der Öffentlichkeitsarbeit, etwa beim Vorlesungsverzeichnis oder der redaktionellen Betreuung der Uni-Homepage, große Verdienste erworben. Seit Februar 2003 ist sie nun am ZID angestellt und kümmert sich um Change Management und Öffentlichkeitsarbeit im UNIVIS-Projekt. Für das UNIVIS-Projekt wird auch der Aufbau eines eigenen Softwareentwicklungs-Teams notwendig: **Mark Guttenbrunner** wird ab März 2003 die Softwareentwicklung im Bereich der Universitätsverwaltung leiten.

Im *Comment 02/1* (März 2002) wurde berichtet, daß **Heinz Pötzl**, der Leiter unseres Referats *Lokale Netze*, einen mehrmonatigen Karenzurlaub angetreten hat, um sich anderen Aufgaben zu widmen. Unsere Hoffnung, daß er anschließend wieder zurückkehren würde, ist nicht in Erfüllung gegangen; er wird uns künftig jedoch als selbständiger Gewerbetreibender bei manchen Projekten unterstützen.

Mit Ende November 2002 hat auch **Roland Zoder** den ZID verlassen, um eine seiner Ausbildung entsprechende Tätigkeit in der Industrie zu übernehmen. Roland Zoder war am ZID maßgeblich in der Softwareentwicklung für das Projekt der Internet-Domainverwaltung tätig. An seine Stelle ist mit Jahresbeginn 2003 **Florian Helmberger** getreten.

Zwei Mitarbeiterinnen sind im Jänner 2003 aus unserem Personalstand ausgeschieden: **Christa Berschlinghofer**, die im Sekretariat des ZID tätig war, und **Hedwig Kettner**, die nach ihrer Tätigkeit in der Telefonvermittlung den lang ersehnten Ruhestand antreten konnte. Den neuen wie auch den scheidenden Mitarbeiterinnen und Mitarbeitern wünschen wir alles Gute für ihren neuen Lebensabschnitt!

*Peter Rastl* ■

# Notizen Notizen Notizen Notizen Notizen

## Alles Fassade

Über den Umbau des NIG

Die Fassaden-Erneuerung des Neuen Institutsgebäudes, die unüberseh- und unüberhörbar voranschreitet, umfaßt auch den Austausch aller Fenster der Außenfassade. Während des Fenstertausches muß der jeweils betroffene Raum etwa zwei Wochen lang gesperrt werden. Leider sind davon auch die PC-Räume im NIG – sofern sie an der Außenseite des Gebäudes liegen – nicht ausgenommen.

In den vom ZID betriebenen PC-Räumen ist der Fenstertausch zu folgenden Terminen geplant:

- **PC-Raum des Instituts für Ethnologie, Kultur- und Sozialanthropologie** (4. Stock): voraussichtlich 2. – 16. April 2003
- **PC-Räume 5 bis 7 des ZID** (1. Stock): voraussichtlich 9. – 23. April 2003
- **PC-Räume 2 bis 4 des ZID** (1. Stock): voraussichtlich 23. April – 7. Mai 2003

Die Kernzeit der Umbauarbeiten umfaßt ca. eine Woche; zusätzlich werden jeweils mehrere Tage vorher und nachher für die Evakuierung bzw. neuerliche Bereitstellung der Geräte benötigt. Bitte verwenden Sie während der Umbauphase auch die PC-Räume an Ihrem Institut bzw. an anderen Universitätsstandorten (siehe `http://www.univie.ac.at/ZID/PC-Raeume/standorte.html`) – und wundern Sie sich nicht, wenn Sie in den nächsten Monaten die im NIG beschäftigten Uni-Mitarbeiter nicht immer an ihren angestammten Plätzen vorfinden.

*Vera Potuzak* ■

## Änderungen bei Uni-internen Massenmailsendungen

Seit der ZID vor rund einem Jahr die Möglichkeit universitätsinterner Massenmailsendungen geschaffen hat (siehe *Comment 02/1*, Seite 24 bzw. `http://www.univie.ac.at/comment/02-1/021_24.html`), erfreut sich dieses Service immer größerer Beliebtheit: Zahlreiche Einrichtungen der Uni Wien haben damit bereits Informationen und Neuigkeiten an verschiedenste Empfängerkreise verschickt. Die gestiegene Popularität zeigte aber auch einige Schwächen dieses Service auf, die vor allem unter den Empfängern für Verwirrungen sorgten – inbesondere wurde es mit der Zeit immer undurchschaubarer, in welche Listen man denn eigentlich eingetragen war. Um die Qualität des Service zu verbessern und den Komfort für die Empfänger zu erhöhen, waren daher einige Änderungen notwendig.

Das neue Konzept, das vom ZID gemeinsam mit dem Rektorenteam ausgearbeitet wurde, sieht vor, daß alle vorhandenen und zukünftigen Listen einer bestimmten Kategorie zugeordnet sind. Diese Kategorien sind einerseits hierarchisch geordnet (universitätsweit, fakultätsweit) und andererseits in ihrer Dringlichkeit gestaffelt (offizielle Aussendungen, allgemeine Nachrichten, Nachrichten von Dritten). Beispiele für solche Kategorien sind etwa *Offizielle Aussendungen des Rektorats*, *Nachrichten des Dekanats* oder *Nachrichten von Dritten mit Genehmigung des Rektorats*.

Als Empfänger wählt man nun nicht mehr einzelne Listen, sondern nur mehr ganze Kategorien. Da deren Anzahl klein ist und nur in Ausnahmefällen neue Kategorien angelegt werden, ist das Service nun für die Empfänger übersichtlicher; darüber hinaus muß man allfällige zukünftige Listen, die einer „unerwünschten" Kategorie angehören, nicht extra abbestellen.

*Lukas Ertl* ■

## Programmierlehrgang nun auch mit JavaScript

Die im letzten Semester erstmalig durchgeführten Vorträge und Workshops zum Thema Programmieren wurden erfreulicherweise mit großem Interesse aufgenommen. Von den beiden angebotenen Programmiersprachen Perl und Visual Basic for Applications (VBA) war Perl etwas stärker nachgefragt. Im Sommersemester 2003 wird wieder der komplette Programmierlehrgang abgehalten, wobei diesmal VBA durch JavaScript ersetzt wird. Gestartet wird mit zwei Vorträgen ***Einführung in das Programmieren – Teil 1 & 2***, die die Grundlagen des Programmierens vermitteln, gefolgt von jeweils einem Vortrag ***Einführung in das Programmieren mit JavaScript*** bzw. ***Einführung in das Programmieren mit Perl***, die auf die einzelnen Programmiersprachen eingehen. Alle vier Vorträge sind frei zugänglich und kostenlos. Wenn sich genügend Interessenten finden, werden weiterführende Workshops angeboten, um die Kenntnisse zu vertiefen und erste Programmier-Praxis zu erwerben.

*Eveline Platzer* ■

## Abschaltung der VM-Rechenanlage

Ende 2002 wurde die VM-Rechenanlage des Zentralen Informatikdienstes endgültig außer Betrieb genommen. Der allgemeine Benutzerbetrieb auf diesem letzten Mainframe-Rechner des ZID war bereits 1999 eingestellt worden, die Umstellung der zahlreichen Applikationen der Universitätsverwaltung nahm dann aber doch noch fast vier Jahre in Anspruch. Mit der Abschaltung ging nun nach beinahe vierzig Jahren das Zeitalter der zentralen Großrechenanlagen an der Uni Wien zu Ende.

*Herbert Stappler* ■

# Neuer Newsserver – auch für die Uni Wien

Der betagte Newsserver der Uni Wien NEWS.UNIVIE.AC.AT wird aufgrund seines fortgeschrittenen Alters und technischer Unzulänglichkeiten am **31. März 2003** außer Betrieb genommen. Seine Nachfolge tritt der Server **USENET.UNIVIE.AC.AT** an, den der Zentrale Informatikdienst in Kooperation mit ACOnet bereits seit einiger Zeit betreibt und der auch von anderen österreichischen Universitäten als News-Lese-Server genutzt werden kann. Der neue Server, der neben deutlich schnellerer Hardware auch eine teilweise längere Artikel-Verfügbarkeit bietet, kann ab sofort von allen Benutzern des bisherigen Newsservers NEWS.UNIVIE.AC.AT verwendet werden.

Vorsicht: Die Klientenprogramme („Newsreader") markieren bereits gelesene Artikel anhand einer vom Server vorgegebenen Artikelnumerierung. Da jeder Newsserver die verfügbaren Artikel unterschiedlich numeriert und der neue Server eine andere Zählart als der bisherige verfolgt, sind für eine erfolgreiche Umstellung des Newsreaders zwei Schritte notwendig:

- Der Servername muß geändert werden, und
- alle subskribierten Newsgruppen müssen einmalig neu subskribiert werden.

Konkret sind folgende Änderungen durchzuführen:

- **Mozilla, Netscape, Outlook, Forte Agent:**
  Legen Sie ein neues News-Konto an und geben Sie dabei als Server `usenet.univie.ac.at` an. Subskribieren Sie für dieses Konto alle Gruppen, die Sie bislang auf NEWS.UNIVIE.AC.AT gelesen haben, und löschen Sie danach das alte News-Konto.
- **Newsreader, die direkt am Mailbox- und Unet-Server verwendet werden:**
  Die Umstellung wird vom Zentralen Informatikdienst für Sie durchgeführt, sofern Sie in den Startup-Skripts Ihrer Shell diesbezüglich nichts geändert haben.
- **tin, slrn und ähnliche Unix-Klienten auf anderen Rechnern:**
  Setzen Sie die Environment-Variable `NNTPSERVER` auf den neuen Servernamen `usenet.univie.ac.at`. Löschen Sie die Datei `~/.newsrc` bzw. `~/.jnewsrc` und subskribieren Sie die gewünschten Gruppen neu.

Bei Fragen zu diversen Newsreadern steht Ihnen das Service- und Beratungszentrum unter `helpdesk.zid@univie.ac.at` zur Verfügung; Wünsche, die die Auswahl der angebotenen Newsgruppen betreffen (siehe `http://www.univie.ac.at/ZID/usenet.html`), richten Sie bitte wie bisher an die Adresse `news-adm@news.univie.ac.at`.

*Markus Reicher* ■

# *Internetzugang von daheim:* Änderungen & Neues

### Mailbox-Rufnummern aufgelassen

Breitband-Internetverbindungen (chello, ADSL, ...) haben dem klassischen Modemzugang längst den Rang abgelaufen. Auch die Wählleitungszugänge der Uni Wien werden nicht mehr so stark genutzt wie noch vor einigen Jahren, sodaß etliche Leitungen abgemeldet werden konnten. Im Zuge dessen hat der ZID die Einwahlnummern für Uni-Mitarbeiter und Studierende vereinheitlicht – für beide Benutzergruppen gelten nun die bisherigen Unet-Einwahlnummern:

- **07189 14012** (Onlinetarif, nur 50 km um Wien)
- **01 40122** (Normaltarif)

Wer außerhalb der Regionalzone Wien wohnt, sollte einen Gratiszugang bei einem Telekom-Anbieter (UTA, Tele2, Telekom Austria, ...) verwenden: Diese bieten einen Onlinetarif für ganz Österreich an, sodaß die Verbindung meist günstiger ist als über die Uni Wien. Nähere Informationen finden Sie auf den Webseiten des jeweiligen Anbieters.

Beachten Sie bitte, daß Sie in diesen Fällen den *Postausgangs(SMTP)*-Server Ihres Providers im eMail-Programm angeben müssen: Das Versenden von Nachrichten über die Mailserver der Uni Wien funktioniert nur dann, wenn Sie sich direkt bei der Uni Wien einwählen.

### Neu: *xDSL@student* von inode

Seit November 2002 existiert neben *uniADSL* ein weiterer Breitband-Internetzugang zum Datennetz der Uni Wien. Das Angebot *xDSL@student* des Internet-Providers inode weist folgende Eckdaten auf:

- **768/128 kBit/s** Datenübertragungsgeschwindigkeit (Down-/Upload)
- **4 GB** Downloadlimit (*Fair Use*)
- **EUR 35,–** monatliche Kosten (inkl. USt)

Da es sich um ein entbündeltes Angebot handelt, ist kein Festnetz-Telefonanschluß notwendig. Wie bei *uniADSL* schützt eine Firewall die *xDSL@student*-Rechner gegen Zugriffe aus dem Internet. Der Support wird von der Firma inode durchgeführt (Tel.: **05 9999-0**). Weitere Infos finden Sie im WWW unter `http://www6.inode.at/produkte/privat/internetzugang/xdsl/xdsl_student_768.html`.

### 4 GB Downloadlimit für *uniADSL*

Das Downloadlimit für *uniADSL* wurde im November 2002 von 2 GB auf 4 GB (*Fair Use*) erhöht. Nach mehreren Warnungen per eMail wird der Zugang nun bei Überschreiten von 5 GB Downloadvolumen bis zum Monatsende gesperrt (dies gilt sowohl für *uniADSL* als auch für *xDSL@student*). ■

# Vom Prototyp zur Serienreife

## Seriendruck mit Word XP

Wieder sind Sie ein paar Jährchen älter geworden. Das Konzept für Ihre Geburtstagseinladung ist fertig, aber jedem einzelnen Ihrer vielen Verwandten und Bekannten einen eigenen Brief zu schreiben, erscheint Ihnen nicht sehr rationell. Bei der Suche nach einer Lösung des Problems stoßen Sie auf die in Word XP integrierte Seriendruckfunktion.

Klingt gut – aber was ist eigentlich ein Serienbrief? Welche Voraussetzungen müssen dafür erfüllt sein? Und vor allem: Wann und wie kann man diese Funktion sinnvoll anwenden? Fragen über Fragen, die im Zuge dieses Artikels beantwortet werden sollen.

## Grundlagen

Die Erstellung eines Serienbriefes empfiehlt sich immer dann, wenn Sie ein Schreiben mit identischem oder zumindest ähnlichem Inhalt an mehrere Empfänger senden wollen. Die einfachste Form davon ist das Verschicken eines Standardtextes an verschiedene Adressaten.

Charakteristisches Merkmal von Serienbriefen ist die Kombination von variablen und fixen Textelementen. Der Text, der für jeden Serienbrief gleich lautet, wird im sogenannten **Hauptdokument** erfaßt und gespeichert. Dieses enthält neben dem Standardtext auch die entsprechenden Seriendruckfelder (Platzhalter), mit deren Hilfe die variablen Textelemente – z.B. Name und Adresse – an den gewünschten Stellen eingefügt werden können.

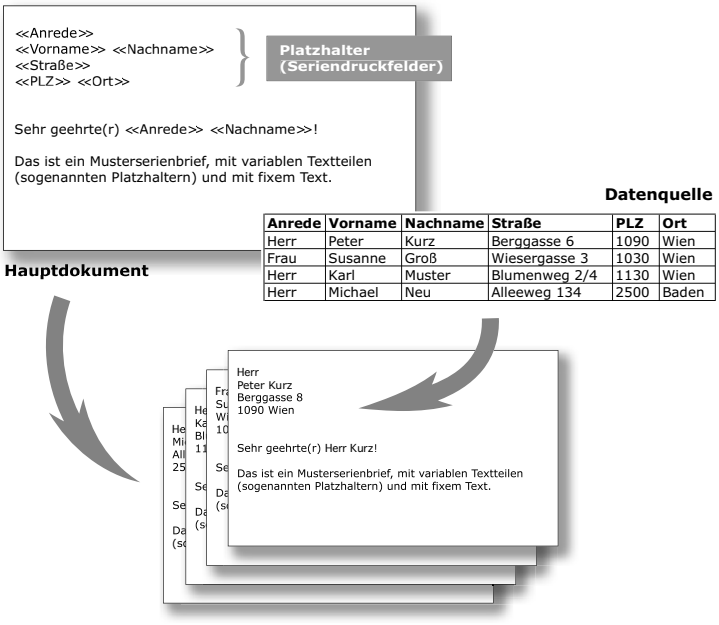



**Abb. 1: Die Seriendruck-Funktion**

Diese variablen Textelemente werden in der sogenannten **Datenquelle** erfaßt und gespeichert. Diese Datenquelle liegt in der Regel datenbankmäßig (tabellarisch) aufbereitet vor – das bedeutet, daß jedem einzelnen Empfänger ein individueller Datensatz zugeordnet ist.

Die **Seriendruckfunktion** sorgt letztendlich dafür, daß diese beiden Dokumenttypen – Hauptdokument und Datenquelle – miteinander verbunden werden. Dabei werden die Seriendruckfelder im Hauptdokument durch die empfängerspezifischen Daten aus der Datenquelle ersetzt. Das Ergebnis sind einzelne Briefe mit gleichem Inhalt, aber z.B. unterschiedlichen Empfängernamen und -adressen.

## Voraussetzungen

### Die Datenquelle

Bevor Sie mit Ihrem Serienbrief beginnen, sollten Sie sich um das benötigte Datenmaterial kümmern. Dazu können Sie entweder im Zuge des Seriendrucks eine neue Datenquelle in Word erstellen oder aber auf bereits vorhandene Datenquellen zugreifen. Geeignet sind hierbei vor allem Datenbestände, die Sie aus dem Outlook-Adreßbuch, aus einer Access- oder Excel-Adreßliste, aber auch aus einer Word-Tabelle beziehen. Bei der Verwendung bereits existierender Datenquellen ist lediglich darauf zu achten, daß die Tabelle richtig strukturiert ist: Word benötigt für die korrekte Abwicklung des Seriendrucks zwei Bestandteile innerhalb der Datenquelle – den Steuersatz und den Datensatzbereich.

Der **Steuersatz** ist die Spaltenbezeichnung (der sogenannte *Header*). Damit wird gekennzeichnet, welche Einträge in welcher Spalte zu finden sind – z.B. Anrede, Vorname, Nachname. Der Steuersatz muß unbedingt in der ersten Zeile der Datenquelle stehen (siehe Abb. 1), da er die einzelnen Felder kennzeichnet und Word ansonsten bei der Verknüpfung von Hauptdokument und Datenquelle eine Fehlermeldung ausgibt.

Der **Datensatzbereich** enthält die entsprechenden empfängerspezifischen Datensätze, wie z.B. die Anrede „Frau“, den Vornamen „Karin“, den Nachnamen „Klein“ und die dazugehörige Adresse.

Falls noch keine Datenquelle vorliegt, sollten Sie anhand der Menge der benötigten Adressen entscheiden, welches Programm Sie für die Erfassung der Daten verwenden. Beachten Sie bitte, daß die Bearbeitung von Word-Tabellen mit zunehmender Größe immer unkomfortabler wird. Bei

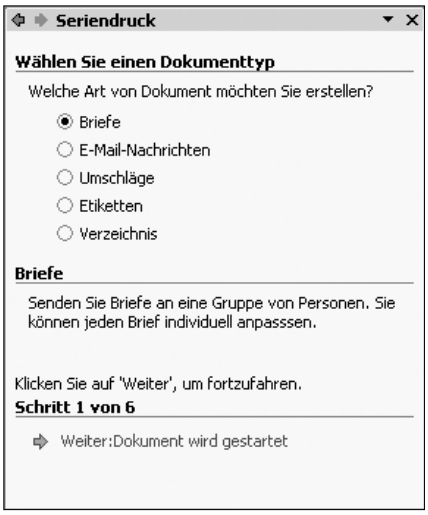



**Abb. 2: Seriendruck-Assistent – Erster Schritt (Anlegen des Hauptdokuments)**

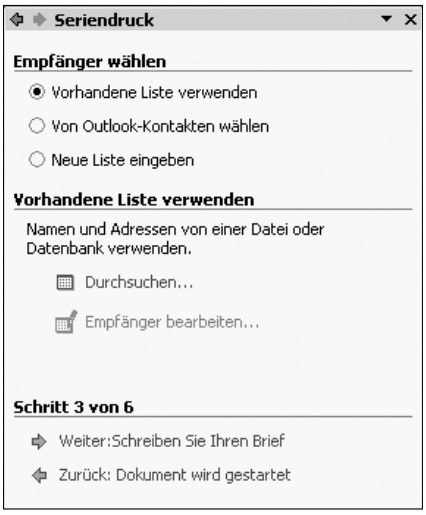



**Abb. 3: Seriendruck-Assistent – Dritter Schritt (Auswählen der Datenquelle)**


**Abb. 4: Dialogfenster *Seriendruckempfänger***

sehr umfangreichem Datenmaterial ist es daher ratsam, auf andere, besser geeignete Programme zurückzugreifen (z.B. Excel oder Access).

### Das Hauptdokument

Das Hauptdokument beinhaltet in erster Linie die für alle Empfänger gleichlautenden Text- bzw. Grafikelemente, die wie gewohnt formatiert werden können. Weiters müssen im Hauptdokument die Seriendruckfelder eingefügt werden, an deren Stelle dann im Zuge des Seriendrucks automatisch die entsprechenden empfängerspezifischen Daten eingesetzt werden (vgl. Abb. 1 auf Seite 17).

## Der Seriendruck-Assistent

Beginnen wir nun mit der Erstellung von Serienbriefen. Rufen Sie dazu aus dem Menü ***Datei*** ein neues Dokument auf und geben Sie alle Textelemente ein, die vor der Empfängeradresse stehen sollen (beispielsweise die Absenderadresse). Positionieren Sie dann die Einfügemarke an der Stelle, wo mit der Eingabe der Empfängeradresse begonnen werden soll, und wählen Sie aus dem Menü ***Extras*** die Option ***Briefe und Sendungen***. Klicken Sie im Untermenü den Eintrag ***Seriendruck-Assistent*** an. Daraufhin wird im *Aufgabenbereich* der erste von sechs Schritten für die Erstellung von Seriendruck-Dokumenten angezeigt (siehe Abb. 2).

Wählen Sie aus der Liste der mittels Seriendruck erstellbaren Dokumente die Option ***Briefe*** aus und klicken Sie in der unteren Hälfte des Aufgabenbereichs auf die Option ***Weiter: Dokument wird gestartet***. Damit gelangen Sie zum zweiten Schritt innerhalb des Seriendruck-Assistenten. Wählen Sie hier die Option ***Aktuelles Dokument verwenden***, um das soeben erstellte Dokument als Hauptdokument zu definieren.

Durch einen Klick auf die Schaltfläche ***Weiter: Empfänger wählen*** kommen Sie zum dritten Schritt, in dem Sie auf die gewünschte Datenquelle zugreifen müssen. Zur Auswahl stehen die Optionen *Vorhandene Liste verwenden*, *Von Outlook-Kontakten wählen* sowie *Neue Liste eingeben*. Wir gehen davon aus, daß bereits eine Datenquelle vorhanden ist – wählen Sie daher die Option ***Vorhandene Liste verwenden***. Im unteren Bereich wird nun ein Symbol mit dem Text ***Durchsuchen*** angezeigt, das Sie anklicken müssen (siehe Abb. 3).

Daraufhin wird das Dialogfenster *Datenquelle auswählen* eingeblendet, in dem Sie die gewünschte Datei auswählen können. Sie erhalten ein Dialogfenster mit dem Namen *Seriendruckempfänger*, das den Inhalt der gewählten Datenquelle anzeigt (siehe Abb. 4).

Sie können in diesem Dialogfenster bereits einzelne Personen aus dem Empfängerkreis ausschließen, indem Sie das Hakerl vor dem jeweiligen Datensatz durch Anklicken entfernen. Ebenso ist es möglich, mit Hilfe der Filtermöglichkeit den Empfängerkreis anhand bestimmter Kriterien einzuschränken. Klicken Sie dazu auf den Pfeil neben der Spaltenüberschrift und wählen Sie das Filterkriterium durch Anklicken aus. Daraufhin werden nur noch jene Datensätze angezeigt, die dem gewählten Filterkriterium entsprechen (z.B. *Ort = Wien*). Sobald Sie die gewünschte Auswahl getroffen haben, klicken Sie auf die Schaltfläche ***OK***. Sie kehren damit zum Seriendruck-Assistenten zurück, wo Sie nun auf die Option ***Weiter: Schreiben Sie Ihren Brief*** klicken müssen.

Im folgenden vierten Schritt werden Sie aufgefordert, Ihr Hauptdokument zu vervollständigen und an den entsprechenden Stellen mit Hilfe verschiedener Standardelemente die gewünschten Seriendruckfelder (Platzhalter) einzufügen (siehe Abb. 5).

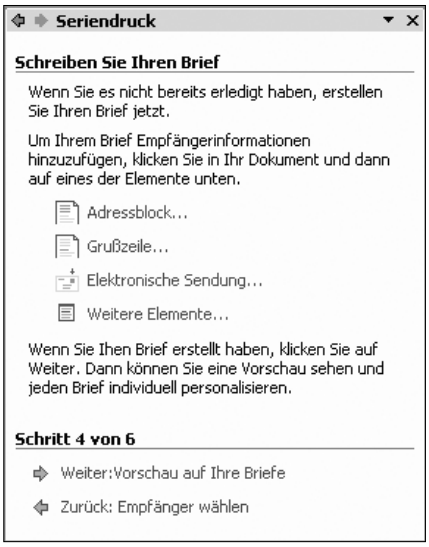



**Abb. 5: Seriendruck-Assistent – Vierter Schritt (Hauptdokument bearbeiten)**

Empfehlenswert ist hier beispielsweise die Option *Adressblock*. Wenn Sie diese Option anklicken, wird das Dialogfenster ***Adressblock einfügen*** angezeigt, das eine Auswahl unterschiedlicher Darstellungen für die Empfängeradresse anbietet (siehe Abb. 6). Beachten Sie jedoch, daß Word hierbei auf standardisierte Seriendruckfelder zugreift, die oft mit den in Ihrer Datenquelle verwendeten Bezeichnungen für die einzelnen Spalten nicht übereinstimmen. Klicken Sie daher zwecks Überprüfung und Korrektur der Seriendruckfelder auf die Schaltfläche ***Felder wählen***. Es erscheint nun das Dialogfenster *Übereinstimmende Felder festlegen* (siehe Abb. 7).

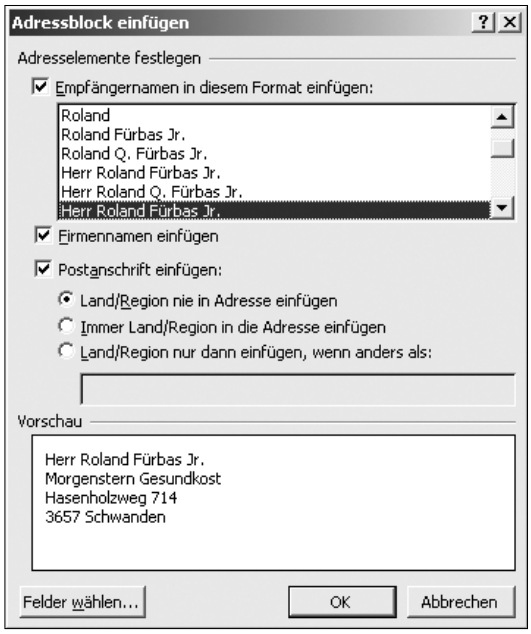



**Abb. 6: Dialogfenster *Adressblock einfügen***

Hier finden Sie auf der linken Seite eine Auflistung der Standard-Adreßfelder von Word und rechts daneben *Drop-Down*-Listen, die Sie durch Anklicken des Listenpfeils öffnen können. Diese Listen enthalten alle in Ihrer Datenquelle verwendeten Spaltenbezeichnungen. Durch Anklicken der gewünschten Spaltenbezeichnung können Sie diese dem jeweiligen Adreßfeld zuordnen. Beispielsweise wählen Sie hier für das Adreßfeld *Name* die Spaltenbezeichnung ***Nachname***. Wiederholen Sie den Vorgang für alle Felder, die Sie Ihrer Datenquelle entsprechend modifizieren müssen. Falls es für ein Adreßfeld keinen passenden Eintrag in Ihrer Datenquelle gibt, wählen Sie die Option (***nicht verfügbar***). Klicken Sie anschließend auf die Schaltfläche ***OK***, um zum Seriendruck-Assistenten zurückzukehren. In Ihrem Hauptdokument wird nun das Seriendruckfeld *AdressBlock* angezeigt.

Wenn Sie weitere Seriendruckfelder benötigen (z.B. für die Anrede), müssen Sie im Seriendruck-Assistenten auf die Option ***Weitere Elemente*** klicken. Sie erhalten daraufhin wiederum ein Dialogfenster, in dem Sie die Wahl zwischen der Anzeige der standardisierten Elemente (*Adressfelder*) oder Ihrer *Datenbankfelder* haben. Sobald Sie die Option ***Datenbankfelder*** auswählen, erscheinen unterhalb in der Liste *Felder* die Spaltenbezeichnungen, die Sie in Ihrer Datenquelle verwenden. Durch Anklicken des gewünschten Feldes und anschließendes Anklicken der Schaltfläche ***Einfügen*** wird das gewählte Feld an der Position der Einfügemarke in das Hauptdokument integriert (noch schneller geht es mit einem Doppelklick auf das gewünschte Seriendruckfeld).

Haben Sie ein Seriendruckfeld irrtümlich an der falschen Stelle oder doppelt eingefügt, können Sie es mit Hilfe der Taste *Entf* löschen. Beim ersten Drücken der Taste ***Entf*** wird das Feld allerdings nur markiert; um es auch tatsächlich zu löschen, müssen Sie die Taste ***Entf*** noch ein zweites Mal drücken.

Falls Sie feststellen, daß Sie beim Einfügen der Seriendruckfelder in das Hauptdokument eine falsche Auswahl getroffen haben, können Sie dies durch Anklicken der Option ***Zurück*** im Seriendruck-Assistenten korrigieren.

Sobald Sie im Seriendruck-Assistenten die Option ***Weiter: Vorschau auf Ihre Briefe*** wählen, gelangen Sie zum vorletzten und wichtigsten Schritt bei der Erstellung Ihres Serienbriefs: der Vorschau (siehe Abb. 8 auf Seite 20).

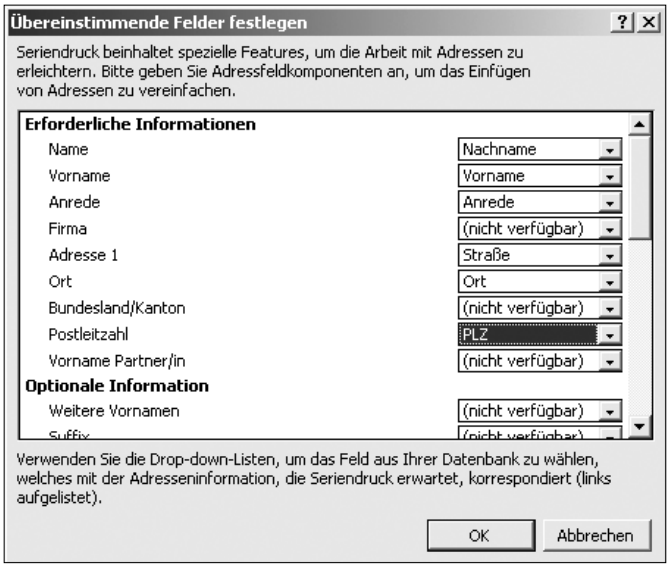



**Abb. 7: Dialogfenster *Übereinstimmende Felder festlegen***

Abgesehen von der Möglichkeit, die im Hauptdokument eingefügten Seriendruckfelder durch Echtdaten zu ersetzen (durch Anklicken der Schaltflächen << bzw. >> neben dem Eintrag *Empfänger*), stehen Ihnen hier umfangreiche Korrekturmöglichkeiten zur Verfügung. Beispielsweise können Sie mit Hilfe der Schaltfläche ***Empfänger ausschließen*** den aktuell im Dokument angezeigten Datensatz vom Seriendruck ausschließen. Ebenso ist es möglich, durch Anklicken der Option ***Empfängerliste bearbeiten*** direkt auf das Dialogfenster *Seriendruckempfänger* zuzugreifen und dort durch Anklicken der Schaltfläche *Bearbeiten* den gewählten Datensatz zu korrigieren.

Sobald Sie mit dem Ergebnis zufrieden sind, klicken Sie auf ***Weiter: Seriendruck beenden***, um zum letzten Schritt zu gelangen. Die einzelnen Serienbriefe können nun entweder durch Anklicken der Option ***Drucken*** im Bereich *Zusammenführen* direkt an den Drucker geschickt oder mit Hilfe der Option ***Individuelle Briefe bearbeiten*** in eine neue Word-Datei mit dem Namen *Serienbriefe1* ausgegeben werden. In der Regel empfiehlt sich die zweite Variante, weil Sie damit das Seriendruck-Ergebnis vor dem endgültigen Druck noch auf dem Bildschirm überprüfen bzw. bei einzelnen Empfängern den Inhalt geringfügig abändern können. In beiden Fällen erhalten Sie ein Dialogfenster, mit dem Sie die (Druck-)Ausgabe bezüglich des Umfangs einschränken können. Zur Auswahl stehen die Optionen *Alle*, *Aktueller Datensatz* oder *Von – Bis*.

Haben Sie die erste Option *Drucken* gewählt, so ist Ihr Seriendruck hiermit abgeschlossen. Haben Sie hingegen die zweite Option *Individuelle Briefe bearbeiten* gewählt und das Seriendruck-Ergebnis auf dem Bildschirm überprüft, dann müssen Sie im Menü ***Datei*** die Option ***Drucken*** wählen (bzw. die Schaltfläche ***Drucken*** anklicken), damit die einzelnen Serienbriefe in weiterer Folge auch wirklich ausgedruckt werden.

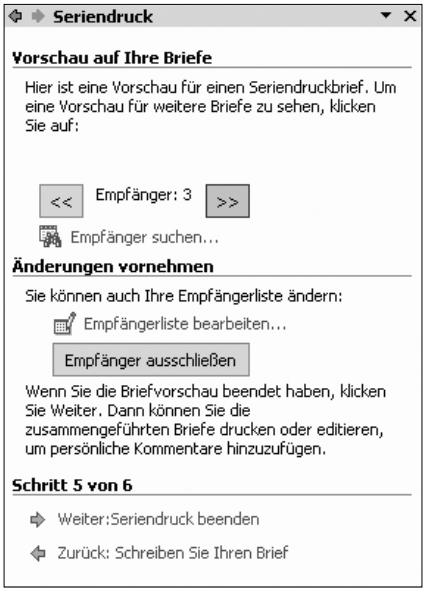



**Abb. 8: Seriendruck-Assistent – Fünfter Schritt (Vorschau)**

Beachten Sie, daß die Datenquelle unbedingt gespeichert werden sollte, damit Sie jederzeit auf Ihr Adreßmaterial zugreifen können. Vergessen Sie bitte auch nicht auf die Wartung Ihrer Datenquelle, um sicherzustellen, daß keine veralteten Datensätze vorliegen!

Darüber hinaus ist es meistens sinnvoll, auch das Hauptdokument zu speichern – vor allem wenn dieses in periodischen Abständen immer wieder verwendet wird. Sie ersparen sich dadurch in weiterer Folge die Neuerstellung des Dokuments, die Zuordnung der verwendeten Datenquelle und die Positionierung der Seriendruckfelder.

## Bedingungsfelder

Soweit funktioniert der Seriendruck ja reibungslos – die Tücke liegt wie immer im Detail. Was, wenn Sie statt der Anrede „Sehr geehrte Damen und Herren!“ eine persönliche Anrede wie beispielsweise „Sehr geehrter Herr Kurz!“ für die einzelnen Empfänger verwenden möchten? Problematisch ist die persönliche Anrede deshalb, weil Sie in der Datenquelle vermutlich nicht nur Herren erfaßt haben und die korrekte Anrede für Herren „Sehr geehrter Herr …“ und für Damen „Sehr geehrte Frau …“ lautet. Um das Problem zu lösen, müssen Sie sich etwas näher mit den verschiedenen Funktionen des Seriendrucks beschäftigen – insbesondere mit den sogenannten Bedingungsfeldern.

Für das Arbeiten mit Bedingungsfeldern benötigen Sie die Symbolleiste für den Seriendruck. Klicken Sie dazu auf das Menü ***Ansicht*** und die Option ***Symbolleisten***. Aus dem Untermenü wählen Sie die Symbolleiste ***Seriendruck***.

In dieser Symbolleiste finden Sie eine Schaltfläche für ***Bedingungsfeld einfügen***. Wenn Sie diese Schaltfläche anklicken, öffnet sich eine Liste, die alle möglichen Bedingungen enthält. Für unser konkretes Problem müssen Sie eine Bedingung vom Typ *Wenn-Dann-Sonst* definieren. Weiters ist es wichtig, daß innerhalb der Datenquelle eine Spalte existiert, die eine eindeutige Unterscheidung zwischen Herren und Damen ermöglicht. In unserer Datenquelle ist das die

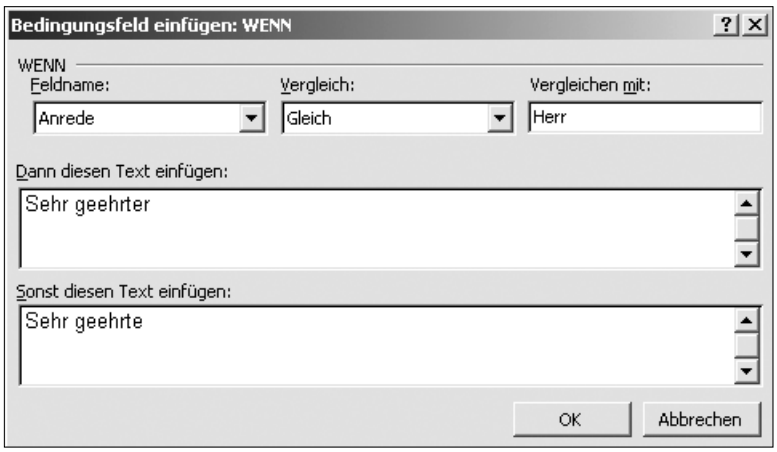



**Abb. 9: Dialogfenster *Bedingungsfeld einfügen: WENN***

Spalte *Anrede* mit den Einträgen *Herr* bzw. *Frau*. Beachten Sie bitte die Position Ihrer Einfügemarke, damit die Bedingung auch an der richtigen Stelle im Hauptdokument definiert wird.

Sobald Sie auf den Eintrag ***Wenn-Dann-Sonst*** geklickt haben, erscheint das entsprechende Dialogfenster (siehe Abb. 9 auf Seite 20). Wählen Sie nun aus der Liste *Feldname* die Spaltenbezeichnung aus, die jene Kriterien enthält, an die die beiden nachfolgenden Bedingungen geknüpft sind (für unser Beispiel ist das die Spalte ***Anrede***). Aus der Liste *Vergleich* wählen Sie die Option ***Gleich*** aus. Nun müssen Sie nur noch den entsprechenden Vergleich im Eingabefeld *Vergleichen mit* eintragen (in unserem Beispiel ist das der Eintrag ***Herr***).

Als nächstes müssen Sie die *Dann*-Bedingung eingeben: Wenn in der Spalte *Anrede* der Eintrag *Herr* lautet, dann soll folgender Text eingefügt werden: ***Sehr geehrter***. Zuletzt ist noch die *Sonst*-Bedingung zu definieren: Wenn in der Spalte *Anrede* ein anderer Eintrag als *Herr* (in unserem Beispiel ist dies der Eintrag *Frau*) aufscheint, ist folgendes einzugeben: ***Sehr geehrte***. Klicken Sie nun noch auf ***OK*** – damit ist Ihre Bedingung fertig definiert.

Da Bedingungen zur Gruppe der Felder gehören, können Sie die dahinterstehende Feldfunktion sichtbar machen, indem Sie die Einfügemarke innerhalb des Feldes positionieren und die Tastenkombination ***Shift + F9*** drücken. Alternativ dazu können Sie das entsprechende Feld auch mit der rechten Maustaste anklicken; daraufhin wird das Kontextmenü eingeblendet, aus dem Sie den Eintrag ***Feldfunktionen ein/aus*** wählen. In beiden Fällen erhalten Sie folgendes Ergebnis:

```
{ IF { MERGEFIELD Anrede } = "Herr" "Sehr
geehrter" "Sehr geehrte" }
```

Sie finden hier also (jeweils unter Hochkomma) die Angaben, die Sie in den jeweiligen Eingabefeldern definiert haben, und können diese im Bedarfsfall jederzeit korrigieren. Um die Feldfunktionen wieder auszublenden, drücken Sie erneut die Tastenkombination ***Shift + F9*** bzw. wählen aus dem Kontextmenü den entsprechenden Eintrag.

## Serienreife eMail-Nachrichten

Mittlerweile können nicht nur Standardbriefe mittels Seriendruckfunktion komfortabel erstellt und verschickt werden, sondern auch eMail-Nachrichten. Die Voraussetzungen und die Arbeitsschritte zur Erstellung sind dabei nahezu identisch mit denen für Serienbriefe. Zu beachten ist aber, daß innerhalb der Datenquelle eine eigene Spalte für die eMail-Adresse vorhanden sein muß.

Im Gegensatz zur Erstellung von Serienbriefen müssen Sie weiters im ersten Schritt des Seriendruck-Assistenten die Option ***E-Mail-Nachrichten*** auswählen. Die folgenden

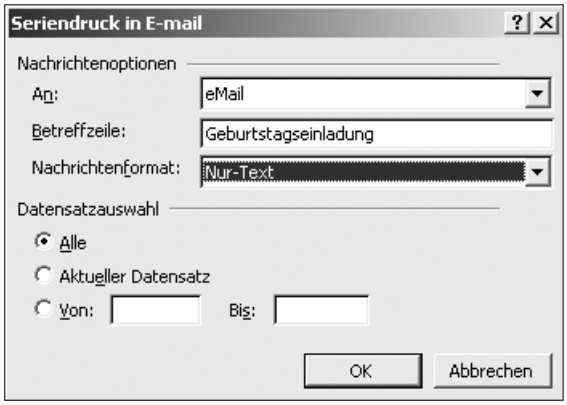



**Abb. 10: Dialogfenster *Seriendruck in E-mail***

vier Schritte bringen keine Änderungen. Beim letzten Schritt des Seriendruck-Assistenten müssen Sie im Bereich *Zusammenführen* die Option ***E-Mail*** anklicken – eine andere Möglichkeit ist ohnehin nicht vorgesehen – und erhalten daraufhin ein Dialogfenster mit dem Titel *Seriendruck in E-mail* (siehe Abb. 10).

Wählen Sie aus der Liste *An* die Spaltenbezeichnung, die Ihre eMail-Adressen enthält (z.B. ***eMail*** ). In das Eingabefeld *Betreffzeile* tragen Sie den gewünschten Betreff ein, zum Beispiel ***Geburtstagseinladung***. Für das Verschicken der Nachricht stehen drei Optionen zur Verfügung, die Sie aus der Liste *Nachrichtenformat* auswählen können:

- Die Option *Anlage* sendet das Word-Dokument mit Ihrer Einladung als Attachment (Dateianhang) per eMail. Das ist nur dann sinnvoll, wenn Sie sicher sind, daß alle Empfänger dieses Dateiformat öffnen können, und wenn das Dokument nicht allzu viel Speicherplatz benötigt.

- Mit der Option ***Nur-Text*** werden sämtliche Formatierungen und Grafiken des Dokuments ignoriert und nur der reine Text der Einladung als eMail-Nachricht an die jeweiligen Empfänger geschickt. Im allgemeinen ist dies das für den Versand von eMail geeignetste Format.

- Die Option *HTML* wandelt Ihre Einladung in eine HTML-Datei um (dabei werden sowohl die eingebundenen Grafiken als auch die Textformatierungen des Dokuments übernommen) und verschickt diese per eMail. eMail-Nachrichten im HTML-Format sehen im Idealfall ansprechender aus als reine Text-Dateien; falls allerdings im Mailprogramm des Empfängers die HTML-Funktion nicht integriert oder deaktiviert ist, erhält dieser die Nachricht als HTML-Quelltext – also weitgehend unleserlich.

Der Versand der Nachrichten an die einzelnen Empfänger erfolgt via MS-Outlook ohne weitere Mitteilungen oder Hinweise des Programms. Um zu überprüfen, ob das Serien-Mailing auch funktioniert hat, sollten Sie daher anschließend einen Blick in den Ordner *Gesendete Objekte* von MS-Outlook werfen.

*Eva & Michel Birnbacher* ■

# DESKTOPS IN DER FERNE:
## Windows-Terminalservices

Windows-Terminalservices bieten die Möglichkeit, einzelne Windows-Programme oder das komplette Windows-Betriebssystem nicht am eigenen Rechner (der natürlich ebenfalls ein Betriebssystem benötigt), sondern auf einem Server laufen zu lassen. Am Arbeitsplatzrechner befindet sich nur ein relativ kleines Programm, der sogenannte *Terminalservices-Klient*, der bei aktuellen Windows-Systemen bereits standardmäßig integriert ist (z.B. die *Remotedesktopverbindung* in Windows XP). Der Klient leitet einerseits die Tastatureingaben und die Mausbewegungen bzw. -klicks zum Server weiter; andererseits übernimmt er die Bildschirmausgabe vom Server und stellt sie – als Fenster oder im Vollbildmodus – am lokalen Monitor dar (siehe Abb. 1). Aus der Sicht des Benutzers scheint das Programm am eigenen Computer zu laufen, und es besteht jederzeit die Möglichkeit, zwischen der Terminalserver-Ansicht und der des lokalen Rechners zu wechseln.

Windows-Terminalservices bieten folgende Vorteile:

- Ein Benutzer kann über Programme bzw. Windows-Versionen verfügen, die nicht auf seinem Rechner installiert sind (*Remote*-Zugriff), und muß dazu nicht einmal einen Windows-PC verwenden.

- Da der Terminalservices-Klient kaum Ansprüche an den lokalen Rechner stellt, können auch Applikationen mit hohen Ressourcen-Anforderungen auf älteren oder weniger gut ausgestatteten Geräten benutzt werden.

- Der Server, auf dem die Terminalservices laufen, kann viele Benutzer gleichzeitig bedienen.

- Die bereitgestellten Programme können zentral am Server gewartet werden und müssen nicht auf die einzelnen lokalen Rechner verteilt werden.

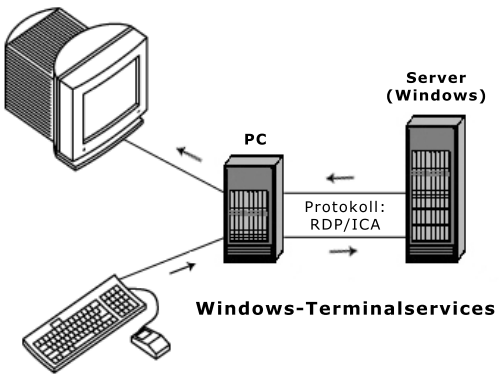



**Abb. 1: Tastatur- und Mauseingaben am lokalen Rechner werden zum Terminalserver übertragen, der die Bildschirmausgabe zurückliefert**

Darüber hinaus hat man folgende Möglichkeiten:

- **Zugriff auf lokale Laufwerke**
  Obwohl die Anwendungen in einer Terminalservices-Sitzung auf dem Server laufen, kann man auch auf Daten am lokalen Rechner zugreifen, da im Windows Explorer neben den Laufwerken des Servers auch alle lokalen Laufwerke (Disketten-, CD-ROM-Laufwerk und Festplatten) sichtbar sind.

- **Zugriff auf lokale Drucker**
  Der lokale Drucker wird bei der Verbindung zu einem Terminalserver automatisch der Liste aller am Server verfügbaren Drucker hinzugefügt. Möchte man Dokumente auf einem lokal angeschlossenen Drucker ausgeben, muß dieser nur aus der Liste ausgewählt werden.

- **Kopieren und Einfügen zwischen Terminalserver und lokalem Rechner**
  Möchte man die Zwischenablage oder Dateien übertragen, genügt es, den jeweiligen Text, das Bild oder die gewünschten Dateien im Kontextmenü (rechte Maustaste) zu kopieren, auf die Ansicht des anderen Computers zu wechseln und die Daten wieder einzufügen.

Verwendet man auf dem Terminalserver Netzwerkdienste, muß man sich der Tatsache bewußt sein, daß man dessen Netzwerkregeln unterliegt. Ist man z.B. am lokalen Computer berechtigt, auf bestimmte Internetseiten zuzugreifen, ist dies bei Verwendung eines Webbrowsers auf dem Server eventuell nicht möglich. Auch Firewall-Einstellungen sind von dieser Regelung betroffen.

## Remote, aber wie?

Im aktuellen ***Windows Server*** sind die Terminalservices bereits integriert. Hier wird zur Kommunikation zwischen Server und Klient und zur Übertragung der Benutzer-Daten RDP (*Remote Desktop Protocol*) in der Version 5.1 verwendet. Bei den aktuellen Windows-Plattformen ist ein Klient bereits enthalten. Mit dem kostenlosen *rdesktop* steht für die meisten Unix-Plattformen unter X-Windows ebenfalls ein Klient zur Verfügung, und selbst für MacOS X existiert ein Microsoft-Klient. Falls nicht anders angegeben, beziehen sich die in diesem Artikel vorgestellten Funktionen auf RDP 5.1, das unter Windows XP und dem künftigen Windows Server 2003 zum Einsatz kommt.

Von der Firma Citrix stammt das Produkt ***MetaFrame XP***, das einen bereits vorhandenen Windows Server voraussetzt. Die Citrix-Produkte verwenden als Protokoll ICA (*Independent Computing Architecture*), das im wesentlichen dieselbe

Funktion wie RDP besitzt. Allerdings waren ICA-Klienten schon viel früher für verschiedene Plattformen verfügbar, und auch Features wie beispielsweise hohe Farbtiefe, Umleiten der seriellen Schnittstelle (*COM-Port*) und Audioausgabe wurden wesentlich früher implementiert als bei RDP.

MetaFrame XP bietet im Vergleich mit Microsofts Windows Server einige zusätzliche Funktionen:

- **Lastverteilung über mehrere Server**
  Gesetzt den Fall, es existieren zwei oder mehr Windows-Terminalserver und man möchte für 50 Benutzer in öffentlichen PC-Räumen MS-Office zur Verfügung stellen, so ist es auch ohne MetaFrame-Erweiterung möglich, die Benutzer auf mehrere Server zu verteilen. Dies geschieht jedoch eher zufällig – ist also aus irgendeinem Grund ein beteiligter Server schon sehr ausgelastet, bekommt er weiterhin Benutzer zugewiesen. Mit der MetaFrame-Erweiterung (im folgenden MetaFrame-Server genannt) wird die Verteilung der Benutzersitzungen jedoch der Auslastung der einzelnen Server angepaßt. Damit ist der Aufbau einer *Server-Farm* möglich, die im Gegensatz zu einer Server-Farm unter Windows auch die Anzahl der Instanzen des Programms, die CPU- und Speicherbelegung und die maximale Netzwerkbandbreite berücksichtigt.

- **Veröffentlichen von Anwendungen unabhängig vom Desktop des Servers**
  Unter Windows-Terminalserver (d.h. via RDP) ist nur eine Verbindung zum Desktop des Terminalservers, jedoch nicht zu einer einzelnen Anwendung möglich – das gewünschte Programm kann also erst dann ausgewählt werden, wenn die Verbindung mit dem Server bereits besteht. Die auf einem MetaFrame-Server verfügbaren Anwendungen scheinen hingegen unabhängig von der Verbindung zum Server auf dem Desktop des PCs auf und sind von Verknüpfungen mit lokalen Anwendungen nicht zu unterscheiden.

- **Rahmenlose Fenster**
  Nachdem eine Sitzung mit einem MetaFrame-Server zustande gekommen ist, wird nur die Anwendung selbst angezeigt, ohne Hinweis darauf, daß es sich dabei um ein Netzwerk-Service handelt (also ohne den für Terminalservices typischen Rahmen bei der Ansicht eines Desktop-Ausschnitts). Die Anwendung erscheint so, als ob sie direkt auf dem lokalen Rechner laufen würde. Es könnte aber auch statt einer einzelnen Anwendung der gesamte Desktop zur Verfügung gestellt werden.

- **Lokales Drucken von allen Windows-Plattformen**
  Im Gegensatz zu RDP-Klienten ist das Drucken auf lokalen Druckern auch von älteren Windows-Plattformen aus möglich, wenn die entsprechenden Treiber auf dem Server unter MetaFrame zur Verfügung gestellt werden.

- **Integration in WWW-Umgebungen**
  Der Verbindungsaufbau zu einem MetaFrame-Server kann auch durch einen Hyperlink gestartet werden.

- **Unix-Integration**
  Die *UNIX Integration Services* (eine auf MetaFrame aufbauende Erweiterung) vermögen die Bildschirmausgabe eines MetaFrame-Servers auch via X11-Protokoll an einen beliebigen X-Server zu schicken.

## Einsatz am ZID

Am ZID werden Terminalservices sowohl mit als auch ohne MetaFrame-Erweiterung eingesetzt. Für Office- und Acrobat-Kurse steht ein einzelner Server unter Windows 2000 Terminal Services zur Verfügung. Es handelt sich dabei um eine Pentium III-Doppelprozessormaschine mit je 1 GHz und insgesamt 1,6 GB RAM, was für rund 30 bis 40 Office-Benutzer ausreichend ist.

Wie im Artikel *Software, Everywhere...* beschrieben (siehe *Comment 02/1*, Seite 20 bzw. `http://www.univie.ac.at/comment/02-1/021_20.html`), bringt die Fernwartung einer großen Anzahl von PCs einiges an Problemen mit sich, sodaß es an Instituten nicht möglich ist, individuelle Software für Lehrveranstaltungen in den PC-Räumen zu installieren. Dieses Problem läßt sich mit Hilfe der Terminalservices umgehen, da die benötigte Software, sofern sie in einer Terminalserver-Umgebung läuft, unabhängig vom Software-Angebot der PC-Räume verwendet werden kann. Wird an einem Institut ein Terminalserver betrieben, stellt der Zentrale Informatikdienst bei Bedarf in den betreffenden PC-Räumen die Terminalservices-Klienten zur Verfügung.

Den größten Einsatz am ZID erfahren die Terminalservices bei den Datenbank-Services der Universitätsbibliothek. Diese starteten 1998 mit einem Server, auf dem Citrix WinFrame unter Windows NT 3.51 verwendet wurde, das später durch Citrix MetaFrame 1.8 unter Windows NT 4.0 Terminal Server Edition abgelöst wurde. Nach der Übernahme der Datenbank-Services durch den ZID erfolgte schließlich die Umstellung auf Windows 2000 mit MetaFrame XP. Die Funktionen des ICA-Protokolls waren insofern unabdingbar, als sie von Anfang an das lokale Speichern von Ergebnissen einer Datenbankrecherche ermöglichten; darüber hinaus muß dafür nur das (kostenlose) ICA-Plugin für den verwendeten Webbrowser installiert werden. Mittlerweile befindet sich hinter den Kulissen ein MetaFrame XP-Cluster aus sieben Servern, die unter Windows 2000 Server laufen. Der Grund für diese Aufteilung liegt nicht nur in der Last durch viele Benutzer, sondern auch in der großen Anzahl verschiedener Retrievalprogramme und den daraus resultierenden Datenmengen.

## Tips für Systemadministratoren

Für den Systemadministrator eines aktuellen Windows-Servers ist es relativ leicht, die Terminalservices zu aktivieren, wobei jedoch folgende Punkte beachtet werden sollten:

- **Hardwareausstattung**
  Da die Rechen- und Dateiverwaltungsarbeit aller ver-

bundenen Benutzer serverseitig abläuft, ist eine stärkere Hardware (beispielsweise ein bis zwei schnelle CPUs und deutlich mehr Hauptspeicher) als bei einem Arbeitsplatzrechner vonnöten.

- **Zeitpunkt der Aktivierung**
  Die Terminalservices müssen *vor* der Installation von Programmen aktiviert werden: Um die bei der Programminstallation vorgenommenen Standardeinstellungen allen Benutzern zugänglich zu machen, werden diese in einen benutzerunabhängigen Bereich der *Registry* (Windows-Konfigurationsdatenbank) umgeleitet. Programme, die bereits vor der Aktivierung der Terminalservices installiert wurden, müssen daher nach der erfolgten Aktivierung neu installiert werden.

- **Softwareinstallation**
  Ein Großteil der aktuellen Software funktioniert auch auf einem Terminalserver. Bei 16-Bit-Programmen kann es jedoch insofern zu Problemen kommen, als diese oft auf Systembereiche zugreifen müssen, die seit Windows 2000 standardmäßig geschützt sind. Auch die früheren Office-Pakete können bei der Installation auf einem Terminalserver Probleme bereiten. Mit entsprechenden Anpassungen des Systems ist es aber meist möglich, die jeweilige Software zu installieren.

- **Benutzerverwaltung**
  Bei einem einzelnen Server müssen natürlich auch die Benutzerkonten zusätzlich angelegt und verwaltet werden – außer wenn eine Windows-Domäne vorhanden ist oder wenn man sich für die Verwendung anonymer Benutzerkonten entschließt.

- **Filesystem und Security**
  Falls das Vertrauen in die Umsicht der Benutzer nicht ausreichend gegeben ist, lohnt es sich, eine grundlegende Absicherung des Filesystems und eine Einschränkung der Benutzerrechte durchzuführen, da einige sensible Teile des Betriebssystems jedem Benutzer zugänglich (sprich: zerstörbar) sind. Das Ausmaß der Einschränkungen ist stark von den Anforderungen des geplanten Einsatzgebiets abhängig. Grundsätzlich sollte man möglichst wenig Schreibrechte auf Systemverzeichnisse und (im Idealfall) keine auf Programmverzeichnisse gestatten.

- **Policies**
  Um den Benutzern den Zugriff auf verschiedene Systembereiche zu untersagen (oder zumindest zu erschweren), muß man ihre diesbezüglichen Rechte einschränken. Dies ist zwar in einer Active Directory-Domäne relativ leicht zu lösen (durch Anwenden von Policies auf Organisationseinheiten – engl. *Organizational Units* –, in denen sich die Benutzer befinden), jedoch mit einem erheblichen administrativen und finanziellen Mehraufwand verbunden. Auch auf einem einzelnen Server ist es möglich, die Benutzer durch die lokalen Richtlinien mit den gleichen Optionen zu beschränken wie in einer Active Directory-Domäne. Der kleine Nachteil daran ist, daß davon auch der Systemadministrator betroffen ist, was dieser aber durch ein Login-Skript beheben kann: Da Policies nichts anderes sind als Registry-Einträge, kann man sie durch das Skript wieder entfernen, was unter Zuhilfenahme der für die jeweilige Policy zuständigen ADM-Datei (zu finden in `%windir%\inf`) mit etwas Tüftelei zu bewerkstelligen ist.

- **Drucken**
  Für die Druckausgabe ist es zwar prinzipiell möglich, einen am PC installierten Drucker über den Server anzusprechen; es muß sich beim PC-Betriebssystem aber zumindest um Windows 2000 handeln. Als Alternative kann vom Administrator ein Druckserver direkt am Terminalserver installiert werden.

- **Zugriff auf lokale Laufwerke**
  Dem Benutzer werden zwar alle lokalen Laufwerke automatisch zur Verfügung gestellt, sie sind aber keinen Laufwerksbuchstaben zugeordnet. Um den Zugriff zu erleichtern, ist es sinnvoll, wenn der Systemadministrator dies in den Login-Skripts berücksichtigt.

- **Citrix MetaFrame**
  Benötigt man Funktionen der MetaFrame-Erweiterung, darf man nicht vergessen, daß diese neben den zusätzlichen Funktionen auch einen höheren Implementierungsaufwand und höhere Kosten mit sich bringt.

- **Lizenzierung**
  Zwar sind die Klienten sowohl für die Windows-eigenen Terminalservices als auch für MetaFrame XP kostenlos, die Zugriffslizenzen auf den Server jedoch nicht. Für verschiedene Klienten-/Server-Kombinationen sind unterschiedliche Lizenzierungsmodelle vorgesehen, die an die Art der Installation angepaßt werden müssen. Die Lizenzen für RDP sind nur bei den aktuellen Klienten ab Windows 2000 inkludiert (was sich mit der Veröffentlichung von Windows Server 2003 jedoch noch ändern kann), für ältere Klienten betragen die Lizenzkosten jeweils € 5. Nähere Informationen zu Terminalserver-Zugriffslizenzen (*Client Access Licenses*) an der Uni Wien erhalten Sie bei Peter Wienerroither (Tel.: 4277-14138).

  Citrix-Produkte hingegen sind nicht im Rahmen der Standardsoftware, sondern nur im Handel erhältlich. Für universitäre Einrichtungen betragen die Kosten für eine MetaFrame XP-Lizenz inklusive fünf Benutzerlizenzen € 2157 und für fünf zusätzliche Lizenzen weitere € 1354. Darüber hinaus müssen auch noch Lizenzen für Windows-Terminalservices erworben werden.

So hilfreich ein Terminalserver in bestimmten Situationen auch sein mag – der Planungs-, Installations- und Wartungsaufwand ist auf jeden Fall zu bedenken: Abhängig von den Vorkenntnissen sind für eine einfache Installation ein bis zwei Wochen, für eine ausgeklügeltere Konfiguration weitere zwei bis drei Wochen zu veranschlagen.

*Ralph Staudigl* ■

# Design in InDesign

## Ein Layoutprogramm unter der Lupe

Das Layoutprogramm InDesign der Firma Adobe ist eines der aktuelleren Werkzeuge zum Erstellen von optisch anspruchsvollen Publikationen (und für Uni-Mitarbeiter als Standardsoftware erhältlich; siehe `http://www.univie.ac.at/zid-swd/`). Gleich vorweg sei erwähnt, daß InDesign dem Vergleich mit anderen Layoutprogrammen nicht nur standhält, sondern diese teilweise (siehe Abschnitt *InDesign-Spezialitäten*) deutlich übertrifft. Dieser Artikel ist allerdings nicht für Grafiker gedacht, die mit dem Gedanken spielen, auf Adobe InDesign umzusteigen, sondern für den interessierten Laien, dessen Bedürfnisse mit den Funktionalitäten einer herkömmlichen Textverarbeitung nicht abgedeckt werden. Einen gewissen Startvorteil bei der Verwendung von InDesign verschaffen rudimentäre Photoshop- bzw. Illustrator-Kenntnisse, da bei allen Adobe-Programmen eine ähnliche Benutzeroberfläche eingesetzt wird und sich viele Begriffe bzw. Werkzeuge in InDesign wiederfinden.

Wie die meisten neueren Softwareprodukte benötigt auch InDesign für den problemlosen Gebrauch einen gut ausgestatteten Rechner – laut Adobe sind die Mindestanforderungen unter Windows ein Pentium II-Prozessor mit 300 MHz und unter MacOS ein Power Macintosh 604 (besser ein G3). Als Betriebssystem ist zumindest Windows 98, NT 4.0 (ServicePack 4) oder MacOS 8.5 erforderlich. Um flott arbeiten zu können, sind 128 MB Arbeitsspeicher notwendig, für weniger Ungeduldige reichen aber auch 64 MB.

## Der Einstieg in eine komplexe Welt

Der grundlegende Unterschied zwischen einem Textverarbeitungs- (z.B. MS-Word, StarOffice-Writer, WordPerfect) und einem Layoutprogramm (z.B. QuarkXPress, TeX, Adobe Pagemaker, Adobe Framemaker und natürlich auch Adobe InDesign) besteht darin, daß Layoutprogramme rahmenorientiert arbeiten, somit Texte und Grafiken meist zuerst in einen entsprechenden Rahmen geladen werden müssen und erst dann nach Belieben bearbeitet werden können.

Dies ist zu Beginn etwas gewöhnungsbedürftig, bietet aber ein breites Spektrum an Gestaltungsmöglichkeiten – vor allem bei der Anordnung der einzelnen Rahmen, die miteinander verknüpft, ineinander verschachtelt oder gruppiert sein können und auch gemeinsam verschoben werden können. Rahmen müssen überdies nicht rechteckig, sondern können auch rund oder ellipsoid sein. Mittels dieser und frei wählbarer Rahmenformen ist es weiters möglich, den Textfluß variabel auszurichten – beispielsweise an der Kontur einer Grafik (vgl. Abb. 1).

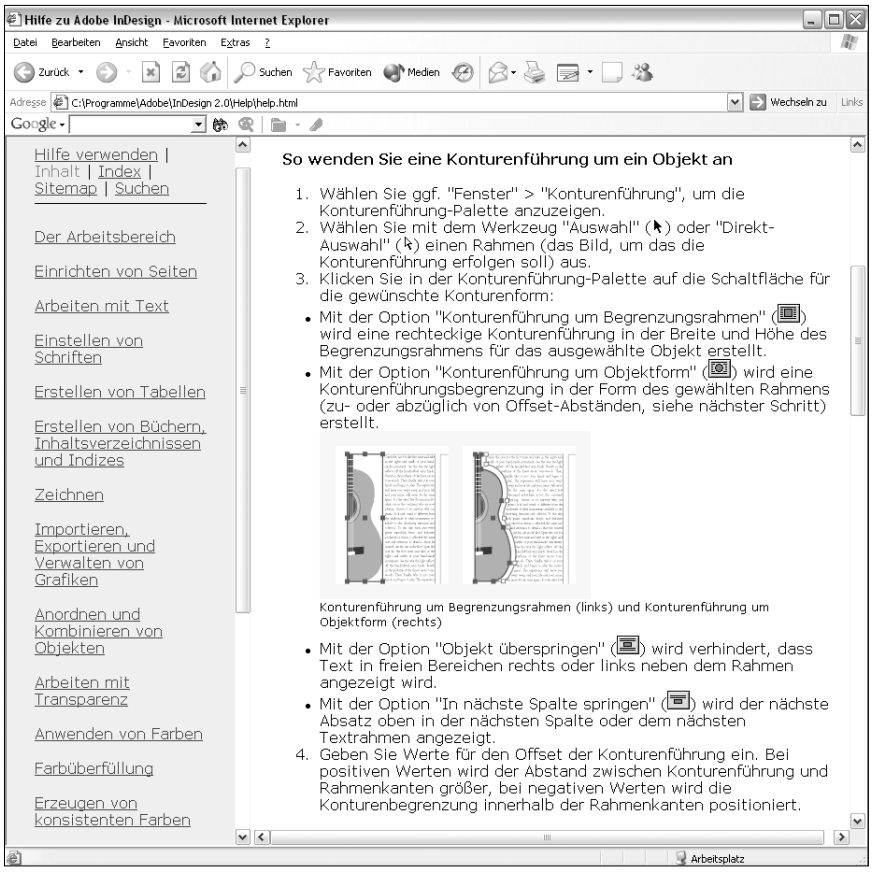



**Abb. 1: Beispiel für die Ausrichtung des Textflusses an der Kontur einer Grafik (*Hilfe*-Funktion von Adobe InDesign)**

Der Text kann innerhalb seines Rahmens wie gewohnt formatiert werden, wobei die typografischen Möglichkeiten aber weit über die eines Textverarbeitungsprogramms hinausgehen: Neben der Schriftart bzw. -größe und der Absatzausrichtung können auch das Kerning (der Abstand zwischen den einzelnen Zeichen), die Zeichenbreite und -höhe, die Zeilenhöhe und der Abstand zwischen den Absätzen gezielt beeinflußt werden.

## InDesign-Spezialitäten

1. Trotz der Rahmenorientierung kann Adobe InDesign – wie ein Textverarbeitungsprogramm – automatisch Inhaltsverzeichnisse und Indizes erstellen.

2. Die Erstellung von Tabellen, in die auch Grafiken und weitere Tabellen integriert werden können, funktioniert im Gegensatz zu den meisten anderen Layoutprogrammen problemlos. Nur die Nachbearbeitung oder Korrektur bestehender Tabellenseiten gestaltet sich kompliziert; deswegen sollte man möglichst zuerst ein Konzept erstellen und danach erst die Umsetzung in Angriff nehmen. Bereits in MS-Word oder MS-Excel formatierte Tabellen lassen sich direkt importieren bzw. konvertieren.

3. InDesign kann alle gängigen Grafik-Dateiformate (TIF, GIF, EPS, JPG, ...) importieren. Daher sollte der spätere Verwendungszweck des Dokuments (z.B. Druck, Veröffentlichung im WWW) ausschlaggebend für die Wahl des Dateiformats sein, wobei der InDesign-Hilfetext (unter *Hilfe – InDesign-Hilfe*) sehr ausführlichen Rat zu diesem Thema bietet.

4. Ein Bild oder eine Grafik kann entweder frei plaziert werden (was in den meisten Fällen aber nicht zu empfehlen ist) oder innerhalb eines Bildrahmens, wobei man zwischen nahezu beliebigen Rahmenformen und -stärken wählen und zusätzlich innerhalb des gewünschten Rahmens skalieren kann. Für den Import von Grafiken sollte der Menüpunkt *Datei – Platzieren* verwendet werden, da er bei den meisten Dateitypen die höchste Unterstützung für Auflösung und Farbe gewährleistet. Die Methoden *Drag & Drop* bzw. *Copy & Paste* funktionieren in der Regel zwar auch, können aber Einbußen bei der Qualität mit sich bringen.

5. Ein großer Vorteil von InDesign ist die enge Zusammenarbeit mit den anderen Programmen der Firma Adobe. So bleiben etwa programmeigene Dateiattribute (z.B. Transparenz) beim Import aus Illustrator oder Photoshop erhalten. Eine sogenannte Farb-Engine sorgt für gleichbleibende Farbtöne beim Wechsel zwischen den verschiedenen Adobe-Produkten. InDesign hat weiters eine eingebaute PDF-Library, um PDF-Dateien im Acrobat 4.0- oder Acrobat 5.0-Format ohne Qualitätsverlust direkt zu exportieren – damit entfällt der Umweg über den Acrobat Distiller.

## Gefinkeltes aus dem Werkzeugkasten

- **Unbegrenztes Rückgängigmachen und Wiederholen von Aktionen**
  Während die meisten Programme nur eine beschränkte Schrittzahl ermöglichen, läßt InDesign den Benutzer zu jeder seiner Aktionen navigieren.

- **Zoom-Vergrößerung von 5% auf 4000% über die Navigations-Palette**
  Das Ein- bzw. Auszoomen kann vor allem bei der Bearbeitung von Grafiken oder bei Inkonsistenzen innerhalb von Schriftsätzen von erheblicher Bedeutung sein – wenn auch die äußersten Enden der Skala (5% bzw. 4000%) etwas übertrieben wirken.

- **Mehrere Musterseiten, die aufeinander basieren können**
  Die Gestaltung von Musterseiten (inklusive Einbindung von Logos und speziell positionierten Bildern bzw. Überschriften) ist vor allem bei der Entwicklung von umfangreicheren Dokumenten wichtig, deren Seiten ein einheitliches Erscheinungsbild bieten sollen (z.B. Zeitschriften). Mit InDesign ist auch die Erstellung mehrerer Musterseiten, die aufeinander basieren können, und die Wahl zwischen den verschiedenen Vorlagen ohne erhöhten Aufwand möglich.

- **Vorschau-Modus**
  Damit sich unliebsame Überraschungen beim Ausdruck eines Dokuments in Grenzen halten, kann man die nicht druckbaren Elemente wie Lineale, Raster und Rahmenkanten mit Klick auf das Symbol *Vorschaumodus* am unteren Rand der Werkzeugpalette einfach und rasch ausblenden. Einzelne nicht druckbare Elemente können mit der entsprechenden Option im Menü *Ansicht* (z.B. *Ansicht – Hilfslinien*) unsichtbar gemacht werden.

- **Preflight-Funktion**
  Mittels Preflight-Funktion kann InDesign ein Dokument auf mögliche Fehler prüfen, die Probleme bei der Ausgabe verursachen könnten. Dabei werden Bilder im falschen Farbmodus ebenso gefunden wie fehlende Schriften (auch innerhalb von importierten EPS-Dateien). Nach Abschluß des Preflight-Vorgangs kann eine Datei „verpackt" werden, wobei sämtliche Bestandteile des Layouts (Schriften, Bilder, nicht eingebettete Schriften in EPS-Dateien) zusammengesucht werden. Bildverknüpfungen werden während des Verpackens aktualisiert, damit beim späteren Öffnen der Datei die Bilder nicht als unaktuell gemeldet werden.

## Und die Moral von der Geschicht' ...

... ohne Aufwand geht es nicht! Der Lernaufwand hält sich in Grenzen, wenn man über Photoshop- bzw. Illustrator-Kenntnisse verfügt oder bereits mit Layoutprogrammen gearbeitet hat. Wenn man aber lediglich Erfahrungen im Umgang mit Textverarbeitungsprogrammen gesammelt hat und über keinerlei grafische Kenntnisse verfügt, kann der Umstieg auf InDesign mühsam erscheinen. Wie in vielen Bereichen des Lebens sollte man abwägen, ob das Ergebnis den Aufwand rechtfertigt und ob man bereit ist, sich grundlegende grafische Kenntnisse anzueignen, die für ein optimales Ergebnis unerläßlich sind.

Bei Wissenslücken braucht man jedenfalls nicht zu verzweifeln: Die Online-Hilfe von InDesign (unter *Hilfe – InDesign-Hilfe*, vgl. Abb. 1 auf Seite 25) ist extrem ausführlich und leicht verständlich formuliert.

*Vera Potuzak* ■

# GO! CREATE A WEBGALLERY!

*„Ich kenne mich mit Bildbearbeitung Null aus und von Web und HTML hab ich keinen blassen Schimmer – wie komme ich nun zu meiner eigenen Fotogalerie im Internet?“*

Web-Fotogalerien sind Webseiten, die über eine Startseite mit Miniaturbildern (*Thumbnails*) sowie einzelne Seiten mit Bildern in voller Größe verfügen. Jede Seite hat Links zum Navigieren: Wenn man z.B. auf ein Miniaturbild klickt, wird eine Galerieseite mit dem dazugehörigen Bild in voller Größe geöffnet. Von dort kann man dann entweder auf die Startseite zurückkehren oder zum nächsten bzw. vorherigen Großbild weiterblättern.

Viele Fotografen, Hobby-Knipser und andere „Bildersammler“ kennen sich mit Bildbearbeitung bzw. mit dem Veröffentlichen im Internet kaum bis gar nicht aus. Im Grunde ist es eine Leichtigkeit, von der wenige wissen. Noch weniger haben wahrscheinlich auf ihrem Computer eine Bildbearbeitungssoftware wie z.B. Adobe Photoshop[1] installiert. Aus diesem Grund habe ich Photoshop mit anderen, kostenlosen Programmen verglichen und auf der Webseite `http://tucows.univie.ac.at/` nach Freeware im Bereich (Web-)Fotogalerien gesucht. Aus der mir gebotenen Liste habe ich fünf Programme ausgewählt, diese installiert und getestet. Mein Augenmerk lag auf einfacher Handhabung und bestem Ergebnis.

Alle getesteten Programme haben Gemeinsamkeiten im Ablauf: Sie erstellen Zielordner, Thumbnails, die Webseiten und die Verlinkung und Navigation der Seiten automatisch. Besondere Optionen sind vom individuellen Programm abhängig. Weiters sind alle fertigen Seiten – für Könner – im HTML-Code editierbar (bis auf ein Programm, das Java-Code erzeugt). Anschließend muß das Endergebnis natürlich noch zum Webserver übertragen werden – z.B. mit FTP. Leider ist es nicht leicht möglich, eine Galerie um weitere Bilder aufzustocken. Man muß entweder händisch die HTML-Seiten anpassen bzw. neu erstellen oder aber den Vorgang wiederholen, eine neue Galerie generieren und die alte am Server austauschen. Oder man verwendet Swiggle (siehe Seite 29).

## Photoshop 7

In Photoshop 7 gibt es die Option einer Web-Fotogalerie (***Datei – Automatisieren – Web-Fotogalerie***). In wenigen wirklich einfach gestalteten Optionsschritten, die sogar Banner, Copyright-Vermerke und erweiterte Dateinamen umfassen, ist im Nu eine Fotogalerie gezaubert. Photoshop 7 ist das einzige der getesteten Programme, das sieben verschiedene HTML-Stile anbietet. Die Palette reicht von einfachen Layouts bis zu horizontal bzw. vertikal geteilten Frameseiten (siehe Abb. 1).

Die erstellten Webseiten haben ein schlichtes Layout (siehe Abb. 2) und sind dank der statisch unterhalb der Titelzeile angesiedelten *Vorwärts*- und *Rückwärts*-Pfeile mühelos zu navigieren. Praktisch ist auch der Photoshop-Dateibrowser, der z.B. eine automatische Umbenennung aller Bilder eines Ordners auf einen beliebigen Dateinamen mit fortlaufender Nummer ermöglicht. So bekommt man Ordnung in das Durcheinander vieler Bilder.

Fazit: Falls man viel mit Photoshop 7 arbeitet und die Arbeitsabläufe gewohnt ist, finde ich es nicht notwendig,

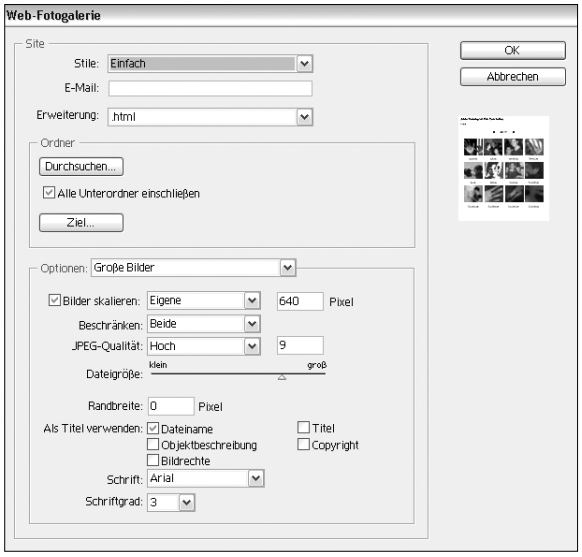



**Abb. 1: Photoshop 7 – Dialogfenster *Web-Fotogalerie***


**Abb. 2: Photoshop 7 – Beispiel für eine fertige Webgalerie**

1) In den PC-Räumen der Uni Wien (siehe `http://www.univie.ac.at/ZID/PC-Raeume/`) findet man Photoshop auf allen Rechnern; für Institute der Universität Wien ist das Programm als Standardsoftware verfügbar (siehe `http://www.univie.ac.at/zid-swd/`).

zusätzliche Software zu installieren, da das Endergebnis hier sehr zufriedenstellend ist.

### Archimage 1.7

Dies ist ein Programm zur Katalogisierung verschiedener Bilddateien (z.B. BMP, JPG, PCX, TGA, TIFF), das auch Web-Fotogalerien erstellen kann und in der Registerkarte ***HTML generation*** sehr viele Einstellungsmöglichkeiten bietet. Um nun zu einer Fotogalerie zu kommen, muß man sich durch all die Optionen durchschlagen – man kann Buttons, Schriftarten, Schriftfarben, die Größe der Bilder und Thumbnails sowie die Bildqualität wählen und hat sogar die Möglichkeit, über den integrierten (!) HTML-Editor in den Code einzugreifen – und bekommt ein ganz gutes und brauchbares Ergebnis. Die fertige Galerie kann nun mittels (ebenfalls integriertem) FTP-Klient online gestellt werden.

Fazit: Ein eher kompliziertes Programm, nicht unbedingt für unwissende Laien; ein weniger attraktives, dennoch zweckdienliches Ergebnis.

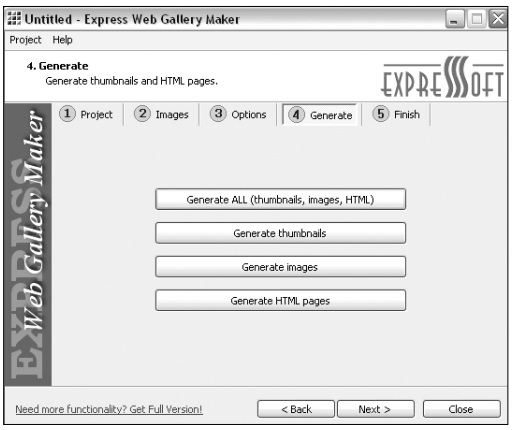
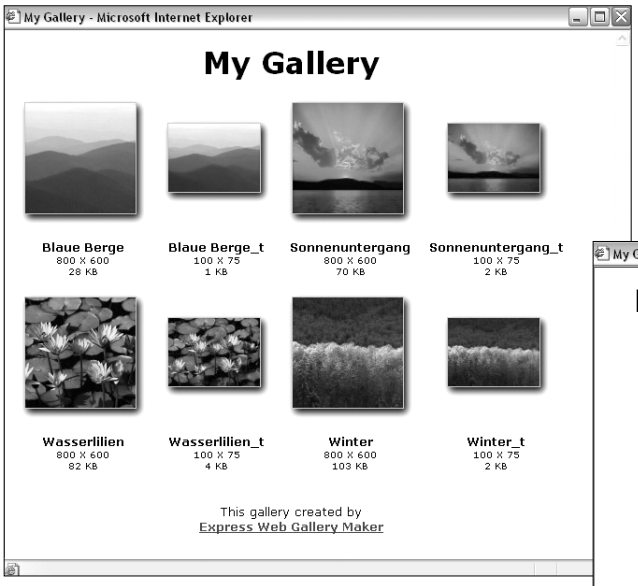



**Abb. 3: Express Web Gallery Maker – Bedienung**



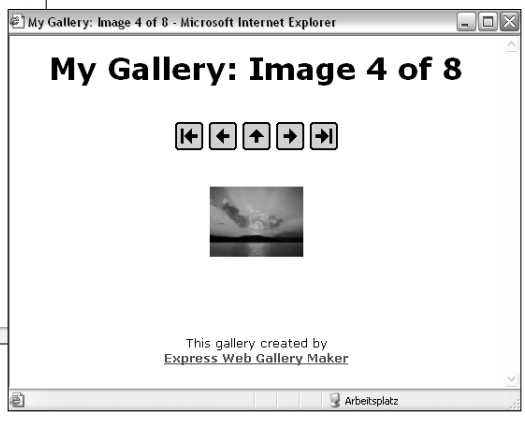




**Abb. 4 & 5: Mit Express Web Gallery Maker erstellte Fotogalerie – Überblick (oben) und Einzelansicht (rechts)**

### ThumbHTML 2.2

Ein besonders einfaches Programm um Webseiten für digitalisierte Bilder herzustellen. Wählen Sie einen Ordner aus und die Thumbnails aller enthaltenen Bilder werden erstellt und mit dem Hauptbild verlinkt. Verschiedene Effekte, Schriftfarben und zusätzliche Infos zu den Bildern stehen zur Verfügung. Sobald alle notwendigen Informationen eingetragen sind, erzeugt das Programm die Webseiten und die dazugehörige Navigation von selbst. Nun müssen Sie Ihre Dateien nur mehr auf den Webserver übertragen. ThumbHTML erlaubt es auch, Anmerkungen zu jedem einzelnen Bild zu schreiben und Slideshows zu erstellen, die ebenfalls mitpubliziert werden.

Fazit: Ein besonders einfaches und angenehmes Programm; die Seiten sehen ein wenig unruhig aus, da die Thumbnails im Hoch- und Querformat nicht die gleiche Größe haben und die Navigations-Buttons hin- und herspringen.

### Easy Gallery Generator 2.1 (EGG)

Dieses Programm ist wohl eines der am einfachsten zu bedienenden. In genau zwei Schritten kommt man damit zu seiner Webgalerie: Man gibt einfach den Ordner mit den zu verwendenden Fotos an und klickt dann auf den Button mit dem Ei (!), und schon generiert Easy Gallery Generator alle Thumbnails, die dazugehörigen HTML-Seiten und speichert alle Dateien. That's it!

Fazit: Super einfach – super schnell! Die fertigen Webseiten sehen sehr hübsch aus. Das einzig Störende ist die Navigation neben den Bildern, die bei unterschiedlicher Bildgröße gezwungenermaßen hüpft.

### Express Web Gallery Maker 1.45

Express Web Gallery Maker erlaubt es, in genau fünf Schritten eine sehr attraktive Webgalerie zu erstellen. Es ist als *Wizard* konzipiert (d.h. man wird schrittweise durch das Programm geführt; siehe Abb. 3), praktisch für jedermann. Eine Webgalerie herzustellen ist – außer mit EGG – nie einfacher gewesen: Bilder laden, Zielordner angeben und durch Klick auf ***Generate All*** werden alle Bilder, alle Thumbnails und der HTML-Code binnen Sekunden generiert. Das Ergebnis ist wirklich schön gelungen, und da sich die Navigations-Buttons immer an derselben Stelle über den Bildern befinden, ist auch bei verschiedenen Bildgrößen ein Weiterklicken, ohne die Maus zu bewegen, sehr einfach (siehe Abb. 4 & 5).

Fazit: Dürfte ich Punkte vergeben, würde Express Web Gallery Maker die höchstmögliche Anzahl erhalten und wäre somit Testsieger!

### Photo Album Studio 1.0.4

Für Java-Fans gibt es Photo Album Studio. Die eigentliche Erstellung der Fotogalerie ist mit diesem Programm sehr einfach: Album benennen, Bilder laden, ***Generate*** anklicken und fertig. Leider ist das Ergebnis weder ansehnlich noch editierbar, da es auf Java-Code basiert.

Fazit: Gutes und durchdachtes Anwenderprogramm mit fast unbrauchbarem Ergebnis, da viele Browser Java nicht unterstützen bzw. Java oft deaktiviert ist. Schade.

### Swiggle

Dieses Programm ist speziell für Linux-/Unix-Rechner programmiert. Als Universitätsmitarbeiter mit Mailbox-UserID kann man damit direkt am Server eine Web-Fotogalerie erzeugen: Man erstellt (am besten im Verzeichnis `html` seines Mailbox-Homedirectorys) einen Zielordner für die Fotogalerie (z.B. `gallery`) mit Unterverzeichnissen für jedes einzelne Album und überträgt die zu verwendenden Bilder ins entsprechende Unterverzeichnis.

Dann mit einem SSH-/Telnet-Klienten (z.B. PuTTY) einloggen, aus dem Hauptmenü `(s) Unix-Shell` auswählen, den Befehl `swiggle pfad/zum/zielordner` eingeben (in unserem Beispiel: `swiggle html/gallery`) und bestätigen. That's it! Swiggle erstellt Thumbnails und alle HTML-Seiten, und falls das Album im Verzeichnis `html` des Benutzers liegt, ist die Fotogalerie sofort online!


**Abb. 6: Mit Swiggle erstellte Web-Fotogalerie**

Wer keine Mailbox-UserID hat, braucht einen Linux-/Unix-Rechner und muß unter `http://mailbox.univie.ac.at/L.Ertl/swiggle/files/swiggle-0.1.tar.gz` Swiggle downloaden und installieren. Die Vorgänge bleiben die gleichen.

Swiggle wurde von unserem Kollegen Lukas Ertl programmiert, ist Open Source-Software und speziell für Fotos aus Digitalkameras gedacht: Es werden nur JPEG-Bilder verarbeitet, und die von der Kamera mitgespeicherten Informationen werden automatisch angezeigt (siehe Abb. 6).

Fazit: Ein sehr einfach zu bedienendes Programm mit ansehnlichem Layout; leider ist es nur für Linux-/Unix-Anwender bzw. Uni-Mitarbeiter verfügbar.

*Barbara Schwindl* ■

# NEUE STANDARDSOFTWARE

## Neue Produkte (Stand: 17. 2. 2003)

- Apple MacOS X 10.2
- Apple QuickTime Pro 6 für Win. und Mac
- Corel Draw 11 für Win. und Mac
- EndNote 6.0 für Win. und Mac
- Exceed 8.0.0 für Win.
- FileMaker Pro 6.0 für Win. und Mac
- Macromedia Director MX 9.0 für Win. und Mac
- MS-MapPoint 2002 Euro und US für Win.
- MS-Office XP Developer für Win.
- MS-Project 2002 Standard und Prof. für Win.
- MS-Visual FoxPro Prof. 7.0 für Win.
- ScanSoft OmniPage Pro 12.0 für Win.
- SPSS 11.0 für Mac
- SPSS 11.5 für Win.
- SPSS Neural Connection 2.1 für Win.
- Symantec Norton Internet Security 2003 für Win. (beinhaltet Antivirus, Firewall u.a. und löst daher die Einzelprodukte ab)
- Symantec Norton SystemWorks 2003 für Win. (beinhaltet Norton Utilities, Antivirus u.a. und löst daher die Einzelprodukte ab)

## Updates (Stand: 17. 2. 2003)

- MATLAB 6.5 R13 für Win. und Unix (bisher R12)
- MS-Office 10 Standard SR1 für Mac (bisher ohne SR1)
- MS-Windows 2000 Prof. SR3 (bisher SR2)
- MS-Windows 2000 Server SR3 (bisher SR2)
- MS-Windows XP Prof. SR1 (bisher ohne SR1)

Alle Informationen zur Standardsoftware finden Sie im WWW unter **`http://www.univie.ac.at/zid-swd/.`**

*Peter Wienerroither* ■

# HTML mit Stil – Teil II: CASCADING STYLE SHEETS

## 1. Einleitung

*„Wie gefällt Ihnen der Klang der neuen Homepage der Uni Wien?“* – Diese Frage kommt Ihnen wahrscheinlich absurd vor. Sie ist aber nicht viel absurder als die Frage *„Wie gefällt Ihnen das Aussehen der neuen Uni-Homepage?“* Das Aussehen ist – ebenso wie der Klang – keine unmittelbare Eigenschaft einer Webseite, genauer gesagt, eines HTML-Dokuments. Ein solches Dokument hat einen Inhalt, eine Struktur, und enthält eine Reihe von Anweisungen an ein Endgerät (den sogenannten *User Agent*), wie diese Inhalte darzustellen sind. In den meisten Fällen ist der User Agent ein grafischer Webbrowser, der auf einem PC läuft – er kann aber auch etwas ganz anderes sein: z.B. ein Laserdrucker, ein Mobiltelefon, ein Sprach-Synthesizer oder ein *Robot*, der das Web durchsucht, um es für eine Suchmaschine zu indizieren.

Das Aussehen – oder allgemeiner: die Präsentation – einer Webseite ergibt sich erst dadurch, wie der User Agent diese Anweisungen umsetzt. Hier können die Ergebnisse recht unterschiedlich sein. Abgesehen davon, daß die Anweisungen meistens einen beträchtlichen Spielraum lassen, kann sie der User Agent oft gar nicht befolgen:

- Sie werden vom User Agent nicht unterstützt oder sind nicht anwendbar – z.B. wird ein Schwarzweiß-Drucker Farbangaben ignorieren und ein Text-Browser oder ein Sprach-Synthesizer den gewünschten Zeichensatz; Browser ohne entsprechende Software-Unterstützung werden Java-Applets und dergleichen nicht ausführen usw.

- Sie werden nicht oder falsch verstanden: Die wenigsten HTML-Dokumente sind syntaktisch korrekt und standard-konform. Die meisten enthalten Syntax-Fehler und verwenden alle möglichen Erweiterungen, die über die HTML-Standards hinausgehen – die User Agents können nur raten, was damit gemeint sein könnte. Andererseits ist auch fast kein User Agent fehlerfrei: Browser-Bugs führen oft zu einer falschen Darstellung vollkommen richtiger Dokumente.

Dazu kommt noch, daß der User Agent die Anweisungen manchmal nicht befolgen *will* – beispielsweise bevorzugen Leute mit Sehschwächen oft größere Schriften, auch wenn viele Webdesigner winzige Schriften für besonders elegant halten. Werbe-Popups werden von vielen als lästig empfunden – von mir nicht, weil ich keine sehe: Ich habe meinen Browser so konfiguriert, daß er unaufgefordert keine Fenster öffnet.

Soweit die Theorie, oder besser gesagt, die Absichten der Erfinder des WorldWideWeb. In der Zwischenzeit wird das Web hauptsächlich für ganz andere Zwecke genutzt als für den Informationsaustausch unter Teilchenphysikern. Damit ist auch eine neue Generation von Webdesignern herangewachsen, der die Prinzipien der Web-Pioniere am CERN von Herzen egal sind: Sie betrachten Webseiten ausschließlich als grafisches Medium – vor allem in der Werbebranche ist die grafische Gestaltung oft wichtiger als der Inhalt –, sie verwenden WYSIWYG-Editoren (*What You See Is What You Get*) und erwarten, daß ihre Webseiten immer und überall so aussehen wie auf ihrem eigenen Bildschirm. Sie haben wenig Verständnis für Benutzer-Präferenzen, die von ihren eigenen Design-Vorstellungen abweichen.

Dieser Standpunkt hat durchaus seine Berechtigung: Es ist legitim, daß Werbeagenturen andere Bedürfnisse haben als Physiker. Das ändert aber nichts an der Tatsache, daß sich diese Ziele mittels HTML bestenfalls nur annähernd und mit allen möglichen Tricks (z.B. Layout mittels komplizierter Tabellen) erreichen lassen: HTML ist schlicht und einfach nicht dazu gedacht, das Layout und die grafische Gestaltung einer Seite zu beschreiben.

Es gibt noch immer keine perfekte Lösung, diese beiden widersprüchlichen Auffassungen miteinander zu vereinen, aber immerhin gibt es eine gute Näherung: Die Lösung besteht darin, HTML als Sprache ausschließlich oder zumindest weitgehend dazu zu verwenden, wozu sie ursprünglich erfunden wurde, nämlich um die Struktur von Text-Dokumenten zu beschreiben. Für alles andere – Farben, Zeichensätze, Schriftgrößen, Layout, Hintergrundbilder usw. – wird eine eigene Sprache verwendet, die speziell für solche *presentational hints* gedacht ist: Cascading Style Sheets.

## 2. Das Prinzip von CSS – ein einfaches Beispiel

Wie jede Computersprache haben Cascading Style Sheets (üblicherweise mit CSS abgekürzt) eine wohldefinierte Syntax mit strengen Regeln, was gültig ist und was nicht. Wie bei vielen Sprachen gibt es mehrere Varianten. In diesem Artikel wird ausschließlich auf den derzeit aktuellen Standard eingegangen, das sind *Cascading Style Sheets Level 2* (CSS2).

Betrachten wir ein Beispiel[1)] eines Style Sheet:

```
body {
   /* Style Sheets können Kommentare enthalten */
    background-image: url(”wolken.jpg”);
    background-color: white;
    color: #333333;
    font-family: Verdana, Helvetica, sans-serif;
    margin: 1em;
}
```

```
/* Styles können sich auf mehrere Elemente
   beziehen */
h1, h2, h3 { text-align: center; }
h1 { color: rgb(200,0,0) } /* dunkelrot */
```

Dieser Style Sheet enthält eine Reihe von Style-Definitionen zu den HTML-Elementen `body`, `h1`, `h2` und `h3`. Diese Definitionen stehen, durch Strichpunkte getrennt, in geschwungenen Klammern. Jede dieser Definitionen besteht aus einem Attribut wie Größe, Farbe, Zeichensatz usw., dem ein Wert zugewiesen wird, manchmal auch mehrere. So bedeutet `font-family: Verdana, Helvetica, sans-serif`, daß für Text der Zeichensatz Verdana verwendet werden soll. Steht dieser nicht zur Verfügung, so soll stattdessen Helvetica verwendet werden und statt Helvetica ein beliebiger Zeichensatz der Schriftfamilie *sans serif*. Der gesamte Inhalt des Dokuments soll einen Abstand von einem `em` zum Browserfenster haben. Diese Einheit (abgeleitet vom Buchstaben M, der in den meisten Zeichensätzen der größte ist), bezeichnet die Größe (`font-size`) des verwendeten Zeichensatzes. Es gibt noch viele andere absolute und relative Größeneinheiten, z.B. `px` (Pixel), `pt` (Point = 1/72 Zoll), `cm` (Zentimeter). Auch Werte wie `small` oder `large` können angegeben werden – dann werden die Details dem User Agent überlassen. Es gibt mehrere Methoden, die gewünschten Farben anzugeben: Für 16 Farben sind im Standard Namen definiert,[2] für alle anderen Farben müssen RGB-Werte verwendet werden – entweder in hexadezimaler Form wie in `#333333` oder in Dezimalform wie in `rgb(200,0,0)`.

## 3. HTML und CSS

Wie kombiniert man nun HTML-Dokumente mit Style Sheets? Die aktuellen Standards XHTML 1.0 (`http://www.w3.org/TR/xhtml1/`) und HTML 4.01 (`http://www.w3.org/TR/html401/`) bieten mehrere Möglichkeiten, ein HTML-Dokument um Style-Angaben zu erweitern:

- Für fast jedes Element kann ein `style`-Attribut angegeben werden, z.B.:

```
<h1 style="color: green;
text-align: right">
   Diese Überschrift ist grün und
   steht am rechten Rand
</h1>

<p style="margin-left: 2em; font-size: 0.8em">
   Dieser Absatz ist eingerückt und
   kleingedruckt.
</p>
```

- Im `head` eines HTML-Dokuments können Styles mit Hilfe eines oder mehrerer `style`-Elemente definiert werden, z.B.:

```
<head>
 <style type="text/css">
    /* grosser Zeilenabstand */
    p { font-size: 1em; line-height: 2em; }
    /* Überschriften fett und kursiv */
    h1, h2, h3 { font-style: italic;
    font-weight: bold; }
 </style>
</head>
```

- Mit Hilfe eines `link`-Elements im `head` kann auf einen externen Style Sheet (oder auch mehrere) verwiesen werden:

```
<head>
   <link rel="stylesheet" href="external.css"
   type="text/css">
   <link rel="alternate stylesheet"
   title="Mit Verzierungen"
   href="fancy.css" type="text/css">
</head>
```

Im obigen Beispiel ist `external.css` der primäre Style Sheet. Der User Agent sollte den Benutzern eine Liste aller alternativen Style Sheets anbieten, was allerdings nur von wenigen Browsern (z.B. Mozilla) unterstützt wird. Auch mit `@import` kann ein externer Style Sheet importiert werden (siehe Abschnitt *Browser-Unterstützung*). In den meisten Fällen ist ein externer Style Sheet empfehlenswert: Ein einziger Style Sheet für sämtliche HTML-Dokumente ist eine effiziente Methode, die grafische Gestaltung einer Webpräsenz zu vereinheitlichen. Zusätzlich werden so die Dateigrößen reduziert.

Es gibt einige HTML-Elemente und Attribute, die zwar unmittelbar nichts mit Style Sheets zu tun haben, aber in Verbindung mit solchen besonders nützlich sind. Mit dem Attribut `class` können beliebige HTML-Elemente Klassen zugeordnet werden, z.B:

```
<p class="footnote">
```

Der Name einer Klasse ist dabei willkürlich und kann frei gewählt werden. In einem Style Sheet können die Eigenschaften von Elementen definiert werden, die einer bestimmten Klasse angehören:

```
.footnote {
   font-size: 0.7em;
   margin-left: 2em;
}
```

Das Attribut `id` hat eine ähnliche Funktion wie das Attribut `class`: Der wesentliche Unterschied ist, daß ein Element mit einem solchen Attribut in einem HTML-Dokument nur einmal vorkommen darf; ein korrektes HTML-Dokument kann also nur einmal die Zeile

```
<p id="header">
```

enthalten. Mit folgender Syntax wird für ein solches Element ein Style definiert:

---

1) Alle Beispiele mit Erläuterungen sind unter `http://www.univie.ac.at/css-demo/` zu finden.

2) `aqua`, `black`, `blue`, `fuchsia`, `gray`, `green`, `lime`, `maroon`, `navy`, `olive`, `purple`, `red`, `silver`, `teal`, `white`, `yellow`

```
#header {
    /* sehr groß, rot, fett und zentriert */
    text-align: center;
    font-size: xx-large;
    font-weight: bold;
    color: red;
}
```

Das HTML-Element `div` bezeichnet eine „neutrale" Unterteilung eines HTML-Dokuments, d.h. es ist damit keine besondere Bedeutung wie Überschrift, Absatz oder dergleichen assoziiert. `div`-Elemente können mehrere unterschiedliche HTML-Elemente enthalten:

```
<div class="kasten">
<h1>Das ist die Überschrift</h1>
<p>Das ist der erste Absatz</p>
<p>... und das ist der zweite</p>
<p>... und alles miteinander ist blau eingerahmt</p>
</div>
```

Eine spezielle Bedeutung erhält ein solches `div`-Element erst durch den dazugehörigen Style Sheet:

```
.kasten {
    padding: 6px;
    border-width: 4px;
    border-style: solid;
    border-color: blue;
}
```

Das HTML-Element `span` hat eine ähnliche Funktion wie `div`, ist aber auf „Inline-Elemente" beschränkt:

```
<p>
  In diesem Absatz stehen mehrere Namen, z.B.
  <span class="person">Meier</span>,
  <span class="person">Müller</span> und
  <span class="person">Huber</span>. In einem
  Style Sheet kann definiert werden, wie Namen
  von Personen darzustellen sind.
</p>
```

## 4. Was bedeutet Cascading?

Der Style Sheet, der in einem HTML-Dokument angegeben wird (der *Author Style Sheet*), ist nicht der einzige, der bei der Darstellung dieses Dokuments durch einen User Agent berücksichtigt wird. Jeder standard-konforme User Agent hat einen *Default Style Sheet* oder verhält sich zumindest so, als hätte er einen. Dazu kommt noch der *User Style Sheet*: Jeder Benutzer eines User Agent kann seine Präferenzen bezüglich Farben, Zeichensätzen, Größen usw. bekannt geben.[3] Der CSS 2-Standard liefert in Kapitel 6.4 eine genaue Definition der *Kaskade*, d.h der Reihenfolge, in welcher die Regeln aus den verschiedenen Style Sheets zum Tragen kommen. Vereinfacht gesagt, gelten zuerst die Regeln des Author Style Sheet, dann die des User Style Sheet und zuletzt die des Default Style Sheet. Eine Ausnahme sind Regeln im User Style Sheet, die mit `important!` gekennzeichnet sind – diese haben höhere Priorität als der Author Style Sheet.

Generell sind die Konzepte der *Präzedenz* und der *Vererbung* sehr wichtig bei Style Sheets: Wenn für ein bestimmtes Element mehrere Style-Definitionen in Frage kommen, so entscheiden Präzedenz-Regeln, welche Definitionen höheres Gewicht haben. Schließlich können manche abgeleiteten Elemente (*descendants*) Eigenschaften ihrer „Vorfahren" (*parent elements*) erben. Eine detaillierte Diskussion der Präzedenz-Regeln würde hier zu weit führen; im wesentlichen aber gilt: Spezifische Regeln haben ein höheres Gewicht als allgemeine Regeln.

Das folgende Beispiel illustriert einige dieser Regeln:

```
p.blue  { color: blue  }  /* Nr. 1 */
p       { color: green }  /* Nr. 2 */
.green  { color: green }  /* Nr. 3 */
p       { color: red }    /* Nr. 4 */
div     { color: yellow } /* Nr. 5 */
/* Es folgt "p span" – nicht verwechseln
  mit "p, span" */
p span  { color: green }  /* Nr 6. */
```

Die letzte Zeile dieses Style Sheet hat eine besondere Bedeutung: Sie definiert einen Style, der nur für Elemente des Typs `span` gilt, die sich innerhalb eines Elements `p` befinden. Die folgenden HTML-Fragmente zeigen, welche dieser sechs Styles unter welchen Umständen zu tragen kommen:

```
<p class="blue">Dieser Text ist blau.</p>
```

Für Elemente des Typs `p` gibt es drei Styles (Nr. 1, Nr. 2 und Nr. 4). Die Style-Definition für `p.blue` ist spezifischer als die für `p` alleine.

```
<p>Dieser Text ist rot
   <span>und dieser ist grün.</span>
</p>
```

Die beiden Style-Definitionen für `p` (Nr. 2 und Nr. 4) sind gleichwertig; in solchen Fällen gilt die letzte. Derartige einander widersprechende Regeln sind zwar sinnlos, aber nicht falsch. Für „`span` innerhalb von `p`" gilt die spezielle Style-Definition Nr. 6.

```
<div class="green">Dieser Text ist grün.</div>
```

Die Style-Definiton einer Klasse (`.green`) ist spezifischer als die eines Elements (`div`), daher gilt Nr. 3.

```
<div class="blue">Dieser Text ist gelb
   <span>und dieser auch.</span>
</div>
```

Die Klasse `blue` ist für Elemente des Typs `div` nicht definiert, deshalb gilt die Style-Definition des Elements `div` (Nr. 5). Das Element `span` ist in diesem Fall kein „Nachfahre" (*descendant*) eines Elements `p`, daher kommt die Regel Nr. 6 nicht zum Tragen. Das Element erbt die Farbe seines „Vorfahren" (*parent element*), also des `div`.

Zu guter Letzt können Style Sheets noch mit Formatierungsangaben kollidieren, die im HTML-Code selbst stehen. Im

3) Die meisten Browser unterstützen User Style Sheets nur in sehr rudimentärer Form, deshalb werden sie auch recht selten verwendet.

*Comment*-Artikel *HTML mit Stil* (`http://www.univie.ac.at/comment/98-2/982_23.html`) vom Juni 1998 wurde folgendes Beispiel eines HTML-Codes mit übermäßig vielen Formatierungs-Anweisungen gebracht:

```
<FONT SIZE="6" COLOR="#123CFB" TYPE="Arial">
<B>Test</B></FONT>
```

Laut CSS-Standard steht es Browsern frei, solche Anweisungen zu berücksichtigen: *The User Agent may choose to honor presentational hints from other sources than style sheets, for example the FONT element or the „align" attribute in HTML.* Es wird empfohlen, auf solche Attribute so weit wie möglich zu verzichten: Die HTML-Standards XHTML 1.0 und HTML 4.01 haben jeweils eine *Strict*- und eine *Transitional*-Variante, wobei letztere eine Übergangslösung darstellt, die mit älteren HTML-Standards weitgehend kompatibel ist. In den (für Neuentwicklungen empfohlenen) *Strict*-Varianten der Standards sind diese Attribute nicht mehr enthalten.

## 5. Browser-Unterstützung

Im oben erwähnten *Comment*-Artikel steht folgendes zum Thema Style Sheets: *Zur Zeit werden jedoch etliche Features von HTML 4.0 nur von wenigen Browsern unterstützt, sodaß man damit noch ein wenig warten sollte. Ein typisches Beispiel eines solchen Features sind Style Sheets, mit denen das [...] Problem des Konflikts zwischen logischer Struktur und grafischer Darstellung eines Dokuments elegant gelöst wird.*

Seither sind fast fünf Jahre vergangen, und inzwischen werden Style Sheets von allen modernen grafischen Browsern (Netscape und MS-Internet Explorer seit Version 4, Opera seit Version 3, Mozilla u.a.) weitgehend unterstützt. Allerdings versteht selbst die neueste Version des Internet Explorer etliche Features von CSS noch immer nicht (siehe dazu auch die Beispiele im folgenden Abschnitt). Es handelt sich aber hauptsächlich um fortgeschrittene Features, deren mangelnde Unterstützung die Funktion und das Erscheinungsbild einer Webseite nur marginal beeinträchtigt.

Ein Sonderfall ist Netscape Version 4, genauer gesagt, die verschiedenen Versionen von 4.0 bis 4.79: Jede dieser Versionen unterstützt Style Sheets, jede anders und jede so fehlerhaft, daß Webseiten mit komplexeren Style Sheets unter Netscape Version 4 praktisch unbrauchbar sind. Vor allem werden Abstände und Abmessungen oft vollkommen falsch berechnet. Leider ist dieser Browser noch immer nicht ausgestorben,[4] sodaß man seine Fehler nicht guten Gewissens ignorieren kann. Mit folgendem Trick lassen sie sich aber umgehen:

```
<link rel="stylesheet" media="screen"
href="simple.css" type="text/css">


<style media="screen,print,aural"
type="text/css">
@import url("complex.css");
</style>
```

Hier ist `simple.css` ein einfacher Style Sheet, der nur Anweisungen enthält, die auch Netscape 4 versteht und halbwegs richtig umsetzt. Der vollständige Style Sheet, der zusätzlich zu `simple.css` von allen CSS-fähigen Browsern verwendet wird, steht in `complex.css`: Weil Netscape 4 die Syntax von `@import` nicht versteht, ignoriert es diesen Style Sheet einfach.[5]

## 6. CSS für Fortgeschrittene: Ausgewählte Beispiele

Eine vollständige Diskussion von Cascading Style Sheets ist in diesem Rahmen selbstverständlich nicht möglich (dazu sei auf die Literaturangaben im Kasten auf Seite 34 verwiesen). Im folgenden illustrieren einige Beispiele, daß Style Sheets Möglichkeiten bieten, die weit über HTML hinausgehen – allerdings immer unter der Voraussetzung, daß die Browser mitspielen.

### 6.1 Style Sheets für verschiedene Medien

Viele Webdesigner vergessen, daß der Bildschirm nicht das einzige Ausgabemedium für Webseiten ist. Mit `@media` können Regeln definiert werden, die nur für bestimmte Medien gelten, z.B. `print` für Druckausgabe, `aural` für Sprach-Synthesizer, `handheld` für Geräte wie Palmtops und Mobiltelefone und noch einige mehr.

```
@media screen { p { font-size: 12pt; } }
/* kleinere Schrift für die Druckausgabe */
@media print { p { font-size: 10pt; } }
```

Ein wichtiger Unterschied zwischen der Darstellung auf dem Bildschirm und der Ausgabe auf einem Drucker ist, daß es bei letzterem kein Scrolling gibt und ein Dokument daher manchmal auf mehrere Seiten aufgeteilt werden muß. Mit `@page` können die Eigenschaften einer Seite festgelegt werden: Größe, Hoch- oder Querformat, Hinweise, wo eine neue Seite begonnen werden soll, und vieles mehr. Leider wird dies zur Zeit von den meisten Browsern nicht unterstützt.

Style Sheets für akustische Medien (`aural`) enthalten meist Anweisungen über die zu verwendenden Stimmen: Frauen- oder Männerstimme, Tonhöhe, Lautstärke, Klangfarbe, ...

### 6.2 Automatisch erzeugte Inhalte: `content`

Auf vielen Webseiten findet sich die Aufforderung *Klicken Sie hier!* Wer eine solche Webseite in gedruckter Form vor sich hat, sieht ein unterstrichenes *hier*, kann aber natürlich dort nicht klicken und weiß nicht, wo der Link hinzeigt. Mit

4) Etwa 4% aller Zugriffe auf die Webseiten der Uni Wien erfolgen derzeit mit Netscape 4. Auch weltweit dürfte der Anteil dieses Browsers bei 4% liegen.

5) Für die neue Homepage der Uni Wien wird ein anderer, aber ähnlicher Trick verwendet: Mit Hilfe von *Server-Side Includes* (siehe `http://httpd.apache.org/docs/mod/mod_include.html`) wird Netscape 4 vom Server ein anderes HTML-Dokument geliefert als allen anderen Browsern.

folgendem Fragment eines Style Sheet (das in einen `@media print`-Block gehört) wird diese wichtige Information nachgeliefert:

```
a {
   quotes: ' (' ') ';
   text-decoration: none;
}

a:after {
    content: open-quote attr(href) close-quote
}
```

Für alle Elemente des Typs `a` (also im wesentlichen Links) werden mit `quotes` Anführungszeichen definiert, nämlich runde Klammern, von Leerzeichen umgeben. Links sollen nicht unterstrichen werden, daher `text-decoration: none`. Das „Pseudo-Element" `a:after` definiert, was nach einem Element des Typs `a` geschehen soll: Es wird `content` eingefügt, also Inhalt, bestehend aus: Klammer auf, dem Attribut `href` (d.h. dem Link), Klammer zu. Statt *Klicken Sie bier!* steht also z.B. *Klicken Sie hier* (`http://link.to/some/page/`) *!* – vorausgesetzt, die Seite wurde z.B. mit Mozilla oder einer neuen Netscape-Version ausgedruckt und nicht mit dem Internet Explorer, der kann das nämlich nicht.

## Literatur

- ***Cascading Style Sheets, level 2: CSS2 recommendation*** (`http://www.w3.org/TR/REC-CSS2/`):
  Der offizielle Standard des W3C (*World Wide Web Consortium*).
- ***CSS Pointers Group*** (`http://css.nu/`):
  Eine Sammlung von Online-Ressourcen zum Thema Style Sheets.
- ***SELFHTML*** (`http://selfhtml.teamone.de/`):
  Das bekannte HTML-Tutorial von Stefan Münz enthält auch ausführliche Informationen über CSS.
- ***Cascading Style Sheets: The Definitive Guide*** (`http://www.oreilly.com/catalog/css/`):
  Ein Lehrbuch von Eric Meyer aus dem renommierten O'Reilly-Verlag.
- ***Cascading Stylesheets – Stil mit <Stil>*** (`http://www.mediaevent.de/css2/`):
  Ein Buch von Ulrike Häßler mit umfangreichen Online-Materialien.
- ***Dan's Web Tips*** (`http://webtips.dan.info/`):
  Allgemeine Informationen zum Thema Webdesign mit zahlreichen Hinweisen auf Style Sheets; die Einleitung (`http://webtips.dan.info/intro.html`) enthält eine ausgezeichnete Diskussion der verschiedenen Standpunkte (*structuralists* vs. *presentationalists*).
- **`comp.infosystems.www.authoring.stylesheets`** (Newsgruppe)

### 6.3 Positionierung von Boxen

Wer komplexere Style Sheets verwendet, muß sich mit dem *Box Model* vertraut machen: Fast alle HTML-Elemente befinden sich in einer (meist unsichtbaren) rechteckigen Box. Zur Darstellung einer Webseite berechnet der User Agent die Größe und die Position aller Boxen. Viele Eigenschaften von Boxen können mit Style Sheets definiert werden – Größe (`width`, `height`), Rahmen (`border`), innerer und äußerer Rand (`padding` und `margin`) und auch die Position (`position`). Letztere ergibt sich meistens automatisch, kann aber auch explizit angegeben werden: Mit `position: fixed` kann beispielsweise die Position einzelner Elemente auf dem Bildschirm fixiert werden, sodaß diese Elemente beim Scrollen nicht mitwandern. Ein Beispiel ist der Kasten rechts oben auf der CSS-Seite des *World Wide Web Consortium* (`http://www.w3.org/Style/CSS/`). Leider kann man diesen Effekt mit dem Internet Explorer nicht bewundern, da er von diesem Browser nicht unterstützt wird.

## 7. Style Sheets – pro und contra

Wer schon einige Webseiten erstellt hat, die Grundzüge von HTML und vielleicht den Umgang mit einem HTML-Editor wie Dreamweaver oder Frontpage gelernt hat, steht früher oder später vor der Frage: *Soll ich Cascading Style Sheets erlernen und meine weiteren Webseiten damit gestalten?* Vieles spricht dafür, aber auch einiges dagegen.

- Style Sheets in Kombination mit HTML sind ein viel mächtigeres Werkzeug als HTML alleine, selbst mit allen möglichen proprietären Erweiterungen. Viele Aufgaben, die mit HTML gar nicht oder nur sehr schwierig zu lösen sind, werden mit Style Sheets trivial.

- Das „händische" Design von HTML-Dokumenten in Verbindung mit Style Sheets ist sehr weit entfernt von WYSIWYG-Editoren[6] und erfordert ein beträchtliches Abstraktionsvermögen: HTML-Design mit Style Sheets erinnert ein wenig an Textverarbeitung mit TeX.

- Die Browser-Unterstützung – vor allem durch den Internet Explorer – ist noch immer nicht vollständig und fehlerfrei, obwohl der CSS2-Standard schon vor fast fünf Jahren beschlossen wurde. Die schleppende Implementierung durch die Browser-Hersteller ist sicherlich mit schuld daran, daß Style Sheets nicht weiter verbreitet sind. Solange Netscape 4 einen bedeutenden Marktanteil hatte, waren Style Sheets im kommerziellen Einsatz

6) Etliche HTML-Editoren verwenden intern gelegentlich `style`-Elemente, die allerdings nie die Qualität von manuell erstellten Style Sheets erreichen. Beispielsweise haben manche Versionen von Microsoft Word eine Funktion *Export to HTML*, die für das simpelste Dokument HTML-Code mit seitenlangen `style`-Angaben erzeugt.

praktisch ausgeschlossen. Heute ist es aufgrund des Quasi-Monopols des Internet Explorer ziemlich sinnlos, Features zu verwenden, die dieser nicht unterstützt.

- Die Fehlersuche ist oft außerordentlich mühsam. Wenn eine Webseite mit Style Sheets nicht so aussieht, wie sie soll, so kann das eine Reihe von Ursachen haben. Am leichtesten zu finden sind noch Syntax-Fehler im HTML-Code oder im Style Sheet. Prinzipiell sollte jedes HTML-Dokument syntaktisch korrekt sein – bei Verwendung von Style Sheets wirken sich Syntax-Fehler oft viel gravierender aus. Mittels `http://validator.w3.org/` und `http://jigsaw.w3.org/css-validator/` können HTML-Dokumente und Style Sheets auf korrekte Syntax überprüft werden.

  Manchmal sind HTML-Dokumente und Style Sheets vollkommen korrekt und es funktioniert trotzdem nicht: Dann liegt es an Browser-Bugs oder fehlender Browser-Unterstützung. Daher ist es unbedingt erforderlich, Style Sheets mit mehreren Browsern zu testen. Die häufigste Fehlerursache ist jedoch eine falsche Interpretation der Vererbungs- und Präzedenz-Regeln (siehe Abschnitt 4).

- Style Sheets bedeuten oft einen hohen Initialaufwand, der sich erst später rentiert: Es kostet manchmal Blut, Schweiß und Tränen, bis ein HTML-Dokument mit einem Style Sheet sich mit allen möglichen Browsern so verhält, wie es soll. Sobald dieser Zustand allerdings erreicht ist, ist die Gestaltung von weiteren HTML-Dokumenten, die denselben Style Sheet verwenden, trivial: Der HTML-Code von solchen Dokumenten ist meistens extrem einfach und kann leicht automatisch durch ein *Content Management System* (CMS) erstellt werden.

Cascading Style Sheets sind vielleicht nicht das ideale Werkzeug für Hobby-Webdesigner, für professionelle Anwendungen und größere Projekte sind sie jedoch unerläßlich: Ohne Style Sheets wäre es kaum gelungen, das CMS für die neue Homepage der Universität Wien mit den Ideen des Grafikers zu vereinbaren.

*Peter Marksteiner* ■

# IPv6 – Das Internetprotokoll der nächsten Generation

## Warum etwas ändern, das funktioniert?

Im Internet wird derzeit als Basis-Übertragungsprotokoll das *Internet Protocol, Version 4* (IPv4) verwendet. Jedes Gerät mit Internet-Anschluß benötigt eine weltweit eindeutige IP-Adresse, damit es von den anderen Netzwerkteilnehmern global erreichbar ist. Eine IPv4-Adresse (z.B. `131.130.1.11`) hat eine Länge von 32 Bit, das ergibt $2^{32}$ (rund 4,3 Milliarden) mögliche Adressen, von denen allerdings aus technologischen Gründen nicht alle für Endgeräte verwendet werden können. Der IPv4-Adreßraum wäre schon längst ausgeschöpft, gäbe es nicht diverse Hilfsmittel, mit denen er „künstlich ausgeweitet" werden kann – allen voran NAT (*Network Address Translation*, auch bekannt unter dem Namen *Masquerading*), das hauptsächlich dazu verwendet wird, mit nur einer IP-Adresse mehreren Endgeräten den Zugang zum Internet zu ermöglichen.

Leider haben alle diese Hilfsmittel gewisse Schönheitsfehler, beispielsweise einen hohen Konfigurationsaufwand, Performance-Einbußen, mangelnde Transparenz oder Probleme mit manchen Internet-Services. Abgesehen davon weist IPv4 neben seiner offensichtlichsten Schwachstelle – der Adreßknappheit – noch eine Reihe weiterer Mängel auf: Zum Zeitpunkt seiner Konzeptionierung (IPv4 wurde mit RFC 791[1)] vom 1. September 1981 „offiziell vorgestellt") waren das rasante Wachstum und die globale Verbreitung des Internet für niemanden absehbar, sodaß bald in etlichen Bereichen Probleme auftraten, die ursprünglich einfach nicht bedacht wurden bzw. nicht bedacht werden konnten. Aus diesen Gründen wurde bereits 1995 mit der Entwicklung des Internetprotokolls der nächsten Generation begonnen. Da die Versionsnummer 5 schon für eine andere Neuerung – nämlich das *Internet Stream Protocol, Version ST2* (RFC 1819) – vergeben war, erhielt das neue Protokoll den Namen IPv6.

## Hohe Ziele, fast erreicht

Die augenfälligste Verbesserung von IPv6 ist zweifellos die Vervielfachung des Adreßraums: Eine IPv6-Adresse hat eine Länge von 128 Bit; die Anzahl der möglichen Adressen steigt somit auf $2^{128}$ oder rund $3{,}4 \times 10^{38}$ (zum Vergleich: die Erde hat etwa $5{,}1 \times 10^{14}$ m$^2$). Das ist auch unter Berücksichtigung des erwarteten Bevölkerungszuwachses und unter der Annahme, daß zukünftig jeder Benutzer mehrere Geräte mit Internet-Anbindung einsetzen wird, mehr als ausreichend.

Aufgrund ihrer Länge wird eine IPv6-Adresse nicht mehr in der Form einer IPv4-Adresse (als *Dotted Quad*, z.B.

1) Alle RFCs (*Request for Comment*, der De-facto-Standard im Internet) können über den FTP-Server der Uni Wien abgerufen werden: `http://ftp.univie.ac.at/netinfo/rfc/rfc---.txt` (anstelle der Bindestriche ist die Nummer des Dokuments einzusetzen, z.B. `rfc791.txt`).

## Internationale und nationale IPv6-Projekte

IPv6 befindet sich derzeit in einer intensiven Test- und Konsolidierungsphase. In Europa wurden zu diesem Zweck mehrere Großprojekte ins Leben gerufen, an denen auch das österreichische Wissenschaftsnetz ACOnet beteiligt ist:

### 6NET

Das von der EU auf drei Jahre geförderte Projekt 6NET wurde am 1. Jänner 2002 gestartet. Die mittlerweile 35 Projektteilnehmer (sowohl kommerzielle Partner als auch Forschungs- und Bildungseinrichtungen) sind durch sogenannte *Native Links* miteinander verbunden, also durch Netzwerkverbindungen, die ausschließlich IPv6 als Protokoll verwenden. Das Projekt ist in mehrere *Work Packages* aufgeteilt, die die verschiedenen Bereiche des Projekts abdecken: Im Rahmen der einzelnen *Work Packages* werden Managementaufgaben, Migrationsstrategien, Services und Anwendungen sowie viele andere Aspekte getestet und bewertet. Das Ziel ist, ein internationales IPv6-Netzwerk zu etablieren, das sämtliche Anforderungen erfüllt, die an ein voll funktionsfähiges und verwaltbares Netz gestellt werden.

### 6Bone

6Bone ist eine internationale Test-Infrastruktur für IPv6 und besteht größtenteils aus einem virtuellen Netzwerk, das sich aus IPv6-in-IPv4-Tunneln zusammensetzt. Diese Tunnel werden mittlerweile Schritt für Schritt durch *Native Links* ersetzt, wodurch das Netz dem Teststatus entwächst und sich immer mehr zu einem Produktionsnetz entwickelt. Auch der für 6Bone reservierte IPv6-Adreßbereich wird zunehmend durch die von den RIRs (*Regional Internet Registries*; für den europäischen Bereich: RIPE NCC) vergebenen Adressen ersetzt.

### ACOnet und IPv6

Das österreichische Wissenschaftsnetz ACOnet ist *Lead Partner* für das *Work Package 3* des 6NET-Projekts, in dem vor allem grundlegende Netzwerkdienste behandelt werden – z.B. Routing, Nameservice, Multicast, Quality of Service, aber auch Prozeduren in Zusammenarbeit mit den RIRs. Zusätzlich ist ACOnet durch eine Reihe von Tunneln an 6Bone angebunden. Innerhalb von ACOnet ist derzeit sowohl eine dedizierte IPv6-Anbindung (mittels VLAN über die Gigabit-Ethernet-Infrastruktur), als auch eine Anbindung über IPv6-in-IPv4-Tunnel möglich. An der Universität Wien sind bereits diverse Services – z.B. Multicast und FTP – über IPv6 verfügbar.

`131.130.1.11`) geschrieben, sondern in acht Bereiche zu je 2 Byte (1 Byte = 8 Bit) geteilt, die in Hexadezimalzahlen notiert und durch Doppelpunkte getrennt werden (z.B. `2001:0628:0402:0002:0230:4fff:fe1b:c63d`). Eine solche Adresse läßt sich nur mehr schwer merken, was aber durch eine weitere signifikante Neuerung von IPv6 ausgeglichen wird: Die sogenannte *Stateless Address Autoconfiguration* ermöglicht die weitgehend automatische Internet-Konfiguration von Endgeräten mittels *Plug & Play*.

Darüber hinaus werden mit IPv6 etliche neue Ansätze verwirklicht bzw. vorhandene Technologien besser integriert, was vor allem Netzwerk-Administratoren das Leben erleichtern soll – beispielsweise:

- *Mobile IP* (Verwendung von mobilen Endgeräten – Laptops, Handys usw. – in fremden Netzen ohne manuelle Rekonfiguration),
- *Multihoming* (Anbindung an das Internet über mehrere Wege und infolgedessen Service-Verbesserung durch Redundanz und/oder Lastverteilung),
- *Quality of Service* (Bereitstellung einer garantierten Dienstgüte, z.B. für Sprachübertragung) und
- *Flow-Management* (Erkennung eines zusammengehörigen Datenstromes und somit raschere Verarbeitung).

Nicht zuletzt wurde in IPv6 auch ein Standard zur sicheren Datenübertragung (*IPsec*) aufgenommen.

IPv6 wird mittlerweile von allen nennenswerten Herstellern von Netzwerk-Ausstattung unterstützt, wenn auch teilweise noch in Beta-Versionen bzw. Vorserienmodellen. Ähnlich verhält es sich bei den Software-Herstellern: Nahezu alle aktuellen Betriebssysteme können bereits mit dem neuen Internet-Protokoll umgehen – alle Unix-Derivate (Linux, die BSD-Varianten, Solaris, AIX, …), MacOS X und auch Windows XP, wobei allerdings bei letzterem die IPv6-Unterstützung noch nicht in die grafische Oberfläche integriert, sondern nur über die Eingabeaufforderung zu erreichen ist. Auch viele Anwendungsprogramme „sprechen" inzwischen IPv6, ebenso wie die meisten Server-Programme – beispielsweise Webserver (Apache), Mailserver (sendmail, qmail, exim, postfix) und FTP-Server. Für all jene Fälle, wo IPv6 nicht unterstützt wird, gibt es diverse Hilfsmittel, mit denen eine Koexistenz von IPv4 und IPv6 (bzw. eine Übersetzung vom einen in das andere Protokoll und zurück) bewerkstelligt werden kann.

## Ausblick

Die Einführung von IPv6 ist ein sehr langfristiges Vorhaben, das – global gesehen – mit unterschiedlichem Elan betrieben wird: Während in Europa (aufgrund neuer Dienste) und im asiatisch-pazifischen Raum (aufgrund der erst jetzt einsetzenden Verbreitung des Internet in Regionen wie China

oder Indien) die verfügbaren IPv4-Adressen in näherer Zukunft knapp werden und dort infolgedessen viel Zeit und Geld in die Entwicklung von IPv6 investiert wird, zeigen die USA weniger Interesse an der raschen Einführung des neuen Protokolls – sie befinden sich in der glücklichen Lage, bereits in den Anfängen des Internet große Teile des IPv4-Adreßraums für sich reserviert zu haben, und verspüren nun entsprechend wenig Handlungsbedarf.

Ein weiterer Faktor, der eine baldige Einführung von IPv6 erforderlich zu machen schien, nämlich der bevorstehende Boom des mobilen Internet mittels UMTS und der damit verbundene sprunghafte Anstieg an benötigten IP-Adressen, hat sich inzwischen aufgrund verschiedener unvorhergesehener Schwierigkeiten um unbestimmte Zeit verzögert. Aber auch diverse *Peer to Peer*-Applikationen könnten den Einsatz von IPv6 vorantreiben: In all jenen Bereichen, wo jedes Endgerät gleichzeitig Client und Server für die jeweilige Anwendung ist, muß eine globale Erreichbarkeit und somit eine weltweit eindeutige IP-Adresse des Geräts gegeben sein. Solche Services und Anwendungen – z.B. IP-Telefonie, Videokonferenzen, Work-Flow-Applikationen, aber auch Videostreaming (Stichwort *Video on Demand*) oder Online-Spiele (auch mit Spielkonsolen wie X-box oder Playstation) – befinden sich derzeit noch überwiegend im Teststatus. Da ihre großräumige Einführung nicht von heute auf morgen geschehen wird, bleibt den Hardware- und Software-Entwicklern und den diversen Dienst-Anbietern noch ein wenig Zeit, um das neue Internet-Protokoll zu implementieren und zu testen, bevor sich die IPv6-Infrastruktur tatsächlich im Produktionsbetrieb bewähren muß.

Wann (bzw. ob) IPv6 flächendeckend eingesetzt werden wird, steht derzeit noch in den Sternen. Für den Benutzer wird der Umstieg auf das neue Internet-Protokoll aber voraussichtlich ohnehin wenig ändern: Ein wesentlicher Bestandteil von IPv6 ist die automatische Konfiguration von Endgeräten, weshalb Grund zur Hoffnung besteht, daß die Umstellung weitestgehend auf der Ebene der Netzwerkbetreiber vollzogen wird und die einzelnen Internet-Anwender nicht allzu viel davon bemerken werden.

## Links

Alle, die sich näher mit IPv6 beschäftigen möchten, können auf den folgenden Webseiten genauere (allerdings teilweise technisch sehr anspruchsvolle) Informationen finden:

- `http://www.6net.org/`
- `http://www.6bone.net/`
- `http://ipv6.aco.net/` *(im Aufbau)*
- `http://www.ipv6forum.com/`
- `http://www.ipv6.org/`
- `http://www.ipv6tf.org/`
- `http://www.isoc.org/briefings/007/index.html`

*Kurt Bauer* ■

# SPAMMER VS. BLACKLISTS:
## Ein ewiges Wettrüsten

Wenn man versucht, mit technischen Mitteln der Spam-Problematik Herr zu werden, können Verzeichnisse der Übeltäter und ihrer Komplizen durchaus von Nutzen sein: Ein automatischer Spam-Filter könnte, wenn er über Annehmen oder Abweisen einer eMail-Nachricht entscheiden soll, sozusagen den Strafregisterauszug des Absenders als Entscheidungsgrundlage heranziehen. *Blacklists* sind die informationstechnische Umsetzung solcher Strafregister. So überzeugend der Gedanke auf den ersten Blick sein mag – bei näherem Hinsehen zeigt sich, daß das alles, wie so oft, sehr kompliziert ist. Das heute anzutreffende Arsenal von Blacklists[1)] ergibt sich aus einer langen Geschichte von Listen, deren Umgehung, wieder neuen Listen, ...

### Blacklists von Absender-Domains

Die klassische Massenmail, bei der einfach vom eigenen Rechner aus Nachrichten an viele Adressen verschickt wurden, war die Technik der Anfangszeiten. Bereits 1994 wurde von Axel Boldt ein Verzeichnis angelegt, das bekannte Spammer mit ihren eMail-Adressen auflistete. Dieses wurde über Newsgruppen und eine Webseite verbreitet und mußte mehr oder weniger manuell in die Mailserver-Konfiguration integriert werden. Aber so wie bis zur Einführung der Bertillonage im späten 19. Jahrhundert (und später des Fingerabdrucks) die Polizei[2)] mit dem Problem zu kämpfen hatte, daß ihre Verbrecherkarteien wertlos waren, weil sich die Übeltäter immer neue Namen zulegten, wurde diese erste Generation von Blacklists dadurch unterlaufen, daß die Spammer dazu übergingen, die Absenderadressen frei zu erfinden.

Seit langem ist es daher schon Stand der Technik, Mail nicht entgegenzunehmen, wenn die Absenderadresse nicht existiert. Dabei kann jedoch im allgemeinen nur der Domain-

1) Ein umfassendes Verzeichnis gibt es unter `http://www.declude.com/junkmail/support/ip4r.htm`.

2) Ein Buchtip für alle, die immer schon wissen wollten, was Sherlock Holmes in seinem Labor getan und in seine Monographien geschrieben hat: Thorwald, Jürgen: *Das Jahrhundert der Detektive*, Zürich 1965, Droemersche Verlagsanstalt A.G.

Teil (also das, was rechts vom @-Zeichen steht) überprüft werden. Für den ernsthaften Spammer stellt diese Maßnahme kein Problem dar: Wenn er schon die Absenderadresse fälscht, kann er auch gleich eine existierende Domain eintragen.

Blacklists, die Absender-Domains verzeichnen, haben deshalb an Bedeutung verloren.[3] Ein Äquivalent des Fingerabdrucks mußte gefunden werden.

### Blacklists von IP-Adressen

Die IP-Adresse des absendenden Mailservers ist ein unfälschbares Merkmal, an dem man Spammer zuverlässig erkennen kann – das war zumindest der Gedanke, der der 1997 in Betrieb gegangenen *Realtime Blackhole List* (RBL) des *Mail Abuse Prevention System* (MAPS[4]) zugrunde gelegt wurde. Diese konnte auch online abgefragt werden, sodaß die Notwendigkeit, regelmäßig Listen in die Mailserver zu laden, entfiel. RBL und ihre Nachfolger funktionieren folgendermaßen: Bevor ein entsprechend konfigurierter Mailserver eine Nachricht empfängt, prüft er über das Netzwerk, ob die IP-Adresse des absendenden Mailservers in einer Blacklist aufscheint. Ist das der Fall, wird die Nachricht nicht angenommen, sondern die Transaktion mit einer Fehlermeldung abgebrochen.

Das Problem dabei: Wird ein Mailserver außer vom Spammer auch noch von anderen Menschen benutzt, kann auch deren Mail nicht mehr zugestellt werden.

### Open Relay-Blacklists

Auch gegen diese – aus Sicht des Spammers doch recht lästigen – Blacklists war bald ein Kraut gewachsen: Durch Verwendung sogenannter Open Relays kann man sie leicht umgehen. Dazu stellt der Absender den Spam nicht direkt zu, sondern sendet ihn stattdessen einem beliebigen anderen Mailserver, der nicht in den Blacklists aufscheint und auch selbst nicht durch Blacklists geschützt ist. Dieser leitet die Nachrichten nun seinerseits weiter (im SMTP-Jargon sagt man: der Mailserver fungiert als Relay), und weil das mißbrauchte Relay nicht in den Blacklists aufscheint, kann der Spammer auf diese Weise seine Werbung zustellen.

Als Adam und Eva noch im Paradies herumtollten und das Internet noch gut war, war es ganz normal, daß Mailserver von überall Mail entgegennehmen und dann nach bestem Wissen und Gewissen zustellen – zu UUCP[5]-Zeiten, als noch nicht jeder Rechner über das Internet mit jedem anderen direkt Kontakt aufnehmen konnte, ging es auch gar nicht anders.

Etwa Mitte der neunziger Jahre mußte diese Politik wegen des Spamproblems geändert werden: Ein Mailserver hat eMail nur zu bearbeiten, wenn

- er Mailserver für den Empfänger ist oder spezielle Abkommen für die Empfänger-Domain bestehen (*Backup Mail Exchanger*) – so wie alle Mailserver des ZID Nachrichten für Adressen der Domain `univie.ac.at` entgegennehmen;
- der absendende Rechner netzwerktechnisch berechtigter Nutzer dieses Mailservers ist – so wie die in den Konfigurationsanleitungen des ZID als *Outgoing Mailserver* oder *Postausgang*(*SMTP*)*-Server* beschriebenen Server Nachrichten von allen Rechnern aus dem Datennetz der Uni Wien zum Versand annehmen;
- auf andere Weise (z.B. *SMTP after POP*, authentifiziertes SMTP) sichergestellt ist, daß der Absender befugt ist, diesen Server als Relay zu verwenden.

Seither gilt es als grober Fehler, wenn ein Mailserver Nachrichten von überall an beliebige Empfänger weiterleitet. Ein solcher Server wird als *Open Third Party Relay* (oder kurz *Open Relay*) bezeichnet. Leider nimmt die Zahl dieser Open Relays nicht ab, sondern zu: Mailserver, die nach dem Klick-Klick-Geht-Schon-Verfahren installiert wurden, in der Standardkonfiguration nicht gesichert bzw. zu leicht unsicher einzustellen sind (MS-Exchange gilt hier als Haupttäter) und obendrein noch über eine schnelle Internet-Anbindung verfügen (Kabel-Provider, xDSL oder besser), erfreuen sich einer kaninchenartigen Vermehrungsrate.

Die Antwort der Antispam-Front ließ nicht lange auf sich warten: Was mit den bösen Spam-Absendern funktioniert hat, sollte auch mit den Open Relays klappen. Neue Blacklists wurden ins Leben gerufen – die bekannteste davon ist die mittlerweile eingestellte ORBS (*Open Relay Blocking System*)-Liste.

Die Methode hat aber einen Haken: Entscheidet sich ein Postmaster, seinen Mailserver durch eine solche Liste zu schützen, sperrt er nicht nur Spammer, sondern auch alle legitimen Anwender des schlecht gewarteten Systems aus. Das Ergebnis: Es werden in nicht zu vernachlässigender Zahl auch erwünschte Nachrichten abgewiesen.[6]

### Wählleitungs-Blacklists

Ein Wählleitungszugang über Modem oder ISDN macht aus dem eingewählten Rechner für die Dauer der Verbindung einen vollwertigen Internet-Host, mit allen Möglichkeiten, die auch die großen Server haben – natürlich vorausgesetzt, die entsprechende Software ist vorhanden.

---

3) Eine historische Spamdomain-Liste aus 1997 ist unter `http://web.archive.org/web/19970419180153/bitgate.com/spam/spamsites.html` zu finden.

4) Man bemerke, daß MAPS, rückwärts gelesen, außerdem das Wort Spam ergibt. Mehr zu MAPS unter `http://www.mail-abuse.org/`.

5) *Unix to Unix CoPy* – ein Verfahren, um Dateien und Befehle z.B. über Modem-Verbindungen zwischen verschiedenen Computern zu übertragen. Hierbei handelt es sich um alte Sagen, die Internet-Opas ihren Enkeln am Kaminfeuer erzählen, darum sei in diesem Artikel nicht näher darauf eingegangen.

6) Hardliner sehen darin sogar einen positiven Effekt: In der Folge werden die unzufriedenen Benutzer, so lautet die Theorie, auf den Administrator des Open Relay Druck ausüben, das Problem zu beheben. Der ZID der Uni Wien hat jedoch auf derartige Erziehungsspielchen zugunsten zuverlässiger Mailzustellung verzichtet.

Durch den Direktversand mit einem eigenen Mailserver und einer Anbindung über Wählleitungszugänge lassen sich Blacklists ebenfalls einfach umgehen: Da im Gegensatz zu Mailservern mit permanenter Internet-Anbindung bei jeder Einwahl eine neue IP-Adresse zugewiesen wird, kann diese nicht in Blacklists aufgenommen werden. Außerdem sind solche Zugänge billig, und ein einmal gesperrter Zugang kann leicht durch einen neuen ersetzt werden.

Gegen diese Spam-Methode wurden wieder Blacklists mit neuer Semantik ins Leben gerufen: Diese Listen – z.B. DUL (*Dialup User List*) – verzeichnen IP-Adressen, die von Spammern für Einwahlzugänge verwendet werden.

Wenn man sich also auf den Standpunkt stellt, daß der Einwahl-Benutzer gefälligst den (möglicherweise schlecht funktionierenden) Mailserver seines Providers verwenden soll, anstatt selbst direkt Mail zuzustellen, kann man seinen Mailserver dadurch schützen, daß man von solchen IP-Adressen keine Mail annimmt. Daß als Nebenwirkung eine eventuell signifikante Zahl legitimer Sendungen ebenfalls abgewiesen wird, versteht sich von selbst.

## Proxy-Blacklists

Gefinkelter als der Versand von eMail über Open Relays ist die Verwendung offener Proxy-Server. Ein Proxy, so wie er hier verwendet wird, nimmt vom Spammer eine Datenverbindung entgegen, baut zu einem Ziel (in unserem Fall dem Mailserver des Opfers) eine neue Verbindung auf und verbindet die beiden Datenströme wie beim *Stille Post*-Spiel miteinander.

Das Subtile an der Methode ist, daß der Proxy nur als „Durchlauferhitzer" für die übertragenen Buchstaben wirkt: Eine verräterische `Received:`-Zeile, die die IP-Adresse des wirklichen Absenders enthält, kann ein Proxy nicht hinzufügen – der Empfänger sieht lediglich die IP-Adresse des Proxy-Servers. Der wahre Absender läßt sich nur ausforschen, wenn der Proxy Log-Dateien geführt hat und auf diese zugegriffen werden kann. Gerade dort, wo solche Administrationspeinlichkeiten anzutreffen sind, ist aber kaum mit brauchbaren Log-Dateien zu rechnen.

Im Bereich der Universität Wien stellen falsch konfigurierte Winproxy, Wingate usw. das Hauptproblem dar. Diese Programme werden typischerweise dann eingesetzt, wenn *StudentConnect*-Benutzer an ihrem chello-Anschluß mehr als einen PC betreiben wollen. Normalerweise ist das nicht möglich, da man nur eine IP-Adresse erhält. Läßt man die PCs jedoch auf einen Proxy zugreifen und diesen die Verbindung (zum Beispiel zum Uni-Mailserver) herstellen, ist das Problem gelöst: Aus der Sicht des Uni-Mailservers kommt die Verbindung vom *StudentConnect*-Anschluß, daher ist das Relaying erlaubt. Wenn aber nicht sichergestellt wird, daß dieses Weiterverbinden nur von innerhalb des Heim-Netzwerks funktioniert, hat man ein neues, großes Problem: Ein Spammer, der den offenen Proxy entdeckt (und sie werden entdeckt!), verbindet sich einfach dorthin, wird als *StudentConnect*-Benutzer zu uns weiterverbunden und kann nun die volle Bandbreite unserer Internet-Anbindung und die Kapazität unserer Server zum Spam-Versand nutzen. Mit mehr oder weniger großem Aufwand lassen sich alle ungeschützten (also fehlkonfigurierten) Winproxy, Wingate, HTTP-Proxies (z.B. Squid) und Socks-Proxies so verwenden.

Die Folge: Die Uni-Server landen auf Blacklists, der Ruf ist ruiniert, die Postmaster-Mailbox geht vor Beschwerden über, der ganze Müll muß aus den Mailspools entsorgt werden. Klarerweise wird, sobald wir auf eine solche Installation aufmerksam werden, die betreffende IP-Adresse sofort gesperrt.

Als Maßnahme gegen offene Proxies wurden wieder neue Blacklists geschaffen. Allerdings gibt es jetzt ein zusätzliches Problem: Es ist durchaus üblich, daß ein Server sowohl Mail- als auch Proxy-Dienste abwickelt. Da einer eingehenden SMTP-Verbindung aber nicht anzumerken ist, ob sie vom Mailserver oder vom Proxy-Server kommt, können Blacklists widersprüchliche Ergebnisse liefern: Der Rechner könnte z.B. als offener Proxy gelistet sein, aber bezüglich seines Mailservers eine weiße Weste haben. Mail von offenen Proxies abzuweisen bedeutet also, auch sämtliche Benutzer auszusperren, die denselben Rechner als Mailserver benutzen – auch wenn dieser ohne Fehl und Tadel ist.

## FormMail-Blacklists

FormMail ist ein CGI-Skript, das ausgefüllte Web-Formulare (Anmeldungen, Feedback usw.) entgegennimmt und die Daten in maschinenlesbarer Form dem Seiteneigentümer per eMail zustellt. Aufgrund des sträflich naiven Designs dieser sehr beliebten Software war es mit älteren FormMail-Versionen[7] – die leider immer noch im Umlauf sind – kein Problem, beliebige „Formularinhalte" an beliebige Adressen zu schicken.

Wenn Sie eine Nachricht erhalten, die mit

```
Below is the result of your feedback form.
It was submitted by (...@...) on Thursday,
January 16, 2003 at 10:03:50
```

beginnt, haben Sie wohl einen FormMail-Spam vor sich – es sei denn, es handelt sich wirklich um „Ihr" FormMail. Natürlich gibt es auch dafür Blacklists, auf die ebenfalls das bereits zu den Proxy-Blacklists Gesagte zutrifft.

## Fazit

Die Unzahl an Blacklists, die verwirrende Vielfalt ihrer Bedeutungen und die zunehmende Zahl von Unschuldigen, die bei konsequentem Einsatz von Blacklists ebenfalls geblockt werden, führen zur Schlußfolgerung, daß allein damit kein sicherer Spamschutz möglich ist. Dennoch sind Blacklists nach wie vor eine unersetzliche Informationsquelle für Spam-Filter.

*Alexander Talos* ■

7) vor Version 1.91 von April 2002 (siehe `http://www.scriptarchive.com/formmail.html`)

# 101 – Der Spam-Filter der Uni Wien

Spam beeinträchtigt zunehmend die schnelle und einfache Kommunikation über das Medium eMail: Schätzungen zufolge erreicht das Spam-Volumen bald das der legitimen Mail. Daß die Mailserver oftmals überfallsartig durch große Mail-Mengen belastet werden, ließe sich noch durch massiven Hardware-Einsatz kompensieren. Die Zeit und die Nerven, die die Empfänger mittlerweile für Spam aufwenden müssen, sind aber für Geld nicht zu haben: Das Durchforsten Spam-gefüllter Mailboxen gleicht der Suche nach der Nadel im Heuhaufen. Auch das Risiko, wichtige Nachrichten zu übersehen, ist zu einem ernstzunehmenden Problem geworden. Wie in den beiden Artikeln *Forever Spam!?* (Seite 2) und *Spammer vs. Blacklists: Ein ewiges Wettrüsten* (Seite 37) ausführlich dargelegt wurde, sind wirkungsvolle Maßnahmen gegen Spam aber alles andere als trivial.

## Status quo

Kurz zusammengefaßt, ist die Ausgangssituation folgende:

- Blacklists brandmarken ganze Mailserver und damit alle ihre Benutzer als Spammer. Zwar kann man mit Blacklists eine Zeitlang gute Ergebnisse erzielen, weil die betroffenen Server selten zu denen gehören, mit denen man kommunizieren möchte; wird aber doch einmal ein solcher gelistet (wozu das Fehlverhalten eines einzigen Benutzers ausreichen kann!), ist die Katastrophe dafür umso größer.[1)]

- Content Filter leiden darunter, daß am Inhalt allein nicht zwischen Spam und Nicht-Spam unterschieden werden kann – dies vor allem deshalb, weil es keine verallgemeinerbaren Reizwort-Listen gibt.

- Filter auf Basis von Bayesscher Statistik haben eine gute Erkennungsrate, müssen aber von jedem Empfänger persönlich „trainiert“ werden und scheiden somit für die Verwendung in einem zentralen Spam-Filter weitgehend aus.

- Spam-Traps erlauben eine äußerst trennscharfe Spam-Erkennung, dieses aber meist zu spät.

- Es ist kein Ende des Wettrüstens zwischen Spam-Versendern und Spam-Blockern abzusehen.

Obwohl durchaus Werkzeuge existieren, die mit guter Treffsicherheit Spam als solchen erkennen, bleibt ein gewisses Restrisiko: Wird eine erwünschte Nachricht fälschlicherweise als Spam klassifiziert (*False Positive*) und abgewiesen, d.h. mit einer Fehlermeldung an den Absender zurückgeschickt, besteht die Gefahr, daß die Fehlermeldung nicht ankommt (sei es aufgrund einer irrtümlich falschen Absenderadresse oder aufgrund sonstiger Probleme außerhalb unseres Bereichs) oder daß der Absender die Fehlermeldung nicht liest, zu spät liest oder nicht versteht. In solchen Fällen geht eine legitime Nachricht effektiv verloren.

Spam-Filter verringern also einerseits die Zuverlässigkeit des Mediums eMail, weil False Positives unter Umständen nicht bemerkt werden. Andererseits erhöhen sie sie aber dadurch, daß legitime Nachrichten nicht so leicht vom Empfänger übersehen oder irrtümlich gelöscht werden.

### Spam-Filter optimieren

Leider kann man bei einem Filter nicht einfach an einer Schraube drehen und ihn damit ohne Nebenwirkungen sicherer machen. Wie bei Antikörpermessungen oder Fingerprint-Scans wird auch bei vielen Spam-Filtern aus dem vorliegenden Material – in diesem Fall die eMail-Nachricht – ein Ergebnis in Form einer Zahl errechnet. Ob der Test positiv oder negativ ausgefallen ist, wird anhand einer Entscheidungsschwelle beurteilt, die je nach Anforderung individuell zu definieren ist: Setzt man die Entscheidungsschwelle niedrig an (d.h. der Test wird bereits bei einigen wenigen entsprechenden Indizien als positiv erachtet), ist zwar mit einer sehr guten Erkennungsrate, aber auch mit relativ vielen False Positives zu rechnen. Wählt man die Entscheidungsschwelle hoch, sodaß der Test nur bei großer Übereinstimmung als positiv gilt, werden False Positives weitgehend vermieden, dafür aber umso mehr tatsächlich positive Proben nicht erkannt.

Im Falle eines Spam-Filters wiegt eine irrtümlich abgewiesene Nachricht unverhältnismäßig schwerer als eine irrtümlich zugestellte. Ein Spam-Filter muß also mit extrem hoher Entscheidungsschwelle betrieben werden, wodurch aber die Effizienz sehr gering wird bzw. manche Methoden (etwa Blacklists) weitestgehend ausscheiden.

Durch Kombination mehrerer unabhängiger Erkennungsmethoden kann man jedoch – rein wahrscheinlichkeitsrechnerisch – auf deutlich bessere Ergebnisse hoffen.[2)] Auf Spam-Filter angewandt: Daß Spam gleichzeitig vom Inhalt her nach Spam aussieht und von einem Server kommt, der auf einer Blacklist verzeichnet ist, ist zumindest einige Zeit nach Beginn des Spam-Versandes sehr wahrscheinlich. Daß

1) In der Newsgruppe `at.internet.provider` gab es einen Aufschrei, als chello-Benutzer plötzlich nicht mehr an den Mailserver einer österreichischen Universität schreiben konnten. Die Schuld daran trägt weder chello noch die betroffene Uni noch die verwendete Blacklist – daß so etwas früher oder später passiert, ist die unvermeidliche Konsequenz von hostbasiertem Blacklisting.

2) Ein leicht verständliches Beispiel, bei dem als Alzheimer-Test zwei simple Tests kombiniert und auch die Begriffe von positivem und negativem Vorhersagewert anschaulich illustriert werden, findet man unter dem URL `http://www.healthandage.com/DHome/gm=2!gid2=1394`.

aber eine legitime Nachricht sowohl verdächtigen Text enthält, der bei einem Content Filter Fehlalarm auslöst, als auch von einem gelisteten Server kommt, ist extrem unwahrscheinlich. Der Grundgedanke beim Design des Spam-Filters für die Universität Wien war folglich, die zahlreichen, in ihrer Disziplin jeweils hervorragenden Spam-Filtermethoden zusammenzufassen.

### Uni Wien ist anders

Die Situation an der Uni Wien unterscheidet sich von vielen anderen Organisationen. Sie ist gekennzeichnet durch

- die prinzipielle Unmöglichkeit, die eMail-Adressen geheimzuhalten (zumindest was die Uni-Mitarbeiter/innen betrifft),
- eine große Anzahl aufgelassener eMail-Adressen,
- eine große Anzahl von Benutzer/innen und weitgehend autonomen Gruppen – daher große Benutzer-Diversität hinsichtlich
  - „gefährlicher" Schlüsselwörter in der Korrespondenz,
  - der Länder und der Sprachen, mit bzw. in denen Mailverkehr stattfindet,
  - der verwendeten Betriebssysteme, Mailklienten und Zeichensätze, und
  - der Erwartungen an einen Spamfilter.

Daraus ergeben sich zwar einerseits Probleme (z.B. mit dem Content Filtering), andererseits aber auch Chancen. Beispielsweise ist es möglich, die aufgelassenen Mailadressen – an die ohnehin nur mehr von Spammern Nachrichten gesendet werden – als Spam-Traps zu verwenden: Bevor eine solche Nachricht ordnungsgemäß zurückgewiesen wird, kann ihre Prüfsumme berechnet und in einer lokalen DCC-Datenbank[3)] gespeichert werden.[4)]

Außer Zweifel steht, daß es dem einzelnen Benutzer überlassen bleiben muß, ob und inwieweit seine eMail gefiltert wird. Manche Filterprogramme wie z.B. SpamAssassin unterstützen dies, indem sie nach einem Punktesystem für jede Nachricht eine Spam-Bewertung in Form einer Zahl berechnen und als Headerzeile vermerken. Das ermöglicht ein empfängerseitiges Filtern, wobei der Empfänger durch Wahl der Entscheidungsschwelle selbst bestimmen kann, wie sensitiv (gute Spam-Erkennung) bzw. selektiv (wenig False Positives) der Filter sein soll.

Diese Herangehensweise hat aber einige Nachteile:

- Der Benutzer muß in seinem Mailklienten einen Filter konfigurieren.
- Die Spam-Nachrichten müssen trotzdem zugestellt werden, belasten also nach wie vor die Server.
- Je nach verwendetem Zugriffsprotokoll müssen die Nachrichten weiterhin – unter Umständen sogar von daheim per Modem – geladen werden, bevor sie gelöscht werden können.
- Es gibt keine Möglichkeit, verdächtige Nachrichten differenziert zu behandeln (z.B. durch „Einkühlen" bei bestimmten Konstellationen von Spam-Indikatoren; siehe weiter unten).
- Der Filter-Software geht eine Informationsquelle verloren: Würde der Mailserver die verdächtigen Nachrichten abweisen und Fehlermeldungen an die Absender schicken, könnte deren Nichterreichbarkeit als Spam-Indiz gewertet werden.

## Mit Patchwork gegen Spam

Die Implementation eines Spam-Filters an der Uni Wien stellt eine besondere Herausforderung dar: Obwohl es die Aufgabe eines Spam-Filters ist, die Zustellung bestimmter Nachrichten zu verhindern, muß natürlich die hohe Qualität des eMail-Service erhalten bleiben. Das setzt höchstmögliche Trennschärfe bei den Filtermechanismen und die freie Entscheidung des Empfängers über deren Einsatz voraus. Vor allem muß der Spam-Filter vollautomatisch funktionieren: Ein „Probelesen" durch ZID-Mitarbeiter kommt aus moralischen, personellen und rechtlichen Gründen sowieso nicht in Frage – aber auch die manuelle Wartung von Filterlisten jeglicher Art (etwa aufgrund von Beschwerden unserer Benutzer) ist bei Systemen dieser Größe schlichtweg unmöglich.

Vor diesem Hintergrund hat sich für den neuen Spam-Filter der Universität Wien, der in Anlehnung an § 101 TKG den Namen *101* erhielt, folgendes Arbeitsmodell herauskristallisiert:

- Jeder Benutzer kann den Spam-Filter über eine Webmaske entweder mit den vom ZID empfohlenen Einstellungen aktivieren oder nach eigenem Geschmack konfigurieren. Die Konfigurationsdaten werden in einer Oracle-Datenbank gespeichert und von dort zu den Filterservern übertragen.
- Die Mailserver des ZID legen einlangende Nachrichten dem Spam-Filter zur Prüfung vor. Dort werden die Nachrichten von mehreren Modulen bearbeitet:
  - HTML-Mail wird in Text umgewandelt.
  - Base64-codierte Nachrichten werden decodiert.
  - Allfällige Blacklist-Einträge werden abgefragt.

3) DCC: siehe Seite 11

4) Die Zahl der Exemplare einer Nachricht, die an nichtexistente Adressen geschickt wurden, ist eine ungemein wertvolle Informationsquelle, über die kleine und mittlere Institutionen nicht verfügen. Aufgelassene Adressen sind aber natürlich mit geringerer Gewichtung zu behandeln als dedizierte Spam-Traps, da es z.B. durchaus vorkommen kann, daß jemand eine Nachricht an die neue und sicherheitshalber als Kopie auch an die alte Adresse des Empfängers schickt.

  - Es wird überprüft, ob die Absenderadresse bereits als unzustellbar erkannt wurde.[5)]
  - Aus dem Inhalt werden Prüfsummen berechnet und mit den in DCC gespeicherten verglichen, um festzustellen, ob es sich um Massenmail handelt oder Nachrichten mit gleicher Prüfsumme bereits bei Spam-Trap-Adressen angekommen sind.
  - Content Filter suchen nach Spam-typischen Phrasen und Wörtern.
  - Die Filterkonfiguration des Empfängers wird aus der Datenbank abgerufen.
  - Die Envelope-Absenderadresse und die Headerzeilen werden mit der benutzerspezifizierten White- und Blacklist abgeglichen.

- Die gewonnenen Informationen werden ausgewertet, und je nach Ergebnis kann die Nachricht
  - angenommen und normal zugestellt,
  - mit einer Headerzeile als Spam markiert,
  - bei IMAP-Benutzern bereits am Server in einen Spam-Folder einsortiert,[6)]
  - abgewiesen (d.h. der Absender erhält eine Fehlermeldung) oder
  - eine Zeitlang „auf Eis gelegt"

  werden.

### Gut gekühlt

Ein besonderes Feature, das unseres Wissens bei 101 erstmals eingesetzt wird, ist die Möglichkeit, eMail vorläufig auf Eis zu legen: Wird eine Nachricht (z.B. von den Content Filter-Mechanismen) als „verdächtig" eingestuft, kann der Filter sie vorerst weder abweisen noch zustellen, sondern weitere Informationen abwarten. Nach einiger Zeit wird die Nachricht dann erneut bewertet. Inzwischen kann sich einiges geändert haben:

- Die DCC-Mechanismen haben die Nachricht als Massenmail erkannt;

- eine Nachricht mit derselben Prüfsumme ist auch an eine oder mehrere Spam-Trap-Adresse(n) zugestellt worden;

- der absendende Mailserver ist in (weitere) Blacklists aufgenommen worden;

- Nachrichten – z.B. Fehlermeldungen – an die Absenderadresse haben sich als unzustellbar erwiesen.

Indem man verdächtige Nachrichten ein wenig nachreifen läßt, kann gerade in der Grauzone eine Trennschärfe erreicht werden, die bei sofortiger Beurteilung auch durch noch so sorgfältige Wahl einer Entscheidungsschwelle nicht zu erzielen wäre.

### Realisierung

Beim Design des neuen Spam-Filters wurde besonderer Wert auf einen modularen Aufbau gelegt, um bereits existierende Spam-Filter (z.B. SpamAssassin) leicht einfügen und die Techniken zur Spam-Bekämpfung ständig weiterentwickeln zu können. 101 besteht nun aus einem Filter-Kern und mehreren Plugins, die die eigentliche Filterarbeit durchführen.

Der Kern übernimmt die Koordination des Filtervorgangs: Er kümmert sich darum, daß die Plugin-Prozesse gestartet werden, daß den Plugins Nachrichten zur Verarbeitung zugewiesen werden, usw. Neue Plugins lassen sich im laufenden Betrieb hinzufügen – der Kern sorgt dann dafür, daß Transaktionen, die mit einer älteren Konfiguration begonnen wurden, auch mit dieser beendet werden.

Plugins gibt es mit verschiedenen Funktionen:

- Das Milter-Interface[7)] für die Kommunikation mit dem Mailserver;

- Sensoren, um Informationen über die behandelte Nachricht zu gewinnen (Blacklist-Abfragen, Content Filter, ...);

- ein Modul,[8)] das die gewonnenen Informationen auswertet und anhand eines einfachen Regelwerks entscheidet, wie mit der Nachricht zu verfahren ist;

- Aktoren, die das Ergebnis des Entscheidungsmoduls umsetzen und statistische Auswertungen für die Optimierung und Weiterentwicklung des Filters vornehmen.

In diesen Rahmen können leicht zusätzliche Plugins eingebaut werden; einige neue Funktionen befinden sich bereits in Entwicklung.

## Was können Sie einstellen?

Wie bereits erwähnt, ist es Ihnen überlassen, ob und in welchem Ausmaß Sie den neuen Spam-Filter einsetzen wollen – 101 wird nur auf Ihren ausdrücklichen Wunsch hin für Sie tätig. Solange Sie den Filter nicht aktivieren, bleibt für Sie alles beim alten: Sie erhalten wie bisher alle an Ihre Mailadresse gerichteten Nachrichten einschließlich allfälliger

5) Da in der Vergangenheit die Mailserver der Uni Wien ständig durch notorisch unzustellbare Mail verstopft wurden, wird diese bereits seit einiger Zeit mit geringerer Priorität behandelt. Die Information über unzustellbare Adressen ist somit ohnehin vorhanden und kann auch für den Spam-Filter verwendet werden.

6) Dieses Feature ist ab Frühjahr 2003 für Mailbox-Benutzer und voraussichtlich ab Sommer 2003 auch für Unet-Benutzer verfügbar.

7) Diese Technik wird bereits beim Virenscanner erfolgreich eingesetzt (siehe *Comment 01/1*, Seite 28 bzw. `http://www.univie.ac.at/comment/01-1/011_28.html`). Mittlerweile haben wir die Serversoftware sendmail dahingehend erweitert, daß der Mailserver die Last auf mehrere Filterserver verteilen und im Falle von Problemen mit einem Server auf die anderen ausweichen kann.

8) Dieses Plugin beruht derzeit auf den für unsere Zwecke angenehm schlanken RICE (*Routines for Implementing C Expert systems*) von René Jager: `http://www-2.cs.cmu.edu/afs/cs/project/ai-repository/ai/areas/fuzzy/systems/rice/0.html`.

`X-Spam-Flags:`-Header (siehe URL `http://www.univie.ac.at/ZID/faq/spam-rbl.html`).

Wenn Sie sich entschlossen haben, den Spam-Filter zu aktivieren, rufen Sie die Webseite

- **`https://data.univie.ac.at/mailbox/antispam.html`** (Uni-Mitarbeiter/innen) bzw.

- **`https://data.univie.ac.at/unet/antispam.html`** (Studierende)

auf. Nach dem Login mittels Mailbox- bzw. Unet-UserID können Sie entweder die vom ZID empfohlene Einstellung auswählen oder den Filter nach Wunsch konfigurieren. Unabhängig von den Filtereinstellungen ist es hier auch möglich, persönliche White- und Blacklists anzulegen.

Eine Übersicht über die Einstellungsmöglichkeiten finden Sie im nebenstehenden Kasten. Die ZID-Empfehlung lautet folgendermaßen:

- *Mit einer Headerzeile markieren:* ***Nie***
  Gerade im Falle von False Positives ist es sinnvoller, die Nachricht abzuweisen, als den Spam-Folder zur nie befragten, aber allwissenden Müllhalde werden zu lassen.

- *Abweisen:*
  ***Ziemlich sicher Spam***
  Mit dieser Einstellung wird relativ viel Spam erkannt; gleichzeitig ist das Risiko, irrtümlich legitime Nachrichten abzuweisen, äußerst gering.

- *FormMail, Bekanntermaßen unzustellbare Absender, Nachrichten ohne Domain-Angabe im* `From:` *-Feld:* ***Abweisen***
  Solche Nachrichten sollten normalerweise nicht durch das Internet gehen.

- *Verdächtige Nachrichten maximal* ***12 Stunden*** *zurückhalten*
  Dies mag im Verhältnis zu ei-

## Die Filtereinstellungen im Detail

101 kann Nachrichten, die Spam-Merkmale aufweisen, derzeit auf zwei Arten behandeln:

- ***Mit einer Headerzeile markieren***
  Dies dient üblicherweise dazu, die markierten Nachrichten in einen eigenen Spam-Folder zu verschieben, und sollte nur gewählt werden, wenn Sie sicher sind, daß Sie diesen auch nach der Phase anfänglicher Begeisterung noch regelmäßig kontrollieren werden.
- ***Abweisen***
  Die Nachricht wird nicht angenommen; der Absender erhält eine Fehlermeldung.

Bei welchen Nachrichten dies geschehen soll, können Sie jeweils in vier Stufen einstellen:

- ***Sicher Spam***
  Es werden nur jene Nachrichten markiert bzw. abgewiesen, bei denen ein Irrtum praktisch ausgeschlossen ist – d.h. wenn sie auch an Spam-Trap-Adressen gesendet wurden oder (fast) alle sonstigen Verfahren hohe Erkennungswerte geliefert haben.
- ***Ziemlich sicher Spam***
  Der Filter sortiert all jene Nachrichten aus, bei denen mehrere unabhängige Filterkriterien auf Spam hindeuten und False Positives kaum zu erwarten sind.
- ***Wahrscheinlich Spam***
  Vorsichtige sollten diese Einstellung nicht wählen – sie besagt, daß ein oder mehrere Spam-Indikatoren Spam signalisiert haben, andere aber nicht. Ein Beispiel wäre etwa eine Nachricht mit sehr häufigem Auftreten des Wortes *Viagra*, die aber weder über ein Open Relay noch als Massenmail eingetroffen ist.
- ***Nie***
  Keine Nachricht wird markiert bzw. abgewiesen.

Darüber hinaus ist es möglich, durch Ankreuzen der entsprechenden Kontrollkästchen bestimmte Klassen von eMail generell zurückzuschicken:

- ***FormMail-Nachrichten***
  Wenn Sie von FormMail noch nie gehört haben, können Sie solche Nachrichten bedenkenlos abweisen. Falls Sie FormMail auf Ihren Webseiten verwenden, können Sie entweder diese Option deaktivieren oder Ihr FormMail-Skript in Ihre Whitelist eintragen.
- ***Bekanntermaßen unzustellbare Absender***
  Dies betrifft alle Adressen, an die unsere Mailserver kürzlich keine Nachrichten senden konnten. Das Hauptrisiko bei dieser Einstellung besteht darin, Benutzer (z.B. von Freemail-Accounts) auszusperren, deren Mailbox voll war. Dagegen können Sie sich aber bis zu einem gewissen Grad schützen, indem Sie die Ihnen bekannten eMail-Adressen in Ihre Whitelist aufnehmen.
- ***Nachrichten ohne Domain-Angabe im*** `From:` ***-Feld***
  Solche Nachrichten sind nach den einschlägigen Internetstandard-Dokumenten unzulässig und obendrein häufig bei Spam anzutreffen. Allerdings hat sich gezeigt, daß auch einige von unseren Benutzern bestellte Newsletters diesen Defekt aufweisen.

In der Webmaske können Sie außerdem noch festlegen, wie lange verdächtige Nachrichten für eine spätere Begutachtung maximal zurückgehalten werden dürfen. Dies betrifft nur jene Nachrichten, bei denen beispielsweise der Text auf Spam hindeutet, aber Erkennungsmethoden, die typischerweise mit Verspätung funktionieren (also Blacklists und Spam-Traps), keine weiteren Hinweise liefern.

nem Arbeitstag lang erscheinen. Da aber gleichlautender Spam erfahrungsgemäß über einen längeren Zeitraum an viele Adressen verschickt wird und sich daher möglicherweise erst recht spät ein Exemplar in den Spam-Traps verfängt, ist das eher eine kurze Zeit.

### Keine Regel ohne Ausnahmen

Über die Filter-Einstellungen hinaus können Sie in der Webmaske noch persönliche Whitelist- und Blacklist-Einträge vornehmen:

- Nachrichten, auf die eines Ihrer Whitelist-Kriterien zutrifft, werden ungeachtet aller anderen Filtereinstellungen oder Blacklists ohne Verzögerung zugestellt.

- Nachrichten, die einem Blacklist-Eintrag, aber keinem Whitelist-Kriterium entsprechen, werden unabhängig von den sonstigen Filtereinstellungen abgewiesen und mit einer Fehlermeldung an den Absender zurückgeschickt.

Whitelist-Einträge können Sie nach der Absenderadresse oder (besonders praktisch für Mailinglisten) dem `Sender:`- bzw. dem `List-ID:`-Header vornehmen. Weiters ist es möglich, mit Hilfe der Whitelist Ausnahmen für Nachrichten zu definieren, die im Subject oder einigen anderen Headern bestimmte Zeichenfolgen enthalten. Das ermöglicht beispielsweise Vereinbarungen wie die, daß Nachrichten mit dem Codewort *Spunk*[9] im Subject stets zugestellt werden sollen.

Blacklist-Einträge können nach denselben Kriterien wie Whitelist-Einträge angelegt werden, haben aber den umgekehrten Effekt: Sie definieren Nachrichten, die abgewiesen werden sollen. Damit können Sie sich – falls die automatischen Spam-Filter nicht ausreichen sollten – grundsätzlich vor allen Nachrichten mit *Viagra* oder *Sex* im Subject wie auch vor Zusendungen von unliebsamen Zeitgenossen schützen.

## Zukunftspläne

101 wird laufend weiterentwickelt – sowohl was die Spam-Erkennung als auch was Strategien zur Vermeidung von False Positives betrifft. In näherer Zukunft sollen folgende Funktionen implementiert werden:

- Besseres Feedback für die Benutzer: Über Webmaske[10] (oder wahlweise auch als täglich per eMail zugesandter Bericht) wird es möglich sein, Datum, Absenderadresse und Subject der gefilterten Nachrichten abzurufen.

- Prüfsummen-Vergleich von eingebetteten Bildern und anderen Attachments in HTML-Mail: Es hat sich gezeigt, daß auch neue Spam-Nachrichten mit neuem Text oft dieselben Bilder enthalten wie frühere Spams. Diese Bilder können – ebenso wie die besonders berüchtigten Dialer – mit dem Prüfsummen-Mechanismus wiedererkannt werden.

- Berücksichtigung von URLs bzw. IP-Adressen, auf die in Nachrichten verwiesen wird: Da auch Spammer nur vergleichsweise wenige IP-Adressen für Webserver zur Verfügung haben, bestehen gute Chancen, daß die IP-Adresse des Servers bereits in einer einschlägigen Blacklist aufscheint.

- Auf Wunsch soll es möglich sein, Nachrichten von Adressen, an die man kürzlich Mail geschickt hat, eher als Nicht-Spam einzustufen als andere.

- Die Empfänger sollen weitere Klassen von eMail generell ablehnen können – beispielsweise Zeichensätze wie *KS_C_5601-1987*, den die meisten von uns nur als „koreanischen Spam“ kennen.

- Es ist geplant, die `Received:`-Zeilen automatisch zu analysieren, um Fälschungen zu erkennen (was auf Spam hindeuten würde) oder Ketten von Proxy – Relay – Empfänger zu entdecken.

- Die Benutzer sollen die Möglichkeit erhalten, eigenhändig temporäre Mailadressen einzurichten. Dabei handelt es sich um eine organisatorische Maßnahme, die vor allem für die Teilnehmer von Newsgruppen gedacht ist: Wird eine solche Adresse „zugespammt“, kann sie problemlos durch eine andere ersetzt werden.

- Ein Wunsch bleibt vorerst die Idee, zentral gespeicherte Adreßbücher einzurichten. Dieses Service wäre eine hervorragende Erweiterung sowohl für das Webmail-Service als auch für die Spam-Whitelists. Wirklich sinnvoll sind am Server verwaltete Adreßbücher aber nur, wenn auch der „normale“ Mailklient mitarbeitet, d.h. auf einfache Weise neue Mailadressen eintragen kann. Genau hierbei hakt es: Zwar kann fast jeder Mailklient LDAP-Verzeichnisse abfragen, aber leider nichts hineinschreiben.

Mit dem serverseitigen Spam-Filter ist ein entscheidender Schritt getan, die Mailboxen der Uni Wien von unerwünschtem Datenmüll zu befreien. Es bleibt zu hoffen, daß dadurch das Thema Spam – zumindest auf absehbare Zeit – ebenso an Bedeutung verliert wie die Virenproblematik nach der Einführung der zentralen eMail-Virenscanner.

Ein zentraler Spam-Filter am Mailserver bietet eine bequeme Möglichkeit, sich der unerwünschten Botschaften zu entledigen. Wer aber gern selbst alles unter Kontrolle hat und den Aufwand nicht scheut, kann auch auf einen Desktop-Spam-Blocker (siehe Seite 45) zurückgreifen.

*Alexander Talos* ■

9) Lindgren, Astrid: *Pippi Långstrump i Söderhavet*, Stockholm 1948, Rabén & Sjögren

10) Dieses Feature geht auf einen Vorschlag von Gerhard Gonter (ZID der WU Wien) zurück.

# Spam-Bekämpfung auf eigene Faust

Wer den auf Seite 40 beschriebenen, serverseitig arbeitenden Spam-Filtern des ZID (noch) nicht vertraut, kann auch mit diversen Desktop-Programmen versuchen, der Spam-Flut in seiner Mailbox Herr zu werden. Die deutsche Fachzeitschrift *c't* hat im Herbst des vergangenen Jahres aus über 60 derartigen, am eigenen PC zu installierenden Spam-Blockern die sieben brauchbarsten vorausgewählt und diese anschließend einem Härtetest unterzogen. Um die Vorauswahl zu bestehen, mußten die Programme unter anderem mit bereits vorhandenen Mailkonten umgehen können, ihre Filter selbständig – ohne regelmäßige händische Anpassungen seitens des Benutzers – aktuell halten können und imstande sein, die als Spam erkannten Nachrichten zu markieren oder in einen bestimmten Ordner zu verschieben (kommentarloses Löschen wurde als K.O.-Faktor gewertet).

Die sieben Finalisten, die in der Tabelle unten aufgelistet sind, wurden anhand eines bereits vorhandenen („historischen") Datensatzes von 6000 unerwünschten und 500 erwünschten eMail-Nachrichten sowie eines zweiten Datensatzes von ca. 200 aktuell einlangenden Nachrichten gründlich getestet. Die Resultate dieses Tests werden im folgenden kurz wiedergegeben – wer mehr darüber wissen möchte, findet den kompletten Bericht im ***c't 22/2002*** auf Seite 158. Mailbox- und Unet-Benutzer können diese *c't*-Ausgabe ab März 2003 auch über das Datenbank-Service der UB-Wien (`http://ub-datenbanken.univie.ac.at/`) online abrufen.

## Die Ergebnisse im Überblick

- Die getesteten Programme können jeweils beliebig viele Mailkonten überprüfen. Die einzige Ausnahme bildet MailShield, das mit maximal 3 Mailkonten limitiert ist.

- Alle Programme bieten die Möglichkeit, eine *Whitelist* anzulegen (das ist ein Verzeichnis aller Absender, deren Nachrichten man auf jeden Fall empfangen möchte), wobei alle außer SpamPal und SpamNet einen automatischen Adreßbuch-Abgleich durchführen können.

- In der Regel filtern die Desktop-Spam-Blocker (ausgenommen Apple Mail, SpamKiller und SpamNet) unter anderem mit Hilfe von *Blacklists* – das sind Datenbanken im Internet, die alle Rechner/Provider auflisten, die als Spammer bzw. „Spammer-freundlich" bekannt sind. Die Richtlinien für die Aufnahme eines Rechners in eine Blacklist sind allerdings sehr unterschiedlich und oft auch sehr unscharf, sodaß diese Methode umstritten und jedenfalls als alleiniges Filterkriterium ungeeignet ist.

- Die meisten der getesteten Programme beherrschen nur POP. IMAP-Konten können nur von Apple Mail und MailShield überprüft werden, Hotmail- und MAPI-Konten nur von MailShield und SpamKiller. Mit Exchange-Konten kann ausschließlich SpamAssassin Pro umgehen.

- Der Benutzerkomfort wurde allgemein als „gut" bewertet; SpamAssassin Pro erreichte sogar ein „sehr gut".

- Bei der Erkennungsrate wurde zwischen den historischen und den aktuellen Test-Nachrichten unterschieden. Im großen und ganzen erreichten hier Apple Mail und MailShield die besten Werte; bei SpamKiller fällt die viel zu hohe Rate (6%) von als Spam eingestuften, tatsächlich aber erwünschten Nachrichten (*False Positives*) auf.

### Apple Mail

Ein besonderes Feature von Apple Mail ist ein Spam-Filter auf Basis von künstlicher Intelligenz, der in einer Lernphase darauf trainiert wird, unerwünschte Mail zu erkennen. Ausgefilterte Nachrichten können nach Wunsch gelöscht, markiert oder verschoben werden. Nach einigen Wochen gezielten

| Produkt | Plattform | Preis/Monat | Hersteller | Bezugsquelle |
|---|---|---|---|---|
| **Apple Mail 1.2** | MacOS X 10.2 (Teil des Betriebssystems) | kostenlos | Apple | `http://www.apple.com/macosx/jaguar/mail.html` |
| **MailShield Desktop 2.13** | Windows 95, 98, NT, 2000, ME, XP | $ 60 | Lyris | `http://www.lyris.com/products/mailshield/desktop/` |
| **Spam Sleuth 1.0.0.28** | Windows 95, 98, NT, 2000, ME, XP | $ 30 | Blue Squirrel | `http://www.bluesquirrel.com/products/SpamSleuth/` |
| **SpamKiller 4.0.40.0** | Windows 95, 98, NT, 2000, ME, XP | $ 40 | McAfee | `http://www.mcafee.com/myapps/msk/default.asp` |
| **SpamPal 1.06** | Windows 95, 98, NT, 2000, ME, XP | kostenlos | James Farmer | `http://www.spampal.org.uk/` |
| **SpamAssassin Pro** | Outlook 2000, 2002 (Outlook-Plugin) | $ 30 | Deersoft | `http://www.deersoft.com/sp_pro.html` |
| **SpamNet Beta 6f** | Outlook 2000, XP (Outlook-Plugin) | kostenlos | Cloudmark | `http://www.cloudmark.com/products/spamnet/` |

Trainings erreicht ein solches System sehr hohe Trefferquoten – im Test waren es 98,6% des aktuellen Spams und 0% False Positives. Bei der historischen Mail schnitt das Programm aber deutlich schlechter ab; darüber hinaus ließ die Spam-Erkennung auch im aktuellen Datensatz nach, nachdem das Programm eine Zeitlang mit den älteren Nachrichten „gefüttert" worden war. Den Grund dafür vermuten die Tester darin, daß die beiden Datenquellen zu unterschiedlich waren, während es für den Erfolg des Systems ganz wesentlich ist, in der Lernphase möglichst typische Nachrichten zu verwenden.

### MailShield

MailShield beurteilt die Nachrichten anhand von Blacklists und Textfiltern, wobei der Benutzer die Möglichkeit hat, die Analyse-Kriterien gezielt zu beeinflussen. Als Spam eingestufte Nachrichten werden aus dem Postfach entfernt und in einer eigenen Datenbank zur späteren Durchsicht gespeichert. Im *c't*-Test erreichte MailShield sowohl bei der historischen als auch bei der aktuellen Mail Erkennungsraten von 90% bei jeweils 0% an False Positives – dies allerdings nur unter Windows NT, 2000 oder XP bzw. in Verbindung mit Internet Explorer 6.0, weil es in diesen Fällen mit Hilfe einer System-DLL die Absenderadressen überprüfen kann. Bei anderen Plattformen lagen die Trefferquoten nur bei 50%.

### Spam Sleuth

Spam Sleuth sucht nach Schlüsselwörtern, HTML-Code und eingebundenen Skripts und greift zusätzlich auf frei wählbare Blacklists zurück. Die Trefferquote liegt mit den voreingestellten Werten bei etwa 80% und läßt sich durch händische Feinabstimmung weiter steigern. Andererseits scheinen im Testergebnis auch 2% False Positives bei den historischen und 1% False Positives bei den aktuellen Nachrichten auf. Auch auf langsamen Rechnern arbeitet das Programm recht flott; im Falle einer bestehenden Internetverbindung ist außerdem ein automatisches Update möglich. Der Nachteil: Bei mehr als 2000 Nachrichten im Postfach stürzt Spam Sleuth schlicht und einfach ab – ein Problem, das aber hoffentlich in der nächsten Version behoben sein wird.

### SpamKiller

SpamKiller wies im Test mit 6% an False Positives bei beiden Datensätzen eine inakzeptabel hohe Quote auf. Korrekt als Spam eingestuft wurden bei den historischen Nachrichten 80% und bei den aktuellen Nachrichten 65%. Dieses insgesamt eher schlechte Ergebnis liegt daran, daß SpamKiller bei der Analyse der Nachrichten ausschließlich auf Textfilter setzt. Obwohl es hunderte davon verwendet, und trotz der möglichen Kombination mit einer aus dem Adreßbuch importierten Whitelist, kann es im direkten Vergleich mit den anderen getesteten Programmen nicht wirklich bestehen.

### SpamPal

Dieses Programm verwendet in der Standardinstallation hauptsächlich Blacklists als Beurteilungskriterium und erreichte infolgedessen im Test sehr mäßige Trefferquoten: Die Erkennungsrate lag bei historischen und aktuellen Nachrichten bei 62%, die Quote der False Positives jeweils bei 4%, was wie bei SpamKiller eindeutig zu hoch ist. Allerdings hat der Benutzer die Möglichkeit, z.B. durch individuelle Black- oder Whitelists sowie durch Filter-Plugins die Ergebnisse zu verbessern. Einzigartig – zumindest im Rahmen dieses Tests – ist der „RegEx-Filter" von SpamPal, der es erlaubt, Regular Expressions für Filter und Whitelist zu verwenden. Die *c't*-Tester kommen zu folgendem Schluß: *Alles in allem ist SpamPal ein leistungsfähiger, vielseitiger und vor allem kostenloser Spam-Blocker, an dem man aber ein wenig schrauben muß, bis er optimale Ergebnisse liefert.*

### SpamAssassin Pro

Bei der Desktop-Variante von SpamAssassin handelt es sich um ein Plugin für Outlook 2000 bzw. 2002, das sehr einfach zu bedienen ist und sehr gute Erkennungsraten erzielt (88% bei historischer, 90% bei aktueller Mail; 0,02% bzw. 0% False Positives). Im Gegensatz zur Server-Version bietet es allerdings kaum Konfigurationsmöglichkeiten: Der Benutzer muß mit einer White- und Blacklist sowie einem Sprachfilter das Auslangen finden, sodaß sich die Trefferquote kaum mehr steigern läßt. Zudem werden die einzelnen Nachrichten in Echtzeit während des Ladevorgangs geprüft, was auf Dauer eher unangenehm auffällt, falls man keine ständige Internetverbindung hat bzw. die Mailbox permanent gut gefüllt ist.

### SpamNet

Auch SpamNet ist ein Plugin für Outlook (2000 und XP), überprüft im Gegensatz zu SpamAssassin Pro die Nachrichten aber erst, wenn sie bereits eingetroffen sind. Das führt dazu, daß man mitunter unerwünschte Nachrichten in der Mailbox vorfindet, die nach der Überprüfung jedoch selbständig in den Spam-Ordner entschwinden. Die Trefferquote lag im Test bei den historischen Nachrichten zwar nur bei 40%, bei der aktuellen Mail aber bei 80%. Die Konfigurationsmöglichkeiten beschränken sich auf Buttons, mit deren Hilfe die Mailadressen einzelner Nachrichten in die Black- oder Whitelist übernommen werden können. Lobend erwähnt wird von den Testern, daß SpamNet keine einzige Nachricht fälschlicherweise als Spam klassifizierte. Ein weiterer Pluspunkt: Das Programm ist kostenlos.

## Quintessenz

Wie im Artikel *Forever Spam!?* (Seite 2) dargestellt wurde, sind Spammer sehr erfinderisch und ihren Gegnern oft um eine Nasenlänge voraus. Der *c't*-Test bestätigt die Linie des ZID: Wenn man die Spam-Flut effizient eindämmen will, muß man mehrere Filterkriterien miteinander verknüpfen. Blacklists, Whitelists und Textfilter haben jeweils ihre Schwachstellen – eine sinnvolle Kombination der verschiedenen Methoden, gemeinsam mit einem übergeordneten Bewertungssystem, kann jedoch sehr wirkungsvoll sein.

*Elisabeth Zoppoth* ■

# KURSE BIS JULI 2003

## Kurskalender

Auf den folgenden Seiten finden Sie detaillierte Beschreibungen zu den von März bis Juli 2003 geplanten Kursen des Zentralen Informatikdienstes. Wir sind bemüht, keine Änderungen mehr vorzunehmen. Da jedoch Kurse hinzukommen oder entfallen können, **beachten Sie bitte auch die aktuellen Informationen** im Service- und Beratungszentrum sowie die Kursterminblätter in den Formularspendern vor den PC-Räumen im NIG sowie im Service- und Beratungszentrum. Alle Informationen zu den Kursen finden Sie im WWW unter **`http://data.univie.ac.at/kurs/bin/kursang.pl`**; die aktuellen Kursbelegungen können unter `http://data.univie.ac.at/kurs/bin/kursall.pl` abgerufen werden.

## Anmeldungen

Teilnahmeberechtigt sind Studierende und Universitätsmitarbeiter. Als solche gelten die Angestellten aller Universitäten, sie müssen jedoch nachweisen, daß sie an einer Universität beschäftigt sind (Bestätigung). Angehörige universitätsnaher oder wissenschaftlicher Institutionen haben nach Maßgabe der freien Plätze die Möglichkeit, an den Kursen des ZID teilzunehmen, daher ist die Anmeldung erst nach dem Ende der Anmeldefrist möglich. Für diese Teilnehmer gilt der Tarif *Externe*. Für Kurse mit beschränkter Teilnehmerzahl ist eine **Anmeldung im Service- und Beratungszentrum des ZID** erforderlich (NIG, Stg. II, 1. Stock; Öffnungszeiten: **Mo – Fr 9.00 – 17.00 Uhr**). Kostenpflichtige Kurse sind bei der Anmeldung bar zu bezahlen; Studierende müssen dabei ihren **Studienausweis** vorweisen. Für Mitarbeiter der Institute und Dienststellen der Uni Wien besteht die Möglichkeit, sich mit einem *Zahlungs- und Verrechnungsauftrag* (ZVA) bargeldlos zu den Kursen anzumelden. Der ZVA ist vollständig ausgefüllt und unterschrieben zur Kursanmeldung mitzubringen. Das Formular ist im Service- und Beratungszentrum des ZID oder unter `http://www.univie.ac.at/ZID/formulare.html` erhältlich.

## Absagen/Rücktritte

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

## Kursorte

**Kursraum A des ZID:** NIG (1010 Wien, Universitätsstraße 7), Erdgeschoß, Stiege I
**Kursraum B des ZID:** NIG (1010 Wien, Universitätsstraße 7), Erdgeschoß, Stiege III
**PC-Raum 2 des ZID:** NIG (1010 Wien, Universitätsstraße 7), 1. Stock, Stiege I
**Hörsaal 3 des Neuen Institutsgebäudes:** NIG (1010 Wien, Universitätsstraße 7), Erdgeschoß, Stiege I

# WINDOWS-ANWENDER

## *Textverarbeitung*

### MS-Word für Windows – Fortsetzung

Zielgruppe: PC-Benutzer, die grundlegende Word-Kenntnisse besitzen und zusätzliche Möglichkeiten erlernen und nützen wollen
Voraussetzung: Kurse *Arbeiten mit MS-Windows* und *MS-Word für Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Tabellen / Seriendruck / Formatvorlagen / Verknüpfung mit anderen Programmen
Ort: 1. Termin: Kursraum A / 2. Termin: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **17.03.2003** | 09.00 – 16.00 h | 17.02.03 – 07.03.03 |
| **04.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### Wissenschaftliches Arbeiten mit MS-Word für Windows

Zielgruppe: Word-Benutzer, die wissenschaftliche Arbeiten (z.B. Diplomarbeiten) erstellen wollen
Voraussetzung: Beherrschen der Word-Grundlagen (Kurse *MS-Word für Windows – Einf.* & *Forts.*)
Dauer: 6 Stunden (1 Tag)
Inhalt: Zentraldokument – Filialdokument / Verzeichnisse erstellen / Fußnoten einfügen und bearbeiten / Kopf- und Fußzeilen einfügen und gestalten / Excel-Tabellen einfügen
Ort: 1. Termin: Kursraum A / 2. Termin: Kursraum B

Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 10

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **11.04.2003** | 09.00 – 16.00 h | 10.03.03 – 28.03.03 |
| **06.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### MS-Word für Windows im Büroeinsatz

Zielgruppe: Word-erfahrene Anwender, die sich ihre Büroarbeit durch einfache Automatisierungen erheblich erleichtern wollen
Voraussetzung: Beherrschen der Word-Grundlagen (Kurse *MS-Word für Windows – Einf.* & *Forts.*)
Dauer: 6 Stunden (1 Tag)
Inhalt: Textbaustein mit der AutoText-Funktion erstellen / Dokumentvorlagen / Das Formular / Seriendruck für Profis
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **01.04.2003** | 09.00 – 16.00 h | 03.03.03 – 21.03.03 |

## *Tabellenkalkulation*

### MS-Excel – Einführung

Zielgruppe: Neueinsteiger im Bereich Tabellenkalkulation, die mit Excel Berechnungen erfassen, modifizieren und grafisch darstellen wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Excel-Arbeitsoberfläche / Arbeiten mit Arbeitsmappen und Tabellenblättern / Erstellen einfacher Tabellen / Formatierungsmöglichkeiten / Diagramm erstellen und bearbeiten / Drucken
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **10.03.2003** | 09.00 – 16.00 h | 27.01.03 – 28.02.03 |
| **05.05.2003** | 09.00 – 16.00 h | 07.04.03 – 25.04.03 |

### MS-Excel – Fortsetzung

Zielgruppe: Erfahrene Excel-Anwender, die an komplexeren Berechnungen bzw. an weiteren Funktionen interessiert sind
Voraussetzung: EDV-Grundkenntnisse bzw. Kurse *Arbeiten mit MS-Windows – Einführung* und *MS-Excel – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Anpassen der Arbeitsoberfläche / Komplexe Berechnungen / Arbeitsmappen verknüpfen / Mustervorlagen und Formulare
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **11.03.2003** | 09.00 – 16.00 h | 27.01.03 – 28.02.03 |
| **06.05.2003** | 09.00 – 16.00 h | 07.04.03 – 25.04.03 |

### MS-Excel – Das Werkzeug zur Datenanalyse

Zielgruppe: Excel-erfahrene PC-Benutzer, die Excel-Daten verwalten, analysieren und filtern wollen
Voraussetzung: Beherrschen der Excel-Grundlagen (Kurse *MS-Excel – Einführung* und *Fortsetzung*)
Dauer: 6 Stunden (1 Tag)
Inhalt: Listen verwalten / Tabellenblätter gliedern / Pivot-Tabelle / Aufgaben automatisieren
Ort: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 10

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **15.05.2003** | 09.00 – 16.00 h | 14.04.03 – 02.05.03 |

## *Datenbanken*

### MS-Access für Windows – Einführung

Zielgruppe: Neueinsteiger, die eine Datenbank mit MS-Access für Windows selbständig anlegen und verwalten wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 12 Stunden (2 Tage)
Inhalt: Datenbankgrundlagen / Erstellen eines Tabellenentwurfs / Arbeiten mit Tabellen / Abfragen / Erstellen von Formularen / Berichte / Drucken / Einfache Makros
Ort: 1. Termin: Kursraum B / 2. Termin: Kursraum A
Preis: € 60,– für Studierende
€ 120,– für Mitarbeiter
€ 180,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **24.03. – 25.03.03** | 09.00 – 16.00 h | 24.02.03 – 14.03.03 |
| **05.06. – 06.06.03** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### MS-Access für Windows – Fortsetzung

Zielgruppe: PC-Benutzer, die ihre Access-Kenntnisse vertiefen wollen
Voraussetzung: Kurse *Arbeiten mit MS-Windows* und *MS-*

*Access für Windows – Einführung*

Dauer: 12 Stunden (2 Tage)
Inhalt: Datenbankdesign und -pflege / Tabellen einbinden / Abfragen / Automatisieren von Arbeitsabläufen mittels Makroprogrammierung
Ort: Kursraum A
Preis: € 60,– für Studierende
€ 120,– für Mitarbeiter
€ 180,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **10.06. – 11.06.03** | 09.00 – 16.00 h | 05.05.03 – 30.05.03 |

## Diverse Applikationen

### SPSS – Einführung

Zielgruppe: PC-Benutzer, die das Statistikprogramm SPSS unter Windows einsetzen wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 12 Stunden (2 Tage)
Inhalt: Fragebogenerstellung / Dateneditor / Datentransformation / Datenselektion / Ausgewählte statistische Verfahren / Grafiken
Ort: 1. Termin: Kursraum A / 2. Termin: Kursraum B
Preis: € 60,– für Studierende
€ 120,– für Mitarbeiter
€ 180,– für Externe
Teilnehmer: maximal 12

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **13.03. – 14.03.03** | 09.00 – 16.00 h | 27.01.03 – 28.02.03 |
| **15.05. – 16.05.03** | 09.00 – 16.00 h | 14.04.03 – 02.05.03 |

### Adobe Photoshop – Einführung

Zielgruppe: PC-Benutzer, die mit einem professionellen Programm Bilder bearbeiten wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Photoshop-Arbeitsoberfläche / Bildbearbeitung / Ebenen und Filtereffekte / Text erzeugen & bearbeiten / Bilder importieren, scannen, ins Web exportieren / Drucken
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **07.04.2003** | 09.00 – 16.00 h | 10.03.03 – 28.03.03 |
| **02.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### Adobe Photoshop für Webgrafiken

Zielgruppe: Benutzer, die mit Adobe Photoshop für die Publikation im Web gedachte Grafiken bearbeiten und optimieren möchten
Voraussetzung: Kurs *Adobe Photoshop – Einführung* oder gleichwertige Kenntnisse
Dauer: 6 Stunden (1 Tag)
Inhalt: Grundlagen / Photoshop- & ImageReady-Voreinstellungen / Geeignete Dateiformate fürs Web / Bildoptimierung fürs Web / Arbeiten mit der Palette *Optimieren* / Optimierte Bilder speichern / HTML-Codes kopieren / Textgestaltung / Textattribute definieren / Formatierungsmöglichkeiten / Rollovers erzeugen & gestalten / Ausgabe des HTML-Codes / Animationen & Slices / Arbeiten mit Benutzer-Slices / Slice-Typ definieren / Slices fürs Web optimieren / Imagemaps
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **05.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### MS-PowerPoint – Einführung

Zielgruppe: PC-Benutzer, die Folien bzw. Bildschirmpräsentationen für Vorträge, Seminararbeiten etc. erstellen wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: PowerPoint-Arbeitsoberfläche / Texteingabe und Korrektur / Grafik & Text / Drucken / Animierter Text
Ort: 1. und 3. Termin: Kursraum B
2. Termin: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **12.03.2003** | 09.00 – 16.00 h | 27.01.03 – 28.02.03 |
| **16.05.2003** | 09.00 – 16.00 h | 14.04.03 – 02.05.03 |
| **27.06.2003** | 09.00 – 16.00 h | 26.05.03 – 13.06.03 |

### MS-PowerPoint – Fortsetzung

Zielgruppe: PowerPoint-Anwender, die ihre Fähigkeiten in der Gestaltung von PowerPoint-Folien erweitern wollen
Voraussetzung: Kurse *Arbeiten mit MS-Windows – Einführung* und *MS-PowerPoint – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Die zielgruppenorientierte Präsentation / Einfügen von Fremddaten (-objekten) / Handzettel und Notizzettel / Animationsmöglichkeiten / Veröffentlichen im WWW / Folien aus einer Gliederung erstellen

Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **13.03.2003** | 09.00 – 16.00 h | 27.01.03 – 28.02.03 |
| **28.05.2003** | 09.00 – 16.00 h | 28.04.03 – 16.05.03 |
| **30.06.2003** | 09.00 – 16.00 h | 02.06.03 – 13.06.03 |

### Adobe Acrobat

Zielgruppe: PC-Benutzer, die PDF-Dokumente erstellen, verwenden und bearbeiten wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Acrobat Programmpaket und Komponenten / Erstellen und Bearbeiten von PDF-Dateien
Ort: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **21.05.2003** | 09.00 – 16.00 h | 22.04.03 – 09.05.03 |

## UNIX-ANWENDER

### Einführung in die Anwendung von Unix

Zielgruppe: alle Benutzer, die als Anwender auf Unix-Systemen arbeiten möchten
Voraussetzung: EDV-Grundkenntnisse
Dauer: 12 Stunden (3 Halbtage)
Inhalt: Betriebssystem Unix / Einfache Befehle / Dateisystem / Editor / Shell / Prozesse
Ort: Kursraum A
Preis: € 30,- für Studierende und Mitarbeiter
€ 45,- für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **28.04. – 30.04.03** | 12.00 – 16.00 h | 24.03.03 – 18.04.03 |

## INTERNET

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

Zielgruppe: Anwender, die eigene Webpages erstellen möchten
Voraussetzung: EDV-Grundkenntnisse
Dauer: ca. 2,5 Stunden
Inhalt: Grundlagen / Erste Schritte / Die strukturierte Webpage / Webpage auf Server kopieren
Ort: Hörsaal 3
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **14.03.2003** | 12.30 – 15.00 h | keine Anmeldung |
| **16.05.2003** | 12.30 – 15.00 h | keine Anmeldung |

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

Zielgruppe: Anwender, die Webpages erstellen wollen
Voraussetzung: EDV-Grundkenntnisse und *Einführung in das Erstellen von Webpages – Teil 1*
Dauer: ca. 2,5 Stunden
Inhalt: Tabellen / Frames (Aufbau und Aussehen) / Interaktive Grafiken / Einbinden von Java-Applets
Ort: Hörsaal 3
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **21.03.2003** | 12.30 – 15.00 h | keine Anmeldung |
| **23.05.2003** | 12.30 – 15.00 h | keine Anmeldung |

### Einführung in das Erstellen von Webpages – Teil 3 (HTML-Workshop)

Zielgruppe: PC-Benutzer, die eigene Webpages erstellen und professionell formatieren wollen
Voraussetzung: EDV-Grundkenntnisse (Kurs *Arbeiten mit MS-Windows – Einführung*), *Einführung in das Erstellen von Webpages – Teil 1 & 2*
Dauer: 6 Stunden (1 Tag)
Inhalt: Erstellen von HTML-Seiten mit einem Texteditor / Formatieren erfaßter Texte / Strukturieren von HTML-Seiten / Tabellen / Grafik
Ort: 1. Termin: Kursraum B / 2. Termin: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **31.03.2003** | 09.00 – 16.00 h | 03.03.03 – 28.03.03 |
| **04.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### MS-Frontpage

Zielgruppe: Anwender, die Frontpage 2000 zur Erstellung von Webpages einsetzen möchten
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Frontpage Editor & Explorer / Grundlagen Webseitengestaltung / Bilder/Grafiken einfügen / Verweise – Hyperlinks / Frame-Seiten / Webseiten veröffentlichen / Projektverwaltung und -planung / Gestaltungsprinzipien
Ort: Kursraum A

Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **08.04.2003** | 9.00 – 16.00 h | 10.03.03 – 28.03.03 |
| **13.06.2003** | 9.00 – 16.00 h | 12.05.03 – 30.05.03 |

### Webdesign – Konzeption und Gestaltung

Zielgruppe: PC-Benutzer, die ein umfangreiches Informationsangebot gestalten und betreuen wollen
Voraussetzung: Erfahrung im Erstellen von Webpages
Dauer: 12 Stunden (2 Tage)
Inhalt: Die menschliche Wahrnehmung / Strukturierung des Informationsmaterials / Gestaltungsprinzipien / Konsistenz & Lesbarkeit / Einsatz von Grafiken / HTML-Validierung
Ort: Kursraum B
Preis: € 60,– für Studierende
€ 120,– für Mitarbeiter
€ 180,– für Externe
Teilnehmer: maximal 12

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **29.04. – 30.04.03** | 9.00 – 16.00 h | 24.03.03 – 18.04.03 |
| **09.07. – 10.07.03** | 9.00 – 16.00 h | 10.06.03 – 27.06.03 |

## SYSTEMBETREUUNG

### Hardware-Grundlagen

Zielgruppe: Systemadministratoren, die im Bereich der Software bereits erfahren sind, aber wenig Praxis im Umgang mit Hardware haben. Es soll jenes Wissen vermittelt werden, das für folgende Aufgaben erforderlich ist:
- einfache Fehlersuche/-behebung
- Aus- und Umbau des Rechners
- Auswahl neuer PCs

Voraussetzung: gute EDV-Grundkenntnisse
Dauer: 6 Stunden (1 Tag)
Inhalt: Die Komponenten des PCs / Funktion und Zusammenspiel der Komponenten
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 10

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **03.06.2003** | 09.00 – 16.00 h | 05.05.03 – 23.05.03 |

### Netzwerk-Grundlagen

Zielgruppe: Systemadministratoren, die Rechner mit Zugang zum Datennetz betreuen und Hintergrundwissen über Aufbau und Arbeitsweise von Netzwerken erwerben wollen
Voraussetzung: EDV-Grundkenntnisse
Dauer: 6 Stunden (1 Tag)
Inhalt: Einführung und Überblick: LANs, WANs, Internet / Übertragungsmedien / LAN-Topologien / OSI Layer / 802 Standards / Media Access / Ethernet, FastEthernet, Netzwerkkarten / Repeater, Hubs, Bridges und Switches / TCP/IP, IP-Adressen, DHCP / Betriebssystem-Tools für Fehlersuche / Namensauflösung mit DNS / Server (NetBIOS) Name Resolution / Grundlagen über Firewalls
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für Mitarbeiter
€ 90,– für Externe
Teilnehmer: maximal 10

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **22.05.2003** | 09.00 – 16.00 h | 22.04.03 – 09.05.03 |

### Windows XP Professional – Systembetreuung

Zielgruppe: Benutzer, die eine Windows XP Professional Workstation installieren und konfigurieren, Benutzer verwalten und Internetzugang einrichten wollen
Voraussetzung: EDV-Grundkenntnisse (Ordner, Laufwerke, Oberfläche)
Dauer: 12 Stunden (2 Tage)
Inhalt: Netzwerkgrundlagen / Hardwaregrundlagen / Installation / Systemverwaltung / Windows XP-Benutzeroberfläche / Lokale Benutzerverwaltung und Gruppenrichtlinien / Datei und Druckerfreigabe / Datenträgerverwaltung / Systemüberwachung & -pflege
Ort: Kursraum B
Preis: € 130,– für Studierende und Mitarbeiter
€ 195,– für Externe
Teilnehmer: maximal 10

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **16.06. – 17.06.03** | 09.00 – 16.00 h | 19.05.03 – 06.06.03 |

## PROGRAMMIERUNG

### Einführung in das Programmieren – Teil 1

Zielgruppe: Anwender, die grundlegende Kenntnisse zum Erlernen einer Programmiersprache erwerben wollen
Voraussetzung: EDV-Grundkenntnisse
Dauer: ca. 3 Stunden
Inhalt: Was ist Programmieren? / Überblick Programmiersprachen / Arbeitsschritte beim Programmieren / Struktogramme bzw. Programmablaufpläne / Vom Programmablaufplan zum Programm
Ort: Hörsaal 3 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **28.03.2003** | 12.30 – 15.30 h | keine Anmeldung |

## Einführung in das Programmieren – Teil 2

Zielgruppe: Anwender, die grundlegende Kenntnisse zum Erlernen einer Programmiersprache erwerben wollen
Voraussetzung: *Einführung in das Programmieren – Teil 1*
Dauer: ca. 3 Stunden
Inhalt: Zeichenketten / Werte, Operatoren, Variablen / Bedingungen und Entscheidungen / Schleifen / Prozeduren / Objektorientierte Programmierung
Ort: Hörsaal 3 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **04.04.2003** | 12.30 – 15.30 h | keine Anmeldung |

## Einführung in das Programmieren mit Perl

Zielgruppe: Anwender, die die Programmiersprache Perl mit Schwerpunkt CGI-Programmierung erlernen möchten
Voraussetzung: *Einführung in das Programmieren – Teil 1 & Teil 2*
Dauer: ca. 3 Stunden
Inhalt: Die Perl-Programmierumgebung / Der Perl-Interpreter und seine Parameter / Behandlung syntaktischer Fehler / Vorstellung und Beschreibung diverser einfacher Programme / Testen und Fehlersuche bei der Programmerstellung / Erstellen einer einfachen servergesteuerten HTML-Datei / Übernahme und Auswertung von Formulardaten
Ort: Hörsaal 3 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **11.04.2003** | 12.30 – 15.30 h | keine Anmeldung |

## Programmieren von CGIs mit Perl – Einführung (Workshop)

Zielgruppe: Anwender, die die Programmierung von CGI-Skripts unter Einsatz der Programmiersprache Perl erlernen möchten
Voraussetzung: Vorträge *Einführung in das Programmieren – Teil 1 & 2* und *Einführung in das Programmieren mit Perl*
Dauer: 5 x 2,5 Stunden (montags und mittwochs)
Inhalt: Vertiefung der Perl-Kenntnisse / gemeinsame und selbständige Entwicklung kleinerer Programme / Die CGI-Schnittstelle von Perl / Wichtige Perl-Packages / Behandlung von Fehlern
Ablauf: ständige Betreuung durch Trainer während des Workshops / Lösen von Aufgaben zwischen den Workshops / Besprechung und Korrektur der gelösten Beispiele
Ort: Kursraum B
Preis: € 70,– für Studierende
€ 140,– für Mitarbeiter
€ 210,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **28.04. – 12.05.03** | 16.30 – 19.00 h | 24.03.03 – 18.04.03 |

## Programmieren von CGIs mit Perl – Fortsetzung (Workshop)

Zielgruppe: Anwender, die ihre CGI-Programmierkenntnisse unter Einsatz der Programmiersprache Perl vertiefen möchten
Voraussetzung: Vorträge *Einführung in das Programmieren – Teil 1 & 2*, *Einführung in das Programmieren mit Perl* und *Programmieren von CGIs mit Perl – Einführung (Workshop)*
Dauer: 5 x 2,5 Stunden (montags und mittwochs)
Inhalt: Formulardaten per e-Mail versenden / Suchen und Ersetzen mit regulären Ausdrücken / Formatierte Ausgabe (Zahlen, Datum, Text) / Verwendung von Subroutinen / Perl außerhalb des CGI verwenden
Ablauf: ständige Betreuung durch Trainer während des Workshops / Lösen von Aufgaben zwischen den Workshops / Besprechung und Korrektur der gelösten Beispiele
Ort: Kursraum A
Preis: € 70,– für Studierende
€ 140,– für Mitarbeiter
€ 210,– für Externe
Teilnehmer: maximal 16

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **19.05. – 02.06.03** | 16.30 – 19.00 h | 22.04.03 – 09.05.03 |

## Einführung in das Programmieren mit JavaScript

Zielgruppe: Anwender, die JavaScript erlernen möchten
Voraussetzung: *Einführung in das Programmieren – Teil 1 & Teil 2*
Dauer: ca. 3 Stunden
Inhalt: Einbindung und Verwendung von JavaScript / Die JavaScript Sprachelemente / Das Document Object Model (DOM) / Manipulation des Browserfensters (Größe, Inhalt, Aussehen, Öffnen und Schliessen) / Reaktion auf Ereignisse (OnClick, OnSubmit, OnMouseOver, ...) / Änderungen der Seite (Farbe, Grafiken, Links, ...)
Ort: Hörsaal 3 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt; keine Anmeldung erforderlich

| Termin | Zeit | Anmeldefrist |
|---|---|---|
| **09.05.2003** | 12.30 – 15.30 h | keine Anmeldung |

# INFORMATIONSVERANSTALTUNGEN

Die folgenden Vorträge finden im **Hörsaal 3 des Neuen Institutsgebäudes** (NIG, 1010 Wien, Universitätsstraße 7, Stiege I, Erdgeschoß) statt und sind kostenlos zugänglich.

## *Einführung in das Erstellen von Webpages (HTML), Teil 1 & 2*

Termine: Teil 1: Freitag, 14. März 2003; Freitag, 16. Mai 2003, jeweils 12.30 Uhr (s.t.)
Teil 2: Freitag, 21. März 2003; Freitag, 23. Mai 2003, jeweils 12.30 Uhr (s.t.)

Dauer: jeweils ca. 2,5 Stunden

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

## *Einführung in das Programmieren, Teil 1 & 2*

Termine: Teil 1: Freitag, 28. März 2003, 12.30 Uhr (s.t.)
Teil 2: Freitag, 4. April 2003, 12.30 Uhr (s.t.)

Dauer: jeweils ca. 3 Stunden

Diese Vorträge sind für Anwender gedacht, die das Programmieren erlernen wollen. Dabei werden sie mit den dafür erforderlichen Grundlagen – jedoch nicht auf Basis einer konkreten Programmiersprache – vertraut gemacht. Es werden die Grundelemente gängiger Programmiersprachen vorgestellt und die Arbeitsschritte beim Programmieren erläutert. Ferner wird ein Überblick über die gebräuchlichsten Programmiersprachen geboten.

## *Einführung in das Programmieren mit Perl*

Termin: Freitag, 11. April 2003, 12.30 Uhr (s.t.)

Dauer: ca. 3 Stunden

Aufbauend auf die beiden Vorträge *Einführung in das Programmieren, Teil 1 & 2* wird in dieser Veranstaltung Perl, eine weitverbreitete und sehr leistungsfähige Programmiersprache, vorgestellt. In diesem Vortrag liegt der Schwerpunkt auf der Erstellung von CGI-Skripts, wie sie z.B. für dynamisch generierte HTML-Seiten oder für die Übernahme und Auswertung von Daten, die in ein Web-Formular eingegeben wurden, benötigt werden.

## *Einführung in das Programmieren mit JavaScript*

Termin: Freitag, 9. Mai 2003, 12.30 Uhr (s.t.)

Dauer: ca. 3 Stunden

JavaScript ist eine moderne Skriptsprache, die es ermöglicht, Webseiten mit wesentlich mehr Funktionalität und Dynamik zu versehen, als dies bei ausschließlicher Verwendung von HTML der Fall ist. In diesem Vortrag, der auf den beiden Vorträgen *Einführung in das Programmieren, Teil 1 & 2* aufbaut, werden die Grundzüge von JavaScript und die Anwendungsmöglichkeiten zur dynamischen Gestaltung von Webseiten vorgestellt.

## *Suchen und Finden im Internet*

Termin: Freitag, 13. Juni 2003, 12.30 Uhr (s.t.)

Dauer: ca. 1,5 Stunden

Technisch gesehen ist der Zugriff auf riesige Informationsmengen durch den Einsatz moderner Netzwerke und Datenbanksysteme kein Problem mehr. Nur: Wie findet man die gewünschten Datenbestände? Dieser Vortrag gibt einen Überblick, mit welchen Methoden und Werkzeugen eine effiziente Suche möglich ist. Neben den allgemein im Internet verwendeten Suchmaschinen, Katalogen, Nachschlagewerken usw. wird auch der Gebrauch von wissenschaftlichen Datenbanken, Bibliothekskatalogen und Informationsdiensten besprochen.

# Personal- & Telefonverzeichnis

| | | |
|---|---|---|
| **Vermittlung** | 4277-14001 | |
| **Fax** | 4277-9140 | |

**Direktor des Zentralen Informatikdienstes**

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

**Sekretariat**

| | | |
|---|---|---|
| Pulzer Ingrid | 4277-14017 | Zi.B0116 |

**Buchhaltung**

| | | |
|---|---|---|
| Deusch Maria | 4277-14016 | Zi.B0113 |
| Haumer Claudia | 4277-14018 | Zi.B0113 |

## Abteilung Dezentrale Systeme & Außenstellen

| | | |
|---|---|---|
| Karlsreiter Peter *(Leiter)* | 4277-14131 | Zi.D0108 |
| Egger Jörg | 4277-14135 | Zi.D0104 |
| Marzluf Christian | 4277-14136 | Zi.D0110 |
| Osmanovic Richard | 4277-14132 | Zi.D0113 |
| Pfeiffer Günter | 4277-14134 | AAKH/2H EG31 |
| Römer Alfred | 4277-14139 | Zi.C0028 |
| Wienerroither Peter | 4277-14138 | Zi.D0110 |

**Außenstelle Altes AKH (AAKH)**,
*Spitalgasse 2, 1090 Wien (Fax: 4277-14119):*

| | | |
|---|---|---|
| Hönigsperger Helmuth | 4277-14114 | 2H EG35 |
| Paunzen Ernst | 4277-14111 | 2H EG35 |
| Pechter Karl | 4277-14068 | 2H EG29 |

**Außenstelle Biochemie**,
*Dr. Bohr-Gasse 9, 1030 Wien (Fax: 4277-12876):*

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

**Außenstelle Physik**,
*Boltzmanngasse 5, 1090 Wien (Fax: 4277-9141):*

| | | |
|---|---|---|
| Kind Mario | 4277-14101 | 2.St.Zi.3227 |
| Vrtala Aron | 4277-14102 | 1.St.Zi.3129 |

**Außenstelle UZA**,
*Althanstraße 14, 1090 Wien (Fax: 4277-14153):*

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

## Abteilung Software & Benutzerbetreuung

| | | |
|---|---|---|
| Stappler Herbert *(Leiter)* | 4277-14051 | Zi.B0110 |
| Berndl Christoph | 4277-14064 | Zi.C0102A |
| Brabec Erich | 4277-14075 | Zi.D0109 |
| Brugger Nikolaus | 4277-14069 | Zi.D0106 |
| Ertl Lukas | 4277-14073 | Zi.B0117 |
| Hurka Franz | 4277-14067 | Zi.D0112 |
| Kaider Thomas | 4277-14066 | Zi.B0120 |
| Kaltenbrunner Franz | 4277-14061 | Zi.C0102A |
| Köberl Dieter | 4277-14058 | Zi.D0111 |
| Kunitzky Walter | 4277-14086 | Zi.C0102 |
| Ljesevic Nasret | 4277-14062 | Zi.C0102 |
| Marksteiner Peter | 4277-14055 | Zi.B0117 |
| Mislik Heinrich | 4277-14056 | Zi.B0117 |
| Muharemagic Mirza | 4277-14082 | Zi.D0106 |
| Neuwirth Ernst | 4277-14052 | Zi.B0115 |
| Platzer Eveline | 4277-14071 | Zi.C0102B |
| Potuzak Vera | 4277-14072 | Zi.B0111 |
| Pytlik Andreas | 4277-14065 | Zi.B0120 |
| Reicher Markus | 4277-14059 | Zi.B0117 |
| Scherzer Horst | 4277-14053 | Zi.B0115 |
| Schreiner Willibald | 4277-14076 | Zi.D0112 |
| Schwindl Barbara | 4277-14054 | Zi.B0111 |
| Stadlmann Uwe | 4277-14037 | Zi.D0111 |
| Stampfer Dieter | 4277-14063 | Zi.B0104 |
| Staudigl Ralph | 4277-14224 | Zi.D0106 |
| Szabo August | 4277-14085 | Zi.D0109 |
| Talos Alexander | 4277-14057 | Zi.B0117 |
| Zoppoth Elisabeth | 4277-14074 | Zi.B0111 |

## Abteilung Zentrale Systeme & Datennetze

| | | |
|---|---|---|
| Steinringer Hermann *(Leiter)* | 4277-14021 | Zi.B0108 |
| Adam Achim | 4277-14273 | AAKH, Hof 1 |
| Ankner Markus | 4277-14077 | Zi.B0107 |
| Bauer Kurt | 4277-14070 | Zi.D0105 |
| Bogad Manfred | 4277-14029 | Zi.B0105 |
| Cikan Edwin | 4277-14022 | Zi.B0106 |
| Domschitz Eduard | 4277-14133 | Zi.B0104 |
| Englisch Holger | 4277-14270 | AAKH, Hof 1 |
| Faustin Christian | 4277-14080 | Zi.B0107 |
| Geicsnek Karin | 4277-14245 | Zi.D0114 |
| Gruber Hildegard | 4277-14079 | Zi.D0105 |
| Gruber Manfred | 4277-14241 | Zi.D0115 |
| Hartwig Günther | 4277-14243 | Zi.D0117 |
| Heimhilcher Markus | 4277-14277 | AAKH, Hof 1 |

| | | |
|---|---|---|
| Helmberger Florian | 4277-14276 | AAKH, Hof 1 |
| Hof Markus | 4277-14248 | Zi.D0115 |
| Hofstetter Mark | 4277-14275 | AAKH, Hof 1 |
| Just Stefan | 4277-14081 | Zi.B0106 |
| Kiermayr Ulrich | 4277-14104 | Zi.B0105 |
| Kunft Walter | 4277-14031 | Zi.D0107 |
| Leißer Roman | 4277-14026 | Zi.B0107 |
| Michl Harald | 4277-14078 | Zi.D0105 |
| Panigl Christian | 4277-14032 | Zi.D0105 |
| Papst Andreas | 4277-14036 | AAKH, Hof 1 |
| Parcalaboiu Paul | 4277-14246 | Zi.D0114 |
| Perzi Michael | 4277-14078 | Zi.D0105 |
| Regius Rene | 4277-14242 | Zi.D0117 |
| Rosenwirth Thomas | 4277-14025 | Zi.B0106 |
| Schaidl Christian | 4277-14026 | Zi.B0107 |
| Schirmer Daniel | 4277-14277 | AAKH, Hof 1 |
| Schneider Monika | 4277-14048 | Zi.B0107 |
| Szvasztics René | 4277-14271 | AAKH, Hof 1 |
| Vidovic Dejan | 4277-14027 | Zi.B0102 |
| Vogler Martin | 4277-14113 | Zi.C0028 |
| Wandler Alexander | 4277-14244 | Zi.D0114 |
| Winkler Gerhard | 4277-14035 | AAKH, Hof 1 |
| Wöber Wilfried | 4277-14033 | Zi.D0107 |
| Zettl Friedrich | 4277-14041 | Zi.D0113 |

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

| | |
|---|---|
| Drnek Jeanette | 4277-14313 |
| Engel Herbert | 4277-14315 |
| Erasmus Karl | 4277-14311 |
| Feigl Gabriele | 4277-14319 |
| Kammerer Jürgen | 4277-14316 |
| Mayr Karl | 4277-14314 |
| Sylla-Widon Margaretha | 4277-14318 |
| Waba Theodor | 4277-14312 |
| Wolf Maria | 4277-14317 |

## Abteilung Universitätsverwaltung

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

| | | |
|---|---|---|
| Riedel-Taschner Harald (*Leiter*) | 4277-14211 | |
| Aschauer Johann | 4277-14213 | |
| Böck Susanne | 4277-14223 | |
| Dreiseitel Thomas | 4277-14216 | |
| Filz Michael | 4277-14233 | |
| Freunschlag Martin | 4277-14203 | |
| Fuchs Alexander | 4277-14228 | |
| Hoys Peter | 4277-14215 | |
| Kauer Josef | 4277-14210 | |
| Klünger Gerhard | 4277-14219 | |
| Kößlbacher Eva | 4277-14214 | |
| Lackner Herbert | 4277-14217 | |
| Linhart Leopold | 4277-14221 | |
| Lohner Gertraud | 4277-14222 | |
| Pauer-Faulmann Barbara | 4277-14227 | |
| Payer Markus | 4277-14229 | |
| Plattner Dieter | 4277-14232 | |
| Polaschek Martin | 4277-14200 | |
| Rast Wolfgang | 4277-14124 | AAKH/2H EG31 |
| Url Clemens | 4277-14220 | |
| Zalcmann Erich | 4277-14226 | |

# ÖFFNUNGSZEITEN

**(Achtung: An vorlesungsfreien Tagen keine Tutorenbetreuung!)**

### Service- und Beratungszentrum des ZID

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

Mo – Fr 9.00 – 17.00

### Sekretariat

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

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

### Außenstelle Physik

*1090 Wien, Boltzmanngasse 5*

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

## PC-Räume

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

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

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

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

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

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

Alle Informationen zu den PC-Räumen an Instituten (Standorte, Öffnungszeiten, ...) finden Sie unter **http://www.univie.ac.at/ZID/PC-Raeume/**.

# ANSPRECHPARTNER

**In grundsätzlichen Angelegenheiten wenden Sie sich bitte an den Direktor des Zentralen Informatikdienstes oder an die Abteilungsleiter** (siehe *Personal- & Telefonverzeichnis,* Seite 54).

## Service- und Beratungszentrum

**als erste Anlaufstelle** bei EDV-Problemen und technischen Schwierigkeiten,

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

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

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

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

bei Problemen mit dem **Internet-Zugang von daheim** (*uniADSL*, *StudentConnect*, *xDSL@student*, Wählleitungszugänge der Uni Wien),

für **Kursanmeldungen**,

für **Verkauf von Handbüchern, Netzwerkkarten und -kabel**:

**eMail:** `helpdesk.zid@univie.ac.at`
**Telefon:** **4277-14060**
**Öffnungszeiten:** **Mo – Fr 9.00 – 17.00 Uhr**
NIG (1010 Wien, Universitätsstraße 7), Stg. II, 1. Stock, links

---

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

stehen Ihnen die Mitarbeiter der jeweiligen Außenstelle zur Verfügung (siehe *Personal- & Telefonverzeichnis*, Seite 54).

---

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

| | |
|---|---|
| Lackner Herbert | 4277-14217 |

---

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

| | |
|---|---|
| Rastl Peter | 4277-14011 |
| Karlsreiter Peter | 4277-14131 |

---

**für Netzwerkplanung & Gebäudeverkabelung:**

| | |
|---|---|
| Steinringer Hermann | 4277-14021 |

---

**für Kursraumvergabe:**

| | |
|---|---|
| Pechter Karl | 4277-14068 |

---

**bei Fragen zur Standardsoftware:**

| | |
|---|---|
| Wienerroither Peter | 4277-14138 |

---

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

| | |
|---|---|
| Grabner Martin | 4277-14141 |

---

**bei Fragen zum Telefonsystem der Uni Wien:**

eMail: `telefon@univie.ac.at`

---

**für Öffentlichkeitsarbeit:**

| | | |
|---|---|---|
| *Comment*-Redaktion: | Potuzak Vera | 4277-14072 |
| | Zoppoth Elisabeth | 4277-14074 |
| WWW-Redaktion: | Schwindl Barbara | 4277-14054 |

# WÄHLLEITUNGSZUGÄNGE & EMAIL-ADRESSEN

**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 (€ 0,0654/min.) |

Die Mitarbeiter des Zentralen Informatikdienstes sind unter eMail-Adressen der Form **`vorname.nachname@univie.ac.at`** erreichbar (Ausnahme: Lukas Ertl hat die Adresse `l.ertl@univie.ac.at`).
Umlaute sind mit zwei Buchstaben zu schreiben (ö = oe).

# BESTELLEN SIE IHR *E-ABO*!

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

- **e-Abo:** Unter `http://www.univie.ac.at/comment/abo.html` finden Sie ein Eingabefeld, in dem Sie Ihre eMail-Adresse angeben müssen, um Ihr e-Abo an- bzw. abzumelden.

- **Abo für Universitätsangehörige:** Mitarbeiter/innen und Studierende der Uni Wien können unter `http://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 (bitte geben Sie dabei auch Ihre bisherigen Daten an!), kontaktieren Sie uns per eMail an `comment.zid@univie.ac.at`. Bitte richten Sie alle Fragen zum neuen Abo-System ebenfalls an diese Adresse.