1 04/1 04/1 04/1 04/1 Mitteilungen des Zentralen Informatikdienstes der Universität Wien Mitteilungen des Zentralen Informatikdienstes der Universität Wien Mitteilungen des Zentralen Informatikdienstes der Universität Wien Mitteilungen des Zentralen Informatikdienstes der Universität Wien

vienna
university
computer
center

Comment

März 2004

DHCP-Service

McAfee VirusScan

Trojaner am Windows-PC

AT43 – Telefonieren im Internet

CTI – Computer Telephone Interface

Österreichische Post AG
Info.Mail Entgelt 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:	Michaela Bociurko
	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: 3 500 Stk. – ISSN: 1727-6071

Editorial

Liebe Leserin, lieber Leser!

Im Sinne eines „frühlingshaften Neubeginns“ haben wir uns in der aktuellen Ausgabe des *Comment* dazu durchgerungen, gleich zwei Neuerungen umzusetzen: Zum einen die Umstellung auf die neue deutsche Rechtschreibung, zum anderen das Bemühen um geschlechtsneutrale Formulierungen. In einzelnen Fällen hat uns jedoch der Wunsch, die „Ästhetik der Sprache“ zu bewahren, dazu veranlasst auf eine allzu rigide Umsetzung zu verzichten. Vermutlich werden Sie beim Lesen noch manches sprachliche Manko entdecken; wir bitten deshalb um Nachsicht bei unseren ersten Gehversuchen auf neuem Terrain.

Inhaltlich haben wir die zuletzt omnipräsenten Warnungen vor Viren, Würmern und Windows-Sicherheitsproblemen zum Anlass genommen und den Schwerpunkt dieser Ausgabe – wieder einmal – dem Thema Sicherheit gewidmet: Wer Trojanische Pferde bisher lediglich mit der griechischen Mythologie verbinden konnte, wird im Artikel *Ungebetene Gäste: Trojaner am Windows-PC* (Seite 10) viel Neues und Wissenswertes erfahren. Nicht neu, aber leider immer wieder hochaktuell ist das Thema Virenschutz, das im Beitrag *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* ausführlich behandelt wird (siehe Seite 21). Weitere nützliche Ratschläge zum Schutz Ihres Windows-Rechners finden Sie in den Artikeln *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* (Seite 16), *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* (Seite 18) und *Sicherheit von Anfang an – Windows XP mit Firewall-Schutz installieren* (Seite 20).

Abgesehen davon können wir auch dieses Mal von neuen Services des Zentralen Informatikdienstes berichten, wie etwa dem *Computer Telephone Interface*, das im Artikel *CTI – Computer Telefonieren Intelligenter* beschrieben ist (siehe Seite 3). Ein weiteres neues Projekt, das den Studierenden und MitarbeiterInnen der Universität Wien das Telefonieren über Internet ermöglichen soll, wird im Beitrag *All you have to do is call – Telefonieren im Internet mit AT43* (Seite 32) vorgestellt. Netzwerk-BetreuerInnen sei auch der Artikel *IP-Adressen nach Bedarf: Das DHCP-Service des ZID* (siehe Seite 30) ans Herz gelegt. Für all unsere „WebbastlerInnen“ bietet der Beitrag *Die Macht der Farben – Optimale Farbgestaltung im WWW* (siehe Seite 35) hoffentlich wieder einige nützliche Tipps und Tricks.

In diesem Sinne viel Vergnügen beim Lesen wünscht
Die *Comment*-Redaktion

Inhalt

Aktuelles

PCs & Workstations

Netzwerk- & Infodienste

Anhang

IT-Services für die Medizinische Universität

Über *Die Tücken der Trennung*, die im EDV-Bereich mit der Ausgliederung der Medizinischen Fakultät einhergehen, wurde bereits im *Comment 03/2* ausführlich berichtet (siehe `http://www.univie.ac.at/comment/03-2/032_2.html`). Inzwischen ist die „Medizinische Universität Wien" (`http://www.meduniwien.ac.at/`) Realität geworden, und auch das ZID-Äquivalent an der Med-Uni hat per 1. Jänner 2004 unter dem Namen *IT-Systems & Communications* (ITSC) den Betrieb aufgenommen.

Wie im oben erwähnten Artikel beschrieben, werden viele der EDV-Dienstleistungen, die bisher vom Zentralen Informatikdienst der Uni Wien für die Medizinische Fakultät erbracht wurden, bis auf weiteres auch der neuen Med-Uni zur Verfügung stehen. Dies betrifft insbesondere die IT-Infrastruktur an den medizinischen Instituten außerhalb des AKH – beispielsweise den Betrieb des Datennetzes und des Telefonsystems. Auch die PC-Räume der Medizinischen Universität werden weiterhin vom ZID der Uni Wien betreut.

Andere Services, wie die Verteilung von Software-Campuslizenzen und die Internet-Services für die Angehörigen der Med-Uni, sollen hingegen im Laufe der nächsten ein bis zwei Jahre nach und nach vom ITSC übernommen werden. Schon jetzt sind an der Medizinischen Universität in den Bereichen eMail, Webspace, Standardsoftware, Backup-Service, Telefonie und UNIVIS teilweise andere Verwaltungsabläufe einzuhalten. Einzelheiten dazu sowie die Kontaktadresse des EDV-Helpdesk des ITSC finden Sie am Webserver der Medizinischen Universität Wien unter `http://www.meduniwien.ac.at/itsc/changes/`.

- Für die Studierenden der Medizinischen Universität ändert sich im IT-Bereich vorläufig nicht viel: Sie können weiterhin das Unet-Service der Uni Wien in Anspruch nehmen. Neue Medizin-Studierende erhalten ihre Unet-UserID wie bisher vom Zentralen Informatikdienst der Universität Wien (siehe `http://www.unet.univie.ac.at/`). Ein „Ablaufdatum" für dieses Procedere wurde noch nicht festgelegt.

- Etwas komplizierter ist die Lage für die MitarbeiterInnen der Medizinischen Universität. Alle jene, die bereits vor dem 1. Jänner 2004 eine Mailbox-UserID an der Universität Wien hatten, können vorerst die dazugehörigen Services weiterhin verwenden – mit der Einschränkung, dass es (wie schon angesprochen) bei manchen EDV-Dienstleistungen nun neue administrative Abläufe zu beachten gilt. Bereits bestehende Mailbox-UserIDs von MitarbeiterInnen der Med-Uni bleiben bis mindestens 30. Juni 2005 gültig. Durch die geplante sukzessive Erweiterung des Service-Angebots des ITSC ist jedoch ständig mit Änderungen in Detailfragen zu rechnen.

- Alle MitarbeiterInnen der Med-Uni, die ab dem 1. 1. 2004 angestellt wurden bzw. vorher keine Mailbox-UserID hatten, kommen mit dem ZID der Uni Wien nur mehr in seltenen Fällen in Berührung: Sie erhalten ihre UserID von der Medizinischen Universität. Der Uni-ZID stellt in diesem Fall nur die Diensthandys (siehe `http://www.univie.ac.at/handy/`), die Public Network Services (`http://www.univie.ac.at/ZID/pns.html`) sowie den Breitband-Internetzugang von daheim (siehe `http://mailbox.univie.ac.at/teledial.html`) zur Verfügung. Der Internetzugang via Wählleitung (Modem bzw. ISDN) sowie alle weiteren IT-Services müssen hingegen bei der Med-Uni beantragt werden.

Die *Comment*-AbonnentInnen an der Medizinischen Universität werden die vorliegende und die nächste Ausgabe der Zeitschrift noch in gedruckter Form erhalten. Danach gelten auch die Angehörigen der Med-Uni als „externe LeserInnen", können aber auf Wunsch ein e-Abo anmelden (siehe `http://www.univie.ac.at/comment/03-2/032_7.html`).

Ein kleiner Trost in diesen schwierigen Zeiten: Selbstverständlich steht der Helpdesk des Uni-ZID (`http://www.univie.ac.at/ZID/helpdesk.html`) für alle Hilfe suchenden Unet- und Mailbox-BenutzerInnen an der Med-Uni weiterhin zur Verfügung.

Elisabeth Zoppoth ■

Standardsoftware für die Med-Uni

Durch die Abtrennung der Medizinischen Universität von der Uni Wien können MitarbeiterInnen der Med-Uni nicht mehr direkt beim ZID Softwarelizenzen bestellen, sondern müssen das *Bestellformular für Standardsoftware* an folgende Adresse senden:

Medizinische Universität Wien
IT Systems & Communications (ITSC)
Spitalgasse 23, Ebene 00
1090 Wien

Bis die Med-Uni eine eigene Infrastruktur dafür aufgebaut hat, wird die Standardsoftware weiterhin vom ZID der Uni Wien distributiert (als Download vom Software-Server oder als CD-ROM). Die Höhe der Lizenzgebühren und deren Verrechnung ist jedoch Angelegenheit der Medizinischen Universität. Bestellungen von MitarbeiterInnen der Med-Uni, die ohne Bestätigung des ITSC einlangen, können daher nicht bearbeitet werden!

Peter Wienerroither

CTI – Computer Telefonieren Intelligenter

1. Das Pferd frisst keinen Gurkensalat: Das schwere Erbe der Festnetztelefonie

Ein durchschnittlicher Festnetzapparat ohne teure Zusatzgeräte ist auch dem billigsten aktuellen Mobiltelefon weit unterlegen, was Funktionalität und Bedienungskomfort betrifft. Auch wer – so wie ich – leichten Herzens auf polyphone Klingeltöne, Multimedia-Messages, Java-Spiele und eingebaute Digitalkameras verzichten kann, weiß die Menüführung, das Namensverzeichnis, die Anrufliste und viele andere Funktionen zu schätzen.

In diesem Artikel wird das CTI-Projekt (*Computer Telephone Interface*) des Zentralen Informatikdienstes vorgestellt, das im März 2004 in Betrieb genommen wird: Durch Verknüpfung der Telefonanlage der Uni Wien mit einem Computer wurde eine komfortable, webbasierte Oberfläche für das Telefon geschaffen, die der eines Mobiltelefons zumindest ebenbürtig, in vielen Punkten jedoch weit überlegen ist.

Vorher möchte ich in einem kurzen historischen Rückblick die Gründe darlegen, warum die Festnetztelefonie gegenüber der mobilen so weit ins Hintertreffen geraten ist. Obwohl die Anfänge der Mobiltelefonie in die Fünfzigerjahre zurückreichen und das erste Mobilnetz (B-Netz) in Österreich bereits 1974 errichtet wurde, kam der Durchbruch erst 1994 mit der Einführung des GSM-Standards. Der Einsatz modernster Computertechniken war dabei selbstverständlich.

Das Festnetztelefon hingegen stammt aus dem 19. Jahrhundert. Als Erfinder werden gewöhnlich Philipp Reis (1861) und Alexander Graham Bell (1876) genannt. Nach den bahnbrechenden Erfindungen im 19. und zu Beginn des 20. Jahrhunderts war der technische Fortschritt viele Jahrzehnte lang sehr bescheiden. Daran waren nicht nur zwei Weltkriege und die Weltwirtschaftskrise der Dreißigerjahre schuld. Wie in vielen Ländern war in Österreich die Telefonie bis vor kurzem ein staatliches Monopol. Das hatte durchaus auch positive Seiten: Die Post- und Telegraphenverwaltung hatte den gesetzlichen Auftrag, ein flächendeckendes Telefonnetz zu errichten, und hat diesen Auftrag zwar gemächlich, aber gewissenhaft erfüllt – selbst in dünn besiedelten Gegenden, die für kommerzielle Anbieter uninteressant wären.

Im allgemeinen hemmte aber die Monopolstellung der wenig innovativen Postverwaltungen den Fortschritt. So dauerte die Umstellung vom handvermittelten auf Selbstwähl-Fernverkehr in Österreich mehr als 60 Jahre: Mit den ersten Versuchen wurde bereits 1910 begonnen, und erst am 14. Dezember 1972 war die Umstellung abgeschlossen (in der DDR gab es bis 1989 in einigen entlegenen Dörfern noch Handvermittlung).

1948 wurde in ganz Österreich ein einheitlicher Standard eingeführt, das *Wählsystem 48*: An diesem System hat sich 40 Jahre lang praktisch nichts geändert. Jahrzehntelang waren Vierteltelefone der Standard für Privatanschlüsse; ganze Anschlüsse waren oft nur mit extrem langen Wartezeiten oder mit Protektion zu bekommen. Auch das Aussehen und die Funktion der Telefonapparate sind in dieser Zeit weitgehend gleichgeblieben: Mit dem Wählsystem 48 verschwand zwar die kryptische Buchstabenkombination `IFABRUMLYZ` von den Wählscheiben, aber sonst blieb alles beim Alten: Außer der Wählscheibe verfügte der Apparat über keinerlei Funktionen, er konnte auch nicht abgeschaltet werden. Telefonapparate waren Eigentum der Post und konnten offiziell nur über diese bezogen werden. Auswahl gab es praktisch keine, eigenmächtige Umbauten und das Anschließen anderer Apparate waren verboten.

Mit langer Verzögerung wurden die rasanten Fortschritte in der Computer- und Nachrichtentechnik schließlich auch von den Postverwaltungen zur Kenntnis genommen. 1981 begann die Entwicklung des digitalen Telefonsystems OES. 1986 wurden erstmals zwei Wählämter in Wien auf digitalen Betrieb umgestellt. Schon der erste Satz einer von der Post herausgegebenen Broschüre zum OES zeugt von wenig Innovationsfreude: *„Auch beim Telefon bleibt die Zeit nicht stehen."* Im Zuge der Digitalisierung wurden die Wählscheibenapparate nach und nach durch Tastentelefone ersetzt – anderswo gab es diese seit Jahrzehnten. Die Post nannte die von ihr angebotenen Modelle „Komfort-Tastwahlapparate". Der Komfort eines solchen Apparates hält sich aber immer noch in Grenzen: Ausschalten kann man ihn ebensowenig, aber immerhin ausstecken. Wer glaubt, dadurch vor unerwünschten Anrufen sicher zu sein, irrt: Bei ausgestecktem Apparat läutet die Steckdose – das muss so sein, weil *„Vurschrift is Vurschrift"*. Das Komfort-Telefon kann aber tatsächlich zum Schweigen gebracht werden: Mit der einleuchtenden und leicht zu merkenden Tastenkombination `*24*01#` wird die OES-Funktion *Anrufumleitung zu Normtexten* aktiviert.

Das OES bietet auch die Möglichkeit, Anrufer zu identifizieren. Die erwähnte Broschüre schreibt dazu: *„Natürlich werden Sie diesen Dienst nur im Notfall in Anspruch nehmen."* Ich finde es bemerkenswert, dass dies für „natürlich" gehalten wird: Wer ein Telefon besitzt, soll sich gefälligst zu jeder Tages- und Nachtzeit bei jeder beliebigen Tätigkeit von jedem Anrufer unterbrechen lassen – und wer da anruft, geht ihn gar nichts an. Diese Einstellung war offensichtlich auch in den Neunzigerjahren noch nicht aus den Köpfen verschwunden. Zu dieser Zeit überstürzten sich aber die Ereignisse: Mobiltelefonie wurde immer populärer, das Bedürfnis nach leistungsfähigen Datenleitungen immer größer. Daher boten die Postverwaltungen eine Reihe von Diensten zur Datenübertragung an (z.B. BTX, Datex-P), die auf den vom *Comité Consultatif International Téléphonique et Télé-*

graphique (CCITT) definierten Standards beruhen (z.B. X.25 als Transportprotokoll, X.400 zur Nachrichtenübermittlung). Es gab zwar Flops wie den MUPID, manche dieser Dienste waren aber durchaus erfolgreich. Durch die rasante Verbreitung des Internets wurden sie dennoch weitgehend verdrängt und werden heute nur mehr in einzelnen Marktnischen eingesetzt. Wohl oder übel musste mit jahrzehntelangen Traditionen gebrochen werden. Mit dem Telekommunikationsgesetz 1997 fiel das staatliche Telefon-Monopol. Die Telefonie wurde als Telekom Austria von der Post ausgegliedert, bald gab es in Mobil- und Festnetz die ersten Konkurrenten. Im August 1999 wurde im Festnetz der Telekom Austria CLIP[1)] aktiviert – ohne diese Funktion wäre das CTI weitgehend nutzlos. Ende der Neunzigerjahre war die Digitalisierung des Festnetzes praktisch abgeschlossen – immerhin dreimal so schnell wie die Umstellung auf Selbstwählfernverkehr.

Mit der Telekom-Liberalisierung gab es auch in der Festnetztelefonie bedeutende Fortschritte: Telefonapparate mit beliebigen Funktionen – Schnurlostelefone, Nebenstellenanlagen auch für private Haushalte usw. – sind im Fachhandel frei erhältlich. Trotz allem mangelt es den heutigen Telefonen oft noch an Komfort. Viele große Telekom-Gesellschaften und -Ausrüster haben ein kommerzielles Interesse daran, dass alles beim Alten bleibt: Die in der Telefonie eingesetzten Übertragungsprotokolle sind proprietär, die Lizenzkosten astronomisch, und selbst für minimale Änderungen sind Unsummen zu bezahlen.

2. CTI – ein Gemeinschaftsprojekt von Kapsch und Uni Wien

Heute stehen praktisch auf jedem Schreibtisch ein Telefon und ein Computerbildschirm. Was liegt näher, als die oben beschriebenen Mängel des Telefons durch den Computer auszugleichen? Auf einem Computerbildschirm haben viel mehr Informationen Platz als auf einem Handy-Display, und selbst SMS-geübte Jugendliche können Texte am Handy nicht so schnell eintippen wie auf einer Computertastatur.

Bereits vor einigen Jahren gab es ein erstes Projekt mit der Firma Schrack, die damals an der Errichtung der neuen Telefonanlage der Uni Wien beteiligt war. Der Prototyp des *Personal Call Assistant* funktionierte durchaus, war aber auf Windows-Systeme beschränkt und in der heterogenen EDV-Landschaft der Universität Wien nur bedingt einsetzbar.

In der Zwischenzeit wurde Schrack von Kapsch übernommen. Das von Kapsch als Nachfolgeprodukt des Personal Call Assistant entwickelte *Computer Telephone Interface* ist weitaus flexibler und leistungsfähiger und wird von Kapsch bereits hausintern und bei etlichen Kunden eingesetzt. Auch dieses System ist primär für ein homogenes Firmen-Netzwerk mit einheitlicher Softwareausstattung gedacht. Es läuft auf dedizierten Servern (*Smart Assistants*) und besteht aus zwei Teilen: Ein Teil ist für die Kommunikation zwischen Telefonanlage und Smart Assistant zuständig, der andere für den Datenaustausch (in Form von XML-Dateien) zwischen Smart Assistant und Windows-Klienten. Für den ersten Teil wird unverändert die von Kapsch entwickelte Software verwendet; der zweite Teil wurde durch eine Eigenentwicklung des Zentralen Informatikdienstes ersetzt: Die Lösung für die Universität Wien ist rein webbasiert. Sie hat zwar den Nachteil, dass sie nicht so gut in die Windows-Oberfläche integriert ist, dafür ist sie aber überall und mit jedem beliebigen Betriebssystem und Webbrowser verwendbar. Auch die Personaldatenbank der Universität Wien kann auf diese Weise nahtlos in das CTI eingebunden werden.

3. Komfortabel telefonieren mit dem CTI

3.1 Anmeldung

Um das CTI zu verwenden, benötigen Sie eine Mailbox-UserID und einen Eintrag Ihrer Universitäts-Telefonklappe in der Online-Personaldatenbank der Uni Wien (`http://`

1) CLIP (*Calling Line Identification Presentation*): Der anrufende Apparat schickt seine Telefonnummer an die Gegenstelle. Mit CLIR (*Calling Line Identification Restriction*) wird die Übermittlung der Telefonnummer unterbunden.

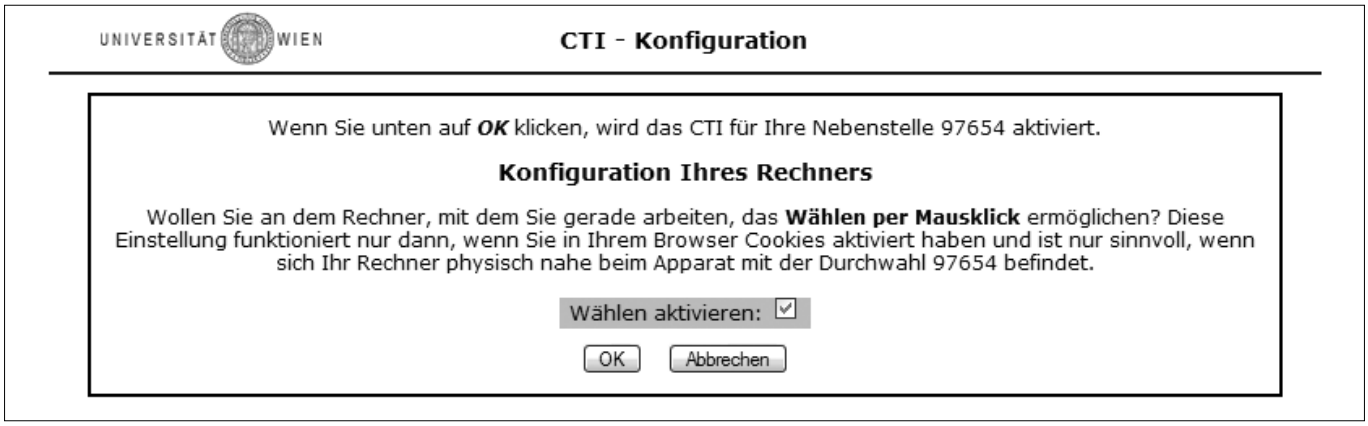

Abb. 1: Konfigurationsfenster des CTI

data.univie.ac.at/pers). Wenn diese Voraussetzungen erfüllt sind, erhalten Sie beim ersten Aufruf der Webseite https://data.univie.ac.at/cti/ eine Anmeldemaske, wie sie in Abb. 1 zu sehen ist.

Für einen Rechner, der an Ihrem Arbeitsplatz neben dem Telefon steht, kreuzen Sie *Wählen aktivieren* an – dann können Sie alle Funktionen des CTI nutzen. Bei einem Rechner zu Hause oder anderswo ist es wenig sinnvoll, wenn Sie mittels Mausklick den Apparat an Ihrem Arbeitsplatz einen Anruf tätigen lassen; daher sollten Sie in diesem Fall die Funktion besser nicht aktivieren. Klicken Sie auf *OK*, und die Anmeldung ist abgeschlossen. Weitere Aufrufe dieser Webseite führen Sie direkt zur Anrufliste.

Falls aus irgendeinem Grund (z.B. fehlender oder falscher Eintrag der Telefonnummer in der Personaldatenbank) die automatische Aktivierung nicht möglich ist, erhalten Sie statt der Anmeldemaske einen entsprechenden Hinweis. In diesem Fall kontaktieren Sie bitte die eMail-Adresse cti.zid@univie.ac.at.

3.2 Anrufliste

Die Anrufliste (https://data.univie.ac.at/cti/) ist die wichtigste Funktion des CTI. Unmittelbar nach der Anmeldung ist sie leer; danach werden die Verbindungsdaten jedes Gesprächs aufgezeichnet und sind wenige Sekunden nach Beenden in der Anrufliste zu finden (siehe Abb. 2).

- Das Symbol ganz links zeigt, um welche Art von Telefongespräch es sich handelt: Ankommende bzw. abgehende Gespräche werden durch die Position des Pfeils symbolisiert; die Farbe des Pfeils (grün bzw. rot) zeigt an, ob das Gespräch zustandegekommen ist oder nicht.

- In der nächsten Spalte steht die Telefonnummer des Gesprächspartners; falls bei der Anmeldung die Funk-

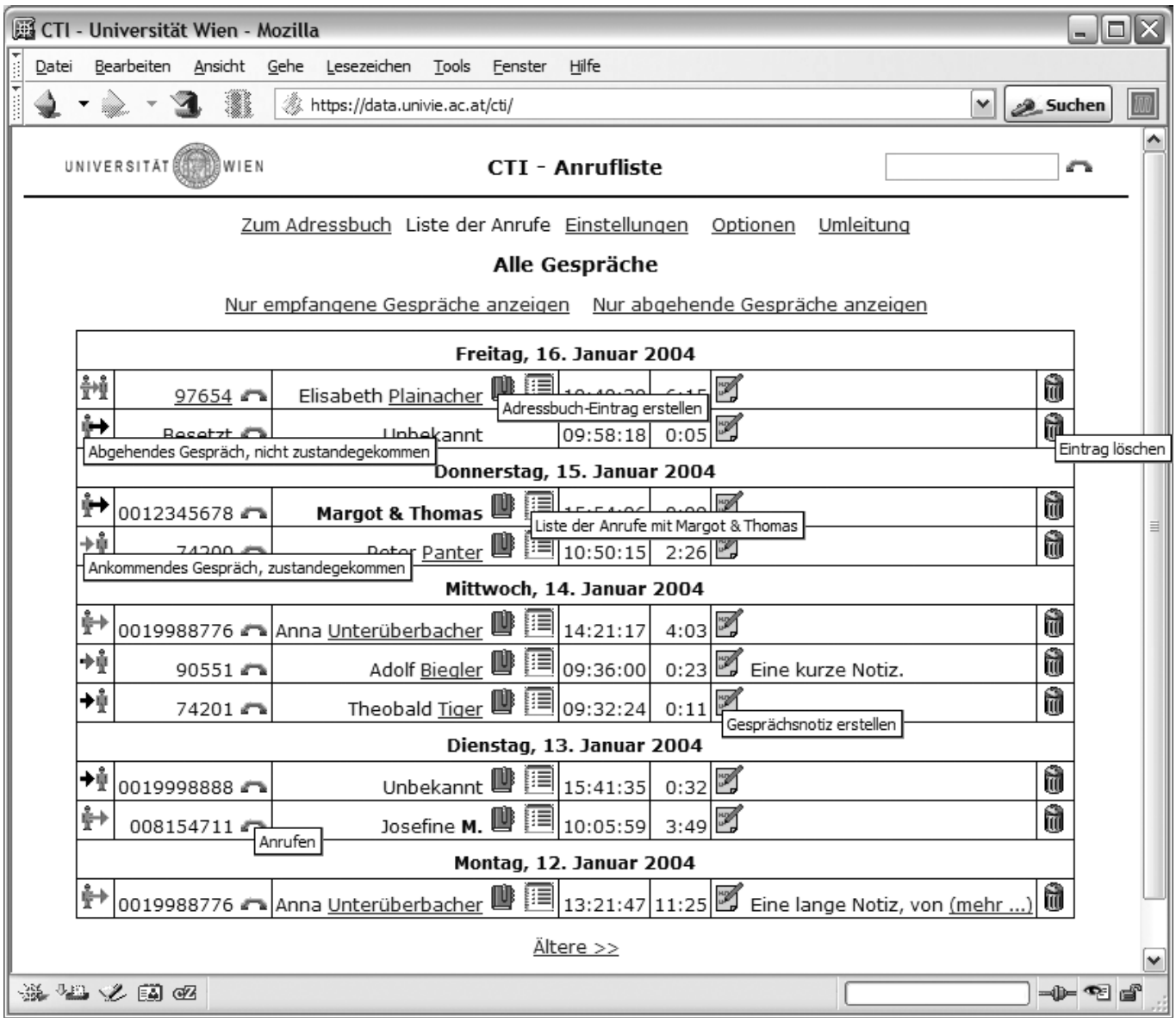

Abb. 2: CTI-Anrufliste – die eingeblendeten Texte werden sichtbar, wenn Sie mit dem Mauscursor auf das entsprechende Symbol zeigen.

tion *Wählen per Mausklick* aktiviert wurde, kann diese Nummer durch Klick auf den Telefonhörer daneben angerufen werden (mehr dazu in Kapitel 3.4). Manchmal ist die Nummer nicht bekannt (z.B. weil die Bekanntgabe der Rufnummer mittels CLIR unterdrückt wurde), dann steht dort *Unbekannt*. Auch wenn die Leitung besetzt ist oder der Anruf auf eine Sprachbox umgeleitet wurde, kann die Nummer meist nicht festgestellt werden.

- Weitergeleitete Gespräche werden auf besondere Art dargestellt: Zum einen gibt es für solche Gespräche ein spezielles Symbol (siehe Abb. 2, erster Eintrag), zum anderen ist dann die Telefonnummer anklickbar und führt zu einem Popup-Fenster mit der Nummer, an die das Gespräch weitergeleitet wurde.

- Die Namen in der nächsten Spalte stammen aus zwei Quellen: entweder aus Ihrem persönlichen Adressbuch (siehe Kapitel 3.3) oder aus der Personaldatenbank (`http://data.univie.ac.at/pers`). Falls beide Einträge (Adressbuch und Personaldatenbank) vorhanden sind, wird nur ersterer angezeigt. Auf den Namen, der am Display der Telefonapparate aufscheint, hat das CTI leider keinen Zugriff.

- Das Buch neben dem Namen symbolisiert das Adressbuch (siehe Kapitel 3.3); durch Klick auf das Listen-Symbol daneben erhalten Sie eine Liste aller Anrufe von und zu dieser Nummer.

- In den nächsten zwei Spalten stehen Zeitpunkt (Beginn) und Dauer (in Minuten und Sekunden) des Gesprächs. Danach folgt – sofern vorhanden – die Gesprächsnotiz (siehe Kapitel 3.5) und das Symbol zum Erstellen und Bearbeiten von Notizen.

- Durch Klick auf die Mülltonne ganz rechts wird der Eintrag des Gesprächs samt allenfalls vorhandener Gesprächsnotiz aus der Datenbank gelöscht.

3.3 Adressbuch

Für jede Telefonnummer, die im CTI aufscheint, können Sie durch Klick auf das Adressbuch-Symbol einen Eintrag in Ihrem persönlichen Adressbuch erstellen (siehe Abb. 3). Ein solcher Eintrag besteht aus vier Teilen: Telefonnummer, Vorname, Nachname und Zusatzinformationen, wobei Vorname und Zusatzinformationen optional sind. Natürlich muss es sich beim Inhalt der Namensfelder nicht um Namen handeln – Sie können dort hineinschreiben, was Sie wollen. Das Adressbuch ist alphabetisch nach Nachnamen geordnet. Wenn das Feld *Weitere Informationen* nicht leer ist, wird der Nachname anklickbar: Die Zusatzinformationen erscheinen dann in einem Popup-Fenster.

Verknüpfungen zu anderen Adressbüchern (z.B. eMail-Verzeichnisse von Outlook oder anderen Mailprogrammen) gibt es derzeit nicht; das Feld mit den Zusatzinformationen kann aber eMail-Adressen oder Links zu Webseiten enthalten. Diese werden automatisch anklickbar gemacht.

Zu jedem Eintrag im Adressbuch gibt es nur eine Telefonnummer: Wenn eine Person unter mehreren Nummern zu erreichen ist, erstellen Sie bitte für jede Nummer einen eigenen Eintrag. Um bei einem Eintrag die Nummer zu ändern, wählen Sie die Funktion *Eintrag kopieren* und löschen Sie nachher den alten Eintrag.

3.4 Wählen, Auflegen und Umleiten

Das CTI ermöglicht es auch, den Apparat aktiv zu beeinflussen. Theoretisch könnten fast alle Aktionen anstatt über die Tastatur des Telefonapparats mittels CTI ausgeführt werden; davon sind vorerst aber nur die wichtigsten implementiert. Sofern bei der Konfiguration (siehe Kapitel 3.1) das *Wählen per Mausklick* aktiviert wurde, wird neben jeder Telefonnummer ein Telefonhörer angezeigt. Wenn Sie darauf klicken, erscheint ein Popup-Fenster *xxxx wird gerufen*, und nach einer kurzen Verzögerung – meistens unter einer Sekunde – beginnt Ihr Apparat, eine Verbindung zu dieser Nummer aufzubauen. Mittels Klick auf das rote Telefon-Symbol im Popup-Fenster können Sie das Gespräch abbrechen.

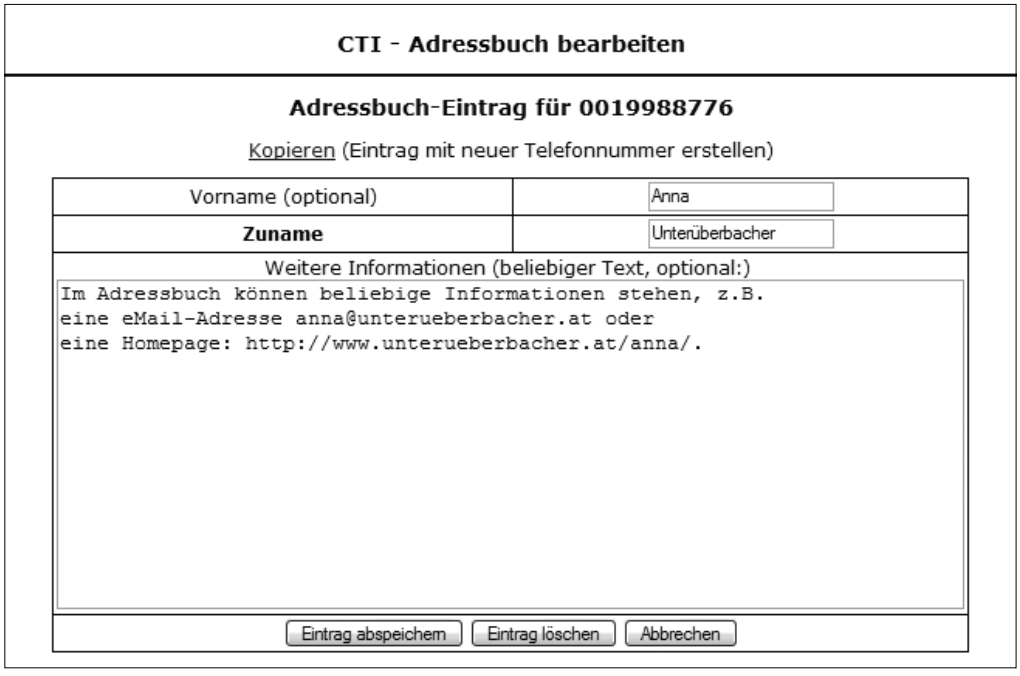

Abb. 3: Adressbuch-Eintrag

- Mit Hilfe des Eingabefelds rechts oben (siehe Abb. 2) können Sie eine beliebige Nummer anrufen. Telefonnummern, die z.B. aus Webseiten oder eMail-Nachrichten mit der Maus kopiert werden, müssen meistens leicht modifiziert werden: Geben Sie Telefonnummern immer genauso ein, wie sie auf den Apparaten der Telefonanlage der Uni Wien einzutippen sind, also nur Ziffern (ohne Leer- und sonstige Trennzeichen) mit führender Null für Auswärtsgespräche. Wundern Sie sich nicht, wenn die Nummer manchmal anders angezeigt wird als Sie diese eingegeben haben (z.B. mit Vorwahl 01 für Wien): Das CTI wandelt die Nummer automatisch in die Form um, die intern benötigt wird.

- Sie begeben sich von Ihrem Arbeitsplatz weg – z.B. in ein Labor oder ein Besprechungszimmer. Sie erwarten einen wichtigen Anruf und haben vergessen, die Anrufumleitung zu Ihrem Standort einzurichten. Kein Problem: Mit der Funktion *Umleitung* können Sie das nachholen, ohne nochmals zu Ihrem Arbeitsplatz zurückzukehren. Bitte beachten Sie, dass die Anrufumleitung mittels CTI denselben Einschränkungen unterliegt wie die Umleitung direkt vom Apparat aus: Beispielsweise muss bei einer Umleitung auf externe Nummern die Chipkarte eingesteckt sein.

3.5 Gesprächsnotizen

Mir passiert es immer wieder: Jemand ruft mich an, ich mache Gesprächsnotizen auf einem Zettel, nachher finde ich den Zettel nicht mehr und vergesse darauf. Die elektronischen Gesprächsnotizen des CTI haben da einen großen Vorteil – sie können nicht verloren gehen.

- Durch Klick auf das Notizsymbol wird die Funktion *Gesprächsnotiz erstellen* (bzw. *bearbeiten*, sofern schon eine vorhanden ist) aufgerufen. Die Notiz kann beliebigen Text enthalten und bis zu 4000 Zeichen lang sein.

- Ist eine Notiz sehr kurz, wird sie zur Gänze in der Anrufliste angezeigt. Von längeren Notizen sind nur die Anfangsworte zu sehen, der Rest erscheint bei Klick auf *(mehr ...)* in einem Popup-Fenster (siehe Abb. 4).

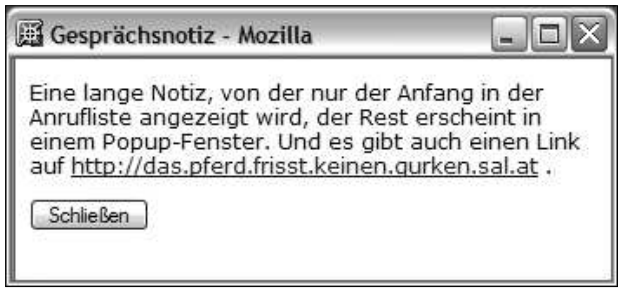

Abb. 4: CTI-Gesprächsnotiz

- Ein kleiner Nachteil: Gesprächsnotizen können erst nach Beendigung des Gesprächs erstellt werden.

3.6 Einstellungen und Optionen

Über den Link *Einstellungen* (`https://data.univie.ac.at/cti/config.html`, siehe Abb. 1 auf Seite 4) werden die grundlegenden Funktionen des CTI geregelt: Aktivieren und Deaktivieren, Wahl der Nebenstelle (falls Sie mehrere haben) sowie Wählen mittels Mausklick ein- oder ausschalten.

Mittels *Optionen* (`https://data.univie.ac.at/cti/options.html`, siehe Abb. 5) können Sie Ihre persönlichen Präferenzen einstellen:

- Wie lange sollen die Einträge gespeichert werden (siehe dazu auch Kapitel 4)?

- Soll die Anrufliste alle Gespräche anzeigen, oder nur die ankommenden, oder nur die abgehenden?

- Wie viele Einträge pro Seite sollen angezeigt werden?

- Soll die Anrufliste regelmäßig automatisch aktualisiert werden? Hier ist das kleinste erlaubte Intervall fünf Minu-

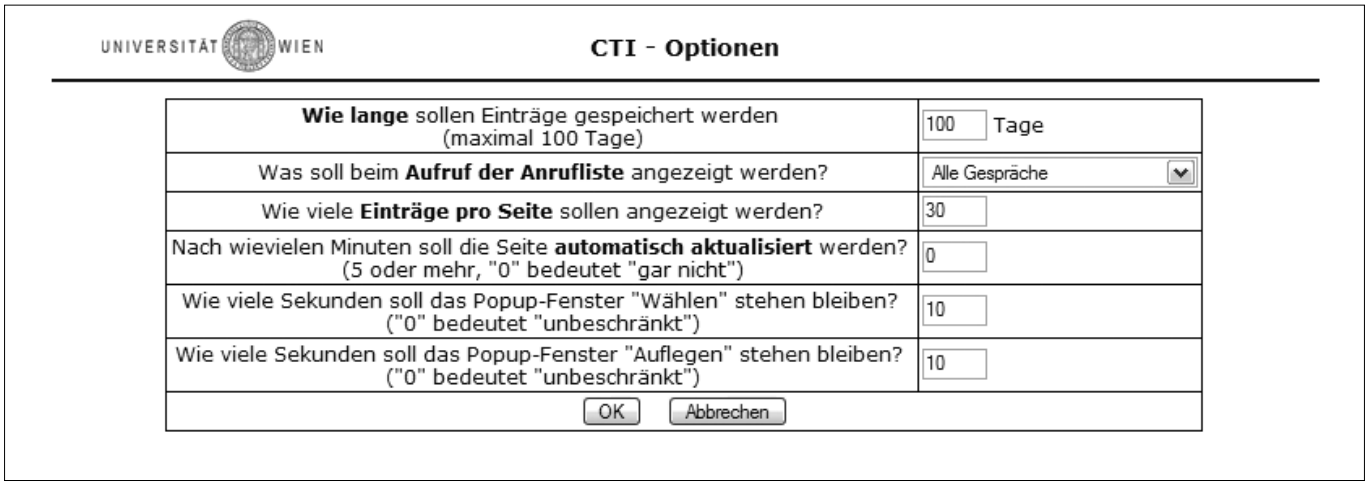

Abb. 5: CTI-Optionen

ten, um den Server nicht zu sehr durch ständige Zugriffe zu belasten.

- Die Popup-Fenster, die beim Wählen und nach Klick auf *Auflegen* erscheinen, verschwinden normalerweise nach einigen Sekunden automatisch wieder: Hier kann eingestellt werden, wie lange sie „leben" sollen – auf Wunsch auch unbegrenzt.

3.7 Verknüpfung mit der Personaldatenbank

Das CTI ist mehrfach mit der Online-Personaldatenbank `http://data.univie.ac.at/pers` verknüpft: Einerseits ist die Verwendung des CTI nur für Nebenstellen möglich, die einer bestimmten Person zugeordnet sind, andererseits werden die Namen aus der Personaldatenbank in der Anrufliste angezeigt.

In beiden Fällen muss die Zuordnung einer Nebenstelle zu einer Person eindeutig sein: Wenn sich mehrere Personen eine Nebenstelle teilen, so können diese nur nach Rücksprache das CTI verwenden (siehe auch Kapitel 4). Auch die Berechtigung für sonstige Nebenstellen – Labors, Seminarräume usw. – muss jeweils einzeln vergeben werden; wenden Sie sich in diesem Fall bitte an die eMail-Adresse `cti.zid@univie.ac.at`.

Falls ein Name in der Anrufliste als *Unbekannt* aufscheint, obwohl die Telefonnummer im Personalverzeichnis zu finden ist, so gibt es dort noch einen zweiten Eintrag mit derselben Nummer. Manchmal liegt das nur an veralteten Personaldaten – es existieren noch etliche Einträge von längst ausgeschiedenen Kolleginnen und Kollegen. Wenden Sie sich bitte an die Adresse `wartung.personaldaten@univie.ac.at`, um die Daten zu aktualisieren. Der Name am Display des Telefonapparats stammt nicht direkt aus der Personaldatenbank und muss daher nicht unbedingt mit dieser übereinstimmen.

Wenn Sie das *Wählen per Mausklick* aktiviert haben, ändert sich auch das Aussehen des Online-Personal- und Institutsverzeichnisses: Neben allen Telefonnummern erscheint der grüne Telefonhörer, d.h. alle Nummern können direkt mittels CTI gewählt werden.

Linux-Workshop

Nach mehrjähriger Pause bietet der ZID im Mai 2004 wieder einen Linux-Workshop an. Der dreitägige Kurs richtet sich an Personen mit grundlegenden Unix-Kenntnissen, die erfahren möchten, wie man einen Linux-Rechner installiert und konfiguriert. Darüber hinaus werden auch die Themenbereiche Serverbetrieb und Systemsicherheit behandelt. Nähere Einzelheiten finden Sie im Kursprogramm des ZID (siehe Seite 44 im Anhang dieses *Comment* bzw. `http://data.univie.ac.at/kurs/bin/kursang.pl`).

4. Datenschutz

Die Daten, die das CTI liefert, unterscheiden sich nicht grundsätzlich von dem, was ein Mobiltelefon in der Anrufliste speichert. Auch gehen sie nicht wesentlich über das hinaus, was durch sorgfältiges Mitschreiben händisch erstellt werden könnte. Dennoch sind Verbindungsdaten (*Wer hat wen wann angerufen?*) besonders sensible Daten, und anders als bei einem Mobiltelefon werden sie hier nicht am Endgerät, sondern in einer Datenbank abgespeichert. Deshalb wurde beim Design und bei der Implementation des CTI besonderes Gewicht auf den Datenschutz gelegt.

Bei den hier aufgezeichneten Daten handelt es sich um „Verkehrsdaten" im Sinne des Telekommunikationsgesetzes, dessen § 96 Datenschutzbestimmungen enthält:

> *§ 96. (1) Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten dürfen nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden.*

Im Falle des CTI handelt es sich um eine „technische Speicherung" für einen „ausdrücklich gewünschten Dienst":

> *§ 96 (3) [...] Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, soweit dies unbedingt erforderlich ist, um einen vom Teilnehmer oder Benutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen. [...]*

Durch folgende Maßnahmen wird Missbrauch der Daten verhindert:

- Die Daten werden nur auf ausdrücklichen Wunsch aufgezeichnet. Im Falle einer Deaktivierung des CTI wird die Aufzeichnung sofort beendet.

- Die Daten werden nur für beschränkte Zeit aufgehoben (maximal 100 Tage); über den Punkt *Optionen* kann auch eine kürzere Aufbewahrungsfrist gewählt werden. Falls Sie Aufzeichnungen über einen längeren Zeitraum benötigen, so speichern Sie die HTML-Seite mit der Anrufliste rechtzeitig auf Ihrem Rechner.

- Einträge zu einzelnen Gesprächen (samt allenfalls vorhandener Notizen) können gelöscht werden.

- Wenn mehrere Personen eine Nebenstelle teilen, hat jeder Beteiligte Informationen über die Telefonate aller anderen. Deshalb kann das CTI in einem solchen Fall nur verwendet werden, wenn alle Beteiligten ausdrücklich zustimmen.

- Die Daten sind durch Ihr Mailbox-Passwort geschützt. Abgesehen von den Systemadministratoren, die notwen-

digerweise auf die Datenbank zugreifen können und dienstlich streng zum Einhalten aller Datenschutzbestimmungen verpflichtet sind, hat niemand außer Ihnen Zugang zu den Daten Ihrer Telefongespräche. Verwahren Sie Ihr Mailbox-Passwort sorgfältig und geben Sie es an niemanden weiter! Beachten Sie auch die *Tipps & Hinweise zum Passwort* unter `http://mailbox.univie.ac.at/passwort.html`.

- Zugriff auf das CTI ist nur mittels Secure HTTP möglich, wobei alle Daten verschlüsselt und abhörsicher übertragen werden.

- Die Daten werden grundsätzlich nicht an Dritte weitergegeben.

Damit keine Missverständnisse aufkommen: Unter keinen Umständen werden die Telefongespräche selbst (die „Inhaltsdaten") aufgezeichnet!

5. Ausblick auf die Zukunft

In der ersten (internen) Testphase waren die Erfahrungen mit dem CTI sehr gut: Die meisten der Personen, die sich als „Versuchskaninchen" zur Verfügung gestellt hatten, wollen keinesfalls mehr darauf verzichten. In nächster Zeit wird sich zeigen, wie sich das System im Großeinsatz verhält. Falls es zu einem starken Andrang kommt, ist eventuell kurzfristig mit Performance-Engpässen zu rechnen, die sich aber mit zusätzlicher Hardware beseitigen lassen.

Die vorliegende Version 1.0 des CTI soll hinkünftig in Zusammenarbeit mit der Firma Kapsch noch weiterentwickelt, verbessert und um zusätzliche Funktionen erweitert werden. Zur Zeit bestehen einige Einschränkungen, von denen manche jedoch durch die Funktionsweise des Systems bedingt sind und sich nicht (oder nur mit enormem Aufwand) beseitigen lassen: Beispielsweise werden Anrufe nicht registriert, wenn eine Umleitung auf eine Sprachbox aktiviert ist; weiters kann das CTI auch nicht gemeinsam mit einer Callcenter-Software eingesetzt werden.

Richten Sie Wünsche, Anregungen und Beschwerden bitte an die Mailadresse `cti.zid@univie.ac.at`. Wir freuen uns über jede Rückmeldung und werden uns bemühen, das CTI noch nützlicher und komfortabler zu gestalten.

Peter Marksteiner ■

Und warum frisst das Pferd keinen Gurkensalat? Angeblich war dieser Satz – neben einigen anderen, ebenso unsinnigen – der Inhalt des ersten Telefongesprächs der Welt, als Philipp Reis 1861 seine Erfindung demonstrierte.

Personalnachrichten

Mit dem Inkrafttreten des Universitätsgesetzes 2002 zu Beginn des heurigen Jahres haben sich auch die rechtlichen Rahmenbedingungen für die Anstellung neuer MitarbeiterInnen geändert: Bisher gab es einerseits die Vertragsbediensteten des Bundes, für deren Beschäftigung ein bürokratisches Korsett aus Stellenplan, Arbeitsplatzbewertungen, Funktionsbeschreibungen, Besoldungsschema und Laufbahnbildern jegliche Flexibilität im Personalmanagement weitgehend zu unterdrücken wusste; andererseits hatten wir im Rahmen der Teilrechtsfähigkeit der Universität (entsprechende Finanzmittel vorausgesetzt) alle Freiheiten, Dienstverträge mit Angestellten jederzeit kurzfristig und unbürokratisch entsprechend unseren Erfordernissen abzuschließen. Davon haben wir reichlich Gebrauch gemacht – mehr als ein Drittel aller MitarbeiterInnen des Zentralen Informatikdienstes sind solche Angestellte in der Teilrechtsfähigkeit.

Mit dem Universitätsgesetz 2002 sind wir nun sowohl die bürokratischen Fesseln der Bundes-Personalverwaltung wie auch die Freiheiten der Teilrechtsfähigkeit los: Die Aufnahme und Anstellung aller MitarbeiterInnen wird durch das UG 2002 geregelt, und es wird sich zeigen, wieviel Flexibilität uns erhalten bleibt.

Jedenfalls haben wir daher noch vor dem Inkrafttreten des UG 2002 die Möglichkeiten der Teilrechtsfähigkeit kräftig ausgenutzt und etliche weitere MitarbeiterInnen angestellt: In der Abteilung Universitätsverwaltung verstärken seit Mitte November 2003 **Mario Stark** und **Andreas Leo Zeiner** die Softwareentwicklungs-Mannschaft, und **Christina Eireiner** wechselte vom Dekanat der Rechtswissenschaftlichen Fakultät ins UNIVIS-Supportteam. Seit Oktober 2003 arbeitet **Farzaneh Hojreh** im UNIVIS-Projektmanagement, und mit März 2004 wechselte auch **Marion Niederhuber** vom Zentrum für Forschungsförderung, Drittmittel und Öffentlichkeitsarbeit der Universität Wien in diese Gruppe. Ein langjähriger Mitarbeiter der Abteilung Universitätsverwaltung, **Peter Hoys**, trat hingegen mit Ende Februar 2004 in den Ruhestand. Wir danken ihm herzlich für die geleistete Arbeit und seine Treue zum Zentralen Informatikdienst und wünschen ihm das Beste für seinen neuen Lebensabschnitt.

Beim PC-Support, den wir im Rahmen der neu gestalteten Universitätsorganisation künftig deutlich erweitern wollen, unterstützen uns seit Jahresbeginn 2004 **Reinhard Nunner**, **Florian Pavelic** und **Pascal Salet** als zusätzliche Mitarbeiter. Seit Anfang November 2003 ergänzt darüber hinaus **Christian Plansky** das Helpdesk-Team am Service- und Beratungszentrum.

Allen diesen MitarbeiterInnen danken wir für ihr Engagement und wünschen ihnen viel Freude und Erfolg in ihrem jeweiligen neuen Arbeitsumfeld!

Peter Rastl

Ungebetene Gäste: TROJANER AM WINDOWS-PC

Das Thema Systemsicherheit betrifft selbstverständlich alle Betriebssysteme – bei MS-Windows entwickelt es sich jedoch zu einem Dauerbrenner: Beinahe täglich werden neue Sicherheitslücken entdeckt, die immer wieder die Endanwender betreffen. Die Firma Microsoft vertritt derzeit die Philosophie, alle ihr bekannt gewordenen Sicherheitsprobleme jeden zweiten Dienstag im Monat zu veröffentlichen. Meistens ist es dann nur mehr eine Frage der Zeit, bis ein Virus, Wurm oder Trojaner im Netz auftaucht, der die Sicherheitslücke für seine Zwecke ausnutzt.

Böse Software

Unerwünschte, schädliche und/oder sich selbst verbreitende Programme werden als *Malicious Software* (kurz *Malware*) bezeichnet. Im wesentlichen unterscheidet man dabei drei Kategorien:

- Ein **Virus** ist ein selbstreplizierendes Programm, das in der Regel auf dem befallenen Rechner verschiedene Störaktionen ausführt. Bis zum Auslösen dieser Störaktionen agiert das Virus meist ohne Wissen des Benutzers. Viren verbreiten sich passiv auf lokalen Systemen (Festplatten und Windows-Shares): Sie infizieren intakte Anwendungsprogramme, indem sie ihren eigenen Programmcode in deren Befehlskette einschleusen. Beim Starten der Anwendung wird dann vorher das Virus ausgeführt.

- Ein **Wurm** kopiert sich selbsttätig über das Netzwerk auf andere Rechner weiter, wobei er oft bestehende Sicherheitslücken ausnutzt. Im Unterschied zu Viren vermehren sich Würmer nicht über Wirtsprogramme, sondern schreiben üblicherweise neue Dateien auf die Festplatte des Opfers oder ersetzen vorhandene Dateien. Eine große Gefahr von Wurmattacken liegt in ihrer enormen Verbreitungsgeschwindigkeit und der daraus resultierenden Netzbelastung: Innerhalb weniger Minuten können dadurch ganze Netzwerke bzw. sogar große Teile des Internet lahm gelegt werden.

- Ein **Trojanisches Pferd** (kurz, wenn auch nicht ganz korrekt: Trojaner) ist per Definition eine Software, die auf dem Rechner eines Benutzers ohne dessen Wissen als Agent eines Angreifers agiert, also im Prinzip jedes Programm mit einer verborgenen Absicht. Trojanische Pferde geben häufig vor, etwas Nützliches zu tun bzw. tun dies wirklich; gleichzeitig führen sie aber auch unerwünschte Aktionen aus – vom Ausspähen der Benutzerdaten und Passwörter bis zur totalen Übernahme des Systems. Trojaner verbreiten sich in der Regel nicht aktiv weiter, sondern werden entweder von Hackern gezielt eingeschleust oder vom Benutzer „eingeladen“: beispielsweise durch das Öffnen von eMail-Attachments, durch Mausklicks auf aktive Web-Inhalte oder durch die Installation verseuchter Freeware- oder Shareware-Programme.

Die Grenze zwischen den verschiedenen Schädlingen ist fließend – Viren und Würmer können auch Trojanerfunktionen mit übertragen. Ein Trojanisches Pferd kann also zum Beispiel durch ein Virus, einen Wurm, ein eMail-Attachment, einen Hacker und sogar durch Zustimmung des Benutzers in das System gelangen. Die Vielfalt der Ausbreitungsmethoden und versteckten Tätigkeiten von Trojanern ist bedrückend.

Wer ist der Feind?

Trojanische Pferde sind ein bunter Haufen: Es gibt unter anderem Adware, Spyware, Trickleware, Browser Helper Objects, RATs, Rootkits, Key Logger, Hijacker, Dialer, Dropper, Loader, Binder und Nuker. Trojaner können den ahnungslosen Benutzer ausspähen, sein Verhalten analysieren, Tastatureingaben mitlesen, ihm bestimmte Informationen aufdrängen, sensible Daten an Dritte weiterleiten und sogar Hintertüren für Hacker öffnen, indem sie den Zugriff von außen auf den Rechner über bestimmte Ports erlauben.

Berüchtigt sind z.B. die so genannten Dialer, die Internetverbindungen über die Telefonleitung aufbauen – und mitunter statt der vom Benutzer vorgesehenen Nummer teure 0900- oder 01900-Nummern anwählen. Einen Dialer erhält man oft durch einen unbedachten Mausklick im Browser. Andere Trojaner tarnen sich, indem sie sich als hilfreiche Zusatzprogramme ausgeben oder sich – wie Rootkits – den Augen des Benutzers überhaupt entziehen.

Adware

Als Adware bezeichnet man Programme, die angeblich nützliche Extrafunktionen bringen und nur mit expliziter Zustimmung des Benutzers installiert werden. Zu dieser Gruppe gehören auch die so genannten „Download-Beschleuniger“ – die tatsächlich Download-Bremsen sind, da sie für Abfragen und Informationen des Werbeträgers einen guten Teil der vorhandenen Bandbreite verbrauchen.

Adware registriert oft die persönlichen Daten und Gewohnheiten des Benutzers und sendet diese an einen zentralen Server. Der Benutzer kann sich dagegen rechtlich kaum zur Wehr setzen – schließlich hat er bei der Installation ausdrücklich der Informationspolitik (*Policy*) des Werbeträgers zugestimmt bzw. wurde informiert, wo er diese im WWW nachlesen kann.

Beispielsweise wird derzeit bei vielen Versionen des *Peer-to-Peer* (P2P)-Programms KaZaa (siehe *Freeware und Shareware*, Seite 13) die Adware Bullguard mitgeliefert: Bullguard ist ein so genannter Data Miner, der unter anderem den Namen des Benutzers, seine eMail-Adresse, Informationen über die auf dem PC installierten Anwendungen sowie Kreditkarteninformationen sammelt und an Tochterfirmen, Geschäftspartner usw. des Herstellers weiterleitet. Dies ist im *End-User License Agreement* von Bullguard explizit angeführt; auf der Webseite von Bullguard erfährt man, dass die Offenlegung der Policy nur zur Information des Benutzers dient und dass dieser keinerlei Anspruch darauf hat, dass

Alarmstufe Rot: Rootkits

Rootkits sind die mächtigsten und tückischsten aller Trojaner: Diese Software-Werkzeuge (*Kits*) verschaffen dem Angreifer alle Rechte des Administrators (unter Unix *Root* genannt) und somit volle Kontrolle über das befallene System. Zusätzlich sind sie in der Lage, ihre Existenz durch gefinkelte Mechanismen nahezu perfekt zu verschleiern. Ein Rootkit ist daher der ultimative Schrecken jedes Systemverantwortlichen.

Während Rootkits in der Unix-Welt schon lange ein Problem darstellen, sind Windows-Rootkits relativ neu: 1999 wurde erstmals gezeigt, dass es technisch möglich ist, in den Betriebssystem-Kern von MS-Windows einen Trojaner einzubauen. Ein Angriff auf dieser Ebene umgeht sämtliche Sicherheitsvorkehrungen des Systems. Windows-Rootkits – die glücklicherweise derzeit noch eher selten anzutreffen sind – verstecken sich gern in DLLs (*Dynamic Link Libraries*) oder tarnen sich als Gerätetreiber. Sie setzen üblicherweise bei den Schnittstellen zwischen Anwendungsprogrammen und Betriebssystem-Kern (*Application Programming Interfaces*, kurz APIs) an und filtern jede Kommunikation zwischen der Anwendung und dem Betriebssystem. An dieser Stelle kann der Angreifer den Datenfluss manipulieren und somit dem ahnungslosen Administrator eine heile Welt vorgaukeln. Auch der Systemleerlauf-Prozess, der immer dann aktiv ist, wenn der Windows-PC nichts zu tun hat, ist ein ideales Versteck für Rootkits: Dadurch, dass der Trojaner nur bei Leerlauf tätig wird, bleiben allfällige Performance-Einbußen aufgrund verborgener Aktivitäten garantiert unbemerkt.

Rootkits bestehen typischerweise aus mehreren Komponenten:

- Die „Hintertür" (*Backdoor*) für den Angreifer sichert diesem uneingeschränkten Zugang zum System – unter Windows als Administrator. Gängige Backdoor-Methoden sind z.B. bestimmte Benutzername-/Kennwort-Kombinationen zur Autorisierung gegenüber einem Service des Systems oder zusätzliche Programme, die dem Angreifer volle Rechte erteilen.
- Die Trojaner-Komponente stellt sicher, dass alle zum Rootkit gehörigen Dateien sowie die anfallenden Daten unsichtbar bleiben. Zu diesem Zweck kann der Trojaner sogar die Systemereignis-Protokolle (*Logfiles*) bzw. den Windows Task-Manager manipulieren. Meistens ist dies jedoch überflüssig: Programme, die der Hacker für seine Schandtaten benötigt, werden normalerweise bei ihrer Ausführung gar nicht erst angezeigt. Der echte Administrator sieht in der Systemanzeige von den verdeckt durchgeführten Aktionen in der Regel nichts – und wenn er zufällig doch einmal einen *Process Identifier* (PID) des Trojaners entdeckt, bleibt jeder Versuch, diese Anwendung zu stoppen, erfolglos.
- Oft sind auch Key Logger oder Packet Sniffer integriert, um weitere Benutzerberechtigungen auszuspähen.
- Zu guter Letzt wird meist noch die ursprüngliche Lücke geschlossen, durch die der Angreifer ins System kam: So kann ihm kein anderer Hacker den übernommenen Rechner streitig machen.

Ist ein Rootkit erst einmal installiert, wird es schwierig. Handelsübliche Virenscanner versagen – sie können nur auf der Programmebene suchen und müssen sich darauf verlassen, dass das Dateisystem ihnen vollen Zugang zu allen Daten gewährt. Ein Scanprogramm für Rootkits muss aber den Betriebssystem-Kern durchsuchen und darf sich auf nichts verlassen: Da ein Rootkit imstande ist, die Ausführung eines Programms auf beliebige andere umzuleiten, kann es sogar die korrekte Ausführung des Scanprogramms unterbinden.

Ein Virenscanner hat gegen ein Rootkit nur dann eine Chance, wenn es ihm gelingt, eine Signatur des Trojaners vor dessen Installation zu erkennen und sein Einnisten zu verhindern. Daher ist der ununterbrochene Betrieb eines Virenscanners mit stets aktueller Virendatenbank die beste Vorbeugungsmaßnahme gegen Windows-Rootkits. Weitere Informationen zu diesem Thema finden Sie unter `http://www.rootkit.com/`.

die Firma sich daran hält. Zur Ehrenrettung von Bullguard sei gesagt, dass dies durchaus branchenüblich ist.

Eine extreme Verbreitung erlebt derzeit die Adware StopSign, die „huckepack" mit mehreren P2P-Programmen mitkommt. StopSign dient als Träger für Werbeeinschaltungen; nebenbei stoppt es verschiedene Security-Programme (Firewalls, Virenscanner) auf dem Rechner des Opfers. Wenn es dazu selbst nicht in der Lage ist, wird der Benutzer aufgefordert, dies zu tun – mit durchaus plausibel klingenden Anfragen: Beispielsweise schlägt die Software vor, das Programm Norton Antivirus temporär abzuschalten, weil ein „Initialisierungskonflikt" bei der Installation von StopSign besteht. StopSign wird beim Starten des Rechners in dessen Arbeitsspeicher geladen und bleibt dadurch selbst nach der Entfernung des Programms noch aktiv. Darüber hinaus ist StopSign ein so genannter Loader, d.h. es lädt, installiert und startet heimlich weitere Programme auf dem PC des Opfers. Installiert der Benutzer bestimmte Personal Firewalls (Sygate, ZoneAlarm) nach StopSign, können die betroffenen PCs nicht mehr starten.

Spyware

Spyware funktioniert ähnlich wie Adware, allerdings mit zwei gravierenden Unterschieden: Zum einen wird der Benutzer über die Präsenz des Trojaners nicht informiert, zum anderen kann dieser auch durch eine Deinstallation der jeweiligen Trägersoftware (z.B. KaZaa) nicht entfernt oder gestoppt werden.

Sehr verbreitet ist beispielsweise Aureate/Radiate – eine Spyware, die mit Freeware-Virenscannern, Bildschirmschonern, Spielen, HTML-Convertern, ZIP-Software, Callcenter-Software usw. „frei Haus" geliefert wird. Aureate informiert seine zentralen Server zunächst über den Benutzer des bespitzelten PCs: Sein Name, seine Internetadresse und eine Liste aller installierten Softwareprodukte werden aus dem PC ausgelesen und weitergeleitet. Anschließend wird den Aureate-Servern über jede Browseraktivität und alle Datei-Downloads berichtet; wenn der Benutzer einen Modemzugang verwendet, werden auch die Telefonnummer des Providers und das Zugangspasswort übermittelt.

Ein häufig anzutreffender Vertreter der Spyware ist auch der BDE Projector, der sich oft als Anhängsel von P2P-Software auf dem Rechner einnistet (z.B. war er Teil älterer KaZaa-Versionen). „Im Interesse des Anwenders", der mit diesem Werkzeug alle Arten von digitalen Medien suchen, erhalten und wiedergeben kann, verfolgt die Software jede Aktion des Benutzers und des Browsers und berichtet darüber einem zentralen Server. Der BDE Projector lädt Updates und andere Programme aus dem Internet, ohne den Benutzer darüber zu informieren. Da er diese Software nur auf dem PC ablegt, ohne sie zu starten, ist er zur Klasse der Dropper zu zählen. Nebst allen anderen Übeln bewirkt der BDE Projector aufgrund seiner engen Verknüpfung mit Grafikbeschleunigern und Musikwiedergabefunktionen im Betriebssystem auch oft Systemabstürze oder starke Performance-Einbußen.

Die „Elite" unter der Spyware ist die so genannte Trickleware: Diese spioniert ebenfalls persönliche Informationen und Gewohnheiten des Anwenders aus, tarnt ihre Präsenz im System aber zusätzlich durch sehr geschicktes Timing der Datenübermittlung an die zentralen Server.

Browser Helper Objects

Browser Helper Objects (BHOs) sind Programme, die innerhalb des Webbrowsers aktiv sind. Dadurch sitzen sie sozusagen „an der Datenquelle" und wissen über jede aufgerufene Webseite Bescheid. Der Erfinder dieser Softwaretechnik ist Microsoft: BHOs sollten ursprünglich dazu dienen, Webseiten mit unerwünschtem Inhalt für Kinder zu sperren.

Ein verbreitetes BHO ist HotBar, das oft bei iMesh beigepackt ist bzw. sich per eMail als vermeintliches Outlook-Update zu verbreiten versucht. HotBar „befällt" sowohl den Internet Explorer als auch MS-Outlook. Der Benutzer wird zwar gefragt, ob er HotBar installieren will; jedoch führt auch eine Ablehnung zu einer teilweisen Installation der Software. Aus dem *SignUp*-Fenster erfährt HotBar neben Name, Telefonnummer, Anschrift, Mailadresse und Geburtstag des Benutzers auch sein Arbeitsgebiet. Der Internet Explorer erhält durch zusätzliche Schaltleisten ein neues Aussehen.

BHOs haben volle Kontrolle über den Browser. Auch ActiveX-Applets, die der Browser – oft vom Benutzer unbemerkt – über eine Webseite lädt, können BHOs sein. Eine besonders bösartige Variante davon sind die so genannten Hijacker: Sie bewirken, dass der Benutzer manche Seiten nicht mehr ansteuern kann, oder sie verbinden ihn stur nur mehr mit einer bestimmten Werbeseite.

Viele Wege führen nach Troja

Neben eMail gibt es heute für Trojaner vor allem drei Verbreitungswege: Sicherheitslücken des Betriebssystems, Freeware- und Shareware-Programme mit „Nebenwirkungen" sowie aktive Web-Inhalte, die durch allzu sorgloses Surfen im Internet auf den Rechner gelangen.

Sicherheitslücken

Sicherheitslöcher in Betriebssystemen entstehen üblicherweise durch mangelnde Sorgfalt des Herstellers; die häufigsten Ursachen sind Designfehler der Software oder Schlampigkeitsfehler im Code – meist bedingt durch die weit verbreitete „Featuritis" (der Zwang, bei jeder Version einer Software einige neue Funktionen anzubieten) und den enormen Zeitdruck in der IT-Branche. Der Programmcode von MS-Windows umfasst mehrere Millionen Zeilen, sodass die Existenz zahlreicher Sicherheitslücken nicht verwunderlich ist.

Eine Sicherheitslücke wird oft durch Zufall gefunden. Glücklicherweise ist es meistens der Softwarehersteller selbst, der bei seinen Weiterentwicklungen den Fehler entdeckt, ihn korrigiert und eine entsprechende Softwarekorrektur (*Secu-*

rity Patch) im Internet zur Verfügung stellt. Spätestens ab diesem Zeitpunkt wissen auch Hacker über die Sicherheitslücke Bescheid; daher ist es extrem wichtig, vorhandene Security Patches umgehend zu installieren (idealerweise mit Hilfe der Funktion *Automatische Updates*; siehe Seite 18).

Als Beispiel für die nachhaltige Verheerung, die Sicherheitslücken auslösen können, sei der MS-Blaster-Wurm genannt, der sich seit August 2003 von Windows-PC zu Windows-PC fortpflanzt, indem er ein bekanntes Sicherheitsproblem ausnutzt. Zwar gab es beim ersten Auftreten des Wurms längst einen entsprechenden Patch von Microsoft; viele Windows-Benutzer hatten diesen jedoch nicht bzw. nur in einer fehlerhaften Version installiert (Microsoft konnte das Problem erst im zweiten Anlauf vollständig beheben). MS-Blaster verbreitete sich entsprechend rasant. Parallel dazu beobachteten zahlreiche Netzwerkadministratoren massive Scans nach einem bestimmten geöffneten Port auf allen Rechnern mit Internetanschluss. Bald war klar: Im Wurm steckte ein *Remote Access Trojan* (RAT), der auf unzähligen infizierten Rechnern einen Administrator-Zugang von außen über Port 4444 öffnete – die Hacker mussten die befallenen Rechner nur noch mittels Portscans ausfindig machen.

Auch der Bugbear-Wurm, der seit Herbst 2002 bekannt ist und sich über eMail und Netzwerkfreigaben (Windows-Shares) verbreitet, ist ein RAT. Via eMail nutzt er eine Sicherheitslücke in MS-Outlook bzw. Outlook Express und wird sofort aktiv, wenn die Nachricht gelesen wird bzw. die Vorschaufunktion aktiviert ist. Der Wurm öffnet ein bestimmtes Port für den Zugang von außen und beendet jede ihm bekannte Antiviren- und Firewall-Software. Zusätzlich installiert er einen so genannten Key Logger (ein Programm, das Passwörter sammelt) und sendet an alle freigegebenen Netzwerkdrucker unsinnige Druckaufträge, sodass es auch zu einer Blockade von Druckern kommen kann. Die Präsenz eines Bugbear-Wurms ist für aufmerksame Benutzer daran erkennbar, dass im Infobereich der Taskleiste ein durchgestrichenes Programmsymbol erscheint (siehe Abb. 1), wenn eine vorhandene Antiviren-Software bzw. Personal Firewall plötzlich gestoppt wird.

Abb. 1: Infobereich mit gestoppter Personal Firewall (Windows XP)

Freeware und Shareware

Während Sicherheitslöcher im Betriebssystem dem Hersteller angekreidet werden können, ist in den meisten anderen Fällen der Benutzer durch sein Verhalten selbst schuld an der Misere. Ein besonders häufiger Fehler ist das oft zu vertrauensselige Installieren (häufig sogar als Administrator!) von unbekannten Freeware- oder Shareware-Programmen. Viele davon sind jedoch nur deshalb so „kostengünstig", weil sich der Entwickler seinen Lohn noch von einer dritten Stelle holt – z.B. indem er dem Produkt Adware oder Spyware beipackt, die dann Werbefirmen gezielt über die Vorlieben des Opfers informiert.

Ein besonders bequemer Ausbreitungsweg für binäres Ungeziefer sind *Peer-to-Peer* (P2P)-Programme, also z.B. Austauschbörsen wie KaZaa oder Morpheus. Damit lässt sich jede Firewall umgehen, die den Benutzer nicht auf ganz wenige Systeme außerhalb der eigenen Organisation einschränkt. P2P-Programme sind das internetweite Analogon zu Netzwerklaufwerken (Windows-Shares): So wie die Verbreitung von Viren über Netzwerklaufwerke eine Gefahr für einzelne vernetzte PCs darstellt, werden P2P-Mechanismen zum weltweiten Träger von Malware aller Art. Die für P2P-Programme freigegebene Festplattenkapazität von Anwender-PCs (die als verteilter Speicher für die auszutauschenden Objekte verwendet wird) ist heute der größte vernetzte Speicherplatz der Welt. Da der Benutzer praktisch keine Kontrolle über die dort abgelegten Daten hat, sammeln sich in diesen Festplattenbereichen alle möglichen Inhalte – Programme oder Dateien mit kriminellem Inhalt können hier genauso verteilt werden wie Musik oder Videos. Der vor kurzem ausgebrochene Wurm MyDoom/Novarg verwendet z.B. auch die Speicherbereiche von KaZaa zur Verbreitung.

Aktive Web-Inhalte

Über das WWW kann man bösartige Software ebenfalls wunderbar verteilen; vor allem Microsofts ActiveX und die berüchtigten (beim Internet Explorer mittlerweile innerhalb des ActiveX-Kontextes laufenden) Java-Applets sind aufgrund ihrer diversen Sicherheitslücken bei Designern von Malware sehr beliebt. Auch der Internet Explorer selbst steht immer wieder wegen Security-Problemen in den Schlagzeilen – eine seiner zuletzt entdeckten Sicherheitslücken ermöglichte es Betreibern einschlägiger Webseiten, Software ohne Rückfrage auf den PCs der Besucher zu installieren und zu starten. Beim Internet Explorer sollte man daher besonders auf dessen Sicherheitseinstellungen achten und diese von Zeit zu Zeit auch verifizieren. Wer sein Risiko reduzieren will, verwendet aber sinnvollerweise einen anderen Browser: Zwar haben auch Netscape, Mozilla, Opera usw. immer wieder Sicherheitsprobleme, aber bei weitem nicht so oft wie der Internet Explorer.

Ein weiterer Risikofaktor sind Sicherheitslöcher in der Webserver-Software, die ebenfalls schon so manchen Wurm (z.B. Code Red, Nimda) möglich gemacht haben. Wenn Sie auf Ihrem Rechner einen Webserver betreiben, sollten Sie daher unbedingt darauf achten, das System im Hinblick auf Security Patches stets aktuell zu halten.

Hilfe – ein Hacker!

Adware und Spyware verfolgen in der Regel hauptsächlich kommerzielle Ziele und richten daher im allgemeinen etwas weniger Schaden an als andere Trojaner (insbesondere Rootkits), die den kriminellen Zwecken von Hackern dienen. Leider ist die Uni Wien für die meisten Hacker durchaus interessant – allerdings weniger wegen ihrer Daten als aufgrund ihres Netzwerkstandorts: Da das Datennetz der Universität über eine relativ hohe internationale Bandbreite

verfügt, kann eine von ihm ausgehende Störaktion im Netz großen Schaden anrichten.

Der Angriffszyklus eines Hackers verläuft dabei fast immer nach demselben Schema:

- Zuerst durchsucht der Hacker mittels so genannter Portscans das Netz nach Rechnern, die offene Ports und damit einen Eingang ins System aufweisen.
- Im nächsten Schritt überprüft er das Betriebssystem der angreifbaren Rechner genauer – und wird bei einem Teil davon zweifellos Angriffspunkte finden.
- Nun bricht er mit einem geeigneten Programm in das System ein. War der Angriff erfolgreich, werden sofort die Spuren vernichtet: Der echte Administrator soll tunlichst keine Möglichkeit zur Rückverfolgung erhalten.
- Im letzten Schritt nistet er sich mittels Trojaner ein und versucht seine Rechte zu halten bzw. auszubauen.
- Von diesem Unterschlupf aus kann er dann wieder von vorne beginnen (Portscans, Schwachstellen identifizieren, Angriff, Einnisten im System) – mit dem zusätzlichen Vorteil, dass die neu dazu gewonnene Ausgangsbasis seine Herkunft verschleiert.

Ungenügend geschützte Systeme stellen daher nicht nur für ihren Besitzer, sondern für alle Internet-BenutzerInnen ein ernsthaftes Risiko dar. Besonders bedenklich ist dabei die Tatsache, dass durch das Internet bösartige Programme aller Art auch in die Hände von Leuten gelangen, die ansonsten von ihrem Wissensstand her gar nicht in der Lage wären, eine vergleichbare Software zu erfinden oder einzusetzen.

Die einzige wirkungsvolle Vorbeugungsmaßnahme besteht aus der (mittlerweile auch von Microsoft aufgegriffenen) Dreier-Kombination aus automatischen Sicherheits-Updates, Virenscanner und Personal Firewall. Extrem wichtig ist diese „Kombi-Abwehr" bei Notebooks, die in verschiedenen Netzwerken verwendet werden und somit ideale Überträger für binäres Ungeziefer aller Art bilden.

Wer suchet, der findet: Trojanerjagd

Für alle: Ad-aware

Das Scanprogramm Ad-aware ist in der Lage, die meisten Trojaner aufzuspüren und auszuschalten. Zu diesem Zweck sucht Ad-aware (im Gegensatz zu Virenscannern) nicht nur in Dateien, sondern auch in der Windows-Systemregistratur (*Registry*) nach problematischen Einträgen. Um Trojanern möglichst wenig Spielraum für Aktivitäten zu geben, muss die Suche regelmäßig durchgeführt werden; angesichts des geringen Zeitaufwands (je nach eingestellter Scan-Genauigkeit etwa eine Minute pro Suchlauf) sollte dies aber kein Problem darstellen.

Ad-aware wird in einer Freeware- und einer kommerziellen Version angeboten. Der Unterschied besteht darin, dass das käufliche Produkt ein Modul namens Ad-watch enthält, das wie ein Virenscanner arbeitet, d.h. Ungeziefer bereits bei seinem Installationsversuch abblockt. Für die Freeware-Version von Ad-aware (die nur vorhandene Trojaner findet) gilt natürlich ebenfalls die oben beschriebene Gefahr unerwünschter Nebenwirkungen. Wir haben Ad-aware 6.0 daher mit allen verfügbaren Mitteln gründlich untersucht. Obwohl keinerlei Auffälligkeiten gefunden werden konnten, bleibt – wie bei jeder Software – ein gewisses Restrisiko, dass das Programm in einer neuen Version neben seinem eigentlichen Aufgabengebiet plötzlich zusätzliche Aktivitäten zeigt.

Die Freeware-Version von Ad-aware ist unter `http://www.lavasoft.de/` (bzw. für Mailbox-BenutzerInnen auch unter `http://swd.univie.ac.at/` als *Gratissoftware*) erhältlich. Für ein wirkungsvolles Eingreifen benötigt Ad-aware analog zu einem Virenscanner nach der Installation (und danach in regelmäßigen Zeitabständen) die jeweils aktuellste Datenbank mit den Signaturen der bekannten Trojaner. Dieses Update wird durch einen Klick auf den Link *Check for updates now* im *Status*-Fenster von Ad-aware durchgeführt (siehe Abb. 2). Bei Verfügbarkeit einer neuen Version der Datenbank muss der Anwender bestätigen, dass er sie downloaden und installieren will, was dann mit wenigen Mausklicks erledigt ist.

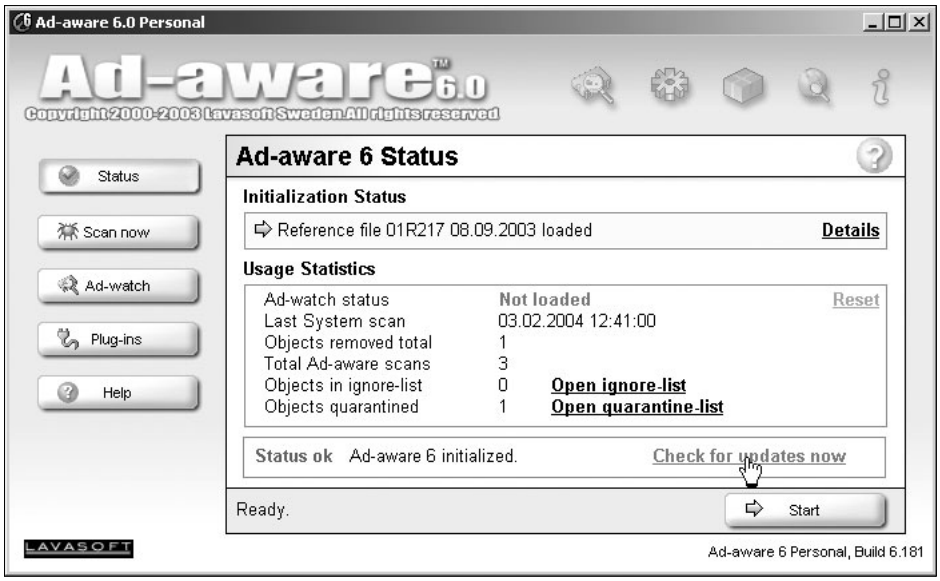

Abb. 2: Ad-aware 6.0 – Fenster *Status*

Der Scan wird durch Anklicken der *Start*-Schaltfläche im *Status*-Fenster in Gang gesetzt. Es erscheint das Fenster *Preparing System Scan*, in

dem Sie den Scan-Modus einstellen können. Die erste, voreingestellte Option *Perform smart system-scan* ist ein durchaus vernünftiger Kompromiss zwischen kurzer Laufzeit und ausreichender Genauigkeit des Scans und kann für den Alltagsgebrauch ruhigen Gewissens verwendet werden. Es empfiehlt sich aber, mindestens einmal wöchentlich einen kompletten Scan über alle Laufwerke vorzunehmen. Wählen Sie dazu im Fenster *Preparing System Scan* die Option *Select drives/folders to scan* und definieren Sie die zu scannenden Laufwerke durch einen Klick in das entsprechende Kontrollkästchen.

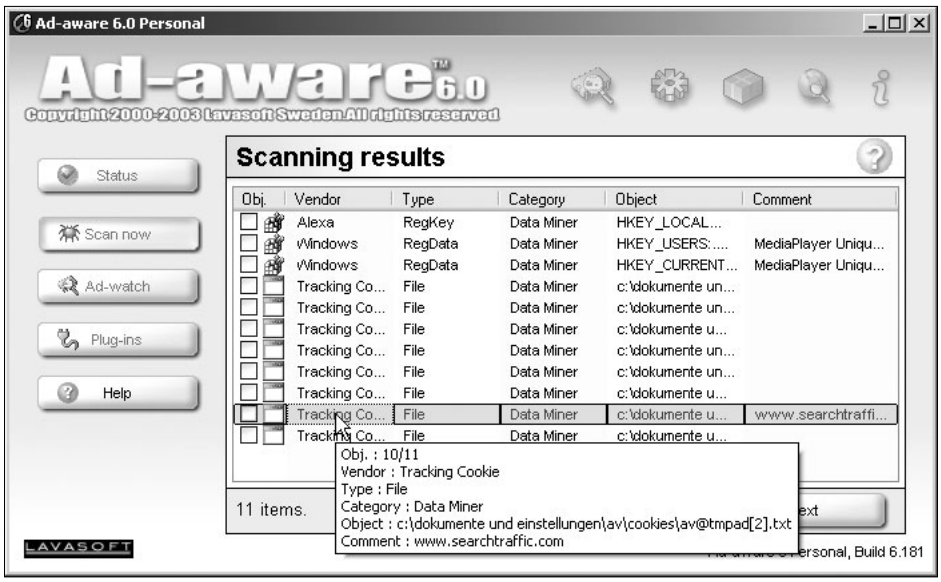

Abb. 3: Ad-aware 6.0 – Fenster *Scanning results*

Der Suchvorgang selbst verläuft wie bei einem herkömmlichen Virenscanner. Ist er abgeschlossen, erhält man eine kurze Zusammenfassung der Ergebnisse; anschließend sollte man sich durch einen Klick auf die Schaltfläche *Show Logfile* (links unten im Ergebnis-Fenster) die Treffer etwas genauer ansehen.

Das Logfile zeigt zuerst jedes im System derzeit laufende Programm (jeden aktiven Prozess) unter Angabe seiner Herkunft, sodass sich Programme unklarer Herkunft identifizieren lassen. Anschließend werden alle Objekte angeführt, die der Klasse des binären Ungeziefers angehören. Durch einen Klick auf die Schaltfläche *Next* werden in einer kurzen Zusammenfassung alle „verdächtigen" Systemeinträge angezeigt (siehe Abb. 3). Aktivieren Sie das Kontrollkästchen ganz links, um ein Objekt für das Entfernen durch Ad-aware freizugeben.

Drei Objekte, die von Microsoft selbst stammen, finden sich auf fast jedem Windows-Rechner: Der Alexa Data Miner (Spyware) ist für die *What's Related*-Links des Internet Explorer verantwortlich. Alexa verfolgt Ihre Gewohnheiten beim Surfen im Netz, um Ihnen Links anzeigen zu können, die Sie vermutlich interessieren. Ein weiterer „MS-Trojaner" ist der MediaPlayer (2 Objekte), der Microsoft über die von Ihnen wiedergegebenen Stücke informiert. Im Sinne Ihrer Privatsphäre ist es sinnvoll, Alexa und den MediaPlayer von Ad-aware stoppen zu lassen.

Achtung: Wenn auf Ihrem PC eine Personal Firewall läuft, müssen Sie für die Update-Funktion der Datenbank den ausgehenden Datenverkehr auf den Rechner `66.117.38.101` (Zielport `80`) für das Programm Ad-aware freigeben.

Für Profis: Selber suchen

Wer es sich zutraut, kann natürlich auch eigenhändig sein System nach verdächtigen Einträgen durchforsten. Für diesen Zweck ist es hilfreich, wenn man unmittelbar nach der Neuinstallation von MS-Windows und der vorgesehenen Anwendungsprogramme (z.B. MS-Office) eine Kopie der Windows-Registry anfertigt und außerhalb des Systems auf einer CD oder Diskette speichert: Sofern man über die nötige Geduld und Sachkenntnis verfügt, hat man damit jederzeit die Möglichkeit, neue oder modifizierte Registry-Einträge zu finden. Unter Windows 2000 und Windows XP wird die Registry mit dem Programm regedit aufgerufen. Beliebte Verstecke für Trojaner sind vor allem die systemrelevanten Einträge (beginnend mit `HKEY_LOCAL_MACHINE`, `HKEY_CURRENT_CONFIG` und `HKEY_CLASSES_ROOT`) und die benutzerrelevanten Einträge (beginnend mit `HKEY_CURRENT_USER` und `HKEY_USERS`). Eine Liste von Einträgen, die für einen Vergleich mit einer gesicherten Registry besonders empfehlenswert sind, finden Sie unter `http://www.univie.ac.at/ZID/security.html`.

Zusätzlich verbergen sich Trojaner gern in Dateien, die nur beim Systemstart (und auch da oft nur nach der Installation neuer Software) ausgeführt werden – z.B. `c:\windows\winstart.bat` und `c:\windows\wininit.ini`. Einen Überblick über die beim Systemstart ausgeführten Programme erhält man bei Windows XP (als Administrator!) unter *Start – Ausführen*: Tippen Sie hier `msconfig` ein und wählen Sie die Registerkarte *Systemstart*.

Ein modernes Rootkit wird man auf allen diesen Wegen jedoch vergeblich suchen, da es selbstverständlich alle benötigten Registry- und Dateieinträge ausblendet. Bei Rootkits kann es manchmal hilfreich sein, die Festplatte des Betriebssystems über ein Netzwerklaufwerk (Windows-Share) einem anderen Rechner zur Verfügung zu stellen und sich von dort aus umzusehen. Aber Achtung: Schalten Sie zuvor die Miniaturansichten des Systems aus (siehe *Goldene Regeln – Systemkonfiguration – Punkt 2* auf Seite 16) – Sie könnten sonst aus Versehen den Trojaner aktivieren, indem Sie auf ein vermeintliches Dokument-Symbol klicken!

Aron Vrtala ■

Goldene Regeln
für ein intaktes (Windows-)Betriebssystem

In einer Stadt mit bekannt hoher Kriminalität sind Sie sicherlich sehr vorsichtig. Im Internet gilt dies um so mehr: Hier sind Sie mit der ganzen Welt verbunden – vertrauen Sie auf nichts und niemanden! Beherzigen Sie die folgenden Tipps (deren Einhaltung garantiert weniger Mühe macht als einen gekaperten Rechner zurückzuerobern) und halten Sie nicht nur Ihr System, sondern auch sich selbst auf dem Laufenden. Die wichtigsten Querverweise zu aktuellen Sicherheitsinformationen finden Sie unter `http://www.univie.ac.at/ZID/security.html`.

Hygiene

1) Aktivieren Sie für MS-Windows unbedingt die Funktion *Automatische Updates*, die sicherheits- und betriebstechnisch wichtige Komponenten des Systems selbständig aktualisiert (siehe dazu Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* auf Seite 18).

2) Installieren Sie einen Virenscanner und einen Trojanerscanner und halten Sie diese immer aktuell (siehe Artikel *McAfee VirusScan: Ihr Goalkeeper im Einsatz gegen virale Offensiven* auf Seite 21).

3) Wiegen Sie sich nicht durch eine vorhandene Institutsfirewall in scheinbarer Sicherheit: Immer wieder gelingt es Hackern, sich durch eine Firewall zu schwindeln; dahinter sind die Angriffsziele oft zahlreich. Installieren Sie daher eine Personal Firewall auf Ihrem Rechner und konfigurieren Sie diese nach Ihren Bedürfnissen: Sperren Sie nicht benötigte (Server-)Dienste, und schränken Sie benötigte Dienste auf den vorgesehenen Benutzerkreis ein.

4) Verwenden Sie immer sichere Passwörter – z.B. die Anfangsbuchstaben eines geheimen Satzes, kombiniert mit Zahlen. Ein solches Passwort lässt sich leicht merken und ist in keinem der elektronischen Wörterbücher zu finden, die von Password Crackern zum Dechiffrieren benutzt werden. Setzen Sie auch einen Bildschirmschoner mit Passwort ein.

5) Denken Sie daran: Der größte Feind eines Rechners sitzt oft vor dessen Tastatur!

Internet

1) Seien Sie beim Bearbeiten von eMail misstrauisch, besonders bei Nachrichten mit Attachments. Sie können davon ausgehen, dass kein einigermaßen seriöses Unternehmen (weder Microsoft noch Hersteller von Virenscannern) Updates oder andere Software per eMail verschickt. Öffnen Sie keine Attachments, die Sie nicht erwartet haben, und bedenken Sie, dass die Mailadresse des Absenders gefälscht sein könnte.

2) Deaktivieren Sie unbedingt die Vorschaufunktion Ihres Mailprogramms – eventuell in einer Nachricht versteckte ausführbare Programme werden sonst automatisch gestartet.

3) Beim Surfen im WWW gilt: Erst nachdenken, dann klicken! So mancher Trojaner kam schon durch ein zu eiliges *OK* ins System.

4) Verwenden Sie nach Möglichkeit verschlüsselte Übertragungsprotokolle: Ersetzen Sie Telnet durch SSH, FTP durch SCP/SFTP und HTTP durch HTTPS. Autorisieren Sie sich im Web nur über HTTPS!

5) Beziehen Sie Free- und Shareware nur von vertrauenswürdigen Quellen (z.B. `http://tucows.univie.ac.at/`) und verzichten Sie auf P2P-Programme – zumindest auf Institutsrechnern und auf Notebooks, die Sie in verschiedenen Netzwerken einsetzen.

Systemkonfiguration

1) Wer stets als Administrator (also mit allen Privilegien) arbeitet, muss bei jedem Mausklick in seinem Webbrowser damit rechnen, dass er durch ein bösartiges ActiveX-Applet die Funktionen seines Rechners gefährdet. Unter Windows 95/98/ME hat man leider keine andere Wahl; unter Windows 2000 und Windows XP kann und soll jedoch ein Einzelnutzer-Betrieb als Administrator vermieden werden.

2) Eine beliebte Aktivierungsmethode für Trojaner sind die standardmäßig leider eingeschalteten Miniaturansichten – das ist jenes Feature, das kleine Abbilder von Grafiken oder Dokumenten erzeugt und diese im Windows Explorer anzeigt. Bei jedem Klick darauf (auch wenn man das Objekt nur zum Löschen markieren möchte!) wird ein allfälliger verborgener Autostart-Trojaner sofort in Gang gesetzt. Unter Windows XP schalten Sie diese Funktion wie folgt aus: Klicken Sie auf ***Arbeitsplatz*** – ***Extras*** – ***Ordneroptionen*** – Registerkarte ***Ansicht*** und entfernen Sie das Häkchen vor der Option *Einfache Ordneransicht in der Ordnerliste des Explorers anzeigen* (siehe Abb. 1). Soll diese Maßnahme die gewünschte Wirkung zeigen, muss zusätzlich die *Details*-Anzeige in der linken Leiste des Windows Explorer geschlossen

sein (d.h. die Pfeile neben *Details* müssen nach unten zeigen; klicken Sie andernfalls auf die Pfeile, um die *Details*-Anzeige zu schließen)!

In der Liste *Ordneroptionen – Ansicht* sollten Sie zusätzlich auch die nächste Option unbedingt deaktivieren (*Erweiterungen bei bekannten Dateitypen ausblenden*; siehe Abb. 1): Manche vermeintliche Grafik wird dann an ihrer zusätzlichen Dateierweiterung als ausführbares Programm erkennbar.

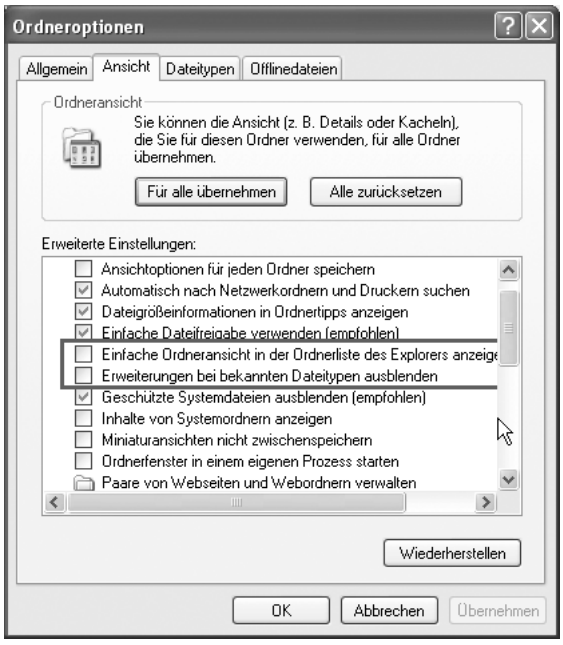

Abb. 1: Windows XP – Fenster *Ordneroptionen*

3) Wenn Sie einen neuen Rechner in Betrieb nehmen, denken Sie über dessen Sicherheitsanforderungen (und die seiner Umgebung!) nach und berücksichtigen Sie das Prinzip der kleinsten benötigten Privilegien. Dies gilt insbesondere auch für Netzwerklaufwerke (Windows-Shares) – öffnen Sie diese nur für Personen, die wirklich auf Ihre Daten zugreifen müssen.

4) Unter Windows NT, 2000, XP und 2003 Server sollten Sie unbedingt NTFS-Dateisysteme einsetzen. Das alte, noch aus DOS-Zeiten stammende FAT- oder FAT32-Dateisystem bietet auf dieser Ebene keinen Schutz vor Fremdzugriff.

5) Erstellen Sie eine Checkliste für die Neuinstallation des Rechners, das hilft in Krisensituationen. Legen Sie diese Checkliste außerhalb des Systems ab!

Weitere nützliche Tipps zum Thema Systemsicherheit finden Sie unter `http://www.univie.ac.at/ZID/security.html` (klicken Sie auf *Vorträge – Vorlesung – Goldene Regeln*).

Aron Vrtala ■

Neue Standardsoftware

Neue Produkte (Stand: 1. 3. 2004)

- Adobe After Effects 6.0 für Win. und Mac
- Adobe GoLive 7 CS für Win. und Mac
- Adobe Illustrator 11 CS für Win. und Mac
- Adobe InDesign 3 CS für Win. und Mac
- Adobe Photoshop 8 CS für Win. und Mac
- Apple MacOS X 10.3
- Corel Designer 10 für Win.
- Corel Painter 8 für Win. und Mac
- Corel Ventura 10 für Win.
- Macromedia Dreamweaver MX 2004 für Win. und Mac
- Macromedia Fireworks MX 2004 für Win. und Mac
- Macromedia Flash MX 2004 für Win. und Mac
- MS-Entourage für Mac
- MS-Frontpage 2003 für Win.
- MS-MapPoint 2004 Euro und US für Win.
- MS-Office 2003 Professional für Win. (Access, Excel, InfoPath, Outlook, PowerPoint, Publisher, Word)
- MS-Office 2003 Standard für Win. (Excel, Outlook, PowerPoint, Word)
- MS-OneNote 2003 für Win.
- MS-Project 2003 Standard und Professional für Win.
- MS-Virtual PC 2004 für Win.
- MS-Visio Standard und Professional 2003 für Win.
- ScanSoft OmniPage Pro 13.0 für Win.
- ScanSoft PaperPort Deluxe 9.0 für Win.
- Sun StarOffice 7 für Win., Linux, Solaris (Lizenz gratis!)
- Symantec pcAnywhere 11.0 für Win.

Updates (Stand: 1. 3. 2004)

- Exceed 9.0 für Win. (bisher 8.0)
- SPSS 12 (bisher 11.5)

Borland-Lizenzen aufgelassen

Wegen geänderter Lizenzbedingungen, äußerst schleppender Lieferungen und sehr schwacher Nachfrage mussten die Softwareprodukte von Borland aus dem Campuslizenz-Programm genommen werden. Bitte kaufen Sie bei Bedarf die Borland-Schulversionen im Fachhandel.

Peter Wienerroither ■

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

Achtung: Änderungen bei Software-Bestellungen für die Med-Uni (siehe Seite 2)!

Department of Desktop Security: **RED ALERT BEI WINDOWS-BETRIEBSSYSTEMEN**

Hacker, Viren, Würmer, trojanische Pferde – das Spektrum möglicher Bedrohungsszenarien ist in der global vernetzten IT-Welt während der letzten Dekade kräftig angewachsen. Um den vielfältigen Herausforderungen zu begegnen und einigermaßen befriedigende Sicherheitskonstruktionen für Rechner und Netzwerke zu schaffen, bemühen sich IT-Security-Experten, gefährdete Bereiche zu analysieren und mögliche Angriffspunkte aufzuspüren. Auch gängige Betriebssysteme weisen – nicht zuletzt aufgrund immer kürzerer Entwicklungszyklen – mehr oder minder gravierende Sicherheitslecks auf. Verursacher sind hier Programmierfehler, welche allzu oft erst in der allgemeinen Anwendungsphase erkannt werden. Möchte der Benutzer diese im Nachhinein beheben, ist er in der Regel davon abhängig, ob und wie bald der Hersteller entsprechende Programmkorrekturen – in Form von so genannten *Patches* („Flicken") – bereitstellt.

In letzter Zeit hat insbesondere das erfolgsverwöhnte Unternehmen Microsoft einen nicht abreißen wollenden Strom an Negativschlagzeilen in der einschlägigen Fachpresse erzeugt: Immer wieder wird von neuen, als „kritisch" eingestuften Sicherheitslücken in Windows-Betriebssystemen berichtet, die unverzüglich durch die Installation der entsprechenden Sicherheits-Updates behoben werden sollten. Wird dies verabsäumt und lernen potentielle Angreifer erst derlei Schwachstellen zu nutzen, stellen sie eine durchaus ernst zu nehmende Gefahr für die Sicherheit ungeschützt betriebener Rechner dar.

Von Seiten Microsofts wird in diesem Zusammenhang gerne darauf hingewiesen, dass es in vielen Fällen bereits effiziente Lösungen gäbe, die den Kunden auch kostenlos zur Verfügung gestellt würden. Nicht das mangelnde Vorhandensein eines Schutzes stelle das eigentliche Problem dar, sondern vielmehr die mangelnde Bereitschaft der Anwender, diesen – in Form der erforderlichen Security Patches – rechtzeitig zu installieren.

Aus Sicht der BenutzerInnen präsentiert sich dies freilich aus einer anderen Perspektive. Das hierfür notwendige regelmäßige „Einspielen" (d.h. das Herunterladen und Installieren) von neuen Patches wird auf Dauer als eine lästige Angelegenheit wahrgenommen. Zudem stößt es vielen sauer auf, durch derartige „Nachbesserungsarbeiten" noch stärker in ein Abhängigkeitsverhältnis zu dem Softwaregiganten zu geraten.

Allen Bedenken zum Trotz: Solange der Erwerb eines hochprozentig sicheren Betriebssystems der Kategorie „visionäres Wunschdenken" zuzuordnen ist, lässt sich bei nüchterner Abwägung der möglichen Risiken nur eine Empfehlung geben: *Take What You Can Get*. Oder besser:

Flicken was das Zeug hält

Um den Aufwand des regelmäßigen Updatens zu minimieren und sicherzustellen, dass zumindest die wichtigsten Security Patches (von Microsoft als *Hotfixes* bezeichnet) rechtzeitig installiert werden, empfiehlt es sich, das lokale Windows-Update-Dienstprogramm *Automatische Updates* zu nutzen. Es wird von den aktuelleren Windows-Versionen Windows XP, Windows 2000 mit Service Pack 3 (SP3) oder höher, Windows ME sowie Windows Server 2003 unterstützt.[1)]

Im Gegensatz zum manuellen Updaten, dem zunächst eine mehr oder minder lange Orientierungs- und Auswahlphase auf den Webseiten von Microsoft vorausgeht, ist das Funktionsprinzip von *Automatische Updates* effizient und benutzerfreundlich: Sobald Sie mit dem Internet verbunden sind, begibt sich *Automatische Updates* auf die Suche nach neuen wichtigen Aktualisierungen für Ihr System. Wird es dabei fündig, orientiert sich seine weitere Vorgehensweise an den von Ihnen gewählten Einstellungen: Entweder informiert es Sie, dass neue, wichtige Updates verfügbar sind und fragt nach, ob diese jetzt heruntergeladen werden sollen, oder es lädt die Patches automatisch im Hintergrund herunter. Sie können währenddessen ungestört an Ihrem Rechner weiterarbeiten.

Nach Beendigung des Downloads erhalten Sie eine Verständigung, dass jetzt neue Updates installiert werden können. Von hier aus trennen Sie nur mehr ein paar Mausklicks und gegebenenfalls ein Neustart Ihres Rechners von der erfolgreichen Behebung einer Reihe von Sicherheitslecks in Ihrem Windows-Betriebssystem.

Das Dienstprogramm *Automatische Updates* unter Windows XP

Eine detaillierte Beschreibung, wie Sie unter Windows XP *Automatische Updates* einrichten und Security Patches korrekt installieren, entnehmen Sie bitte der folgenden Anleitung (wie Sie die Konfiguration unter Windows 2000 vornehmen, können Sie unter `http://www.ap.univie.ac.at/security/minimum_win2k.html` nachlesen). Beachten Sie: Zum Ändern der Einstellungen unter *Automatische*

1) Für die älteren Betriebssysteme Windows 95, Windows 98 und Windows NT stehen Systemupdates von Microsoft nicht mehr bzw. nur mehr in seltenen Ausnahmefällen zur Verfügung. Da die Sicherheit des Systems demnach nicht mehr garantiert werden kann, ist es hier angeraten – sofern irgend möglich – ein Systemupgrade auf Windows XP durchzuführen.

2) Falls Sie in der Systemsteuerung die „klassische Ansicht" voreingestellt haben, überspringen Sie den Punkt *Leistung und Wartung*.

Updates müssen Sie als Administrator oder als Mitglied der Gruppe Administratoren angemeldet sein.

Wählen Sie ***Start – (Einstellungen –) Systemsteuerung – Leistung und Wartung***[2] ***– System***. Mit einem Doppelklick auf *System* öffnen Sie das Fenster *Systemeigenschaften*. Wechseln Sie hier mit einem Klick zur Registerkarte ***Automatische Updates*** (siehe Abb. 1).

Befindet sich ein Häkchen in dem Kästchen neben dem Text ***Den Computer auf dem neuesten Stand halten (Durch Aktivieren dieser Einstellung kann Windows Update-Software automatisch vor dem Anwenden anderer Updates aktualisiert werden.)***, so ist dieser Dienst aktiviert. Sollte dies nicht der Fall sein, aktivieren Sie ihn, indem Sie auf das Kästchen klicken.

Ein Stück weiter unten auf der Registerkarte können Sie unter *Einstellungen* festlegen, welche Vorgangsweise Sie für den automatischen Download und die anschließende Installation wünschen (vgl. Abb. 1). Bei Auswahl der Option 1 werden Sie zweimal benachrichtigt – vor dem Download der Updates und vor deren Installation. Option 2 (üblicherweise voreingestellt) informiert Sie erst, sobald Updates zur Installation bereitstehen. Option 3 (nur Windows XP Professional) ermöglicht es Ihnen, die automatisch heruntergeladenen Updates anhand eines Zeitplanes zu installieren.

Stellen Sie die Konfiguration wie folgt ein: ***Updates automatisch downloaden und über installierbare Updates benachrichtigen*** – oder konfigurieren Sie ein automatisches Downloaden von Updates und lassen Sie das System diese *laut angegebenen Zeitplan installieren*. Wenn Ihr System ohnehin in der Nacht durchläuft, wäre dies die optimale Lösung. Wählen Sie dann *Täglich* und lassen Sie die Installation z.B. um *02:00* Uhr in der Nacht durchführen.

Für den Fall des händischen Startens der Installation müssen Sie sich als Administrator anmelden. Sobald neue Softwarekorrekturen verfügbar sind, erscheint rechts unten in Ihrer Taskleiste eine Sprechblase mit dem Text *Neue Updates können jetzt installiert werden* (siehe Abb. 2). Diese Information erlischt nach kurzer Zeit. Sie können später das Vorhandensein von Updates anhand des (in Abb. 3 ganz links sichtbaren) kleinen Windows-Symbols im Infobereich Ihrer Taskleiste erkennen.

Wenn Sie die Installation starten wollen, doppelklicken Sie auf das Symbol. Es erscheint das Fenster *Automatische Updates – Installationsbereit* (siehe Abb. 4). Unter ***Details*** können Sie eine Liste der empfohlenen Updates einsehen.

Bestätigen Sie dann mit ***Installieren***, um die Installation auszuführen. Für einige Updates ist es möglicherweise erforderlich, Ihren Computer erneut zu starten, um die Installation abzuschließen. Führen Sie in diesem Fall unbedingt einen Neustart durch, da sonst die Korrekturen nicht wirksam werden können!

Ein Tipp zum Abschluss: Sollten Sie sich entschließen, ein bestimmtes heruntergeladenes Update nicht zu installieren,

Abb. 2:
Infobereich von Windows XP – Benachrichtigung über neue Updates

Abb. 3:
Das Symbol ganz links im Infobereich der Windows-Taskleiste zeigt an, dass neue Updates installationsbereit sind.

Abb. 1: Fenster *Systemeigenschaften – Automatische Updates*

Abb. 4: Fenster *Automatische Updates – Installationsbereit*

löscht Windows die zugehörigen Dateien von Ihrem Computer. Falls Sie Ihre Meinung später ändern, ist es relativ einfach möglich, diese Updates erneut herunterzuladen: Unter ***Start – (Einstellungen –) Systemsteuerung – Leistung und Wartung***[2] – ***System*** – Registerkarte ***Automatische Updates*** finden Sie rechts unten die Schaltfläche ***Abgelehnte Updates***. Klicken Sie darauf, um einen wiederholten Download zu initiieren. Wenn die zuvor abgelehnten Updates weiterhin für den Computer geeignet sind, werden sie angezeigt, sobald Sie das System das nächste Mal über verfügbare Updates informiert.

Michaela Bociurko ■

SICHERHEIT VON ANFANG AN

Windows XP mit Firewall-Schutz installieren

Antivirenprogramme und Personal Firewalls sind eine feine Sache – sobald sie einsatzbereit sind. Wenn man aber einen neuen Rechner erstmals an das Netzwerk anschließt, um einen Virenscanner bzw. eine Firewall herunterzuladen und zu installieren, ist der Rechner bis zur Inbetriebnahme dieser Programme ungeschützt. Falls er sich in einem verseuchten Netz befindet, ist er mit hoher Wahrscheinlichkeit dann auch bereits mit Viren und/oder Trojanern infiziert. Bei Windows XP lässt sich diese gefährliche Lücke mit Hilfe der integrierten Firewall (die standardmäßig jedoch deaktiviert ist) schließen.

Hinweis: Eine gesicherte Installation von Windows 2000 verläuft fast genau so wie hier für Windows XP beschrieben – nur bei Punkt 3 sollte eine Personal Firewall von einer CD aus installiert und mit einem „allgemeinen Eintrittsverbot" konfiguriert werden. Nach der Installation der Windows-Updates und des Virenscanners kann man die Konfiguration der Firewall bei Bedarf wieder lockern.

Die folgende Anleitung geht von einem Gerät mit bereits installierter Netzwerkkarte und noch zu installierendem Betriebssystem aus; das Netzwerkkabel ist **nicht** angesteckt. Da sich diverse Schädlinge auch sehr gerne – und in unserem Szenario vom Benutzer leider völlig unbemerkt – über Funk-LANs ausbreiten, muss ein integrierter WLAN-Adapter gegebenenfalls zuerst im BIOS des Rechners deaktiviert werden. Vorsicht: Änderungen an den BIOS-Einstellungen sind eine heikle Angelegenheit und sollten nur von erfahrenen BenutzerInnen mit guten Fachkenntnissen vorgenommen werden!

1. Installieren Sie Windows XP von der CD. Die folgenden Schritte müssen Sie als Administrator durchführen.

2. Konfigurieren Sie die Netzwerkkarte über ***Start – (Einstellungen –) Systemsteuerung – Netzwerkverbindungen*** – Klick mit der **rechten** Maustaste auf ***LAN-Verbindung*** (bei mehreren Netzwerkkarten sind eventuell mehrere LAN-Verbindungen vorhanden) – ***Eigenschaften***. Im Fenster *Eigenschaften von LAN-Verbindung* wählen Sie auf der Registerkarte ***Allgemein*** den Punkt ***Internetprotokoll (TCP/IP)*** und geben dort die erforderlichen Einstellungen an.

3. Klicken Sie nun im Fenster *Eigenschaften von LAN-Verbindung* auf die Registerkarte ***Erweitert*** und aktivieren Sie hier die integrierte Firewall von Windows XP (das Kästchen muss angehakt sein; siehe Abb. 1). Schließen Sie das Fenster durch Klick auf ***OK***.

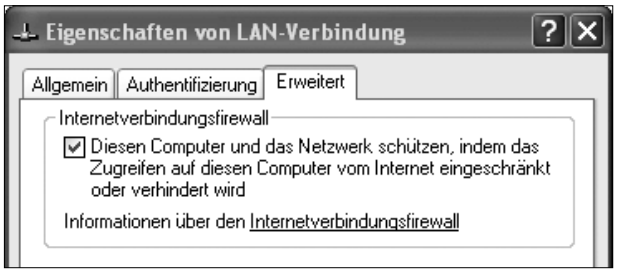

Abb. 1: Fenster *Eigenschaften von LAN-Verbindung* – Internetverbindungsfirewall ist aktiviert

4. Stecken Sie das Netzwerkkabel an.

5. Unmittelbar danach müssen Sie über ***Start – (Einstellungen –) Systemsteuerung – System*** – Registerkarte ***Automatische Updates*** die aktuellen Windows-Updates einspielen (siehe dazu auch Artikel *Department of Desktop Security: Red Alert bei Windows-Betriebssystemen* auf Seite 18).

6. Anschließend installieren Sie den gewünschten Virenscanner und führen sofort ein Update der Virendatenbank durch (siehe dazu auch den Artikel *McAfee VirusScan – Ihr Goalkeeper im Einsatz gegen virale Offensiven* auf Seite 21).

7. Nun können Sie gegebenenfalls weitere Netzwerkadapter (z.B. WLAN) aktivieren. Schützen Sie diese ebenfalls – wie oben beschrieben – über die XP-Firewall.

8. Die weitere Installation verläuft wie gewohnt: Benutzer einrichten, Anwendungssoftware installieren usw. Wenn gewünscht, können Sie jetzt auch eine andere Personal Firewall installieren und einrichten. Die XP-Firewall sollten Sie in diesem Fall nach der Installation der neuen Firewall wieder deaktivieren.

Aron Vrtala ■

McAfee VirusScan

Ihr Goalkeeper im Einsatz gegen virale Offensiven

Die gegnerische Offensive prescht vor, doch kein Verteidiger, kein Schlussmann in Sicht! Der Angreifer kickt in Richtung des unbewachten Tores – die Menge brüllt: TOR! TOR! TOR!

Wäre dieses Szenario wirklich denkbar? Jene, welche dem runden Leder zugetan sind, schütteln jetzt wohl nur verständnislos den Kopf. Dennoch verhalten sich einige EDV-AnwenderInnen durchaus vergleichbar, wenn sie auf den Einsatz effektiver Antivirensoftware verzichten: Ihr Rechner verbleibt ungeschützt gegen jegliche virale Offensive. Was im Sport schlimmstenfalls eine Niederlage herbeiführt, kann jedoch für Ihren Rechner fatale Auswirkungen haben. Hat ein Virus erst einmal „erfolgreich" zugeschlagen, sind Arbeitsaufwand, Datenverlust und – nicht zuletzt – meist beträchtliche Kosten die unweigerlichen Folgen. Für infizierte Notebooks sind noch weitreichendere Konsequenzen denkbar, da diese Geräte aufgrund ihrer Mobilität ein deutlich höheres Risikopotential darstellen. Infektionen können hiermit von einem Netzwerk in ein anderes übertragen werden und in der Folge beispielsweise alle Rechner eines Betriebs verseuchen.

Um Sie vor derartigen Geschehnissen zu bewahren, haben wir Ihnen den folgenden kleinen Crashkurs zusammengestellt, der Ihnen – als frisch gebackenem Manager, Trainer und Präsidenten in einer Person – Schritt für Schritt helfen soll, eine schlagkräftige Verteidigung für Ihren Rechner aufzubauen.

Punkt 1: Kaderauswahl

Selektion einer geeigneten Antivirensoftware

Der Entschluss, eine effektive Abwehr für Ihren Rechner aufzustellen, ist gefällt. Nun drängt sich die Frage auf, wen Sie mit der anspruchsvollen Position des Torwächters betrauen möchten.

Grundsätzlich wird am Softwaremarkt eine breite Palette von Antivirenprogrammen angeboten. Da die Uni Wien für den Virenscanner von McAfee eine Campuslizenz besitzt, steht dieser allen Uni-MitarbeiterInnen kostenlos zur Verfügung. Voraussetzung für den Download vom SWD-Server der Universität Wien ist in jedem Fall eine gültige Mailbox-UserID.

Derzeit sind zwei Versionen in Gebrauch: McAfee VirusScan Enterprise 7.x und die Version 4.5.x.

- McAfee VirusScan Enterprise 7.x ist die aktuellere Version und weist einige neue, durchaus brauchbare Features auf. Betriebssystemvoraussetzung ist für diese Version Windows NT 4.0 (SP6 oder höher), Windows 2000 Professional oder Windows XP.

- Sollten Sie einen Rechner mit Windows 95, 98 bzw. ME-Betriebssystem verwenden, installieren Sie bitte die Version 4.5.x.

Beachten Sie, dass sich die detaillierten Anleitungen in diesem Artikel auf die neuere Version Enterprise 7.x beziehen. Die beiden Versionen sind in Prinzip und Funktionsumfang zwar weitgehend ident, jedoch können diverse Darstellungen bei der Version 4.5.x etwas abweichen.

Download und Installation

1. Rufen Sie in Ihrem Browser den URL **`http://swd.univie.ac.at/`** auf, klicken Sie auf ***Weiter*** und identifizieren Sie sich anhand Ihrer Mailbox-UserID und Ihres Mailbox-Passworts.

2. Sie erhalten eine Liste aller für Sie verfügbaren Softwareprodukte. Klicken Sie ganz oben in der Liste auf ***Gratissoftware*** und auf der folgenden Seite auf ***McAfee Virenscanner***.

3. Sie finden dort einen Link ***zum Server von NAI*** (Network Associates International, der Herstellerfirma von McAfee) und genaue Informationen für den Download des Virenscanners.

4. Nachdem die komprimierte `.zip`-Datei auf Ihren Rechner übertragen wurde, muss sie entpackt werden. Falls Sie dafür keine geeignete Software installiert haben, müssen Sie noch unter ***Gratissoftware – WinZip*** die Datei ***winzip81.exe*** (für Windows 95/98/ME/NT/2000/XP, Englisch) auf Ihren Rechner übertragen. Führen Sie die `.exe`-Datei anschließend durch einen Doppelklick aus, wählen Sie ein Verzeichnis zum Entpacken und installieren Sie dort das Programm durch einen Doppelklick auf die Datei ***setup.exe***.

5. Entpacken Sie nun die `.zip`-Datei durch einen Doppelklick und installieren Sie das Antivirenprogramm durch einen Doppelklick auf ***setup.exe***. Dabei können Sie getrost die Standardvorgaben verwenden; die Installation selbst geht automatisch vor sich.

6. Da die Uni Wien nur über eine begrenzte Anzahl von Lizenzen für McAfee bzw. WinZip verfügt, bitten wir Sie, die Verwendung der Programme per eMail bekannt zu geben (*To*: `peter.wienerroither@univie.ac.at`; *Subject*: McAfee-Registrierung bzw. WinZip-Registrierung; *Inhalt*: Name, Institut, Tel., Anzahl der Lizenzen).

Punkt 2: Training

Halten Sie Ihre Defensive up-to-date

Der Gegner schläft nicht. Täglich ersinnt er neue Taktiken, Ihren Torhüter auszuspielen. Verhindern können Sie dies nur, indem Sie ihn für die jeweils aktuellen Herausforderungen fit erhalten. Zu diesem Zweck sind Updates vorgesehen. Sie sind das unbedingt notwendige, regelmäßige „Training" Ihres „Spielers": Der Virenscanner ist mit einer internen Virendatenbank ausgestattet, in welcher Signaturen von bereits bekannten Viren enthalten sind. Werden während eines Scanprozesses verdächtige Codes entdeckt, vergleicht der Virenscanner seine Untersuchungsergebnisse mit dem Inhalt seiner Datenbank und kann so mutmaßliche Viren einwandfrei identifizieren. Da täglich neue Viren auftauchen, muss dieser Erkenntnisstand regelmäßig aufgefrischt werden. Ohne die aktualisierten Dateien kann die Software neue Viren unter Umständen nicht erkennen oder nicht entsprechend auf diese reagieren. Die Aktualität der Virendatenbank ist demnach entscheidend für die Effektivität der Erkennung.

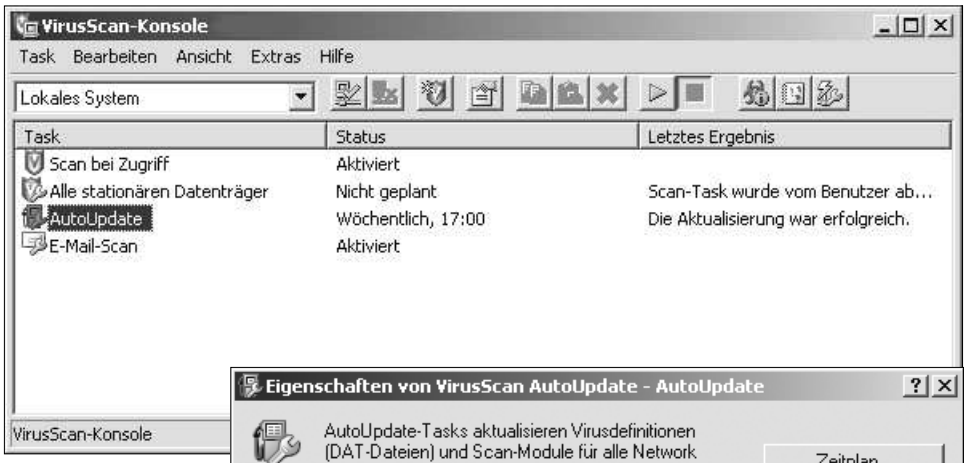

Abb. 1: Die VirusScan-Konsole von McAfee

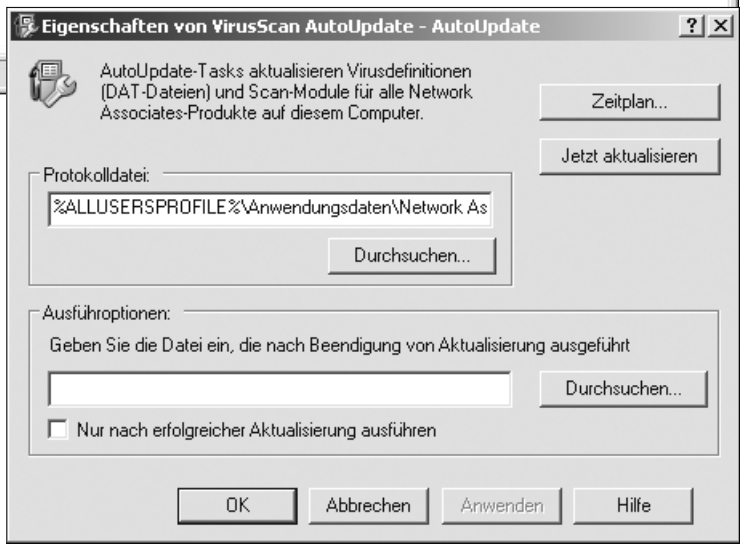

Abb. 2: Fenster *Eigenschaften von VirusScan AutoUpdate*

AutoUpdate

McAfee VirusScan bietet eine AutoUpdate-Funktion, anhand derer das Updaten ohne großen Aufwand für den Benutzer und in garantierter Regelmäßigkeit durchgeführt werden kann. Bei diesem automatisierten Prozess greift das Programm auf eine Download-Seite (ein so genanntes *Repository)* zu und lädt die entsprechenden Aktualisierungen von dort herunter. Standardmäßig bezieht Ihr VirusScan seine Aktualisierungen vom FTP- bzw. HTTP-Repository des Herstellers Network Associates International. Die hierfür notwendige Konfiguration wird nach Abschluss der Installation automatisch vorgenommen. Sie müssen sich also nicht weiter mit der Frage beschäftigen, woher Sie Ihre Updates beziehen. Viel wichtiger ist die Überlegung, wann Sie diese abrufen.

Mithilfe der AutoUpdate-Funktion kann das Updaten sowohl manuell per Direktanfrage als auch anhand eines Zeitplanes durchgeführt werden. Nutzen Sie die äußerst praktische Möglichkeit des Updatens via Zeitplan. Dieser ermöglicht es Ihnen, die verschiedenen Parameter nach Ihren persönlichen Präferenzen festzulegen. Die Aktualisierungen werden dann automatisch anhand dieser Zeitsteuerung vorgenommen. Die Enterprise-Version von McAfee bietet einen vordefinierten Aktualisierungs-Task, der jeden Freitag um 17:00 Uhr durchgeführt wird (mit einstündiger Zufallsfunktion). Es ist ratsam, diesen standardmäßigen Aktualisierungs-Task neu zu konfigurieren. Nehmen Sie sich kurz Zeit, die Einstellungen auf Ihre persönlichen Bedürfnisse abzustimmen. Die entsprechenden Änderungen sind einfach und schnell durchgeführt:

Wählen Sie ***Start – Programme – Network Associates – VirusScan-Konsole*** (siehe Abb. 1). Doppelklicken Sie auf ***AutoUpdate.*** Das Fenster *Eigenschaften von VirusScan AutoUpdate*[1)] öffnet sich (siehe Abb. 2). Durch Anklicken der Schaltfläche ***Zeitplan*** gelangen Sie in das Fenster *Zeitplaneinstellungen.* Da der Task hier bereits aktiviert ist, wechseln Sie gleich mit einem Klick auf die Registerkarte ***Zeitplan*** (siehe Abb. 3).

Unter *Geplanter Task* finden Sie die standardmäßige Konfiguration vor (*Wöchentlich*). Ändern Sie diese, indem Sie den Listenpfeil rechts neben dem Kästchen anklicken. Die nun sichtbare Liste präsentiert Ihnen eine Reihe von Optionen:

- Für BenutzerInnen mit Wählleitungszugang ist es naheliegend, das AutoUpdate ***Beim Einwählen*** durchführen zu lassen.

- Rechner, die via Breitband mit dem Internet verbunden bzw. in LAN-Netze eingebunden sind und beinahe täg-

1) Hier können Sie auch manuell per Direktanfrage neue Updates abrufen, indem Sie auf ***Jetzt aktualisieren*** klicken. Ein AutoUpdate wird dann umgehend durchgeführt.

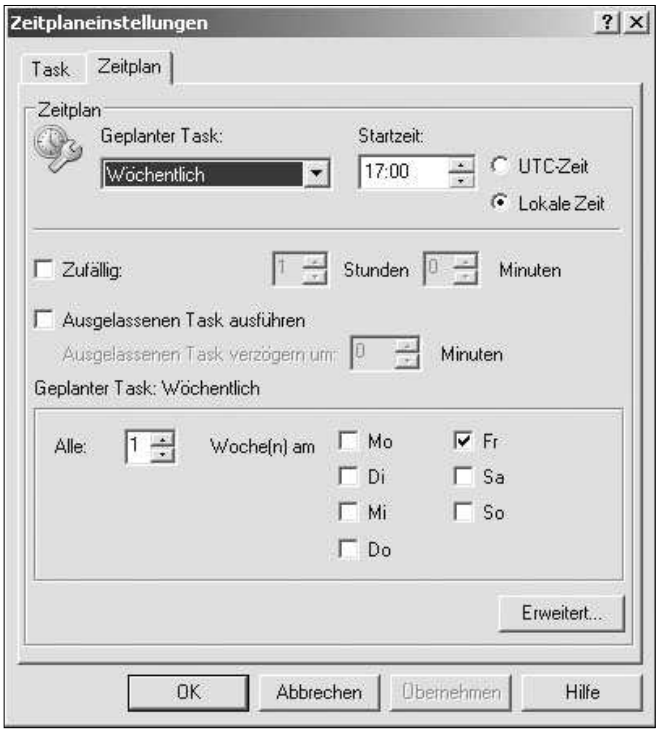

Abb. 3: Fenster *Zeitplaneinstellungen*, Registerkarte *Zeitplan*

lich ein- und ausgeschaltet werden („Werktagsrechner"), sollten zumindest ***Bei Systemstart*** aktualisiert werden.

- Bei Geräten, die auch in der Nacht nicht ausgeschaltet werden, ist wenigstens ein Update ***Täglich*** zu einer von Ihnen gewählten Uhrzeit (z.B. *07:00*) empfehlenswert.

Wählen Sie die für Sie passende Einstellung und schließen Sie den Task ab, indem Sie auf ***Übernehmen*** klicken und mit ***OK*** bestätigen.

Punkt 3: Techniken

Automatisches und manuelles Scannen

Die ersten beiden Punkte haben Sie souverän absolviert. Ihr „Goalie" ist in Ihr Team integriert und erhält ein regelmäßiges, perfekt auf Ihren Spielplan abgestimmtes Fitnessprogramm. Vor einem Einsatz auf dem Feld sollten Sie sich allerdings unbedingt mit den Fertigkeiten Ihres Neuerwerbs vertraut machen. Es gilt, zumindest einige wichtige Techniken Ihres Virenscanners zu kennen und zu wissen, wie Sie diese effektiv anwenden können.

Mit McAfee VirusScan können zwei Arten von Scanvorgängen ausgeführt werden:

- Automatisches Scannen,
- Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten.

Abb. 4: Infobereich von Windows XP – Scannen bei Zugriff ist deaktiviert

Scannen bei Zugriff

Die automatische Virenprüfung wird als *Scannen bei Zugriff* bezeichnet. Diese Funktion scannt in allen Dateien, die Sie öffnen, kopieren, speichern oder anderweitig bearbeiten sowie in allen Dateien, die Sie von Disketten oder Netzwerklaufwerken lesen oder auf diese schreiben. Sie bietet somit ständigen Schutz vor Viren, welche in diesen Quellen lauern.

Scannen bei Zugriff ist gewöhnlich nach erfolgreicher Installation aktiviert. Überprüfen Sie dies, indem Sie nach dem VShield-Symbol im Windows-Infobereich (rechts unten) Ausschau halten. Sollte wider Erwarten *Scannen bei Zugriff* deaktiviert sein, erkennen Sie dies an einem kleinen durchgestrichenen roten Kreis innerhalb des VShield (siehe Abb. 4). In diesem Fall doppelklicken Sie darauf und wählen Sie dann ***Aktivieren***. ***Schließen*** Sie das Fenster. Ihr Virenscanner ist nun stets wachsam.

Detailliertere Optionen können Sie ebenso mit einem Doppelklick auf das VShield aufrufen: Unter ***Eigenschaften*** ist es möglich, umfangreiche Konfigurationen für den Scanvorgang bei Zugriff vorzunehmen. So kann hier speziell definiert werden, welche Bereiche bei Anwendung dieses Tasks mit einbezogen werden sollen, welchen Ordner man für die Quarantäne-Funktion heranziehen möchte und wie lange der Scanvorgang für einzelne Bereiche dauern darf. Darüber hinaus lassen sich Aktionen wie das Versenden von Benutzernachrichten über Virusaktivitäten (*Wer bekommt welche Nachricht?*) oder das Erstellen von Protokollen (*Soll protokolliert werden, wenn ja wo und wie viel?*) genauer spezifizieren.

Unter *Alle Vorgänge* können Sie außerdem *Unterschiedliche Einstellungen für Vorgänge mit niedrigem oder hohem Risiko verwenden*. Dieses Feature mag zum Teil nützlich sein für den erfahrenen Benutzer, der Wert darauf legt, jede Einstellung individuell festzulegen. Für die herkömmliche Anwendung empfiehlt es sich jedoch, die Standardeinstellung des Herstellers (*Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden*) zu belassen.

Scannen auf Anforderung

Neben dem permanenten Scannen sollten Sie auch unbedingt regelmäßig die komplette Festplatte auf Viren durchsuchen. Vielleicht haben Sie ja vor einigen Wochen schon ein Virus auf der Festplatte gespeichert, das der Virenscanner damals noch nicht kannte und das bei Ihnen bis dato noch nicht aktiviert wurde. Mit dem *Scannen auf Anforderung* verfügen Sie über eine Methode, mit der Sie alle Teile des Computers zu für Sie günstigen Zeiten oder in regelmäßigen Abständen auf Viren scannen können. Verwenden Sie den Anforderungsscan als Ergänzung zum kontinuierlichen Schutz durch den Zugriffsscanner. Der integrierte Zeitplan hilft Ihnen dabei, die regelmäßigen Scanvorgänge so festzulegen, dass Ihre Arbeitsabläufe nicht eingeschränkt werden. Wählen Sie vorzugsweise eine Zeit-

spanne aus, in der Sie nicht am Gerät arbeiten (beispielsweise um die Mittagszeit oder nachts), da der Vorgang in den meisten Fällen die Systemleistung Ihres PCs beeinträchtigt.

Die VirusScan-Konsole enthält einen Standard-Task für das *Scannen auf Anforderung* mit dem Namen *Alle stationären Datenträger*. Sie können diesen Task umbenennen und /oder eine unbegrenzte Anzahl von (neuen) Anforderungstasks anlegen. Einen neuen Anforderungsscan erstellen Sie, indem Sie aus dem Menü ***Task*** die Option ***Neuer Scan-Task*** auswählen. In der Task-Liste der VirusScan-Konsole wird jetzt ein ***Neuer Scan*** angezeigt. Doppelklicken Sie darauf um die Konfiguration des Anforderungsscans vorzunehmen. Im Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* können Sie nun festlegen, welche Elemente zu welchem Zeitpunkt gescannt werden sollen, welche Reaktion erfolgt, wenn Viren gefunden werden, und wie Sie in einem solchen Fall benachrichtigt werden wollen.

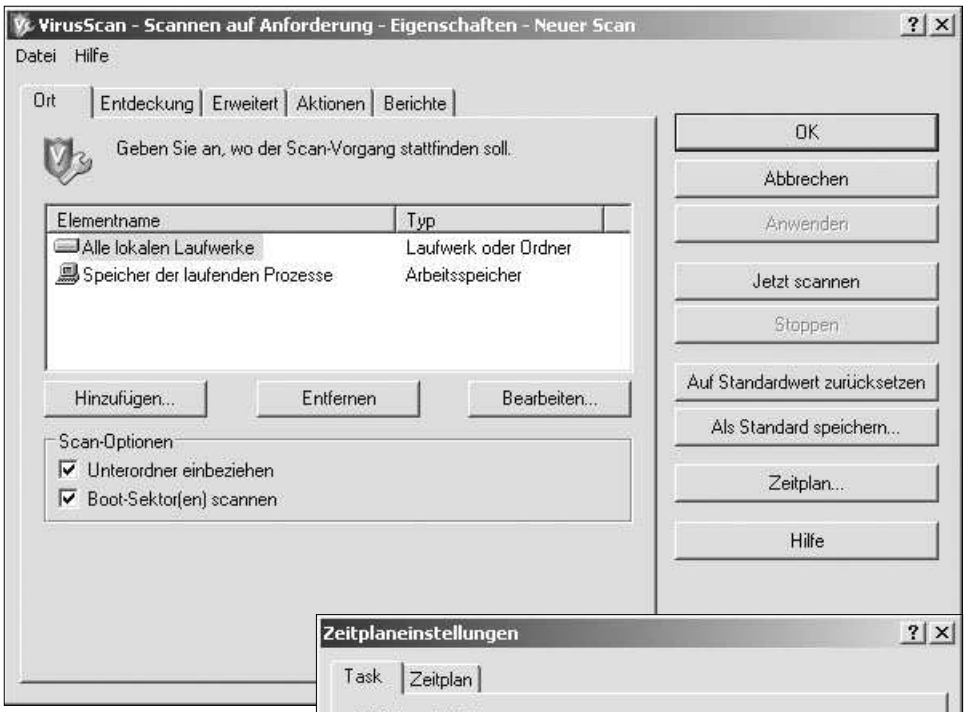

Abb. 5: Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* – Registerkarte *Ort*

Jene Bereiche, die gescannt werden sollen, werden auf der Registerkarte *Ort* definiert (siehe Abb. 5). Standardmäßig werden folgende Einstellungen verwendet: Auf allen lokalen Laufwerken, im Speicher der laufenden Prozesse, in den Unterordnern sowie in den Bootsektoren. Diese voreingestellte Auswahl hat Sinn, kann aber unter Umständen sehr lange dauern. Ändern Sie sie nur in Ausnahmefällen, beispielsweise wenn für den Scanvorgang lediglich ein sehr beschränkter Zeitrahmen zur Verfügung steht.

Auf der Registerkarte *Entdeckung* werden die Elemente definiert, die überprüft werden sollen. Auch hier ist die Voreinstellung *Alle Dateien* als sinnvoll zu erachten und zu belassen. Unter *Erweitert* können Sie – nomen est omen – erweiterte Optionen festlegen. Standardmäßig ist lediglich die *Heuristik* aktiviert. Mit diesem Begriff wird ein Suchverfahren bezeichnet, bei dem Programme nach „verdächtigen" Befehlsfolgen durchsucht werden, also nach (noch) nicht bekannten Virencodes. Die Effizienz dieser Methode ist derzeit jedoch laut Sicherheitsexperten eher minimal. Zudem ist sie äußerst fehleranfällig, was sich in zahlreichen *False Positives* bemerkbar macht. Sie können diese Funktion also unbesorgt deaktivieren.

Unter *Aktionen* wird festgelegt, wie der Virenscanner vorgehen soll, wenn er ein Virus gefunden hat. Generell wird empfohlen, im Zweifelsfall immer die Aktion *Säubern* zu

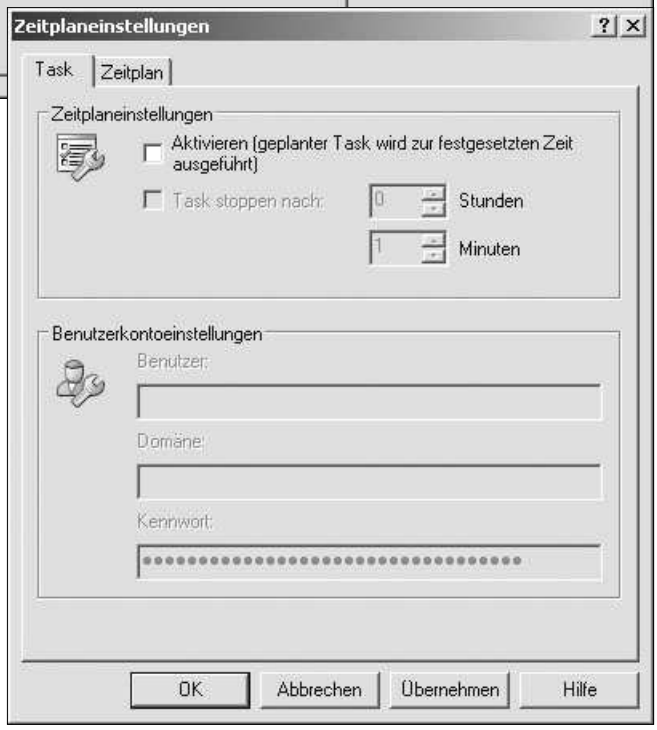

Abb. 6: Fenster *Zeitplaneinstellungen*, Registerkarte *Task*

wählen. Dies ist auch standardmäßig in VirusScan Enterprise vorgegeben. Wenn das Säubern der Datei fehlschlägt, verschiebt Ihr Scanner die Datei automatisch in den Ordner *Quarantäne*, der bereits bei der Installation des Programms angelegt wurde.

Auf der letzten Registerkarte *Berichte* können Sie schließlich diverse Einstellungen zu den Protokolleinträgen vornehmen, die der Virenscanner zu Ihrer Information erstellt. Die Optionen ermöglichen es Ihnen, den Ablageort selbst zu bestimmen (*Durchsuchen*) bzw. die *Größe* der Protokolldatei zu *begrenzen* (1 bis 999 MB). Wenn Sie keine Protokollierung wünschen, deaktivieren Sie einfach die Option *In Datei protokollieren*.

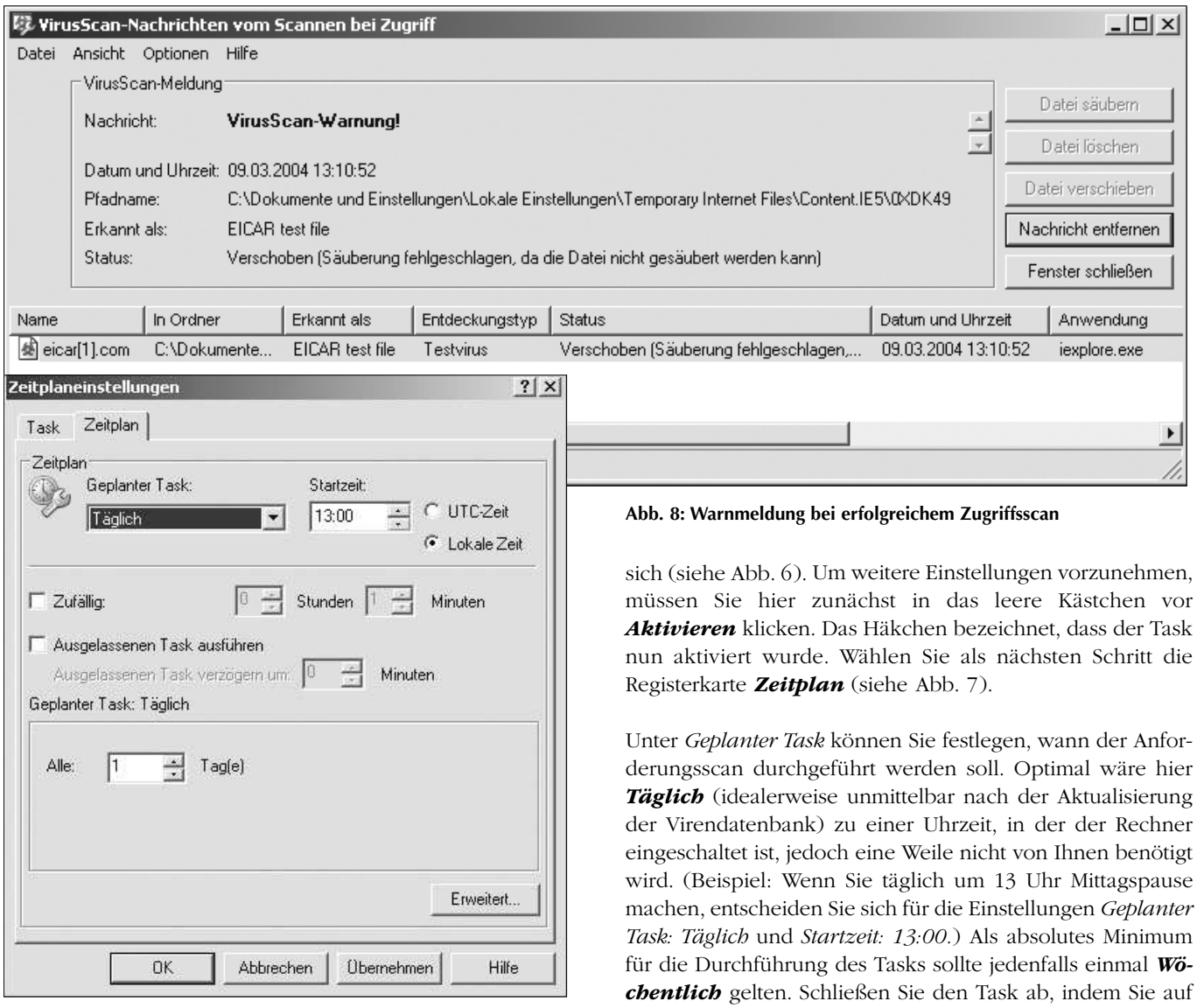

Abb. 7: Fenster *Zeitplaneinstellungen*, Registerkarte *Zeitplan*

Nachdem Sie sich mit den umfangreichen Konfigurationsmöglichkeiten vertraut gemacht haben und eventuell einige individuelle Adaptionen durchgeführt haben, schreiten wir letztendlich zum wichtigsten Kriterium: Und zwar zu jenem der regelmäßigen Durchführung des Tasks.

Garantieren können Sie eine solche regelmäßige Durchführung wiederum am besten mit Hilfe eines Zeitplans. Die weitere Vorgangsweise wird Ihnen schon wie Routine erscheinen: Kehren Sie im Fenster *VirusScan – Scannen auf Anforderung – Eigenschaften – Neuer Scan* auf die Registerkarte ***Ort*** zurück (siehe Abb. 5) und wählen Sie rechts mit einem Klick die Schaltfläche ***Zeitplan***. Sie sehen nun die Registerkarte *Task* des Fensters *Zeitplaneinstellungen* vor

Für Studierende ist McAfee VirusScan (Version 7.0) als Shareware unter `http://tucows.univie.ac.at/` erhältlich.

Abb. 8: Warnmeldung bei erfolgreichem Zugriffsscan

sich (siehe Abb. 6). Um weitere Einstellungen vorzunehmen, müssen Sie hier zunächst in das leere Kästchen vor ***Aktivieren*** klicken. Das Häkchen bezeichnet, dass der Task nun aktiviert wurde. Wählen Sie als nächsten Schritt die Registerkarte ***Zeitplan*** (siehe Abb. 7).

Unter *Geplanter Task* können Sie festlegen, wann der Anforderungsscan durchgeführt werden soll. Optimal wäre hier ***Täglich*** (idealerweise unmittelbar nach der Aktualisierung der Virendatenbank) zu einer Uhrzeit, in der der Rechner eingeschaltet ist, jedoch eine Weile nicht von Ihnen benötigt wird. (Beispiel: Wenn Sie täglich um 13 Uhr Mittagspause machen, entscheiden Sie sich für die Einstellungen *Geplanter Task: Täglich* und *Startzeit: 13:00.*) Als absolutes Minimum für die Durchführung des Tasks sollte jedenfalls einmal ***Wöchentlich*** gelten. Schließen Sie den Task ab, indem Sie auf ***Übernehmen*** klicken und mit ***OK*** bestätigen.

Punkt 4: Agieren im Vorfeld

Umsicht ist die beste Verteidigung

Kein Tormann vermag es, alle Bälle abzublocken. Ebenso kann auch die beste Antivirensoftware nicht alle viralen Attacken abwehren. Es verbleibt ein gewisses Restrisiko, das sich nur durch umsichtiges Handeln auf eine vernachlässigbare Größe reduzieren lässt.

Öffnen Sie deshalb prinzipiell keine eMail-Attachments unbekannten oder verdächtigen Ursprungs. Oft lässt sich bereits anhand des (nicht selten allzu „verlockenden“) Betreffs die (Un-)Seriosität des Inhalts abschätzen. Lassen Sie zudem Vorsicht walten bei Downloads aus dem Internet und achten Sie dabei stets auf namhafte Quellen. Weitere hilfreiche Ratschläge finden Sie im Artikel *Goldene Regeln für ein intaktes (Windows-)Betriebssystem* auf Seite 16. Im Zweifelsfall empfiehlt sich immer die alte Weisheit: *Vorsicht ist besser als Nachsicht.*

Verlängerung: Golden Goal

Der Fall der Fälle

Wenn Ihr Virenscanner erfolgreich ein Virus aufgespürt hat, erhalten Sie umgehend eine Meldung (siehe Abb. 8 auf Seite 25), die Ihnen mitteilt, wann und wo das Virus entdeckt wurde, um welches Virus es sich handelt und wie Ihr Virenscanner gegen den mutmaßlichen Angreifer vorgegangen ist (nachzulesen unter *Status*).

Keine Panik, Ihr Virenscanner hat bereits verlässlich das erste Krisenmanagement übernommen. Im dargestellten Fall hat er die Datei korrekt als *eicar testfile* erkannt und – wie in den Einstellungen festgelegt – in den Quarantäne-Ordner verschoben, weil eine Säuberung fehlschlug. Sollte auf Ihrem Rechner ebenfalls einmal die Situation eintreten, dass die Säuberung einer Datei misslingt, so empfiehlt es sich im Anschluss einen Neustart durchzuführen und die verschobene Datei erneut zu scannen. In den meisten Fällen wird dem Virenscanner die Säuberung nun gelingen.

Sollte dies nicht der Fall sein, ist es besser den Rat von Experten einzuholen, da die Alternative *Datei löschen* eventuell mehr schaden als nutzen könnte. Wenden Sie sich deshalb bei Fragen vertrauensvoll an unser Helpdesk-Team (eMail: `helpdesk.zid@univie.ac.at`, Tel.: 4277-14060).

Wenn Sie selbst überprüfen wollen, wie McAfee VirusScan arbeitet, können Sie unter `http://www.eicar.com/` ein Testvirus herunterladen. Das *eicar testfile* gibt es in mehreren Versionen: Als DOS-Programm, das zur Gänze aus einem ASCII-String besteht, als Kopie mit einem anderen Dateinamen sowie in einfach und doppelt gezippter Form. Ein guter Virenscanner wird das einfach gezippte „Virus" erkennen und vielleicht sogar das doppelt gezippte. Seien Sie unbesorgt, es handelt sich bei dem *eicar testfile* um kein „echtes" Virus, es enthält keinerlei Viruscode-Fragmente. Dennoch reagieren die meisten Virenscanner darauf, als ob es tatsächlich ein Virus wäre. Es eignet sich deshalb optimal für ein kleines „Freundschaftsspiel".

Michaela Bociurko ■

PS – speziell für jene, die einen neuen Rechner unter Windows XP in Betrieb nehmen wollen: Bedenken Sie, dass dieser bis zur Installation eines Antivirenprogramms völlig ungeschützt ist! Es empfiehlt sich daher, den Rechner während dieser Zeitspanne mit Hilfe der im Betriebssystem integrierten Firewall abzusichern. Eine Anleitung hierfür finden Sie im Artikel *Sicherheit von Anfang an – Windows XP mit Firewall-Schutz installieren* (siehe Seite 20).

RedHat Linux goes commerce

Die bereits Mitte letzten Jahres von RedHat angekündigte Auflösung der Standard-Linux-Softwareserie wurde nun endgültig vollzogen: „RedHat Linux" gibt es offiziell nicht mehr. Ab Ende April 2004 werden für RedHat Linux 9 keine Updates und keine Security Patches mehr bereitgestellt. Der Support für die älteren Versionen 7.x und 8.0 lief bereits mit Ende letzten Jahres aus.

Für die Nachfolge hat RedHat seine Produktserie in zwei Linien gespalten:

- Kommerziellen Support, kontinuierliche Updates, Bug- und Security-Fixes wird es hinkünftig nur mehr für die kostenpflichtige **RedHat Enterprise Linux (RHEL)-Serie** geben. Diese auf Unternehmenskunden abzielende Distribution gründet auf einer einheitlichen Code-Basis, was die Stabilität und Sicherheit verbessert sowie die Pflege vereinfacht. Lizenzpflichtige Enterprise-Versionen gibt es – je nach Umfang des Einsatzes – für Workstations, kleinere Server sowie für große Serverbetreiber. Eine Enterprise Linux AS Academic Edition kann um $ 50,– über den ZID erworben werden. Bei Interesse wenden Sie sich bitte an Peter Karlsreiter (eMail: `peter.karlsreiter@univie.ac.at`, Tel.: 4277-14131).
- Für die Weiterentwicklung der bisherigen Linux-Distribution hat RedHat die Quellen der Version 9 dem nicht kommerziellen Projekt Fedora übertragen. Das dort entwickelte freie **Fedora Core Linux** soll als Entwicklungsfeld für neue Linux- und Open Source-Technologien dienen. Fedora Core 1 ist seit November allgemein verfügbar, dessen Nachfolger, Fedora Core 2, bereits in der Testphase. Im Unterschied zu den Enterprise-Versionen kann es bei der Konfiguration eines Softwarepakets unter Fedora Core durchaus zu kleineren Fehlern im Rahmen eines Upgrades kommen. Größere Probleme gab es jedoch bisher nicht.

Fedora Core's tägliches Softwareupgrade mittels YUM

Bei Verwendung von YUM (*Yellowdog Updater Modified*) können Sie die tägliche Update-Funktion von Fedora Core mit den Befehlen **`chkconfig yum on`** und **`/etc/init.d/yum start`** aktivieren.

Da der Zentrale Informatikdienst der Universität Wien auf seinem FTP-Server einen Mirror der Fedora Core-Software hält, sollten Sie in der Datei `/etc/yum.conf` in der Rubrik `[base]` den `baseurl` auf den Wert

```
baseurl=ftp://ftp.univie.ac.at/systems/linux/
fedora/$releasever/$basearch/os
```

setzen. Analog sollte er in der Rubrik `[updates-released]` auf den Wert

```
baseurl=ftp://ftp.univie.ac.at/systems/linux/
fedora/updates/$releasever/$basearch
```

eingestellt werden. Dies erspart Ihnen unnötige Fehlschläge bei den Updates Ihres Betriebssystems.

Aron Vrtala

MAILBOX-SERVICE:

Siehe, ich mache auch hier alles neu…

Wie im *Comment 03/2* berichtet, wurde im August 2003 erfolgreich die zweite große Umstellung des Unet-Service für Studierende durchgeführt (die erste war die Einführung von DCE/DFS im Jahr 1998). Das Mailbox-Service für Uni-MitarbeiterInnen blieb hingegen trotz zahlreicher Ausbauten und Erweiterungen[1] seit seinen Anfängen im Jahr 1994 im Wesentlichen unverändert: Nach wie vor ist ein einziger Server, der so genannte „Mailbox-Rechner", für fast alle Funktionen – eMail, WWW, Login, Fileservice – zuständig. Ein solches Konzept ist heute nicht mehr zeitgemäß; daher wird der Mailbox-Rechner demnächst durch mehrere Server ersetzt werden, die jeweils eine dieser Funktionen anbieten. Das hat folgende Vorteile:

- Höhere Betriebssicherheit und Stabilität: Mailserver und Webserver unterliegen unterschiedlichen Sicherheitsanforderungen. Die Server sollten daher physisch getrennt sein, damit nicht z.B. bei Überlastung des Webservers – durch DoS-Attacken, fehlerhafte Skripts usw. – die Mail-Services beeinträchtigt werden.

- Bessere Skalierbarkeit: Ein verteiltes System kann einfacher dem Bedarf angepaßt werden, indem einzelne Komponenten erweitert oder auf mehrere Server verteilt werden (schon jetzt wird der Mailbox-Rechner von etwa 10 weiteren Servern unterstützt, die z.B. als Spam-Filter oder Virenscanner dienen).

- Das derzeit als Zusatzdienst angebotene File-Service (Zugriff aus dem Uni-Datennetz auf eigene bzw. freigegebene Daten am Mailbox-Rechner mittels *Netzwerklaufwerk verbinden*) wird in Zukunft ein integraler Bestandteil des Mailbox-Service sein. Durch die Anschaffung eines eigenen Fileservers wird auch wesentlich mehr Plattenplatz als bisher zur Verfügung stehen.

- Ein Login in den öffentlichen PC-Räumen wird dann auch mit Mailbox-UserIDs möglich sein.

Nachdem sich die für das Unet-Service gewählte Lösung mit Samba als verteiltem Filesystem sehr gut bewährt hat, wird dasselbe Konzept mit minimalen Änderungen auch für das Mailbox-Service eingesetzt werden.[2] Anstelle des derzeitigen Hostnamens MAILBOX.UNIVIE.AC.AT werden dann Service-Namen treten:

- MAIL.UNIVIE.AC.AT zum Versenden von eMail-Nachrichten,

- IMAP.UNIVIE.AC.AT bzw. POP.UNIVIE.AC.AT zum Empfangen von eMail,

- LOGIN.UNIVIE.AC.AT für interaktives Arbeiten (Login mittels SSH oder Telnet; Datentransfer mittels SCP, SFTP oder FTP).

- Die persönlichen Homepages von Uni-MitarbeiterInnen, die derzeit die Adresse `http://mailbox.univie.ac.at/Vorname.Nachname/` haben, werden dann unter `http://homepage.univie.ac.at/Vorname.Nachname/` zu finden sein. Die bisherigen Adressen werden mit Hilfe entsprechender Weiterleitungen aber nach wie vor funktionieren.

Die Mailbox-Umstellung wird wahrscheinlich in den Osterferien stattfinden (ein genauer Zeitplan steht noch nicht fest) und eine relativ kurze Betriebsunterbrechung bewirken, d.h. nur wenige Stunden in der Nacht oder am Wochenende. Außer den oben erwähnten Namensänderungen wird von der Umstellung vermutlich nicht viel zu bemerken sein – im Wesentlichen sollte danach alles so funktionieren wie bisher. Details über kleinere Änderungen (z.B. eMail-Weiterleitung nur mehr über Webmaske und nicht mehr über `.forward`-Datei) werden noch rechtzeitig bekannt gegeben.

Peter Marksteiner ■

1) siehe z.B. die Artikel *4th Time Around: Ein neuer Mailbox-Rechner* im *Comment 01/2* (`http://www.univie.ac.at/comment/01-2/012_5.html`) oder *Reform des Mailbox-Service* im *Comment 99/2* (`http://www.univie.ac.at/comment/99-2/992_3.html`).

2) Eine Einbindung des Mailbox-Service in DCE/DFS war bereits 1998 geplant, wurde damals aber wegen verschiedener Probleme mit DCE/DFS nicht durchgeführt.

Onlinetarif-Rufnummer 07189 14013 wird aufgelassen

Am 26. April 2004 wird die Onlinetarif-Rufnummer 07189 14013 (= ehemaliger Wählleitungszugang für Mailbox-BenutzerInnen) endgültig außer Betrieb genommen. Falls Ihr Modem noch über diese Nummer einwählt, ändern Sie die Konfiguration bitte rechtzeitig auf die Onlinetarif-Rufnummer **07189 14012**, die sowohl für Studierende als auch für MitarbeiterInnen der Universität Wien zur Verfügung steht.

Bei Einwahl von außerhalb der Regionalzone Wien muss die Normaltarif-Nummer (+43 1) 40122 verwendet werden (siehe *Comment 03/1*, `http:/www.univie.ac.at/comment/03-1/031_16b.html`).

Freiwillige Feuerwehr im Datennetz: DAS ACONET-CERT

Das Thema „Sicherheit im Internet“ wird immer brisanter – Viren, Würmer, Spam und Hacker sind allgegenwärtig und werden mit einer Unzahl technischer Hilfsmittel (Firewalls, Virenscanner und vieles andere mehr) bekämpft. Viele Firmen bieten mittlerweile umfassende Sicherheitslösungen an. Ein Aspekt wird in der Regel aber übersehen: Die technische Ebene der Internet-Security ist nur ein Teil der Wahrheit (wenn auch der, der sich leichter verkaufen lässt). Mindestens genauso wichtig ist eine Infrastruktur, die es ermöglicht, einerseits sicherheitsrelevante Informationen so früh wie möglich zu erhalten und andererseits im Ernstfall rasch und effizient zu reagieren.

Manche Netzwerkspezialisten (vor allem aus dem akademischen Bereich) haben diese Notwendigkeit schon sehr früh erkannt: Bereits im Dezember 1988 – zu einer Zeit, als das Internet noch wenig verbreitet war und Jahre, bevor das WWW erfunden wurde – entstand an der Carnegie Mellon University in Pittsburgh das CERT/CC (*Computer Emergency Response Team / Coordination Center*; siehe `http://www.cert.org/about/1988press-rel.html`) als Vorläufer und Vorbild einer stetig wachsenden Zahl von Security-Teams.

Seit 1993 gibt es auch eine weltweite Dachorganisation für CERTs: das *Forum of Incident Response and Security Teams* (FIRST). Unter den 20 Gründungsmitgliedern von FIRST befanden sich auch drei europäische Teams, allesamt aus dem akademischen Umfeld.

Gigabit-Anbindung für das Vienna Biocenter

Die Institute der Uni Wien und der Med-Uni Wien im Vienna Biocenter (1030 Wien, Dr. Bohr-Gasse 9) haben Grund zur Freude: Seit Dezember 2003 ist dieser Universitätsstandort über eine Glasfaserleitung mit Gigabit-Ethernet an das Uni-Datennetz angebunden.

Diese Neuerung ist der erste bereits realisierte Teil eines Großprojekts, das im Laufe der nächsten Monate für insgesamt 19 Standorte der Universität Wien eine Glasfaser-Anbindung vorsieht. Die neuen Glasfaserleitungen ersetzen in den meisten Fällen bereits vorhandene, langsame Datenleitungen. Darüber hinaus werden aber auch einige Redundanzleitungen für große Universitätsstandorte (Hauptgebäude, Altes AKH, UZA, BWZ, Gebäudekomplex Boltzmanngasse/Strudlhofgasse) errichtet, die bei einer Überlastung der jeweiligen Hauptleitung zum Einsatz kommen.

Security-Initiativen in Österreich

ARGE-Secure

In Österreich wurde im Jahr 2000 die ARGE-Secure gegründet, eine Arbeitsgemeinschaft von Security-Verantwortlichen heimischer Universitäten, die sich zum Ziel gesetzt hat, die nationale Kooperation und Kommunikation in Security-Fragen zu verbessern und für das österreichische Wissenschaftsnetz ACOnet die Funktionen eines CERT zu erfüllen.

Die wichtigsten davon sind *Incident Handling und Incident Response*: Bei sicherheitsrelevanten Netzwerkproblemen in seinem Zuständigkeitsbereich (*Constituency*) ist es Aufgabe des CERT, die entsprechenden Maßnahmen zu koordinieren. In den meisten Fällen bedeutet das, Beschwerden von außen an die Betroffenen weiterzuleiten und diese bei der Lösung ihres Netzwerkproblems so weit wie möglich zu unterstützen. Wenn jemand aus dem Constituency in Schwierigkeiten steckt (beispielsweise durch einen Angriff von außen), hilft das CERT natürlich ebenfalls, die Probleme zu beseitigen und die Kommunikation mit den Verursachern abzuwickeln. Neben dieser Kernaufgabe kann sich ein CERT noch vielen weiteren Tätigkeitsfeldern widmen – beispielsweise Schulungen, Publizieren von Advisories und Warnungen, Forschung oder Produkt-Evaluation (eine umfassende Dokumentation der Aufgaben eines CERT finden Sie unter dem URL `http://www.cert.org/archive/pdf/csirt-handbook.pdf`).

ACOnet-CERT

Die ARGE-Secure hat leider ein gravierendes Handicap: Für eine lose Arbeitsgemeinschaft ohne formelle Verbindungen zu internationalen Organisationen ist es schwierig, rechtzeitig an relevante Informationen zu kommen. Sicherheitsprobleme im Internet haben in der Regel globalen Charakter, und eine entsprechende Einbindung in internationale Strukturen ist unumgänglich, wenn man im Ernstfall rasch und effizient eingreifen will. Daher wurde im Jänner 2003 ein offizielles Security-Team für das österreichische Wissenschaftsnetz gegründet: das ACOnet-CERT.

Neben der oben beschriebenen *Incident Coordination*, die weiterhin überwiegend im Rahmen der ARGE-Secure abgewickelt wird, ist die wichtigste Aufgabe des ACOnet-CERT der ständige Informationsaustausch mit anderen Security-Teams. Zu diesem Zweck ist das ACOnet-CERT Mitglied von FIRST und TF-CSIRT (siehe Kasten *Internationale Security-Bündnisse* auf Seite 29). Diese Infra-

struktur bietet die Möglichkeit, einer drohenden Gefahr bereits vorbeugend entgegenzuwirken („proaktives Handeln"): Da die meisten Sicherheitsprobleme nicht in Österreich ihren Ausgang nehmen, bleibt durch die Vorab-Informationen der internationalen Partner erheblich mehr Zeit zu reagieren. Zwischenfälle, die dennoch die EndanwenderInnen erreichen (z.B. Viren, deren Verbreitungsgeschwindigkeit mittlerweile im Minutenbereich liegt), können schneller, gezielter, mit mehr Know-How und besserer Schadensbegrenzung bekämpft werden („reaktives Handeln").

Darüber hinaus bietet das ACOnet-CERT einen zentralen *Point of Contact* für Security-Fragen im ACOnet: Bei Problemen kontaktiert das CERT die Verantwortlichen der jeweiligen Teilnetze und ermöglicht ihnen dadurch ein rasches Reagieren.

Das Team des ACOnet-CERT besteht derzeit aus sieben Mitarbeitern des ZID der Universität Wien, die sich neben ihren eigentlichen Aufgabenbereichen auch mit Fragen der Security beschäftigen und das *Incident Handling* abwickeln. Da das Spezialwissen der einzelnen Team-Mitglieder praktisch jederzeit schnell verfügbar ist, erlaubt dieses System eine besonders effiziente Bearbeitung der Vorfälle.

Nähere Informationen zum ACOnet-CERT finden Sie auf der Webseite **`https://cert.aco.net/`**; für weitere Fragen steht das CERT-Team unter der Mailadresse `cert@aco.net` zur Verfügung (Tel.: +43 1 4277-14045, Fax: +43 1 4277-9140).

CIRCA

Ein weiteres österreichisches Security-Projekt, das vor allem auf eine verstärkte Kooperation der kommerziellen Internet-Provider (ISPs) in Sicherheitsfragen abzielt, ist CIRCA (*Computer Incident Response Coordination Austria*, siehe dazu auch `http://www.circa.at/`). Das Projekt CIRCA wurde im Oktober letzten Jahres von der ISPA, dem Dachverband der österreichischen Internet-Provider, ins Leben gerufen und ist unter anderem auch als Schnittstelle zwischen ISPs und Security-Firmen einerseits und dem öffentlichen Bereich andererseits gedacht.

Abgesehen von den drei vorgestellten Initiativen ist Österreich, was die Security-Infrastruktur anbelangt, leider immer noch ein eher unbeschriebenes Blatt. Es bleibt zu hoffen, dass die vorhandenen Ressourcen dennoch ausreichend sind, um den zunehmenden Gefahren aus den Weiten des Internet auch in Zukunft angemessen entgegentreten zu können.

Ulrich Kiermayr ■

Internationale Security-Bündnisse

FIRST

Das *Forum of Incident Response and Security Teams* (`http://www.first.org/`) wurde 1993 als internationale Dachorganisation für Security-Teams gegründet. FIRST hat mittlerweile etwa 150 Mitglieder aus allen Bereichen der Informationstechnologie – Softwarehersteller (z.B. *Microsoft Product Support Services Security Team*) genauso wie Hardwarehersteller (z.B. *Cisco PSIRT*), Teams aus dem Finanzwesen (z.B. *VISA-CIRT*) genauso wie nationale CERTs. Das ACOnet-CERT ist seit April 2003 FIRST-Mitglied.

Der Informationsaustausch findet bei FIRST – wie in diesen Kreisen üblich – hauptsächlich über eine Mailingliste statt, die nur für Mitglieder zugänglich ist. So kann weitestgehend vermieden werden, dass vertrauliche Hinweise zu früh an die Öffentlichkeit gelangen und der Informationsvorsprung verloren geht. Zusätzlich veranstaltet FIRST einmal jährlich eine Konferenz und zweimal jährlich ein *Technical Colloquium*, die das gegenseitige Vertrauen und den persönlichen Wissensaustausch unter den Mitgliedern fördern sollen.

TF-CSIRT

Um die Kontakte der europäischen Security-Fachleute untereinander zu verbessern, wurde 1999 eine *Task Force* der TERENA (*Trans European Research and Education Network Association*; siehe `http://www.terena.nl/`) ins Leben gerufen, die sich mit Security-Fragen befasst und die entsprechenden Aktivitäten in Europa koordiniert. Die TF-CSIRT (*Task Force – Collaboration of Security Incident Response Teams*) richtete sich anfänglich eher an die Wissenschaftsnetze, hat sich aber mittlerweile zu einem Forum für europäische CERTs aus allen Bereichen entwickelt.

Unter den zahlreichen Projekten der TF-CSIRT ist der so genannte *Trusted Introducer* (TI; siehe `http://www.ti.terena.nl/`) wohl das wichtigste: Dabei handelt es sich um eine unabhängige Stelle, die CERTs auf der Basis formaler Kriterien akkreditiert. Indem der Trusted Introducer einen gewissen Mindeststandard in Bezug auf Arbeitsweise und Dokumentation der „beglaubigten" Security-Teams sicherstellt und die Informationen über die einzelnen Teams auf dem aktuellen Stand hält, entsteht ein schlagkräftiges *Web of Trust*, dessen Mitglieder auch ohne aufwendige wechselseitige Beziehungen im Ernstfall rasch gemeinsam vorgehen können. Darüber hinaus unterhält die TF-CSIRT auch gute Kontakte zur Europäischen Kommission, sodass in den letzten Jahren im Security-Bereich eine ganze Reihe von EU-geförderten Projekten verwirklicht werden konnte.

ACOnet war in der TF-CSIRT von Anfang an sehr aktiv; das ACOnet-CERT wurde dann im März 2003 durch den *Trusted Introducer* auch formal akkreditiert.

IP-Adressen nach Bedarf: Das DHCP-Service des ZID

Im Datennetz der Universität Wien muss in der Regel jeder angeschlossene Rechner eine fix eingetragene (statische) IP-Adresse besitzen. Diese Praxis bringt jedoch einige Nachteile mit sich: Zum einen können fehlerhafte Angaben dazu führen, dass der Rechner nicht mehr funktioniert bzw. im schlimmsten Fall sogar ganze Netzbereiche lahm legt. Zum anderen hat man als BesitzerIn eines Notebooks das lästige Problem, bei jedem Standortwechsel (am Institut, im Hörsaal, zu Hause, ...) die Netzwerkkonfiguration des Rechners ändern zu müssen.

Die einzige Ausnahme bildeten bisher die Public Network Services des Zentralen Informatikdienstes (Hörsaal-Netz und Datentankstellen; siehe `http://www.univie.ac.at/ZID/pns.html`): Diese Datensteckdosen in öffentlichen Bereichen der Universität Wien ermöglichen allen Mailbox- und Unet-BenutzerInnen einen bequemen, mobilen Internetzugang. Die IP-Adresse wird dem Rechner dabei automatisch mittels DHCP zugewiesen.

Seit kurzem bietet der Zentrale Informatikdienst nun auch den Instituten und Dienststellen der Uni Wien die Möglichkeit, mit Hilfe eines zentral gewarteten DHCP-Servers die IP-Adressvergabe in ihrem Netzbereich dynamisch – und somit flexibler – abzuwickeln.

DHCP, was ist das?

Mit DHCP (*Dynamic Host Configuration Protocol*) kann die Netzwerkkonfiguration von Computern automatisiert werden, die das Internetprotokoll TCP/IP verwenden. Ein DHCP-Server ermöglicht es allen Rechnern in seinem Netzbereich, die für den Internetzugang notwendigen Einstellungen selbständig zu eruieren und anzuwenden (*Plug & Play*). Und so funktioniert es:

1. **Automatische Zuteilung der IP-Adresse**
   Sobald ein für DHCP konfigurierter Rechner an das Netzwerk angeschlossen wird, sendet er eine entsprechende Anfrage an alle anderen Rechner im selben Netzbereich (*Broadcast*). Falls hier ein DHCP-Server vorhanden ist, schickt dieser dem „Neuen" daraufhin eine IP-Adresse aus einem vorkonfigurierten Adress-Pool.

2. **Bereitstellen der TCP/IP-Konfigurationsparameter**
   Außerdem übermittelt der Server eine Reihe anderer wichtiger Einstellungen – z.B. Gateway, Nameserver und Timeserver. Auf Basis dieser Angaben konfiguriert der Rechner seinen Netzzugang. Die Parameter werden nach Ablauf einer vom Server vorgegebenen Zeit (*Lease Time*) automatisch aktualisiert, um Änderungen in der Netz-Topologie zu ermöglichen.

Dieses System ist vor allem in jenen Bereichen vorteilhaft, in denen viele neue bzw. mobile Rechner an das Netzwerk angeschlossen werden (die Public Network Services sind ein typischer Anwendungsfall): Da der DHCP-Server und die einzelnen Rechner die benötigten Informationen ohne Zutun des Benutzers austauschen, sind – solange es freie IP-Adressen im Pool des DHCP-Servers gibt – keinerlei administrative Schritte notwendig, um einem Rechner Internetzugang zu verschaffen.

Zudem können Umstellungen im Netzwerk (z.B. neue Gateway-Adressen) vorgenommen werden, ohne nachher jeden einzelnen Rechner im Netz manuell umzukonfigurieren: Es genügt, wenn der DHCP-Server über die aktuellen Parameter Bescheid weiß. Daher ist es durchaus sinnvoll, DHCP auch für bestehende Arbeitsplatzrechner einzusetzen.

Statische Dynamik

Die Vorteile von DHCP haben allerdings ihre Schattenseiten. Beispielsweise benötigen Server, aber auch manche Anwendungsprogramme einen fixen DNS-Eintrag und somit eine statische IP-Adresse. Darüber hinaus birgt die automatisierte Konfiguration ein gewisses Sicherheitsrisiko. Da einem Netzbetreiber üblicherweise sehr daran gelegen ist, im Falle von Virenattacken oder Missbrauch den Verursacher identifizieren zu können, sind in einem DHCP-Netz zusätzliche Sicherheitsmassnahmen erforderlich (bei den Public Network Services z.B. die Anmeldung mittels Mailbox- oder Unet-UserID).

Ein Ausweg besteht darin, die MAC-Adresse des Computers (die vom Hersteller in die Netzwerkkarte eingebrannte, weltweit eindeutige Hardware-Adresse; z.B. `08:00:20:ae:fd:7e`) mit einer IP-Adresse zu verknüpfen und auf diese Weise einem bestimmten Rechner immer dieselbe IP-Adresse zuzuteilen. Dazu muss der DHCP-Server dessen MAC-Adresse allerdings schon vorher kennen, und auch jede Änderung der MAC-Adresse – beispielsweise durch Tausch der Netzwerkkarte – muss dem DHCP-Server bekannt gegeben werden.

DHCP für Institute

Der Zentrale Informatikdienst bietet nun interessierten Instituten die Möglichkeit, in ihrem Netzwerk einen vom ZID betriebenen, statischen DHCP-Server zu verwenden. Voraussetzung ist jedoch (ähnlich wie bei der Institutsfirewall) eine vollständige Dokumentation des Institutsnetzes – d.h. alle Rechner des Instituts und ihre MAC-Adressen müssen beim ZID registriert sein. (Das DHCP-Service ist daher vor

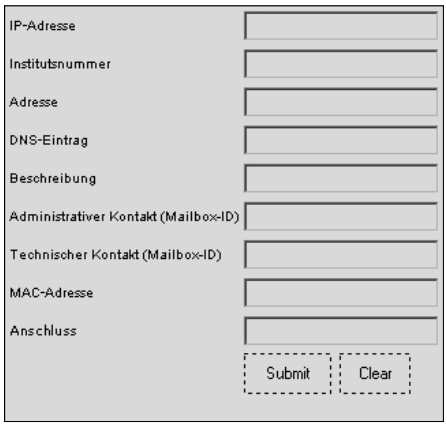

Abb. 1: Webformular – Anmeldung neuer Rechner für das DHCP-Service

allem auch für jene Institute der Universität Wien interessant, die die Institutsfirewall des Zentralen Informatikdienstes einsetzen und deren Netzwerk daher ohnehin bereits dokumentiert ist.) Der DHCP-Server des ZID weist dann anhand dieser Daten die statischen IP-Adressen dynamisch zu – unabhängig von der Datensteckdose, an der der betreffende Rechner angeschlossen ist, und mit der jeweils aktuellen Netzwerkkonfiguration.

Selbstverständlich besteht bei Inanspruchnahme des Service kein DHCP-Zwang für alle Rechner des Instituts – fix eingetragene IP-Adressen funktionieren auch weiterhin. Bei Servern sollte die IP-Adresse sogar fix konfiguriert sein, um zu vermeiden, dass eventuelle DHCP-Störungen den Serverbetrieb in Mitleidenschaft ziehen.

Um die Neuanmeldung von Rechnern zu erleichtern, wurde ein entsprechendes Webformular entwickelt (siehe Abb. 1). Auch neue MAC-Adressen von bereits registrierten Rechnern können über eine Webmaske bekannt gegeben werden. Das Webformular finden Sie unter `http://www.univie.ac.at/ipdb/`; die genaue Vorgangsweise ist im nebenstehenden Kasten *DHCP-Service: An-, Ab- und Ummeldung von Rechnern* beschrieben.

Wenn Sie das DHCP-Service an Ihrem Institut verwenden möchten und/oder weitere Fragen haben, kontaktieren Sie uns bitte per eMail unter der Adresse `netzwerk.zid@univie.ac.at`.

Ulrich Kiermayr ■

DHCP-Service: An-, Ab- und Ummeldung von Rechnern

Rufen Sie mit Ihrem Browser den URL **`http://www.univie.ac.at/ipdb/`** auf und geben Sie Ihre Mailbox-UserID und das dazugehörige Passwort ein. Sie erhalten nun eine Webseite mit den Funktionen *Neues Objekt*, *Objekt löschen* und *MAC-Adresse ändern*.

Neues Objekt

Für die Anmeldung eines Rechners sind folgende Angaben notwendig:

Technische Daten:

IP-Adresse	bei der/dem EDV-Beauftragten zu erfahren
DNS-Name	
MAC-Adresse	
Anschluss	Steckplatz an Dose / Switch

Administrative Daten:

Institutsnummer	z.B. *A140 (ZID)*
Adresse	Standort des Rechners
Beschreibung	z.B. *Notebook Dr. Morgenstern*
Administrativer Kontakt	Benutzer/in des Geräts bzw. EDV-Beauftragte/r
Technischer Kontakt	

Bei bestehenden Rechnern muss das Webformular (siehe Abb. 1) vollständig ausgefüllt werden; neue Rechner, die erstmals in Betrieb genommen werden, erhalten IP-Adresse und DNS-Name vom ZID (für letzteren werden Vorschläge gerne entgegengenommen). Sobald Sie alle Angaben eingetragen und das Formular durch Klick auf *Submit* abgeschickt haben, wird der Neuantrag an einen Bearbeiter weitergeleitet, in Bezug auf die netzwerkspezifischen Angaben überprüft und in das System aufgenommen. Da der Vorgang nicht vollständig automatisiert ist, sind neue Rechner nicht sofort im DHCP-Service sichtbar.

Objekt löschen

Nicht mehr benutzte PCs bzw. Notebooks sollten unbedingt vom DHCP-Service abgemeldet werden! Durch Klick auf *Objekt löschen* in der seitlichen Menüleiste erhalten Sie eine Liste aller Geräte, für die Sie als administrativer Kontakt angegeben sind, und können diese rechts neben dem Eintrag aus der Datenbank *Löschen*. Auch hier geht die Nachricht zunächst an einen Bearbeiter, der nach einer nochmaligen Kontrolle die endgültige Löschung vornimmt. Daher scheinen abgemeldete Rechner noch für einige Zeit im DHCP-Service auf.

MAC-Adresse ändern

Hier müssen Sie gegebenenfalls (z.B. nach Austausch der Netzwerkkarte) für eine bestimmte IP-Adresse eine neue MAC-Adresse eintragen, um das DHCP-Service weiter nutzen zu können. Bei Klick auf die Funktion *MAC-Adresse ändern* werden alle Geräte aufgelistet, für die Sie als administrativer oder technischer Kontakt eingetragen sind (falls Ihr Rechner nicht angezeigt wird, wenden Sie sich bitte an Ihre/n EDV-Beauftragte/n). Geben Sie die IP-Adresse des betreffenden Rechners und seine neue MAC-Adresse ein und klicken Sie auf *Submit*. Die geänderten Daten werden zu jeder vollen Stunde automatisch in den DHCP-Server übernommen.

Daniel Schirmer

ALL YOU HAVE TO DO IS CALL...
Telefonieren im Internet mit AT43

Im Dezember 2003 hat der ZID der Uni Wien in Kooperation mit der österreichischen Domainregistrierungsstelle nic.at ein Projekt gestartet, das allen Universitätsangehörigen das Telefonieren über Internet ermöglichen soll: Die TeilnehmerInnen erhalten eine so genannte SIP-Rufnummer, unter der sie telefonisch und mittels Instant Messaging erreichbar sind. Die Gesprächsverbindungen im Internet sind kostenlos.

Das Projekt mit dem Namen **AT43** – der sich aus der österreichischen Topleveldomain AT und der Telefonvorwahl 43 für Österreich zusammensetzt – verbindet im wesentlichen drei Technologien: VoIP, ENUM und SIP.

- ***Voice over IP*** (VoIP, wobei IP für *Internet Protocol* steht) bedeutet, dass Sprachnachrichten zuerst in digitale Signale umgewandelt, dann in mehrere Datenpakete aufgeteilt und schließlich über das Internet – anstatt über eine direkte Telefonleitung – zum Empfänger übertragen werden. Im internationalen Bereich läuft bereits ein großer Teil der Telefongespräche über Datenleitungen. Auch an der Uni Wien ist die Telefonie mit der Netzwerk-Infrastruktur längst eng verknüpft: Fast alle Telefonverbindungen zwischen den einzelnen Universitätsstandorten werden mittlerweile über Datenleitungen geführt.

- Relativ neu ist hingegen das ***Electronic Number Mapping*** (ENUM), das die Umsetzung von Telefonnummern in so genannte URIs (*Uniform Resource Identifiers*, z.B. `sip:a1234567@sip.unet.univie.ac.at`) für die Adressierung im Internet regelt. Die technischen Details sind im *RFC 2916: E.164 number and DNS* (`http://ftp.univie.ac.at/netinfo/rfc/rfc2916.txt`) festgehalten. Wesentlich für AnwenderInnen ist, dass sie – Internetzugang vorausgesetzt – unter einer solchen Rufnummer überall auf der Welt erreichbar sind.

- Das dritte Standbein des AT43-Projekts ist das ***Session Initiation Protocol*** (SIP). Über den SIP-Server der Uni Wien erfolgt der Aufbau der Gesprächsverbindung bzw. die ENUM-Abfrage bei Anrufen aus dem öffentlichen Telefonnetz. Technisch Interessierte finden die genaue Definition von SIP unter `http://ftp.univie.ac.at/netinfo/rfc/rfc2543.txt und rfc3261.txt`.

Das Ziel von AT43 ist es, in einem breit angelegten Feldversuch die verschiedenen Komponenten der ENUM-Technologie zu testen (und gegebenenfalls zu verbessern) sowie die Benutzerakzeptanz von Internet-Telefonie und Instant Messaging in Forschung, Lehre und Verwaltung zu evaluieren. Die Universität Wien mit ihrer ausgezeichneten Netzwerk-Infrastruktur und zehntausenden potentiellen AnwenderInnen bietet dafür ideale Voraussetzungen. Die Uni-Angehörigen haben durch AT43 die Möglichkeit, aus erster Hand Erfahrungen mit innovativen Technologien zu sammeln und sich von deren Praxistauglichkeit zu überzeugen. Dies wird zusätzlich dadurch erleichtert, dass den Studierenden und MitarbeiterInnen der Uni Wien verschiedene günstige Breitband-Angebote für den Internetzugang von daheim zur Verfügung stehen (z.B. *uniADSL*; siehe `http://www.univie.ac.at/ZID/internetzugang.html`).

Bitte bedenken Sie aber, dass es sich nicht um ein „fertiges" Service handelt, sondern die nötige Infrastruktur teilweise erst aufgebaut werden muss. Beispielsweise sind Hardware-SIP-Telefone in Österreich derzeit noch kaum erhältlich. Bis sich diese Geräte den Weg in den Fachhandel gebahnt haben, werden daher zwei Modelle in Kommission für nic.at über den Helpdesk des ZID vertrieben. Auch die verschiedenen Server-Komponenten von AT43 wurden in dieser Kombination bisher noch nicht in großem Rahmen eingesetzt. „Geburtswehen" in Form von unerwarteten technischen Komplikationen können daher nicht völlig ausgeschlossen werden.

AT43: Hinter den Kulissen

Für die technische Umsetzung von AT43 wurden bewährte Komponenten mit einigen Neuentwicklungen zu einer leistungsfähigen Plattform für mobile Echtzeitkommunikation via Internet verknüpft. Besonderes Augenmerk wurde darauf gelegt, ein System zu schaffen, das nicht nur auf die Gegebenheiten der Uni Wien zugeschnitten ist, sondern mit geringfügigen Anpassungen – z.B. in der Schnittstelle zur Benutzerdatenbank – auch in verschiedenen anderen Netzwerkumgebungen eingesetzt werden kann.

Interessant ist dabei vor allem die enge Verbindung mit der ENUM-Technologie, die im Rahmen von AT43 einen ihrer ersten Produktionseinsätze weltweit erlebt und hier in Bezug auf Stabilität und Skalierbarkeit einem Härtetest unterzogen werden soll. Von nic.at wurde ein entsprechendes ENUM-Registrierungssystem entwickelt, und auch die generische (d.h. vom jeweiligen Teilnehmervertrag unabhängige) Gateway-Funktionalität zwischen öffentlichem Telefonnetz und SIP-Server kann als echte Innovation gelten. Die Teilnehmer-Authentifizierung wird über die Oracle-Benutzerdatenbank und den Radius-Server der Uni Wien abgewickelt. Serverseitig kommen darüber hinaus ein SIP-Proxy (iptel.org), ein ENUM-DNS-Server (PowerDNS), ein Voice-Gateway (Cisco 5300) und ein NAT-Reflector (Jasomi) zum Einsatz. Die Voiceboxes werden mit Hilfe der Linux-Nebenstellenanlage Asterisk PBX (Open Source) realisiert.

Kosten

- Die An- und Abmeldung für AT43 ist kostenlos.
- Bei Gesprächen zwischen AT43-TeilnehmerInnen, die unmittelbar per VoIP erreichbar sind, entstehen (von allfälligen Verbindungskosten des Internetzugangs abgesehen) keinerlei Gebühren.
- AT43-TeilnehmerInnen können selbstverständlich durch direktes Wählen ihrer SIP-Rufnummer auch aus dem öffentlichen Telefonnetz angerufen werden. Der Anrufer bezahlt dabei die Gesprächsgebühren für ein Telefonat mit der Uni Wien – unabhängig davon, wo sich der angerufene Teilnehmer befindet.
- Anrufe von AT43-TeilnehmerInnen in das öffentliche Telefonnetz sind nur dann möglich, wenn ein Vertrag mit einem Call-by-Call-Provider besteht (siehe unten). Als Ausgangspunkt der Gespräche gilt dabei immer die Uni Wien, egal wo sich der Anrufer tatsächlich aufhält.

Die AT43-Services stehen nicht nur aus dem Universitätsdatennetz, sondern aus dem gesamten Internet zur Verfügung (sofern nicht lokale Einschränkungen – z.B. Firewalls – eine Verbindung zur Uni Wien verhindern) und sind daher insbesondere auch für jene Universitätsangehörigen interessant, die sich vorübergehend im Ausland aufhalten.

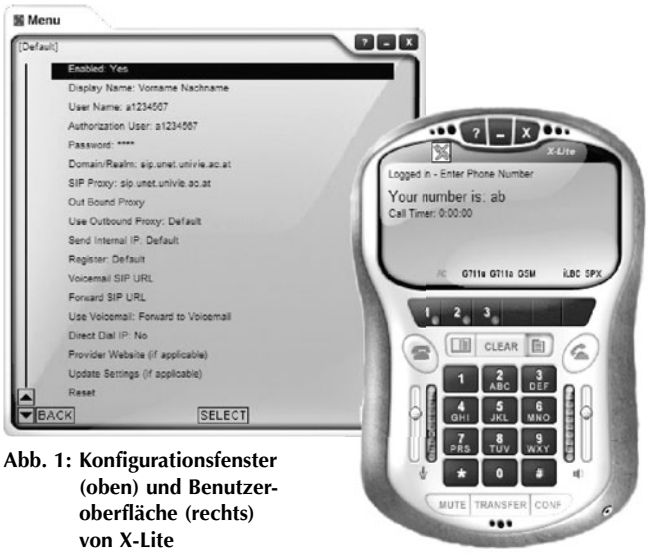

Abb. 1: Konfigurationsfenster (oben) und Benutzeroberfläche (rechts) von X-Lite

Abb. 2: Cisco 7960 (links), Grandstream ATA-286 (unten)

Voraussetzungen

Die Teilnahme an AT43 ist für alle Unet- und Mailbox-BenutzerInnen kostenlos möglich. Die Unet- bzw. Mailbox-UserID wird für die Erstanmeldung und in der Folge für jedes Login bei AT43 benötigt – z.B. wenn Sie Ihre AT43-Einstellungen ändern möchten. Bitte beachten Sie, dass AT43 an diese UserID gekoppelt ist und Sie daher bei Ablauf Ihrer Unet- bzw. Mailbox-UserID auch Ihre SIP-Rufnummer verlieren (keine Rufnummernmitnahme!). Um AT43 sinnvoll verwenden zu können, müssen außerdem noch einige weitere Voraussetzungen erfüllt sein:

Breitband-Internetzugang

Theoretisch ist das Telefonieren via Internet auch über eine Modemverbindung möglich; die geringe Übertragungsgeschwindigkeit macht sich jedoch bei der Sprachqualität unangenehm bemerkbar. Man sollte daher über einen Breitband-Internetzugang verfügen – d.h. entweder ans Uni-Datennetz bzw. ein anderes LAN angeschlossen sein oder (falls man von daheim telefonieren will) eine Kabel- oder DSL-Anbindung sein Eigen nennen.

SIP-Telefon

Für Telefonate via Internet benötigt man ein VoIP-taugliches Endgerät, ein so genanntes SIP-Telefon. Dafür kann man entweder Software-Klienten (Programme, die am PC installiert werden) oder Hardware-Klienten (spezielle Apparate) einsetzen.

- Sofern Sie einen Rechner mit Mikrofon und Lautsprecher (oder ein Headset) besitzen, empfiehlt sich für die ersten Experimente mit AT43 auf jeden Fall ein Software-SIP-Telefon – z.B. das für MS-Windows und MacOS X kostenlos erhältliche X-Lite (siehe Abb. 1; Download unter `http://www.xten.com/`). Auch der MS-Windows Messenger ist als SIP-Telefon verwendbar.
- Wenn man häufig über Internet telefoniert, ist die Anschaffung eines Hardware-SIP-Telefons überlegenswert. Im Rahmen von AT43 werden derzeit zwei Geräte unterstützt: Das Grandstream ATA-286 – ein so genannter *Analog Telephone Adaptor*, mit dessen Hilfe ein Standardtelefon als SIP-Telefon betrieben werden kann – und das Cisco 7960 (siehe Abb. 2). Da Hardware-SIP-Telefone in Österreich schwer erhältlich sind, können diese beiden Modelle bis auf weiteres beim Helpdesk des ZID gegen Barzahlung erstanden werden: Das Grandstream ATA-286 kostet derzeit € 89,–, das Cisco 7960 € 385,–.

Call-by-Call-Provider

AT43 ermöglicht zwar kostenlose Telefonate im Internet, nicht aber kostenlose Gespräche ins öffentliche Telefonnetz

Abb. 3: AT43 – Startseite

(ausgenommen sind 0800-Nummern in Österreich und in den USA). Will man auch Anrufe ins öffentliche Netz tätigen, muss man daher einen Vertrag mit einem Call-by-Call-Provider abschließen (derzeit stehen fünf zur Wahl; siehe `http://www.at43.at/`), der die dabei anfallenden Gesprächsgebühren zu seinen jeweiligen Tarifen verrechnet.

Wie verwendet man AT43?

An-/Abmeldung

Die Erstanmeldung erfolgt online unter `http://www.at43.at/` mit der Unet- bzw. Mailbox-UserID und dem dazugehörigen Passwort. Dabei werden automatisch und kostenlos eine persönliche SIP-Rufnummer, eine Voicebox und ein ENUM-Eintrag mit dem entsprechenden URI eingerichtet. Auf derselben Webseite kann man die Teilnahme an AT43 jederzeit kündigen.

SIP-Rufnummern

Die Rufnummern von AT43-TeilnehmerInnen haben die Form 0 59966 *y xxxxx*. Bei Studierenden ist *y*=5 und *xxxxx* eine zufällig vergebene Nummer (z.B. 0 59966 5 12345); bei Uni-MitarbeiterInnen ist *y*=4 und *xxxxx* die jeweilige Uni-Durchwahl. Ruft man aus dem Ausland an, muss statt der ersten 0 die österreichische Vorwahl 0043 gewählt werden (z.B. 0043 59966 5 12345).

Die neu erworbene SIP-Rufnummer kann man bei der AT43-Anmeldung automatisch in das Online-Personalverzeichnis der Universität Wien bzw. in das Unet-Adressbuch aufnehmen lassen. In beiden Fällen handelt es sich jedoch um freiwillige Einträge – ein vollständiges Verzeichnis aller AT43-TeilnehmerInnen ist derzeit nicht verfügbar.

Konfiguration

Konfigurationsanleitungen für jene SIP-Telefone, für die im Rahmen von AT43 Support angeboten wird, finden Sie unter `http://www.at43.at/de/quickstart/`. Nach der Konfiguration sollten Sie unter der Service-Nummer 8001 einen so genannten Echotest durchführen: Dabei wird nach dem Rufaufbau zunächst eine erklärende Ansage abgespielt. Anschließend wird der eigentliche Echotest gestartet, bei dem das vom SIP-Telefon eintreffende Audiosignal wieder an dasselbe Telefon zurück übertragen wird. Mit diesem Echotest stellen Sie einerseits erstmals eine Verbindung über AT43 her, was für Ihre Registrierung im System unbedingt erforderlich ist; andererseits können Sie damit auch die Latenz und Audioqualität der Verbindung überprüfen.

Voicebox

Bei der AT43-Anmeldung wird eine kostenlose Voicebox eingerichtet, an die alle nicht entgegengenommenen Anrufe umgeleitet werden. Die hinterlassenen Nachrichten werden dem Teilnehmer als Audiodateien (`.wav`-Dateien) per eMail zugestellt. Die Voicebox kann aber auch via Internet bzw. – sofern zuvor ein PIN-Code konfiguriert wurde – aus dem öffentlichen Telefonnetz abgerufen und konfiguriert werden. Einzelheiten dazu können Sie auf der Webseite `http://www.at43.at/` unter *Dokumentation* nachlesen.

Rat & Hilfe

Ausführliche Informationen zu AT43, die Online-Anmeldemaske, die Anmeldeformulare der Call-by-Call-Provider, Links zu Herstellern von SIP-Telefonen sowie Konfigurations- und Bedienungsanleitungen finden Sie im WWW unter **`http://www.at43.at/`** (siehe Abb. 3). Bitte haben Sie Verständnis dafür, dass derzeit nur für einige SIP-Telefone Support angeboten werden kann. Bei Problemen mit den unterstützten Produkten wenden Sie sich an den Helpdesk des ZID (eMail: `helpdesk.zid@univie.ac.at`; Tel.: 4277-14060).

Elisabeth Zoppoth ■

Die Macht der Farben

Optimale Farbgestaltung im WWW

759. Die Menschen empfinden im allgemeinen eine große Freude an der Farbe. Das Auge bedarf ihrer, wie es des Lichtes bedarf. (...)

Sehen Sie manchmal rot – oder gar schwarz? Werden Sie grün vor Neid? Wird Ihnen die Sache schön langsam zu bunt? Es gibt eine ganze Reihe von Beispielen, wie wir unsere Gefühle anhand von Farben beschreiben. Haben Sie sich schon einmal überlegt, was mit solchen Sätzen ausgedrückt wird? Wenn nicht, dann haben Sie vermutlich auch noch keinen Gedanken daran verschwendet, warum für eine Webseite ein roter oder grauer Hintergrund verwendet wurde oder warum einzelne Elemente davon orange oder grün gefärbt sind.

Dabei sind wir alle tagtäglich mit Farben und ihrer geheimen Macht konfrontiert. Farben beeinflussen unser Denken, unser Handeln und unser Empfinden. Beispielsweise spürt man Kälte in einem blau-grün ausgemalten Raum angeblich bereits bei ca. 15° Celsius, während dies in einem orangefarbenen Raum erst bei 2° Celsius der Fall sein soll. Wenn man der folgenden Geschichte (siehe `http://www.farbenundleben.de/koffer.htm`) Glauben schenken darf, wirkt die Farbgebung sogar auf das Gewicht von Gegenständen:

Ein amerikanischer Transportunternehmer beobachtete, dass seine Arbeiter an manchen Tagen deutlich früher als sonst Ermüdungserscheinungen zeigten. Als er dem nachging, stellte er fest, dass an diesen Tagen ausschließlich dunkle Kisten getragen wurden – die zu seinem großen Erstaunen jedoch exakt gleich schwer waren wie helle Kisten, die an anderen Tagen transportiert wurden. Die amerikanischen Psychologen Warden und Flynn untersuchten dieses Phänomen und ließen das Gewicht verschiedenfarbiger, aber gleich schwerer Packungen schätzen. Die Ausgangsrelation war eine weiße, 3 Pfund schwere Packung. Das verblüffende Ergebnis: Gelbe Packungen wurden auf 3,5 Pfund geschätzt, grüne Packungen auf 4,1 Pfund, blaue auf 4,7 Pfund, graue auf 4,8 Pfund und rote auf 4,9 Pfund. Schwarze Packungen wurden als fast doppelt so schwer eingeschätzt wie weiße, nämlich auf 5,8 Pfund.

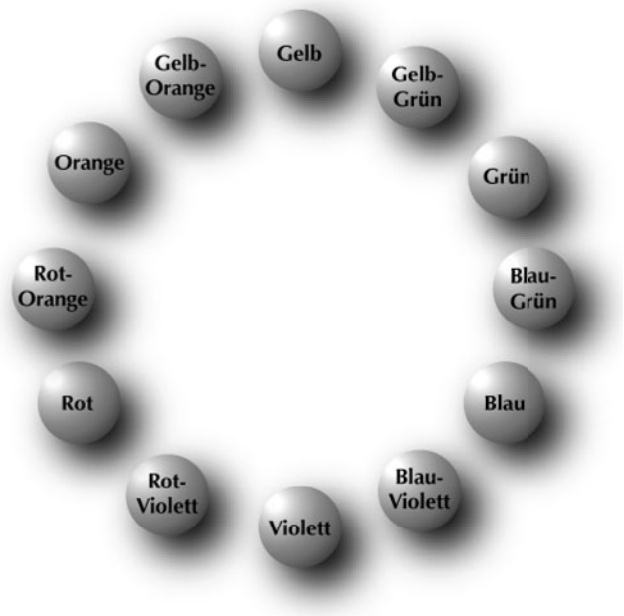

Abb. 1: Der Farbkreis nach Johannes Itten

Diese Ergebnisse wurden von der Industrie natürlich begeistert und erfolgreich aufgegriffen: Da eine dunkle Verpackung selbst bei gleicher Größe und gleichem Gewicht einen konzentrierteren, massiveren und gewichtigeren Inhalt vermittelt, konnten doppelte Böden und Mogelpackungen einfach durch entsprechende Farbgebung vermieden werden.

Ich sehe was, was du nicht siehst

110. (...) Sie nennen den Himmel rosenfarb und die Rose blau, oder umgekehrt. Nun fragt sich: sehen sie beides blau, oder beides rosenfarb? sehen sie das Grün orange, oder das Orange grün?

Farbempfindungen werden in unserem Gehirn hervorgerufen, wenn bestimmte Wellenlängen des Lichts auf die Sinneszellen des Auges treffen. Farben sind sozusagen ein Erfahrungswert, mit der Konsequenz, dass wir sie niemals emotionslos bzw. objektiv wahrnehmen. Diesen Umstand gilt es zu beachten – gerade auch bei der Farbgestaltung von Webseiten. Professionelle WebdesignerInnen wissen, dass ihr persönlicher Geschmack selten gefragt ist: Soll die Farbgebung glaubwürdig wirken, muss sie in erster Linie die Thematik der Seite, die Vorlieben der Zielgruppe sowie die Wünsche und Vorgaben des Eigentümers (z.B. *Corporate Identity*) widerspiegeln.

Abgesehen davon sollte man sich nicht darauf verlassen, dass alle BetrachterInnen der Webseite die gewählten Farben ebenso wahrnehmen wie man selbst. Beispielsweise macht die verbreitete „Rot-Grün-Schwäche" es den Betroffenen nahezu unmöglich, grüne Schrift auf rotem Hintergrund (und vice versa) zu entziffern. Auch Anweisungen wie *„Klicken Sie auf den roten Pfeil"* sind für diese Menschen wenig hilfreich. Farbkombinationen, die für Farbenblinde problematisch sind, sollten daher nach Möglichkeit vermieden werden. Eine empfehlenswerte Webseite zum Thema

Farbfehlsichtigkeit mit Links zu Simulationsprogrammen ist unter `http://www.barrierefreies-webdesign.de/knowhow/behinderung/sehbehinderung.php` zu finden.

Farbsymbolik

829. Gelb und Grün hat immer etwas Gemein-Heiteres, Blau und Grün aber immer etwas Gemein-Widerliches, deswegen unsre guten Vorfahren diese letzte Zusammenstellung auch Narrenfarbe genannt haben.

Eine große Rolle bei der Auswahl von Farben und Farbkombinationen spielt die Farbsymbolik. Beispielsweise verbindet man mit der Farbe Rot oft Liebe, Energie, Entschlossenheit, aber auch Zorn, Hass und Gefahr. Insgesamt eignet sich Rot als kraftvolle und dominante Farbe jedenfalls bestens, um Aufmerksamkeit zu erregen. Dabei darf jedoch nicht vergessen werden, dass Rot nicht gleich Rot ist, sondern jeder Mensch bei der Frage *„Woran denken Sie bei der Farbe Rot?“* einen ganz speziellen Rotton vor Augen hat. Die der Farbe zugeordneten Eigenschaften resultieren daher zu einem guten Teil aus seiner eigenen, von persönlichen Erfahrungen geprägten Wahrnehmung. Darüber hinaus ist die Farbsymbolik auch sehr stark kulturell bedingt – beispielsweise wird die Farbe Weiß in unserem Kulturkreis mit Unschuld und Reinheit in Verbindung gebracht, in China steht sie jedoch für Tod und Trauer.

Unter diesem Blickwinkel ist auch die folgende Auflistung von Farben mit ihren spezifischen Eigenschaften zu sehen:

Farbkombinationen

845. Man ist freilich bei dem Gebrauch der ganzen Farben sehr eingeschränkt, dahingegen die beschmutzten, getöteten sogenannten Modefarben unendlich viele abweichende Grade und Schattierungen zeigen, wovon die meisten nicht ohne Anmut sind.

Nachdem Sie eine zum Inhalt passende Hintergrundfarbe für Ihre Webseite gefunden haben, stellt sich die Frage: Welche Farben passen zum Hintergrund?

Mit dem Thema Farben und den verschiedenen Möglichkeiten, sie zu ordnen, hat sich eine ganze Reihe berühmter Persönlichkeiten beschäftigt. Für die nachfolgenden Beispiele wurde der Farbkreis nach Johannes Itten als Ausgangspunkt herangezogen (siehe Abb. 1 auf Seite 35). Bevor Sie sich auf die Suche nach passenden Farben machen, ist aber zu klären, ob starke Kontraste oder ein harmonisches Erscheinungsbild gewünscht sind.

Farbkontraste

Im WWW sollte vor allem die Kombination von Hintergrund und Text kontrastreich gestaltet werden, damit die Textpassagen ohne Schwierigkeiten gelesen werden können.

- Ein Maximum an Kontrast bieten die **Komplementärfarben** (z.B. Orange und Blau), die sich im Farbkreis direkt gegenüber stehen. Diese Farbkombinationen wirken bei zu starkem Gebrauch jedoch überstimulierend und lassen das Auge rasch ermüden.

Farbe	positive Eigenschaften	negative Eigenschaften
Gelb	die Farbe der Sonne, Wärme, Helligkeit, Glück, Gold, Optimismus	Rachsucht, Egoismus, Geiz, Neid
Orange	Unkonventionalität, Dynamik, Wärme, Spaß, Aktivität	Leichtlebigkeit, Aufdringlichkeit, wirkt billig
Rosa	Zartheit, Baby, Romantik, Weichheit	wirkt kitschig
Rot	Liebe, Kraft, Temperament, Energie, Entschlossenheit	Gefahr, Blut, Zorn, Hass
Braun	Mutter Erde, Behaglichkeit	Langeweile, Vergänglichkeit
Grün	Natur, Vegetation, Frische, Ruhe, Entspannung, Harmonie, Hoffnung	Gift, Neid
Blau	die Farbe von Himmel und Meer, Weite, Ruhe, Vertrauen, Seriosität	Nachlässigkeit, Melancholie, Kühle, Passivität
Violett	Magie, Geheimnis, Kunst, Nostalgie, Frömmigkeit, Opferbereitschaft	Arroganz, Eitelkeit, Dekadenz
Silber/Grau	Eleganz, Sachlichkeit, Neutralität, Technologie	Langeweile, Eintönigkeit, Unsicherheit
Schwarz	Eleganz, Würde, modern, sachlich	Nacht, Geheimnis, Tod, Trauer, Undurchdringlichkeit
Weiß	die Farbe von Eis und Schnee, Reinheit, Klarheit, Ordnung, Vollkommenheit, Unschuld	Unnahbarkeit

- Einen etwas abgemilderten Kontrast erhalten Sie, wenn Sie anstelle der Komplementärfarben die **Teilkomplementärfarben** (z.B. Orange und Blau-Violett) heranziehen, die sich jeweils links und rechts neben der Komplementärfarbe befinden.

- Eine weitere Möglichkeit sind **Bunt-Unbunt-Kontraste**: Dabei werden Farben mit unterschiedlicher Leuchtkraft kombiniert – z.B. leuchtendes Rot mit Grau (die Leuchtkraft einer Farbe sinkt mit einem steigenden Grauanteil). Für Bunt-Unbunt-Kontraste können auch die Farben Schwarz und Weiß verwendet werden.

Farbharmonien

Wenn man eine ruhige und angenehme Atmosphäre schaffen möchte, sollte man harmonierende Farben verwenden.

- Für Farbharmonien eignen sich beispielsweise **analoge Farben** (z.B. Gelb mit Gelb-Grün oder Gelb-Orange), die im Farbkreis direkt nebeneinander zu finden sind. Diese Farben sind einander sehr ähnlich und daher in der Regel einfach zu kombinieren.

- Sollen drei oder mehr verschiedene Farben harmonieren, so empfehlen sich die so genannten **Farbklänge**. Diese haben die Eigenschaft, dass ihr Abstand zueinander im Farbkreis gleich ist. Einen Farbklang erhält man, indem man beispielsweise ein gleichseitiges Dreieck (Farbdreiklang) oder ein Quadrat (Farbvierklang) über den Farbkreis legt. Die Eckpunkte der Flächen zeigen auf die jeweiligen Farbtöne eines Farbklangs.

- Sehr beliebt ist auch die Kombination einer **Volltonfarbe mit Abstufungen davon**, also mit aufgehellten bzw. abgedunkelten Farbwerten.

Webfarben – Ja oder Nein?

593. Den Körpern werden auf mancherlei Weise die Farben entzogen, sie mögen dieselben von Natur besitzen, oder wir mögen ihnen solche mitgeteilt haben. Wir sind daher imstande, ihnen zu unserm Vorteil zweckmäßig die Farbe zu nehmen, aber sie entflieht auch oft zu unserm Nachteil gegen unsern Willen.

Bevor Sie nun die Farben für Ihre Webseite endgültig auswählen, müssen Sie sich noch darüber klar werden, ob Sie auf eine einheitliche Darstellung der Farben auf verschiedenen Hardware-, Betriebssystem- und Browser-Plattformen Wert legen. Falls Ihnen dies ein Anliegen ist, sollten Sie sich auf die so genannten Webfarben beschränken.

Farben, die auf einem Bildschirm dargestellt werden sollen, werden im RGB-Farbmodus festgelegt. Dieser Modus beschreibt Farben anhand ihrer Rot-, Grün- und Blauanteile,

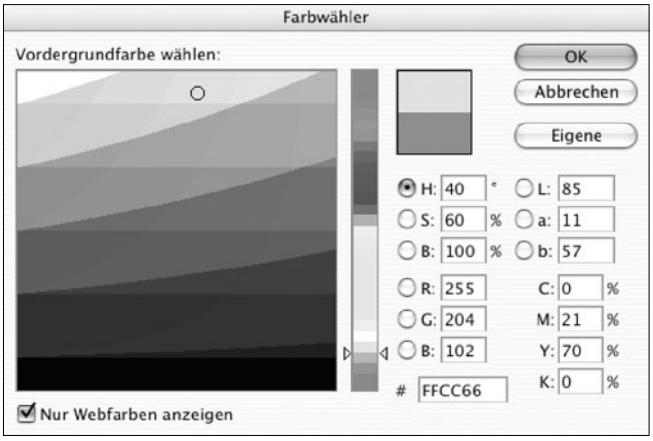

Abb. 2: Der *Farbwähler* von Adobe Photoshop 7

die jeweils einen Wert zwischen 0 und 255 annehmen können (Rot hat z.B. den RGB-Wert 255.0.0 – maximaler Rotanteil, kein Grün- und kein Blauanteil). Im RGB-Modus können somit insgesamt 256^3, also über 16,7 Millionen Farben definiert werden.

Falls Sie einen modernen Rechner, einen leistungsfähigen Monitor und ein entsprechendes Grafikprogramm Ihr Eigen nennen, haben Sie nun also die Qual der Wahl, unter Millionen von Farben eine passende zu finden. Aber selbst wenn Sie diese Herausforderung meistern, ist die Gefahr groß, dass die gewählten Farben auf anderen Rechnern völlig anders wirken. Besonders augenfällig ist dieser Effekt bei älteren Geräten, die mit 8-Bit-Farbtiefe arbeiten und daher nur 256 Farben darstellen können.

Aus diesem Grund wurde seinerzeit von Netscape die so genannte Web-Farbpalette eingeführt. Diese besteht aus 216 Farben, die theoretisch auf allen Farbbildschirmen und bei allen Betriebssystemen gleich dargestellt werden. Die Erfahrung zeigt allerdings, dass dies selbst bei Webfarben nicht immer der Fall ist. Auch die Tatsache, dass alle neueren Computersysteme bereits mit 32-Bit-Farbtiefe arbeiten, lässt die Relevanz der Webfarben verblassen. Dennoch bieten sie eine gewisse Orientierungshilfe innerhalb der Fülle verfügbarer RGB-Farben. (Puristen finden sogar mit den 16 im HTML-Standard definierten Farbnamen das Auslangen, die von jedem VGA-Bildschirm angezeigt werden können.)

Letztendlich bleibt es Ihnen überlassen, ob Sie mit Webfarben arbeiten oder nicht. Für den Fall, dass Sie sich dazu durchringen, bieten Ihnen die meisten Grafikprogramme auch die entsprechende Farbpalette an. Bei Adobe Photoshop können Sie z.B. im Farbwähler durch Anklicken der Option *Nur Webfarben anzeigen* die Farbauswahl auf die 216 „websicheren" Farben beschränken (siehe Abb. 2).

Als zusätzliche Hilfe zeigt Adobe Photoshop neben den RGB- und anderen Farbwerten auch gleich den sechsstelligen Hexadezimalwert der ausgewählten Farbe an (z.B. `#FFCC66`), der im HTML-Dokument bzw. im Style Sheet angegeben werden muss.

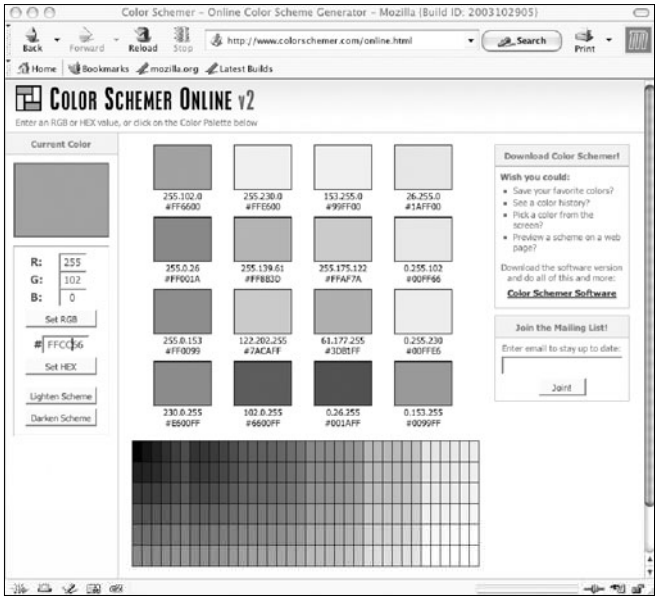

Abb. 3: Der *Color Schemer Online* zeigt passende Farben an

Links

844. Inwiefern der trübe nordische Himmel die Farben nach und nach vertrieben hat, ließe sich vielleicht auch noch untersuchen.

- Wenn Sie bei der Auswahl von Hintergrund- und Textfarbe für Ihre Webseite unsicher sind, finden Sie unter dem URL `http://selfhtml.teamone.de/helferlein/farben.htm` eine sehr bequeme Möglichkeit, verschiedene Kombinationen online zu testen. Dort können Sie auch die RGB-Werte von Farben in Hexadezimalwerte umrechnen lassen.

- Eine Übersicht über die 216 Webfarben mit ihren entsprechenden Hexadezimalwerten erhalten Sie im WWW beispielsweise unter `http://selfhtml.teamone.de/diverses/anzeige/farbpalette_216.htm`.

- Wenn Sie Kombinationen von Webfarben ausprobieren möchten, empfiehlt sich z.B. die Webseite von Visibone (`http://www.visibone.com/colorlab/`).

- Eine weitere Online-Hilfe zur Farbauswahl ist unter `http://www.colorschemer.com/online.html` zu finden (siehe Abb. 3).

- Zum Thema Farbenlehre steht im WWW eine Reihe interessanter Beiträge in deutscher Sprache zur Verfügung – beispielsweise
  `http://www.metacolor.de/`
  `http://www.farbenlehre.com/`
  `http://www.farbenundleben.de/`

Eva & Michel Birnbacher ■

Die kursiv gedruckten, nummerierten Zitate stammen aus Johann Wolfgang Goethe's „Zur Farbenlehre. Didaktischer Teil" (dtv, München 1963).

„Gerda" ist stärker geworden

Vor mehr als zwei Jahren wurde für PHP-, MySQL- und PostgreSQL-Applikationen der Server GERDA.UNIVIE.AC.AT in Betrieb genommen (siehe *Comment 01/3*, Seite 22 bzw. `http://www.univie.ac.at/comment/01-3/013_22.html`). Seither hat sich das *General Repository for Database Applications* – kurz: „die Gerda" – zu einem Fixpunkt im Service-Biotop des ZID entwickelt: Aufgrund der ständig steigenden Beliebtheit der Skriptsprache PHP (und der damit einhergehenden großen Anzahl von fertigen Applikationen) tummeln sich hier mittlerweile zahlreiche Webforen, Content Management-Systeme und Anmeldesysteme für diverse Lehrveranstaltungen – auch wenn man es manchen davon nicht ansieht, weil sie mit eigenen Domains (über virtuelle Hosts) oder vom Server WWW.UNIVIE.AC.AT aus (über eine Weiterleitung) aufgerufen werden.

Obwohl anfangs ein PC „Marke Eigenbau" ausreichend erschien, wurde bald deutlich, dass die ursprüngliche Hardware (1 GHz-Pentium III, 512 MB RAM und 40 GB IDE-Plattenspeicher) für die rasch wachsenden Anforderungen zu schwach ausgelegt war. Insbesondere die Lehrveranstaltungs-Anmeldesysteme stellten den Server immer zu Semesterbeginn vor eine schwere Prüfung: Schließlich sollten alle Anfragen korrekt und möglichst schnell bearbeitet werden, was aber in dieser Form – sehr viele Requests auf einmal – beinahe einer *Denial of Service*-Attacke gleichkam, da der MySQL-Datenbankserver nur eine beschränkte Anzahl an gleichzeitigen Verbindungen zulassen konnte. Daher wurde im September 2003 entschieden, das Problem mit Hilfe einer besseren und stärkeren Hardware-Plattform zu entschärfen. Zum Zuge kam ein DL380 G3-Server von HP/Compaq, ausgestattet mit zwei 2,4 GHz-Xeon-Prozessoren, 4 GB RAM und 140 GB SCSI-Platten – im Vergleich zur ursprünglichen Hardware ein großer Sprung. Gleichzeitig wurde die schon etwas betagte Version 3.x von MySQL durch MySQL 4.x ersetzt. Als Betriebssystem kommt weiterhin FreeBSD zum Einsatz, das sich für diesen Verwendungszweck hervorragend bewährt hat.

„Die neue Gerda" wurde zwar aufgrund von Lieferschwierigkeiten nicht rechtzeitig zum Beginn des Wintersemesters 2003 fertig; eine Woche danach klappte die Umstellung aber innerhalb einer Stunde problemlos. Auch wenn der Server nun gegen zukünftige Anstürme etwas besser gewappnet ist (die erste große Lehrveranstaltungs-Anmeldung im Sommersemester 2004 konnte jedenfalls problemlos abgewickelt werden), ersuchen wir alle BetreuerInnen von „Gerda-Applikationen", Skripts mit vorhersehbaren Belastungsspitzen nur nach Rücksprache mit den Systemadministratoren in Betrieb zu nehmen. Wenden Sie sich dazu bitte an die eMail-Adresse `gerda.zid@univie.ac.at`.

Lukas Ertl

KURSE BIS JULI 2004

Kurskalender

Auf den folgenden Seiten finden Sie detaillierte Beschreibungen zu den von März bis Juli 2004 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** am Helpdesk (Service- und Beratungszentrum) und die Kursterminblätter in den Formularspendern vor den PC-Räumen im NIG bzw. am Helpdesk. Alle Informationen zu den Kursen finden Sie im WWW unter **`http://data.univie.ac.at/kurs/bin/kursang.pl`**; die jeweils aktuellen Kursbelegungen können unter `http://data.univie.ac.at/kurs/bin/kursall.pl` abgerufen werden.

Anmeldungen

Teilnahmeberechtigt sind Studierende und UniversitätsmitarbeiterInnen. Als solche gelten in diesem Zusammenhang 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. Für diese TeilnehmerInnen ist die Anmeldung erst nach dem Ende der Anmeldefrist möglich; es gilt der Tarif *Externe*. Bei Kursen mit beschränkter Teilnehmerzahl ist eine **Anmeldung am Helpdesk (Service- und Beratungszentrum) des ZID** erforderlich (NIG, Stg. II, 1. Stock; Öffnungszeiten: **Mo – Fr 9:00 – 18:00 Uhr**). Kostenpflichtige Kurse sind bei der Anmeldung bar zu bezahlen; Studierende müssen dabei ihren **Studienausweis** vorweisen.

Absagen/Rücktritte

Wenn mit Ende der Anmeldefrist zu wenige Anmeldungen vorliegen, kann der Kurs abgesagt werden. Die angemeldeten TeilnehmerInnen werden nach Möglichkeit rechtzeitig verständigt. Falls ein Kurs abgesagt wird oder jemand sich innerhalb der Anmeldefrist abmeldet, kann die bezahlte Kursgebühr innerhalb eines Jahres (ab Kurstermin) zurückgefordert werden. **TeilnehmerInnen, die sich erst nach Anmeldeschluss des betreffenden Kurses abmelden, müssen 10% der Kursgebühr 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 – Einführung

Zielgruppe: NeueinsteigerInnen im Bereich Textverarbeitung, die mit Word ihre Texte (Briefe, Seminararbeiten, ...) erfassen wollen
Voraussetzung: EDV-Grundkenntnisse bzw. Kurs *Arbeiten mit MS-Windows – Einführung*
Dauer: 6 Stunden (1 Tag)
Inhalt: Word-Arbeitsoberfläche / Erstes Dokument / Formatierungsmöglichkeiten / Seitengestaltung / Drucken
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
19.05.2004	09:00 – 16:00 h	19.04.04 – 07.05.04

MS-Word für Windows – Fortsetzung

Zielgruppe: PC-BenutzerInnen, 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 B
2. Termin: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
20.04.2004	09:00 – 16:00 h	15.03.04 – 09.04.04
09.06.2004	09:00 – 16:00 h	10.05.04 – 28.05.04

Wissenschaftliches Arbeiten mit 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: Zentral- und Filialdokument / Verzeichnisse erstellen / Fußnoten einfügen und bearbeiten / Kopf- & Fußzeilen einfügen und gestalten / Excel-Tabellen einfügen
Ort: 1. Termin: Kursraum B
2. Termin: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
21.04.2004	09:00 – 16:00 h	15.03.04 – 09.04.04
30.06.2004	09:00 – 16:00 h	01.06.04 – 18.06.04

MS-Word für Windows im Büroeinsatz

Zielgruppe: Word-erfahrene AnwenderInnen, 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 A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
16.06.2004	09:00 – 16:00 h	17.05.04 – 04.06.04

Tabellenkalkulation

MS-Excel – Einführung

Zielgruppe: NeueinsteigerInnen 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 MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
04.05.2004	09:00 – 16:00 h	29.03.04 – 23.04.04

MS-Excel – Fortsetzung

Zielgruppe: Erfahrene Excel-AnwenderInnen, welche 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 MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
10.05.2004	09:00 – 16:00 h	05.04.04 – 30.04.04

MS-Excel – Das Werkzeug zur Datenanalyse

Zielgruppe: Excel-erfahrene PC-BenutzerInnen, welche 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 / Automatisieren von Aufgaben
Ort: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
28.06.2004	09:00 – 16:00 h	01.06.04 – 18.06.04

Datenbanken

MS-Access für Windows – Einführung

Zielgruppe: NeueinsteigerInnen, 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: Kursraum B
Preis: € 60,– für Studierende
€ 120,– für MitarbeiterInnen
€ 180,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
29.03. – 30.03.04	09:00 – 16:00 h	23.02.04 – 19.03.04
13.05. – 14.05.04	09:00 – 16:00 h	05.04.04 – 30.04.04

MS-Access für Windows – Fortsetzung

Zielgruppe: PC-BenutzerInnen, 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 & -pflege / Tabellen einbinden / Abfragen / Automatisieren von Arbeitsabläufen mittels Makroprogrammierung
Ort: Kursraum B
Preis: € 60,– für Studierende
€ 120,– für MitarbeiterInnen
€ 180,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
24.06. – 25.06.04	09:00 – 16:00 h	24.05.04 – 11.06.04

Diverse Applikationen

SPSS – Einführung

Zielgruppe: PC-BenutzerInnen, 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: Kursraum A
Preis: € 60,– für Studierende
€ 120,– für MitarbeiterInnen
€ 180,– für Externe
Teilnehmer: maximal 12

Termin	Zeit	Anmeldefrist
21.06. – 22.06.04	09:00 – 16:00 h	24.05.04 – 11.06.04

Adobe Photoshop – Einführung

Zielgruppe: PC-BenutzerInnen, 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 A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
27.05.2004	09:00 – 16:00 h	26.04.04 – 14.05.04

Adobe Photoshop für Webgrafiken

Zielgruppe: BenutzerInnen, 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 MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
28.05.2004	09:00 – 16:00 h	26.04.04 – 14.05.04

MS-PowerPoint – Einführung

Zielgruppe: PC-Benutzer, die professionelle 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 / Die Folie / Der Master / Erstellung von Folien / Zeichnungsobjekte / Standard-Animationen / Präsentation und Druck
Ort: Kursraum A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
18.05.2004	09:00 – 16:00 h	19.04.04 – 07.05.04

MS-PowerPoint – Fortsetzung

Zielgruppe: AnwenderInnen, die ihre PowerPoint-Kenntnisse vertiefen 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 A
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
15.06.2004	09:00 – 16:00 h	17.05.04 – 04.06.04

Adobe Acrobat

Zielgruppe: PC-BenutzerInnen, 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 & Komponenten / Erstellen und Bearbeiten von PDF-Dateien
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
05.05.2004	09:00 – 16:00 h	29.03.04 – 23.04.04

UNIX-ANWENDER

Einführung in die Anwendung von Unix

Zielgruppe: AnwenderInnen, die auf Unix-Systemen arbeiten möchten
Voraussetzung: EDV-Grundkenntnisse
Dauer: ca. 12 Stunden (3 Halbtage)
Inhalt: Betriebssystem Unix / Einfache Befehle / Dateisystem / Editor / Shell / Prozesse
Ort: Kursraum A
Preis: € 30,– für Studierende & MitarbeiterInnen
€ 45,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
21.04. – 23.04.04	12:00 – 16:00 h	01.03.04 – 02.04.04

INTERNET

Einführung in das Erstellen von Webpages – Teil 1

Zielgruppe: Anwender, die Webpages erstellen wollen
Voraussetzung: EDV-Grundkenntnisse
Dauer: ca. 2,5 Stunden
Inhalt: Grundlagen / Begriffserklärung / Grafiken / Struktur / Kopieren auf den Webserver
Ort: Hörsaal 3 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt;
keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
26.03.2004	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 (NIG)
Preis: kostenlos
Teilnehmer: unbeschränkt;
keine Anmeldung erforderlich

Termin	Zeit	Anmeldefrist
02.04.2004	12:30 – 15:00 h	keine Anmeldung

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

Zielgruppe: PC-BenutzerInnen, die das Erstellen von Webpages praktisch üben möchten
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: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
29.04.2004	09:00 – 16:00 h	15.03.04 – 02.04.04

MS-Frontpage

Zielgruppe: AnwenderInnen, 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 und Grafiken einfügen / Verweise – Hyperlinks / Frame-Seiten / Webseiten veröffentlichen / Projektplanung und -verwaltung / Gestaltungsprinzipien
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 16

Termin	Zeit	Anmeldefrist
22.04.2004	9:00 – 16:00 h	15.03.04 – 16.04.04

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 und Lesbarkeit / Einsatz von Grafiken / HTML-Validierung
Ort: Kursraum A
Preis: € 60,– für Studierende
€ 120,– für MitarbeiterInnen
€ 180,– für Externe
Teilnehmer: maximal 12

Termin	Zeit	Anmeldefrist
23.06. – 24.06.04	9:00 – 16:00 h	24.05.04 – 11.06.04

SYSTEMBETREUUNG

Hardware-Grundlagen

Zielgruppe: SystemadministratorInnen, 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 MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
03.06.2004	09:00 – 16:00 h	03.05.04 – 21.05.04

Netzwerk-Grundlagen

Zielgruppe: SystemadministratorInnen, 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 / Firewall-Grundlagen
Ort: Kursraum B
Preis: € 30,– für Studierende
€ 60,– für MitarbeiterInnen
€ 90,– für Externe
Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
17.05.2004	09:00 – 16:00 h	19.04.04 – 07.05.04

Windows 2003 Server - Systemadministration und Installation

Zielgruppe: Benutzer, die Windows 2003 Server installieren, konfigurieren, Benutzer verwalten und Clients anbinden wollen
Voraussetzung: Systemadministrationskenntnisse, Grundlagen Netzwerke
Dauer: 18 Stunden (3 Tage)
Inhalt: Überblick Betriebssystem / Hardware / Partitionieren / Dateisysteme / Active Directory Service / Berechtigungen und Objektverwaltung / Installation und Konfiguration von Windows 2003 Server

Ort: Kursraum B
Preis: € 220,– für Studierende & MitarbeiterInnen
€ 330,– für Externe
Teilnehmer: maximal 8

Termin	Zeit	Anmeldefrist
28.06. – 30.06.04	09:00 – 16:00 h	01.06.04 – 18.06.04

Linux-Workshop

Zielgruppe: BenutzerInnen, die die Installation und Konfiguration eines Linux-Rechners im Rahmen eines Workshops erlernen wollen
Voraussetzung: Kurs *Einführung in Unix* oder gleichwertige Kenntnisse
Dauer: 18 Stunden (3 Tage)
Inhalt: Was ist Linux? / Installation von Linux auf einem PC / Kommandozeile und grafische Benutzeroberfläche / Der Linux-PC als Workstation / Der Linux-PC als Server / Sicherheit
Ort: Kursraum B
Preis: € 90,– für Studierende & MitarbeiterInnen
€ 135,– für Externe
Teilnehmer: maximal 10

Termin	Zeit	Anmeldefrist
25.05. – 27.05.04	09:00 – 16:00 h	26.04.04 – 14.05.04

Programmierung

Einführung in das Programmieren – Teil 1

Zielgruppe: AnwenderInnen, 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
23.04.2004	12:30 – 15:30 h	keine Anmeldung

Einführung in das Programmieren – Teil 2

Zielgruppe: AnwenderInnen, 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
30.04.2004	12:30 – 15:30 h	keine Anmeldung

Einführung in das Programmieren mit Perl

Zielgruppe: AnwenderInnen, welche 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
07.05.2004	12:30 – 15:30 h	keine Anmeldung

Einführung in das Programmieren mit JavaScript

Zielgruppe: AnwenderInnen, 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
28.05.2004	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, 26. März 2004, 12:30 Uhr (s.t.)
Teil 2: Freitag, 2. April 2004, 12:30 Uhr (s.t.)

Dauer: jeweils ca. 2,5 Stunden

Diese beiden Vorträge richten sich an alle BenutzerInnen, 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, 23. April 2004, 12:30 Uhr (s.t.)
Teil 2: Freitag, 30. April 2004, 12:30 Uhr (s.t.)

Dauer: jeweils ca. 3 Stunden

Diese Vorträge sind für AnwenderInnen gedacht, die das Programmieren erlernen wollen: Hier 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, 7. Mai 2004, 12:30 Uhr (s.t.)

Dauer: ca. 3 Stunden

Aufbauend auf den beiden Vorträgen *Einführung in das Programmieren, Teil 1 & 2* wird in dieser Veranstaltung Perl, eine weit verbreitete 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 Webformular eingegeben wurden, benötigt werden.

Einführung in das Programmieren mit JavaScript

Termin: Freitag, 28. Mai 2004, 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, 18. Juni 2004, 12:30 Uhr (s.t.)

Dauer: ca. 2 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

Sekretariat	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.C0028A
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:

Dempf Stefan	4277-14151	UZAII/Zi.2C324
Doppelhofer Johann	4277-14152	UZAII/Zi.2C324

Abteilung Software & Benutzerbetreuung

Stappler Herbert *(Leiter)*	4277-14051	Zi.B0110
Alexe Stefan	4277-14291	Zi.C0028
Berndl Alexander	4277-14163	Zi.B0111
Berndl Christoph	4277-14064	Zi.C0102A
Bociurko Michaela	4277-14072	Zi.B0111
Brabec Erich	4277-14075	Zi.B0104
Brugger Nikolaus	4277-14069	Zi.D0106
Domschitz Eduard	4277-14133	Univ.str. 11/5a
Ertl Lukas	4277-14073	Zi.B0117
Hurka Franz	4277-14067	Zi.D0112
Just Stefan	4277-14281	Univ.str. 11/5a
Kaider Thomas	4277-14066	Zi.C0102A
Kaltenbrunner Franz	4277-14061	Zi.B0120
Köberl Dieter	4277-14058	Zi.D0111
Kunitzky Walter	4277-14086	Zi.C0102
Ljesevic Nasret	4277-14062	Zi.B0120
Marksteiner Peter	4277-14055	Zi.B0117
Mislik Heinrich	4277-14056	Zi.B0117
Muharemagic Mirza	4277-14082	Univ.str. 11/5a
Neuwirth Ernst	4277-14052	Zi.B0115
Pavelic Florian	4277-14284	Zi.D0106
Plansky Christian	4277-14065	Zi.C0102
Platzer Eveline	4277-14071	Zi.C0102B
Pytlik Andreas	4277-14282	Univ.str. 11/5a
Reicher Markus	4277-14059	Zi.B0117
Riesing Martin	4277-14165	Zi.C0102A
Salet Pascal	4277-14285	Zi.D0109
Scherzer Horst	4277-14053	Zi.B0115
Schreiner Willibald	4277-14076	Zi.D0112
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
Zens Birgit	4277-14292	Zi.C0028
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
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
Grünauer Marcel	4277-14272	AAKH, Hof 1
Hartwig Günther	4277-14243	Zi.D0117

Heimhilcher Markus	4277-14274	AAKH, Hof 1
Helmberger Florian	4277-14276	AAKH, Hof 1
Hof Markus	4277-14248	Zi.D0115
Hofstetter Mark	4277-14275	AAKH, Hof 1
Kiermayr Ulrich	4277-14104	Zi.B0105
Kunft Walter	4277-14031	Zi.D0107
Michl Harald	4277-14078	Zi.D0105
Nunner Reinhard	4277-14084	Zi.B0106
Panigl Christian	4277-14032	Zi.D0105
Papst Andreas	4277-14036	AAKH, Hof 1
Parcalaboiu Paul	4277-14246	Zi.D0114
Perzi Michael	4277-14083	Zi.D0105
Regius Rene	4277-14242	Zi.D0117
Rosenwirth Thomas	4277-14025	Zi.B0106
Schaidl Christian	4277-14026	Zi.B0107
Schirmer Daniel	4277-14028	Zi.B0102
Schneider Monika	4277-14048	Zi.B0107
Szvasztics René	4277-14271	AAKH, Hof 1
Vidovic Dejan	4277-14027	Zi.B0102
Vogler Martin	4277-14113	Zi.C0028A
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

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

Riedel-Taschner Harald (*Leiter*)	4277-14211	
Aschauer Johann	4277-14213	
Cutura Wolfgang	4277-14236	
Dreiseitel Thomas	4277-14216	
Eich Hartmut	4277-14237	
Eireiner Christina	4277-14209	
Filz Michael	4277-14233	
Fuchs Alexander	4277-14228	
Guttenbrunner Mark	4277-14235	
Hojreh Farzaneh	4277-14207	
Hordynski Stephan	4277-14238	
Kauer Josef	4277-14210	
Klünger Gerhard	4277-14219	
Koller Markus	4277-14212	
Kößlbacher Eva	4277-14214	
Lackner Herbert	4277-14217	
Linhart Leopold	4277-14221	
Lohner Gertraud	4277-14222	
Niederhuber Marion	4277-14251	
Pauer-Faulmann Barbara	4277-14227	
Payer Markus	4277-14229	
Plattner Dieter	4277-14232	
Polaschek Martin	4277-14200	
Pröll Michaela	4277-14205	
Rast Wolfgang	4277-14124	AAKH/2H EG31
Redl Karin	4277-14223	
Schöller Robert	4277-14230	
Stark Mario	4277-14239	
Url Clemens	4277-14220	
Zalcmann Erich	4277-14226	
Zeiner Andreas Leo	4277-14208	

ÖFFNUNGSZEITEN

(Achtung: An vorlesungsfreien Tagen keine Tutorenbetreuung!)

Helpdesk des ZID (Service- und Beratungszentrum)

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

Mo – Fr 9:00 – 18:00

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

(http://www.univie.ac.at/ZID/PC-Raeume/)

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 ZID (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

AnsprechpartnerInnen

In grundsätzlichen Angelegenheiten wenden Sie sich bitte an den Direktor des Zentralen Informatikdienstes oder an die Abteilungsleiter (siehe *Personal- & Telefonverzeichnis*, Seite 46).

Helpdesk (Service- und Beratungszentrum)

Als erste Anlaufstelle bei EDV-Problemen und technischen Schwierigkeiten,

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

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

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

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

bei Problemen mit dem **Internetzugang 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 – 18:00 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 46).

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 technischen Fragen zum Pilotprojekt Neue Medien:

eMail: elearn.zid@univie.ac.at
Telefon: 4277-14290

bei Fragen zum Telefonsystem der Uni Wien:

eMail: telefon@univie.ac.at

für Öffentlichkeitsarbeit:

Comment-Redaktion: Bociurko Michaela 4277-14072
Zoppoth Elisabeth 4277-14074
WWW-Redaktion: Berndl Alexander 4277-14163

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 (€ 0,16/min.)

Die MitarbeiterInnen 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).

COMMENT-ABO

Der *Comment* erscheint zwei- bis dreimal im Jahr und ist online im HTML- oder PDF-Format verfügbar. MitarbeiterInnen und Studierenden der Uni Wien wird die gedruckte Ausgabe kostenlos zugeschickt; alle anderen interessierten LeserInnen erhalten auf Wunsch eine Verständigung per eMail, sobald eine aktuelle Ausgabe vorliegt (**e-Abo**), und können diese dann online abrufen (**`http://www.univie.ac.at/comment/`**). Ein Teil der gedruckten Ausgabe liegt am Helpdesk (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:** MitarbeiterInnen 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 (geben Sie dabei bitte 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.