zentraler informatik dienst

universität wien

comment

computer & communication

07/3

UNIVIS-Anmeldesystem mit Curriculumsunterstützung

ZID Aktuell

ACOnet feiert "Fifteen-Fifteen"

Breitbandzugänge werden aufgelassen

Software & Arbeitsplatz

Bewährt: Instituts-PCs mit Fernwartung

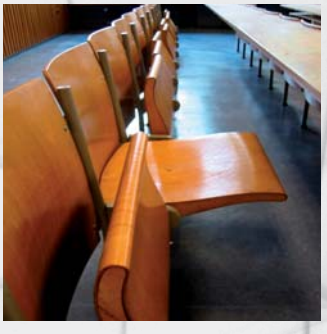
Neue PC-Raum-Software

Online- & Netzwerkdienste

Upgrade des Webservers

Strategien für sicheres Surfen

Hochschulschriften-Server



Oktober 2007

21. Jahrgang

COMMENT-ABO

Der *Comment* erscheint zwei- bis dreimal im Jahr und ist in gedruckter Form sowie online im HTML- und PDF-Format verfügbar. Studierenden und MitarbeiterInnen der Universität Wien wird die Print-Ausgabe auf Wunsch kostenlos zugeschickt. Alle anderen interessierten LeserInnen können das **e-Abo** beziehen: Sie erhalten eine Verständigung per eMail, sobald eine neue Ausgabe vorliegt, und können diese dann online abrufen (**`http://comment.univie.ac.at/`**). Ein Teil der gedruckten Ausgabe liegt am Helpdesk des ZID bzw. vor den PC-Räumen im NIG (1010 Wien, Universitätsstraße 7, 1. Stock) zur freien Entnahme bereit.

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

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

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

Impressum / Offenlegung gemäß § 25 Mediengesetz:

Herausgeber & Medieninhaber:	Zentraler Informatikdienst der Universität Wien
Redaktion & Gestaltung:	Katharina Lüthke Elisabeth Zoppoth
Adresse:	Zentraler Informatikdienst der Universität Wien Universitätsstraße 7, 1010 Wien, Österreich Tel.: +43-1-4277-140 01 Fax: +43-1-4277-9 140 eMail: `comment.zid@univie.ac.at` online: `http://comment.univie.ac.at/`
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!

Wie gewohnt möchten wir Ihnen hier die Höhepunkte der aktuellen Ausgabe ans Herz legen – diesmal zur Abwechslung in umgekehrter Reihenfolge:

Der krönende Abschluss ist auf den Seiten 27–35 zu finden – im Artikel ***Gute Seiten – Schlechte Seiten*** erfahren Sie, mit welchen Methoden man derzeit versucht, ahnungslose AnwenderInnen vor gefährlichen Webseiten zu schützen. Eines sei schon jetzt verraten: Sich allein auf die verfügbaren technischen Hilfsmittel zu verlassen, ist (noch) nicht zu empfehlen.

Ein komplexes Projekt, das uns noch einige Monate beschäftigen wird und das hier entsprechend ausführlich vorgestellt wird, ist die Neugestaltung des Webservers der Uni Wien. Der Beitrag ***WWW.UNIVIE.AC.AT – Alte Adresse, neue Architektur*** auf Seite 20 beschreibt, wie der neue Webserver aufgebaut ist und wie die Migration der bestehenden Webseiten ablaufen wird. Eine entsprechende Erneuerung der Webservices für Studierende und Uni-MitarbeiterInnen (WWW.UNET.UNIVIE.AC.AT, HOMEPAGE.UNIVIE.AC.AT) ist in Vorbereitung, wird aber noch einige Zeit in Anspruch nehmen.

In dieser Ausgabe werden außerdem zwei Jubiläen gefeiert – einerseits hat die Arbeitsgruppe *Fakultätsunterstützung* des ZID mit ihrem System zur Ferninstallation von Universitätsrechnern einen erfreulichen Teilerfolg zu verzeichnen (siehe Artikel ***Ein Konzept bewährt sich: 1000 Instituts-PCs mit Fernwartung*** auf Seite 15), andererseits ist das österreichische Wissenschaftsnetz ACOnet seit 15 Jahren an der Uni Wien beheimatet, wird ebenso lange auf Basis des *Internet Protocol* (IP) betrieben und hat kürzlich den Ausbau des Netzwerks auf eine Glasfaser-Infrastruktur in die Wege geleitet, welche für die nächsten 15 Jahre ausreichend Bandbreite bieten sollte (siehe Artikel ***ACOnet feiert „Fifteen-Fifteen“*** auf Seite 11).

Der „Leitartikel“ dieses *Comment* widmet sich dem neuen Anmeldesystem mit Curriculumsunterstützung, das mit Beginn des Wintersemesters 2007/2008 den Pilotbetrieb aufgenommen hat: Im Beitrag ***UNIVIS online wächst und wächst*** auf Seite 2 können Sie nachlesen, wie sich die Lehr- und Prüfungsverwaltung an der Universität Wien in den kommenden Jahren entwickeln wird – der „elektronische Prüfungspass“ rückt in greifbare Nähe!

Ein erfolgreiches Wintersemester wünscht
die *Comment*-Redaktion

Inhalt

ZID Aktuell

Software & Arbeitsplatz

Online- & Netzwerkdienste

Anhang

UNIVIS online WÄCHST UND WÄCHST

Neues Anmeldesystem mit Curriculumsunterstützung im Pilotbetrieb

Seit einigen Jahren gibt es *UNIVIS online*, ein Webservice des ZID, das es den Studierenden der Uni Wien ermöglicht, selbständig ihre persönlichen Daten zu aktualisieren, ihre Prüfungsleistungen abzufragen, die Fortsetzung des Studiums bekannt zu geben sowie über die Zweckwidmung des Studienbeitrags abzustimmen. *UNIVIS online* greift direkt auf die Universitätsverwaltungssoftware i3v zu, hat sich bewährt und wird daher laufend erweitert – mittlerweile können auch WissenschaftlerInnen und VerwaltungsmitarbeiterInnen über *UNIVIS online* arbeiten, z.B. im Rahmen der Forschungsdokumentation RAD[1)].

Mit Beginn des Wintersemesters 2007/2008 kommt nun ein neuer Anwendungsbereich dazu: ein universitätsweites Anmeldesystem, das weit mehr kann als Anmeldungen zu Lehrveranstaltungen und Prüfungen jeder Studienprogrammleitung (SPL) zu bearbeiten. Dieses Anmeldesystem stellt eine bahnbrechende Neuerung in der Lehr- und Prüfungsverwaltung an der Universität Wien dar – erstmals ist es universitätsweit einsetzbar, außerdem können Studienpläne (seit dem UG 2002 *Curricula* genannt) direkt in i3v modelliert und so die im Curriculum definierten Voraussetzungen überprüft werden. Die Abteilung *Universitätsverwaltung* des ZID (AUV) hat die technische Realisierung dieses Systems übernommen und kooperiert dabei eng mit der Dienstleistungseinrichtung *Studien- und Lehrwesen* der Universität Wien, die für die Daten aus dem Bereich der Lehr-, Prüfungs- und Studierendenverwaltung verantwortlich ist und als direkte Schnittstelle zur jeweiligen SPL fungiert.

Mehrere Monate lang wurde mit den Studienprogrammleitungen Wirtschaftswissenschaften, Philosophie und Bildungswissenschaft intensiv an der Umsetzung der neuen Strukturen und an der Datenpflege für das Anmeldesystem gearbeitet. Am 17. September 2007 begann für diese drei so genannten „Pilot-SPLs“ die erste Anmeldefrist; in den folgenden zwei Wochen meldeten sich 4 300 Studierende über das neue Anmeldesystem für 9 500 Lehrveranstaltungsplätze in 360 Lehrveranstaltungen an.

Wer *UNIVIS online* schon bisher verwendet hat, wird feststellen, dass sich nicht nur die Funktionalität erweitert, sondern auch die Optik verändert hat: Die Inbetriebnahme des neuen Anmeldesystems wurde zum Anlass genommen, die Eingabemasken an das Corporate Design der Uni Wien anzupassen. Darüber hinaus wurde mit dem Stichtag 17. September auch die Zugangsadresse zu *UNIVIS online* auf **`https://univis.univie.ac.at/`** umgestellt; der bisherige Link `www.univie.ac.at/uvo/` wird aber an die neue Adresse weitergeleitet und funktioniert auch weiterhin.

1) siehe Artikel *UNIVIS: Kommt Zeit, kommt RAD – Die neue Research Activities Documentation der Universität Wien* in *Comment 07/1*, Seite 10 bzw. unter `http://comment.univie.ac.at/07-1/10/`

Was macht dieses Anmeldesystem zur besseren Alternative?

Die unterschiedliche Struktur der Studienpläne hat es bisher sehr schwierig gestaltet, ein Anmeldesystem mit Curriculumsunterstützung, das in weiterer Folge einen elektronischen Prüfungspass ermöglicht, zu realisieren. Angesichts der hohen Studierendenzahlen der Universität ist eine elektronische Unterstützung für die Anmeldungen zu Lehrveranstaltungen und Prüfungen (vor allem zu solchen mit beschränkter Teilnehmerzahl) aber ein wichtiges Instrument in der Lehr- und Prüfungsverwaltung. Folgerichtig existieren an den verschiedenen Studienprogrammleitungen zahlreiche Anmeldesysteme – so genannte „dezentrale Systeme“ – unterschiedlichster Bauart:

- Die meisten dieser Systeme basieren derzeit auf dem beliebten ***First come, first served*-Prinzip**, d.h. die Vergabe der Plätze erfolgt in der Reihenfolge des Einlangens der Anmeldung. Das stärkste Plus dieser Methode, die scheinbare Gleichberechtigung aller Studierenden, löst sich jedoch bei genauerem Hinsehen in Luft auf: Während bei einer Anmeldung am Schalter diejenigen profitieren, die sich früh genug anstellen, ist es bei einer elektronischen Anmeldung nach dem *First come, first served*-Prinzip ausschlaggebend, in der richtigen Millisekunde auf den Knopf zu drücken, was einer mehr oder weniger zufälligen Vergabe der Plätze gleichkommt. Darüber hinaus hat dieses System noch mit einem weiteren Problem zu kämpfen: Von Studierenden programmierte Anmeldeautomatismen sorgen immer wieder dafür, dass bei Anmeldungen zu stark frequentierten Veranstaltungen die Server schlichtweg zusammenbrechen. Dagegen helfen nur Serverfarmen à la Google – und für eine Universität ist das leider kein realisierbarer Ausweg.

- Bei einem **Präferenzsystem** werden die verfügbaren Plätze anhand von „Wunschlisten“ zugeteilt: Die Studierenden melden sich zu einem beliebigen Zeitpunkt innerhalb der Anmeldefrist (diese dauert in der Regel ein bis zwei Wochen) zu den gewünschten Lehrveranstaltungen an und reihen sie dabei nach ihrem persönlichen Interesse – z.B. beginnend mit 1 für die subjektiv wichtigste Lehrveranstaltung. Nach Ende der Anmeldefrist einer Veranstaltung werden zuerst alle Studierenden aufgenommen, die diese auf Platz 1 ihrer Wunschliste haben, danach jene, die sie auf Platz 2 haben usw.

- Ein **Punktesystem** erlaubt eine noch feinere Abstufung: Hierbei erhält jeder Studierende pro Semester und pro SPL ein gewisses Punktekontingent. Diese Punkte können auf bestimmte Veranstaltungen gesetzt (vgl. **Abb. 1**) und bis zum Ende der Anmeldefrist auch noch verschoben werden. Je mehr Punkte man auf eine Veranstaltung setzt, desto wahrscheinlicher ist die erfolgreiche Anmeldung.

Abb. 1: Anmeldesystem – Punktevergabe für eine Veranstaltung

Anmeldesysteme auf Basis einer Punkte- bzw. Präferenzwahl sind inhaltlich hoch spezialisiert, durchdacht und gerecht in der Zuteilung; einer ihrer größten Vorteile liegt darin, dass der Zeitpunkt der Anmeldung keine Rolle mehr spielt. Dezentrale Systeme dieser Art haben allerdings das Problem, dass sie nicht direkt auf Studierendendaten wie z.B. Matrikelnummer oder erbrachte Leistungen zugreifen können, sondern nur über Schnittstellen – also zeitverzögert – mit der Universitätsverwaltungssoftware i3v verbunden sind. Das neue Anmeldesystem vereint nun die Logik eines Punkte- bzw. Präferenzsystems mit der Datenbasis von i3v. Damit wird einerseits den Studierenden möglichst viel Flexibilität bei der Planung ihres Studiums und andererseits den SPLs ein hohes Maß an Individualität geboten (Näheres dazu siehe Kasten *Was bringt das Anmeldesystem für die Universitätsadministration?* auf Seite 4).

Ein zentrales Thema des neuen Anmeldesystems ist die erstmals verfügbare **Curriculumsunterstützung**. Da die Umsetzung der neuen Studienarchitektur nach dem Bologna-Prozess[2)] gleiche Richtlinien für alle Curricula vorsieht, ist nun eine universitätsweite IT-unterstützte Administration dieser Curricula möglich: Die für die Absolvierung eines Curriculums notwendigen Leistungen werden auf organisatorischer Ebene als zu erbringende *Studienplanpunkte* abgebildet und auf inhaltlicher Ebene als *Lehrinhalte*, welche die zu erwerbende Kompetenz beschreiben. Voraussetzungen und Abhängigkeiten organisatorischer oder inhaltlicher Natur können auch in i3v erfasst und im Anmeldesystem überprüft werden. So kann bereits bei der Anmeldung zu einer bestimmten Veranstaltung automatisch ermittelt werden, ob der Studierende die nötigen Voraussetzungen erfüllt – beispielsweise wird überprüft, ob er bereits die Einführungsvorlesungen besucht hat, wenn er sich zu einem Aufbauseminar anmeldet.

Ein solches „modelliertes Curriculum" ist die Voraussetzung für den elektronischen Prüfungspass, mit dem der gesamte Studienverlauf eines Studierenden ganz ohne Papierkrieg administriert und nachvollzogen werden kann (mehr dazu im Abschnitt *Der elektronische Prüfungspass – das Ende der Zettelwirtschaft* auf Seite 5).

Wie funktioniert das neue Anmeldesystem?

Grob umrissen, arbeitet das neue Anmeldesystem nach folgendem Prinzip: Vorab muss die jeweilige Studienprogrammleitung alle angebotenen Lehrveranstaltungen mitsamt ihren Anmeldefristen und allfälligen Platzbeschränkungen in i3v erfassen. Die Studierenden können sich dann zu einem beliebigen Zeitpunkt während der Anmeldefrist via Webbrowser anmelden; bei platzbeschränkten Veranstaltungen erscheint der Hinweis *Punktevergabe nötig*. Selbstverständlich ist es auch möglich, die gesetzten Punkte nachträglich zu verschieben oder sich von einer Veranstaltung wieder abzumelden. Der in *UNIVIS online* angezeigte Anmeldestatus des Studierenden (vgl. **Abb. 2** auf Seite 5) lautet bis zum Ende der Anmeldefrist entweder *vorgemerkt* (bei platzbeschränkten Veranstaltungen) oder *angemeldet* (bei nicht platzbeschränkten Veranstaltungen).

Nach Ablauf der Anmeldefrist ändert sich der Anmeldestatus der Studierenden bei platzbeschränkten Veranstaltungen von *vorgemerkt* auf *in Bearbeitung*. Das System errechnet nun anhand eines Zuteilungsalgorithmus, dessen Parameter durch die SPL konfiguriert wurden, einen Vorschlag für die Platzvergabe, der von der Studienprogrammleitung noch freigegeben werden muss. Im Anschluss daran ist die Zuteilung verbindlich – der Anmeldestatus lautet nun entweder *angemeldet* (bei erfolgreicher Anmeldung) oder *auf Warteliste* (sofern man bei der Zuteilung keinen Platz erhalten hat).

- Genaue Anleitungen zur Verwendung des neuen Anmeldesystems sowie die jeweiligen Anmeldefristen können über das Studierenden-Portal der Universität Wien (`http://studieren.univie.ac.at/`) unter dem Link ***Student Management System – Anmeldesystem*** abgerufen werden.

2) siehe `http://bologna.univie.ac.at/`

Was bringt das Anmeldesystem für die Universitätsadministration?

Das neue Anmeldesystem ist weit mehr als eine Anwendung, mit der sich Studierende zu Veranstaltungen anmelden können. Wenn man etwas tiefer in die Materie eintaucht, wird deutlich, dass es vielmehr die gesamte Lehr- und Prüfungsverwaltung der Uni Wien aus ihren Angeln hebt: Bisher war es üblich, die beiden Bereiche zu trennen und in unterschiedlichen Applikationen – oft auch von verschiedenen Personen – durchführen zu lassen. Das neue Anmeldesystem trägt jedoch dem ureigenen Zusammenhang von Lehr- und Prüfungsverwaltung Rechnung, was für die betroffenen VerwaltungsmitarbeiterInnen ein verstärkt bereichsübergreifendes Arbeiten mit sich bringt.

Es ist klar, dass für ein derart komplexes System umfangreiche Vorbereitungen notwendig waren: Bereits 2006 wurden in einer Arbeitsgruppe (bestehend aus MitarbeiterInnen der DLE *Studien- und Lehrwesen*, des ZID, des Bologna-Büros, der Curricularkommission sowie aus ausgewählten Curricula-Verantwortlichen) auf Basis der neuen Curricula die Rahmenbedingungen für eine EDV-Unterstützung erarbeitet. Diese wurden in einem *Kompendium* zusammengefasst, das die Grundlage für die technische Umsetzung bildet. Zudem wurde ein *Fragenkatalog* mit offenen Fragen aus dem Bereich des Anmeldesystems (und teilweise bereits erarbeiteten Antworten) in einer außerordentlichen SPL-Konferenz diskutiert. Basierend auf den Ergebnissen dieser Diskussionen wurden in i3v die nötigen Vorarbeiten für eine Implementierung des Anmeldesystems (einschließlich elektronisch abgebildeter Curricula) durchgeführt. Der letzte Schritt war die Programmierung des Anmeldesystems.

Ein zentral gesteuertes, aber dezentral bewirtschaftetes Anmeldesystem birgt immer die Problematik der Uniformität in sich – der Vereinheitlichung, wo nichts einheitlich ist, eine Einschränkung der Flexibilität. Ein Kernthema beim Designen des Systems war es deshalb, trotz einheitlicher technischer Grundstrukturen die Individualität der verschiedenen Studienprogrammleitungen zu wahren und spezifische Prioritäten von SPLs zu berücksichtigen. Dies wurde durch einen hohen Grad an Parametrisierung realisiert: Jede SPL kann die Parameter des Systems frei konfigurieren – so ist es z.B. möglich, die Flexibilität für den Einzelnen (An-/Abmeldung durch die Studierenden selbst) ebenso in den Vordergrund zu rücken wie das universitätsweite Bereitstellen von Daten für die Ressourcenplanung.

Abläufe & Parametrisierung

Zu Beginn erfasst die Studienprogrammleitung die einzelnen Veranstaltungen und Platzbeschränkungen. Dann werden die Daten für die Veranstaltungen konfiguriert, wobei es auch möglich ist, diese *en bloc* zu behandeln, also z.B. die Anmeldefrist für alle zentral zu verwalten. Selbstverständlich können trotzdem jederzeit für bestimmte Veranstaltungen die Plätze vermehrt oder spezielle Anmeldefristen definiert werden. Wie bereits angedeutet, gibt es zahlreiche Konfigurationsoptionen: Neben der Festlegung von Platzbeschränkungen und Anmeldezeiträumen steht es einer SPL unter anderem auch frei, Bonuspunkte zu vergeben (z.B. für Studienfortschritt, für die Zugehörigkeit von Studierenden zur jeweiligen SPL, ...), „übriggebliebene“ Punkte von vergeblichen Anmeldungen aus dem Vorsemester anzurechnen oder Platzkontingente für Studierende einer bestimmten Studienrichtung zu reservieren. Im Hinblick auf zeitliche Überschneidungen von Veranstaltungen entscheidet die SPL, ob dies berücksichtigt werden soll, und wenn ja, ob zeitliche Überschneidungen zugelassen oder nicht zugelassen werden. Es besteht sogar die Möglichkeit, dass sich mehrere Studienprogrammleitungen zusammenschließen, um ihre Veranstaltungen gemeinsam zu verwalten. Nach Ablauf der Anmeldefrist einer Veranstaltung führt der Studienprogrammleiter einen so genannten „Zuteilungslauf“ in i3v durch. Dabei wird ein Zuteilungsvorschlag erstellt, der bei Bedarf noch abgeändert werden kann. Erst nach der Freigabe durch die SPL ist die Platzvergabe verbindlich und wird im Web veröffentlicht. Sofern die SPL dies entsprechend vorkonfiguriert hat, müssen die erfolgreich angemeldeten Studierenden nun noch bestätigen, dass sie den zugewiesenen Platz in Anspruch nehmen werden. Es sind auch mehrere Zuteilungsläufe pro Semester möglich.

Datenpflege

Um in den Genuss der im Abschnitt *Der elektronische Prüfungspass – das Ende der Zettelwirtschaft* beschriebenen Vorteile zu kommen, ist natürlich ein gewisser Initialaufwand nötig, der sich jedoch bald bezahlt macht. Die anfängliche „Fütterung“ des Systems mit den benötigten Daten ist unumgänglich, um einen reibungslosen Ablauf der neuen Anwendungen zu gewährleisten; in den folgenden Semestern müssen die Daten dann aber nur mehr kontrolliert und bei Bedarf ergänzt bzw. geändert werden. Abgesehen davon bleibt es der jeweiligen Studienprogrammleitung überlassen, in welchem Umfang sie das System nutzen will: Für ein einfaches Anmeldesystem reicht es aus, die Veranstaltungen und die Anmeldefristen zu erfassen. Gibt man zusätzlich die Platzbeschränkungen in i3v ein, kann auch ein Zuteilungsalgorithmus verwendet werden; pflegt man auch die Raumbelegungsdaten, wird eine zeitliche Überschneidungsfreiheit der Veranstaltungen möglich usw. Grundsätzlich gilt: Je umfassender die Daten eingepflegt werden, desto mehr Funktionalitäten bietet das System, und je vollständiger diese genutzt werden, desto geringer wird der administrative Aufwand.

- Der Zugang zum Anmeldesystem erfolgt entweder über *UNIVIS online* (**`https://univis.univie.ac.at/`**) unter dem Punkt ***Anmeldesystem*** oder über das Online-Vorlesungsverzeichnis (**`http://online.univie.ac.at/vlvz?extended=Y`**), wo bei den betreffenden Veranstaltungen der Link ***Anmelden*** aufscheint.

Abgesehen vom Punktesystem, vom direkten i3v-Zugriff und von der Curriculumsunterstützung bietet das neue Anmeldesystem noch etliche weitere Annehmlichkeiten für Studierende und Lehrende:

- Die Anmeldung zu Lehrveranstaltungen und Prüfungen kann über den gewohnten *UNIVIS online*-Zugang erfolgen. Dabei sind sowohl die aktuellen Vormerkungen, die verfügbaren Plätze als auch der eigene Anmeldestatus ersichtlich. Während der Anmeldefrist können jederzeit Änderungen vorgenommen werden.

- Sofern die jeweilige Studienprogrammleitung dies in ihrem Zuteilungsalgorithmus entsprechend festgelegt hat, kann das System verhindern, dass sich ein Studierender zu zwei oder mehr Lehrveranstaltungen anmeldet, die gleichzeitig stattfinden. Eine gewisse zeitliche Überschneidungstoleranz kann dabei von der SPL frei definiert werden.

- Die angemeldeten Studierenden werden automatisch per eMail über das Ergebnis der Platzvergabe verständigt.

- Voraussichtlich ab dem Wintersemester 2008/2009 wird bei modellierten Curricula ein elektronischer Prüfungspass für die Studierenden zur Verfügung stehen (mehr dazu weiter unten).

- Für Lehrende existiert ein eigenes Webinterface, das jedem Lehrenden die vorhandenen Anmeldungen für seine Veranstaltungen anzeigt und über das er direkten eMail-Kontakt zu den jeweiligen Studierenden aufnehmen kann. Ab dem Sommersemester 2008 wird das Lehrenden-Interface um einige zusätzliche Features erweitert. Dann werden Lehrende über dieses Webinterface automatisch generierte Teilnehmerlisten erhalten; zudem werden sie eigenverantwortlich Studierende aus der Warteliste in die Lehrveranstaltung aufnehmen können. Die Noteneingabe nach Prüfungen soll künftig ebenfalls über das Lehrenden-Interface möglich sein und ist dann nicht mehr direkt in i3v notwendig.

Der elektronische Prüfungspass – das Ende der Zettelwirtschaft

Wie eingangs erwähnt, wurde das neue Anmeldesystem mit Beginn des Wintersemesters 2007/2008 an drei Pilot-Studienprogrammleitungen (Wirtschaftswissenschaften, Philosophie und Bildungswissenschaft) in Betrieb genommen. Im Sommersemester 2008 wird das Anmeldesystem mit einigen zusätzlichen Funktionen – beispielsweise einem erweiterten Lehrenden-Interface – ausgestattet werden; parallel dazu sollen weitere Studienprogrammleitungen in das System eingebunden werden.

Ab dem Wintersemester 2008/2009 wird es möglich sein, den Werdegang von Studierenden ohne papierene Nachweise zu administrieren. Anhand des in i3v modellierten Curriculums kann ein elektronischer Prüfungspass erstellt werden: Der Studierende meldet sich im Anmeldesystem für eine Lehrveranstaltung an und gibt den Studienplanpunkt an, für den er die Leistung benötigt. Nachdem die Note eingetragen wurde, gilt der jeweilige Studienplanpunkt als erfüllt und wird im Prüfungspass vermerkt. So ist es möglich, den Studienfortschritt jedes Studierenden schon während des Studiums zu verfolgen, was für die Lehrveranstaltungsplanung von unschätzbarem Wert ist. Auch die unzähligen Ordner in den Prüfungsreferaten, die an anerkannte Prüfungsleistungen von Studierenden erinnern, werden sich dann nicht länger vermehren.

Der Arbeitsalltag des Verwaltungspersonals wird wesentlich erleichtert: Prüfungstermine müssen zwar nach wie vor angelegt werden (jetzt allerdings vorher), das mühsame Eintippen der Namen jedes einzelnen Studierenden – man denke an den Aufwand bei einem Termin mit hunderten Prüflingen! – gehört dann aber der Vergangenheit an. Die Anmeldung erfolgt durch die Studierenden selbst und nach der Zuteilung der Plätze können die Daten der Studierenden automatisch übernommen werden, sodass nur noch die Noten händisch einzutragen sind. Diese werden direkt bei den sonstigen Daten des jeweiligen Studierenden abgespeichert, und sowohl der Studierende selbst als auch die Studienprogrammleitung können dann via *UNIVIS online* nachverfolgen, in welchem Bereich seines Studiums sich der Studierende befindet, welche Leistungen er bereits absolviert hat und welche noch fehlen.

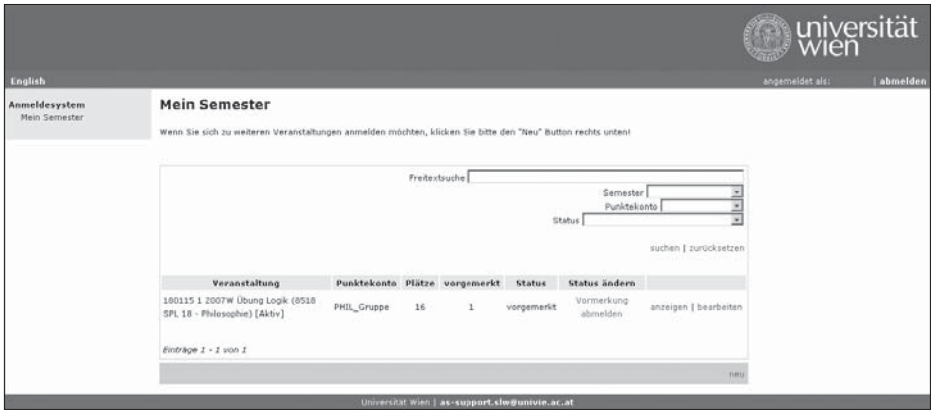


Abb. 2: Anmeldesystem – Übersicht über Veranstaltungen, für die man sich bereits angemeldet hat

Mag. Doris Richling
(DLE Studien- und Lehrwesen)

Die Breitbandzugänge der Uni Wien werden aufgelassen

Seit fast 10 Jahren bietet der Zentrale Informatikdienst in Kooperation mit Telekommunikationsunternehmen den Studierenden und Uni-MitarbeiterInnen Breitbandzugänge zum Internet an (*chello student connect, uniADSL, xDSL Uni*). Damit ist es nun vorbei: Seit 1. Oktober 2007 können sich am ZID keine neuen TeilnehmerInnen mehr anmelden. **Die bestehenden Breitbandzugänge werden weiterhin betreut**, mittelfristig ist jedoch geplant, diese Services aufzulassen und den Support dafür einzustellen. Die Wählleitungszugänge via Modem/ISDN sind von diesen Änderungen nicht betroffen.

Eine Ära geht zu Ende

Anfang 1998 konnte der ZID gemeinsam mit der Firma Telekabel (jetzt UPC) den ersten günstigen Breitbandzugang für Universitätsangehörige anbieten: Dank *TeleWeb StudentConnect* (jetzt ***chello student connect***) durften Studierende und MitarbeiterInnen um öS 390,– über den Proxy-Server der Uni Wien unlimitiert im Web surfen, und zwar mit einer damals beachtlichen Downloadgeschwindigkeit von bis zu 300 kbit/s. Diese Geschwindigkeit hat sich seither versiebenundzwanzigfacht (siehe **Tabelle 1**), die angebotene Proxy-Lösung über den Server der Universität ist aber nicht mehr zeitgemäß.

Die Angebote ***uniADSL*** (mit Telekom Austria) und *xDSL @student* (mit inode, jetzt UPC – das Produkt wurde inzwischen auf ***xDSL Uni*** umbenannt) kamen im Jahr 2002 dazu. *uniADSL* bot Breitbandzugänge auch jenseits der Wiener Stadtgrenzen an und war anfangs am Markt recht gut positioniert: Fair Use-Downloadvolumen ohne Zusatzkosten bei Überziehung, keine Mindestvertragsdauer und eine fixe IP-Adresse über die Uni Wien waren damals bei anderen Anbietern noch nicht Standard. Diese Rahmenbedingungen und der moderate Preis sorgten dafür, dass sich Studierende auch außerhalb der Großstadt einen Breitbandzugang leisten konnten. Dennoch sind *uniADSL* und *xDSL Uni* mit ca. 5 300 Anmeldungen seit 2002 weit hinter unseren Erwartungen geblieben; nur *chello student connect* mit über 22 000 Anmeldungen seit Ende 1998 konnte überzeugen.

Mehrere Jahre lang war der ZID bemüht, neue Breitbandangebote für Uni-Angehörige zu lukrieren. Es ist für die wenigen potentiellen Partnerfirmen allerdings nicht ganz einfach, günstige Produkte für Universitäten anzubieten: Zu wenige Kunden, lange Vertragsbindungen und aufwendige Konfigurationen beschränken in einer schnelllebigen Zeit, in der es bei Telekommunikationsunternehmen um Wachstumskurven, Unternehmenskennzahlen, Gewinnprognosen und Marktanteile geht, die Bereitschaft komplizierte Verträge auszuarbeiten auf ein Minimum. Die derzeitigen Breitbandzugänge der Universität Wien (siehe **Tabelle 1**) unterscheiden sich mittlerweile weder bei Übertragungsgeschwindigkeit und Downloadvolumen noch beim Preis wesentlich von anderen Produkten am österreichischen Markt.

Was die Zukunft bringt

Die beschriebenen Kooperationen wurden hauptsächlich deshalb ins Leben gerufen, weil die „schnellen" Internetzugänge bis vor einigen Jahren sehr teuer waren. Der Zahn der Zeit nagt jedoch in diesem Bereich besonders eifrig – heute locken die Breitbandangebote der Uni Wien niemanden mehr hinter dem Notebook hervor. Leider ist der Support-Aufwand trotzdem beachtlich, sodass sich der ZID entschlossen hat, diese Services schrittweise aufzulassen:

- Wie eingangs erwähnt, werden am ZID **seit 1. Oktober 2007 keine Neuanmeldungen mehr** für die Angebote *chello student connect*, *uniADSL* und *xDSL Uni* entgegengenommen. Die bereits bestehenden Breitbandzugänge werden weiterhin betreut.

- Die Firma UPC (***chello student connect, xDSL Uni***) bietet weiterhin Studentenprodukte an, hat diese aber österreichweit für alle Universitäten vereinheitlicht. Damit ist für die KundInnen auch bei Zugangsproblemen zum Internet die Zuständigkeit klar vorgegeben: Bei jeder An-/Ab-/Ummeldung, bei Verbindungsproblemen und bei allen anderen Fragen ist UPC nun der alleinige Ansprechpartner. Die Einzelheiten zu den neuen Angeboten für Studierende werden direkt von UPC kommuniziert und beworben.

Breitband-Angebot	**Übertragungsrate bei Start des Angebots** (Download / Upload)	**Übertragungsrate Oktober 2007** (Download / Upload)	**Kosten/Monat**
chello student connect	300 / 64 kbit/s (Februar 1998)	8192 / 512 kbit/s	EUR 35,–
uniADSL	512 / 64 kbit/s (März 2002)	2048 / 256 kbit/s	EUR 26,08
xDSL Uni	768 /128 kbit/s (November 2002)	3072 / 512 kbit/s	EUR 35,–

Tabelle 1: Internetzugang von daheim – Überblick über die bisher verfügbaren Angebote der Universität Wien

- Die bestehenden ***uniADSL***-Zugänge werden weiterhin vom Helpdesk des ZID betreut und in den nächsten zwei Jahren nicht auf andere Provider umgestellt.

Falls Sie also bereits einen Breitbandzugang über die Universität Wien haben: Keine Sorge – Sie haben ihn auch weiterhin, wenn Sie wollen. Wir möchten aber darauf hinweisen, dass bereits günstigere Breitbandzugänge erhältlich sind.

Providerwechsel: Worauf ist zu achten?

Die Angebote für Breitband-Internetzugänge sind zahlreich und ähnlich mühsam zu interpretieren wie Handy-Verträge. Bindungsfristen und anfängliche Ermäßigungen sollten genauso sorgsam überprüft werden wie die Kosten bei Überschreiten des Downloadvolumens. Als Orientierungshilfe hier einige Tipps zu den üblichen Fachausdrücken und zum Leben nach einem Providerwechsel (in alphabetischer Reihenfolge):

Drahtlos

Immer mehr Menschen surfen mittels Datenkarte via **GPRS**, **UMTS** oder **EDGE**. Das ist praktisch und mittlerweile auch schon relativ günstig – allerdings nur im Inland. Verwenden Sie Ihre Datenkarte im Ausland nur dann, wenn Sie sich vorher genau erkundigt haben, über welchen Provider dort die „günstigsten" Verbindungen aufgebaut werden können! Es ist auch im Inland nicht ausgeschlossen, dass sich Ihre Datenkarte über einen ausländischen Dienst mit dem Internet verbindet – stellen Sie deshalb fix ein, mit welchem Netz sich Ihre Karte verbinden soll.

Schneller, gratis und unlimitiert geht es mittels Funknetzwerkkarte und *Wireless Local Area Network*: **WLAN** ist in vielen Gebäuden der Universität Wien verfügbar (siehe `www.univie.ac.at/ZID/wlan/`) und kann im Rahmen des eduroam-Projekts auch an zahlreichen anderen Universitäten in Europa und Australien verwendet werden (siehe `www.eduroam.at`).

Entbündelt

Ein Internetzugang ist auch ohne Festnetztelefon möglich. Das sonst übliche Grundentgelt für den Telefonanschluss entfällt bzw. wird oft günstig im Paket angeboten.

Fair Use

Bedeutet normalerweise, dass man einen Überziehungsrahmen beim maximalen Downloadvolumen hat. Mittler-

weile hat sich aber eingebürgert, dass ein Überschreiten kostenpflichtig ist. Oder der Benutzer wird, wenn er drei Monate lang über dem Fair Use-Downloadvolumen liegt, automatisch auf ein teureres Produkt umgestellt. Es gibt auch Produkte am Markt, bei denen nur die Geschwindigkeit reduziert wird, aber keine weiteren Kosten anfallen.

Flat Rate

Die beste Variante für „Poweruser" – keinerlei Beschränkung des Downloadvolumens.

Kleingedrucktes

Hier stehen die wirklich wichtigen Dinge – Bindungsfristen, Bedingungen und Kosten bei vorzeitiger Vertragsauflösung und vieles mehr. Die meisten Lockangebote enttarnen sich im Kleingedruckten. Seien Sie wachsam, die Kleinschreiber werden immer gefinkelter. Manchmal werden auch „Kleinigkeiten" vergessen. Bitte keine falsche Scheu: Rufen Sie den Provider Ihrer Wahl an und fragen Sie nach, wenn Ihnen irgendetwas nicht ganz klar ist.

Postausgangsserver der Uni Wien

Egal über welchen Provider Sie sich mit dem Internet verbinden, ob in Alaska oder in Neuseeland – als Universitätsangehörige/r können Sie Ihre eMail-Nachrichten immer über den Server der Universität Wien verschicken. Damit es funktioniert, müssen Sie in Ihrem Mailprogramm beim Punkt *Postausgangsserver (SMTP)* folgende Einstellungen vornehmen:

- Postausgangsserver: MAIL.UNIVIE.AC.AT
  (für MitarbeiterInnen und Studierende!)
- SSL-Port: 465
  (es wird auch TLS am Port 547 unterstützt)
- mit Authentifizierung (mittels u:net- oder Mailbox-UserID mit dazugehörigem Passwort)
- Achtung: Bei Windows XP-Rechnern darf die *Anmeldung durch gesicherte Kennwortauthentifizierung* nicht aktiviert sein!

Genauere Konfigurationsbeschreibungen finden Sie unter `www.univie.ac.at/ZID/anleitungen-mailing/`.

VPN (Virtual Private Network)

Manche der von der Universitätsbibliothek angebotenen Datenbanken können nur verwendet werden, wenn man mit einer IP-Adresse der Universität Wien darauf zugreift. Von außerhalb des Uni-Datennetzes besteht die einfachste Zugangsmöglichkeit zu diesen Datenbanken darin, mit dem Webbrowser unter `https://univpn.univie.ac.at/` eine Verbindung herzustellen (siehe auch Seite 26). Etwas komplizierter ist es mit einem speziellen VPN-Klienten (siehe `www.univie.ac.at/ZID/anleitungen-vpn/`).

Should I stay or should I go?

Diese Frage müssen Sie naturgemäß selbst beantworten. Wir können Ihnen zu guter Letzt aber noch verraten, was zu tun ist, wenn Sie sich breitbandbezüglich verändern wollen, und was geschieht, wenn Sie nichts unternehmen:

chello student connect und ***xDSL Uni*** wurden von UPC durch andere Angebote für Studierende ersetzt; Bestandskunden können, müssen aber nicht umsteigen. Bestehende Verträge können schriftlich per Fax oder eingeschriebenem Brief direkt an UPC gekündigt werden. Bei Ablauf der u:net- oder Mailbox-UserID wird *chello student connect* automatisch auf *chello classic* umgestellt, *xDSL Uni* wird automatisch zu *xDSL small*.

uniADSL kann unter `https://data.univie.ac.at/adsl` jederzeit gekündigt werden. Das ist allerdings nur dann notwendig, wenn Sie Ihren ADSL-Anschluss auflassen, den Festnetz-Telefonanschluss aber behalten wollen (wenn der Telefonanschluss bei der Telekom Austria abgemeldet wird, muss *uniADSL* nicht extra gekündigt werden). Möchten Sie weg von *uniADSL*, Ihren ADSL-Zugang jedoch über einen anderen Provider weiter verwenden, so müssen Sie sich lediglich beim neuen Provider anmelden – der Provider informiert dann die Telekom Austria und diese wiederum den ZID. Noch ein Hinweis: KundInnen, denen die Herstellung gratis angeboten wurde, haben meist eine Bindungsfrist von 12 Monaten, die aber nicht für *uniADSL*, sondern für den ADSL-Zugang gilt. Ein Providerwechsel ist daher auch innerhalb einer eventuellen Bindungsfrist möglich.

Franz Kaltenbrunner

Rückblick: UNIorientiert

Auch in diesem Jahr beteiligte sich der ZID wieder an der Anfang September 2007 vom Student Point (`http://studieren.univie.ac.at/`) durchgeführten Veranstaltungswoche *UNIorientiert*, in deren Rahmen sich StudienanwärterInnen und alle anderen InteressentInnen bereits vor Studienbeginn ausführlich über die Studienangebote und Serviceleistungen der Universität Wien informieren konnten. Am Infostand des ZID wurde das EDV-Serviceangebot vorgestellt, darunter die universitätsweite eLearning-Plattform, Webspace für Studierende, WLAN, PC-Räume etc. (siehe `www.univie.ac.at/ZID/`). Auch ein EDV-Workshop wurde angeboten.

Die Zukunft der Lernplattform

Modulares eLearning

Endlich Vista 4!

Das lang ersehnte und längst fällige Upgrade von WebCT Vista 3 auf die Version 4, das im Vorjahr aufgrund von Produktschwierigkeiten von der Herstellerfirma Blackboard zurückgezogen wurde und die eLearning-Entwicklungen nicht nur in Wien verzögerte, ist nun endlich verfügbar. Im Juli 2007 wurde ein Testcluster mit einer Vista 4-Betaversion und allen bestehenden eLearning-Lehrveranstaltungen der Uni Wien eingerichtet. Die dreiwöchige Evaluierungsphase und das Feedback der die Installation testenden Lehrenden gaben den Ausschlag für die tatsächliche Migration auf das neue System. Am 10. August fiel der Startschuss, mit erfreulichem Ergebnis: Der neue Vista 4-Cluster läuft stabil, und mit relativ geringem Schulungsaufwand freunden sich sowohl AnfängerInnen als auch Fortgeschrittene mit dem neuen Interface an, das durch den Wegfall einiger redundanter Strukturen in Bedienung und Dateiablage (z.B. *Bestand* und *Dateimanager*) mehr Usability aufweist.[1)] Kürzlich wurde zur Behebung einiger Softwarefehler noch ein Upgrade eingespielt; aktuell läuft die Lernplattform der Uni Wien damit unter Blackboard Vista 4 Service Pack 2 (siehe **Abb. 1**).

Abb. 1: Demokurs in Blackboard Vista 4.2

Wiki-Powerlinks

Mittlerweile sind die so genannten *Powerlinks* (Schnittstellen zur Einbindung externer Applikationen) für die Integration eines Mediawiki in die Blackboard Vista-Lehrveranstaltungen ebenfalls auf Version 4 umgestellt und aktiviert. Die entsprechenden Tools unter *Inhaltsverknüpfung hinzufügen* heißen jetzt *Create Wiki* und *Login Wiki*. Eine genaue Anleitung ist unter `www.univie.ac.at/ZID/bb-wiki/` zu finden. Leider war es nicht möglich, die in Vista 3 bestehenden Wikis automatisch zu migrieren, sie können aber gesondert reaktiviert werden. Das Supportbüro Neue Medien (siehe `www.univie.ac.at/ZID/elearning/`) ist dabei gerne behilflich.

Moodle

Aufgrund zahlreicher Anfragen seitens der Lehrenden gibt es ab dem Wintersemester 2007/2008 zusätzlich zu Blackboard Vista eine Installation der Open Source-Lernplattform Moodle. Das Angebot richtet sich an jene Lehrenden, die bereits mit Moodle gearbeitet haben bzw. damit vertraut sind. Das Supportbüro Neue Medien steht zwar für technische Anfragen zur Verfügung, Moodle-Schulungen für Lehrende werden jedoch nicht abgehalten! Die unter `http://moodle.univie.ac.at/` erreichbare Plattform ist eine Standardinstallation, wobei auch hier die Registrierung der Studierenden über das Online-Vorlesungsverzeichnis bzw. das Lehrenden-Interface unter `https://java.univie.ac.at/lvleiter` erfolgt. Das Login ist auch bei Moodle mittels u:net- bzw. Mailbox-UserID durchzuführen.

Externe BenutzerInnen & externe Plattformen

Lehrende, die Gast-Accounts wünschen, senden bitte eine Personenliste (bestehend aus den Feldern *Vorname*, *Nachname* und *eMail-Adresse*) per eMail an `elearning.zid@univie.ac.at`. Die neuen BenutzerInnen werden in die Lernplattform übernommen und gesondert verständigt. Die betreffenden Lehrenden erhalten eine Liste der User-IDs, die sie wiederum für das Lehrenden-Interface verwenden können.

1) Eine Beschreibung der wichtigsten Änderungen wurde bereits im *Comment 06/3* veröffentlicht (siehe Abschnitt *Vorschau: Was bietet Vista 4?* unter `http://comment.univie.ac.at/06-3/9/`).

Zusätzlich zu den vom Supportbüro Neue Medien betreuten Plattformen Blackboard Vista und Moodle können ab dem Wintersemester 2007/2008 auch jene Lehrveranstaltungen im Online-Vorlesungsverzeichnis als eLearning-Lehrveranstaltungen gekennzeichnet werden, die ein anderes Tool verwenden – z.B. eine institutseigene Plattform. Solche Lehrveranstaltungen sollten ebenfalls unter `www.univie.ac.at/ZID/elearning-elv/` (Option *Andere Plattform*) angemeldet werden: Abgesehen vom eLearning-Link im Online-Vorlesungsverzeichnis hilft diese Registrierung bei der statistischen Erfassung jener Lehrveranstaltungen der Universität Wien, die Blended Learning umsetzen.

Bleibt Blackboard?

Allen, die an der Uni Wien eLearning anwenden, brennt diese Frage schon seit geraumer Zeit unter den Nägeln. Wie bereits im *Comment 07/1* berichtet, läuft der Lizenzvertrag für die Lernplattform im Februar 2009 aus (siehe `http://comment.univie.ac.at/07-1/22/`). In den vergangenen Monaten war eine eigene Arbeitsgruppe – bestehend aus MitarbeiterInnen des ZID und des Projektzentrums Lehrentwicklung – mit der Ausarbeitung von Leistungsverzeichnissen und der Evaluierung verschiedener *Learning Management Systeme* (LMS) beschäftigt, wobei auch der Input der Lehrenden berücksichtigt wurde. Die Ergebnisse dieser Erhebungen werden im November 2007 in einer entsprechenden Ausschreibung ihren Niederschlag finden und auch der Firma Blackboard die Chance geben, sich zu bewerben. So kann anhand von Leistungskriterien objektiv festgestellt werden, ob es sich für die Universität Wien auch weiterhin lohnt, Blackboard als Vertragspartner zu halten, oder ob es sinnvoller ist, das *Learning Management System* zu wechseln.

Diese Frage wird auch deshalb immer wichtiger, weil eLearning an sich einen Paradigmenwechsel durchläuft: Besonderer Wert wird mittlerweile nicht mehr auf den Einsatz eines einzelnen LMS gelegt, sondern auf die Interoperabilität (die viel- und wechselseitige Einsetzbarkeit) und die modulare Wiederverwendbarkeit der Inhalte, sowie zunehmend auch auf internationale Standards wie SCORM oder QTI[2]. Welches LMS zugrunde liegt, wird damit zweitrangig – nicht zuletzt auch im Lichte der so genannten Web 2.0-Entwicklungen[3], in denen *Internet-Nutzung* zunehmend zu *Plattform-Nutzung* evoliert.

Annabell Lorenz

2) SCORM (*Sharable Content Object Reference Model*): siehe `http://de.wikipedia.org/wiki/Scorm`; QTI (*Question & Test Interoperability*): siehe `www.imsproject.org/question/`

3) siehe `http://de.wikipedia.org/wiki/Web_2.0`

Ausdruckstationen für Studierende

Die DLE *Studien- und Lehrwesen* hat in Kooperation mit dem Zentralen Informatikdienst im Wintersemester 2006/2007 das Projekt der Ausdruckstationen ins Leben gerufen, um eine nachhaltige Verbesserung der Servicequalität für die Studierenden zu erzielen. Das neue Service bietet den Studierenden der Universität Wien erstmals die Möglichkeit, folgende Dokumente im Selbstbedienungsbetrieb an den Terminals auszudrucken:

- Sammelzeugnis
- Bestätigung über positiv absolvierte Prüfungen
- Studienbestätigungen (für alle Studien des aktuellen Semesters)
- Studienblatt (für alle Semester mit einer aufrechten Zulassung)
- Zahlschein

Seit dem Start des neuen Service am 3. Oktober 2007 stehen den Studierenden insgesamt sieben Ausdruckterminals an zwei Standorten zur Verfügung:

- 1010 Wien, Dr.-Karl-Lueger-Ring 1, gegenüber Referat Student Point (5 Terminals)
- 1210 Wien, Brünner Straße 72, Bauteil II (2 Terminals)

Erste Analysen haben ergeben, dass die Terminals von den Studierenden bereits sehr intensiv genutzt werden: Zwischen 3. und 10. Oktober wurden insgesamt ca. 2800 Studienunterlagen/Dokumente ausgedruckt.

Mag. Wolfgang Walzer
(DLE Studien- und Lehrwesen)

Neues Service im Uni-Hauptgebäude und im BZW Brünner Straße: Zeugnisse selbst ausdrucken

ACONET FEIERT „FIFTEEN-FIFTEEN“

Der ACONET-Verein (siehe www.aco.net/verein.html) wurde letztes Jahr 20 Jahre alt, das österreichische Internet heuer 17 Jahre[1] – dennoch gibt es 2007 gleich mehrere „15er“ im ACOnet-Kontext zu feiern. Für jene, die mit dem Begriff ACOnet noch nichts anfangen können: Es handelt sich um das österreichische Wissenschaftsnetz, primär gedacht für gemeinnützige Einrichtungen der Forschung, Bildung und Kultur, betrieben vom Zentralen Informatikdienst der Universität Wien in Kooperation mit Universitäten in ganz Österreich (siehe www.aco.net).

Im Juli 1992, also vor 15 Jahren, übersiedelte das gesamte ACOnet-Team[2] aus eigener Initiative von der Technischen Universität Wien an das damalige EDV-Zentrum (heute ZID) der Universität Wien, die meisten davon in die Abteilung *Datennetze*. Noch im selben Jahr wurde unter technischer Federführung von Ewald Jenisch das im ACOnet verwendete Trägerprotokoll von X.25 auf das *Internet Protocol* (IP) umgestellt.

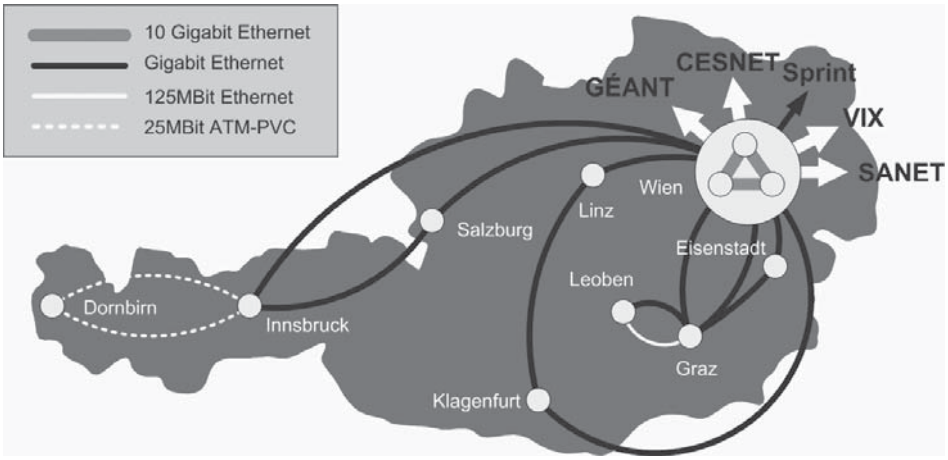


Abb. 1: Die aktuelle ACOnet-Topologie

Wir feiern heuer also sowohl 15 Jahre ACOnet-Betrieb an der Universität Wien als auch 15 Jahre ACOnet als österreichweiter (universitärer) Internet-Backbone. Damit nicht genug, können wir auch gleich noch die Vorfreude auf die kommenden 15 Jahre feiern, die uns nunmehr – nach unserer erfolgreichen Ausschreibung *ACOnet 2007*[3], durchgeführt unter der Leitung von Hermann Steinringer – ins Zeitalter der wellenlängen-transparenten Glasfasertechnologie eintreten lassen.

Die Zukunft von ACOnet: rasant & redundant

Die ersten Jahre waren gekennzeichnet durch den initialen Aufbau und laufende Anpassungen des österreichweiten Backbones, gefolgt und begleitet von zum Teil enormen Anstrengungen, die internationale Anbindung von ACOnet (und Österrreich generell) an das Internet zu verbessern. Heute befinden wir uns in der vergleichsweise angenehmen Lage, bandbreitenmäßig aus dem Vollen schöpfen zu können,[4] zumindest in Wien. Es gilt daher jetzt – und hierzu diente die eben abgeschlossene Ausschreibung –, auch für die ACOnet-Teilnehmer in den anderen Bundesländern durch die grundlegende Erneuerung des ACOnet-Backbones einen dauerhaft gleichberechtigten Zugriff auf die nationalen und internationalen Internet-Bandbreiten sicherzustellen.

Das lokale Netzwerk (LAN) sowie dessen gut dimensionierte Anbindung an das Internet hat in allen Organisationen eine derart selbstverständliche Bedeutung erlangt, dass die meisten ACOnet-Teilnehmer seit einigen Jahren signifikanten Aufwand in die Verbesserung der Ausfallsicherheit ihrer Datennetz-Infrastruktur stecken. Naheliegend ist daher auch deren Bedarf an einer doppelten Anbindung an das Internet. In Wien bieten wir diese Möglichkeit seit einigen Jahren mit den beiden ACOnet-Standorten an der Uni Wien und bei der Firma Interxion in Floridsdorf, an die mittlerweile etliche Wiener ACOnet-Teilnehmer redundant angebunden sind. Auch die ACOnet-Backboneverbindungen sind in geeigneter Weise redundant auf diese beiden Standorte verteilt. An den Anschlusspunkten außerhalb Wiens gab es diese Redundanzmöglichkeit jedoch bisher nicht. Ein ganz klar ausgesprochener Wunsch bei einem Planungstreffen vor zwei Jahren war daher, bei einer Neuausschrei-

1) siehe Artikel *10 Jahre Internet in Österreich* in *Comment 00/2*, Seite 2 bzw. unter http://comment.univie.ac.at/00-2/2/

2) Walter Kunft, Robert Meixner, Christian Panigl, Fritz Plank, Ingrid Pulzer, Wilfried Wöber und Elisabeth Zoppoth; der Teamleiter Manfred Paul wechselte ins Wissenschaftsministerium.

3) siehe Artikel *Ausschreibung für ACOnet-Glasfaserbackbone abgeschlossen* in *Comment 07/2*, Seite 5 bzw. unter http://comment.univie.ac.at/07-2/5a/

4) siehe Artikel *GÉANT2 – Ein Glasfaserbackbone für die Wissenschaft* in *Comment 06/3*, Seite 19 bzw. unter http://comment.univie.ac.at/06-3/19/

bung des ACOnet-Backbone auch dort eine entsprechende Redundanz-Verbesserung vorzusehen.

Dies ist gelungen: Die neue Topologie basiert – bezogen auf jede Stadt – auf vollkommen wege-redundanten Glasfaserverbindungen, mit einer Verdoppelung der ACOnet-POP-Standorte[5)] in den Städten Graz, Innsbruck, Klagenfurt, Linz und Salzburg (siehe **Abb. 2**). Die Glasfaserverbindungen und das zur Signalverstärkung benötigte Equipment wird vom Ausschreibungsgewinner Telekom Austria AG exklusiv für ACOnet bereitgestellt, überwacht und gewartet. Initial werden durch ACOnet auf jeder Strecke 10-Gigabit-Ethernet-Verbindungen errichtet und in Betrieb genommen. Mittels Wellenlängen-Multiplexing-Technologie (DWDM)

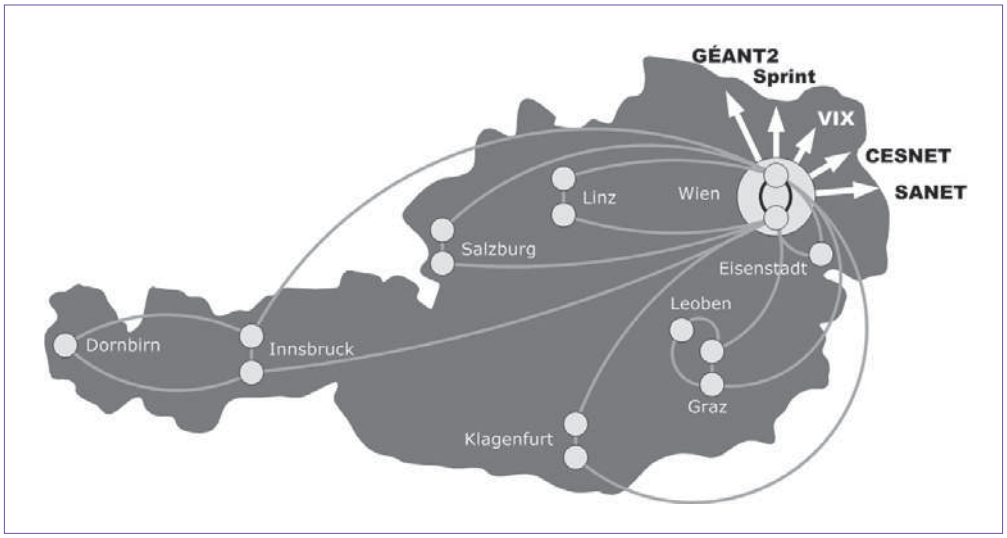


Abb. 2: Die künftige Topologie des ACOnet-Glasfaserbackbone

kann jede Glasfaserstrecke auf bis zu 40-mal 10-Gigabit-Ethernet erweitert werden. Sobald es die Technologieentwicklung ökonomisch vertretbar zulässt und sofern ein entsprechender Bedarf entsteht, können wir in Kooperation mit der Telekom Austria im Rahmen des abgeschlossenen Vertrages sogar auf 100-Gigabit-Technologie (je Multiplex-Kanal!) umstellen.

Das klingt alles reichlich utopisch, aber der Rahmenvertrag wurde immerhin auf 10 Jahre abgeschlossen, mit einer Verlängerungsoption auf 15 Jahre. Und angesichts der Bandbreiten-Entwicklungen der letzten 15 Jahre – von 64 kbit/s auf 10 Gbit/s, also ein Faktor von etwa 150 000 – sollten wir uns nicht der Gefahr verantwortungsloser Kurzsichtigkeit aussetzen.

Das „Rollout" erfolgt von Wien aus westwärts. Der vereinbarte Zeitplan sieht vor, die Standorte Linz und Graz noch heuer auf die neue Technologie umzustellen, und Ende 2008 wollen wir in Innsbruck und Dornbirn angekommen sein. Die Umstellung von der alten auf die neue Topologie und Technologie sollte weitestgehend unterbrechungsfrei erfolgen: Nachdem beide Infrastrukturen von der Telekom Austria bereitgestellt werden und alle ACOnet-Knoten von uns in hervorragender Kooperation mit den jeweiligen Standorten betrieben werden, rechnen wir mit keinen nennenswerten Turbulenzen.

Neue Möglichkeiten tun sich auf – Kooperation ist angesagt

Die neue ACOnet-Infrastruktur kann potentiell wesentlich mehr leisten als nur die klassischen Internet-Anwendungen schneller und in größerem Umfang zu transportieren. Der Phantasie sind hier kaum Grenzen gesetzt – im internationalen Umfeld gibt es bereits einige Projekte, die sich dedizierter Gigabit- und sogar 10-Gigabit-Übertragungskanäle bedienen, um auf vorhersehbaren Performance-Bedingungen aufsetzen zu können. Das Spektrum ist hierbei sehr breit und reicht von der Übertragung von Videostreams in HDTV-Qualität über weltweit verteilte Computer- bzw. Daten-Cluster-Anwendungen (*Grids*) bis hin zu Telemedizin und biometrischer Rasterfahndung (wertfrei aufgelistet). Ganz pragmatisch und national-budgetär gedacht steht mit dem neuen ACOnet-Backbone in Kürze eine Datennetz-Infrastruktur zur Verfügung, die es allen ACOnet-Teilnehmern ermöglicht, untereinander nahezu unbegrenzte Datenmengen zu vergleichsweise geringen Mehrkosten auszutauschen. Gegenseitige Service-Leistungen könnten daher besonders attraktiv angeboten werden. Gemeinsame Projekte mit hohem Datenvolumen, bisher schwierig bis unleistbar, erscheinen nun besonders interessant: qualitativ hochwertige Medienbibliotheken, eLearning-Anwendungen und -Inhalte, gegenseitige Datenspiegelung kritischer Verwaltungsdaten, gemeinsamer Betrieb einer Backup- oder Ausfallsrechenzentrums-Infrastruktur usw. Diese Möglichkeiten hat auch bereits das Bundeskanzleramt erkannt, das sich vor kurzem nicht nur in Wien, sondern auch in Salzburg mit dem so genannten ZAS (das *Zentrale Ausweichsystem* des Bundes in St. Johann im Pongau, das kürzlich sein 25-jähriges Bestehen feierte) an das ACOnet angeschlossen hat.

Jenseits des reinen Gigabit-Zuwachses sehen wir aber auch noch anderen Infrastruktur-Verbesserungen entgegen, die ebenfalls auf eine bessere und einfachere Kooperation unserer Teilnehmer-Organisationen und deren Studierenden abzielen. Bereits recht gut angenommen und umgesetzt wird die internationale Initiative **eduroam** (siehe `www.aco.net/eduroam.html`), die es den Angehörigen einer teilnehmenden Institution ermöglicht, ohne administrativen Aufwand auch die Funknetz-Infrastruktur aller anderen eduroam-Teilnehmer zu nutzen. Während ich diesen Artikel

schreibe, sitze ich am Carolinum in Prag und bin hier mittels eduroam mit meinen Uni-Wien-Benutzerdaten ins WLAN eingestiegen, ohne jeglichen Kontakt zur hiesigen Netzwerk-Administration.

Künftig wollen wir auch – ausgehend von der im Entstehen begriffenen *Authentifizierungs- und Autorisierungs-Infrastruktur* (AAI) an der Universität Wien[6] – gemeinsam mit interessierten ACOnet-Teilnehmern am Aufbau einer **ACOnet AAI Federation** auf Basis von Shibboleth arbeiten[7], wie sie in vielen anderen Wissenschaftsnetzen bereits besteht (z.B. dem Schweizer SWITCH, siehe `www.switch.ch/aai/`) bzw. im Aufbau ist. Solche Authentifizierungs- und Autorisierungs-Verbünde basieren auf einer etablierten Vertrauensgemeinschaft und ermöglichen es Service-Providern (insbesondere Anbietern von Bibliotheken und Datenbanken, aber auch z.B. von Verwaltungsapplikationen), den BenutzerInnen anderer Verbundteilnehmer einen vertraglich geregelten Zugriff einzuräumen, ohne hierfür selbst eine Benutzerverwaltung aufbauen zu müssen. Die BenutzerInnen authentifizieren sich also immer bei ihrer Heimatorganisation und erhalten auf Basis vereinbarter Attribute (z.B. *Student, Mitarbeiter, Verwaltungsangestellter*) die Autorisierung für bestimmte Services anderer Verbundteilnehmer. Im europäischen Wissenschaftsnetz-Backbone GÉANT2 wird unter dem Titel *eduGAIN* bereits an einer Gateway-basierten „Con-Federation" gearbeitet, die eine Verknüpfung der nationalen Federations ermöglichen soll.

Mit unseren **ACOnet-Webseiten** (`www.aco.net`) möchten wir ebenfalls den Kooperations-Aspekt besonders fördern: Im Teilnehmer-Portal gibt es nicht nur Zugriff auf teilnehmerbezogene Betriebsdaten und Statistiken, sondern es sind auch spezielle, getrennt autorisierbare Arbeitsgruppen-Bereiche möglich. Mit einem „Event-Manager" können zudem Anmeldungen und Informationen zu Workshops, Tutorials und Arbeitsgruppen-Treffen verwaltet werden. Das Thema Schulungen soll künftig im ACOnet-Kontext eine noch größere Bedeutung erlangen und vor allem eine breitere Zielgruppe ansprechen.

Das Wichtigste bei all diesen Kooperations-Offensiven ist allerdings, dass wir auf entsprechendes Interesse bei unseren Teilnehmern stoßen und kreative Anregungen erhalten. Das Motto von GÉANT2 lautet in diesem Zusammenhang übrigens *„connect communicate collaborate"*, und diesem Motto kann ich mich nur mit voller Überzeugung anschließen, denn genau das unterscheidet unser Umfeld von einem kommerziellen – nutzen wir es!

5) POP = *Point of Presence*

6) siehe Artikel *AAI in Aktion – Web Single Sign-On an der Uni Wien* in *Comment 07/2*, Seite 21 bzw. unter `http://comment.univie.ac.at/07-2/21/`

7) siehe `www.aco.net/aai.html` und `http://shibboleth.internet2.edu/`

8) siehe *Comment 05/1*, Seite 2 bzw. unter `http://comment.univie.ac.at/05-1/2/`

Neue Kurse & Handbücher zu MS-Office 2007

Beginnend mit dem Wintersemester 2007/2008 führt der ZID nicht nur Schulungen zu MS-Office XP, sondern auch zur neuen Version MS-Office 2007 durch. „Doppelgleisig" angeboten werden derzeit folgende Kurse:

- Access – Einführung
- Excel – Einführung
- Excel – Fortsetzung
- PowerPoint – Einführung
- PowerPoint – Fortsetzung
- Word – Einführung
- Word – Fortsetzung
- Word – Wissenschaftliches Arbeiten

Nähere Details wie Schulungsinhalte und Termine sind auf den Seiten 36–38 sowie unter `www.univie.ac.at/ZID/kurse/` zu finden.

Zu MS-Office 2007 sind inzwischen auch einige neue Handbücher des Regionalen Rechenzentrums für Niedersachsen (RRZN) verfügbar:

- *Access 2007 DB – Grundlagen für Datenbank-Entwickler*
- *Access 2007 DF – Fortgeschrittene Techniken für Datenbank-Entwickler*
- *Excel 2007 FF – Formeln und Funktionen clever nutzen*
- *PowerPoint 2007 F – Fortgeschrittene Techniken*

Neu hinzugekommen sind weiters die RRZN-Handbücher *Photoshop CS3 – Einführung* und *Mathematica – Einführung in das Computeralgebrasystem*. Eine vollständige Liste aller am ZID erhältlichen Handbücher finden Sie auf Seite 39 sowie unter dem URL `www.univie.ac.at/ZID/handbuecher/`.

Eveline Platzer-Stessl

Bei allem Jubel und aller Vorfreude möchte ich abschließend nicht versäumen an einen Menschen zu erinnern, von dem das genannte Motto auch stammen könnte und der durch seine Forschungs-, Schulungs- und Kommunikationsaktivitäten so viele Fäden der österreichischen Vernetzungslandschaft miteinander verknüpft hat wie kaum ein anderer. Er hat den Grundstein für ACOnet gelegt, nahezu Generationen von Netzwerktechnikern sind durch „seine Schule" gegangen, und wir haben ihn manchmal liebevoll „den Knoten" genannt: unseren lieben und unvergessenen Kollegen und Freund Walter Kunft, der am 28. November 2004, also vor fast genau drei Jahren, verstorben ist.[8] Ich hoffe, dass wir ACOnet gemeinsam in seinem Sinne weiterentwickeln und die Kooperations-Idee und -Bereitschaft weitertragen können.

Christian Panigl

Der Virtuelle Campus

Internet für Studentenheime

71 Studentenheime in ganz Österreich nehmen am *Virtuellen Campus* teil, der Internet-Anbindung von Studentenheimen an das österreichische akademische Computernetz ACOnet. Dieses nationale Wissenschaftsnetz, das die österreichischen Forschungs-, Bildungs- und Kultureinrichtungen untereinander und mit dem Internet verbindet, wird seit nunmehr 15 Jahren vom Zentralen Informatikdienst der Universität Wien betrieben (siehe Seite 11).

Das Besondere am „VCampus" ist, dass die ACOnet-Teilnahme den Studentenheimen nichts kostet: Das Wissenschaftsministerium übernimmt nämlich den Kostenbeitrag für die ACOnet-Teilnahme der Studentenheime bis zu einer vertraglichen ACOnet-Bandbreite von 2 Mbit/s pro 100 HeimbewohnerInnen. So bekommt also z.B. ein Studentenheim mit 320 Heimplätzen 8 Mbit/s Bandbreite zugesprochen (die Anzahl der Heimplätze wird jeweils auf ganze Hundert aufgerundet). Die Kosten für die *last mile*, also die physische Leitung vom Studentenheim zum nächsten ACOnet-Knoten[1)], muss jedoch der Heimträger übernehmen.

Diese physische Leitung kann und soll eine deutlich höhere Bandbreite als die „vertragliche ACOnet-Bandbreite" aufweisen, denn dieses Limit gilt nur für den Datenverkehr aus dem kommerziellen Internet. Eine Anbindung an ACOnet ermöglicht dem Studentenheim aber darüber hinaus – entsprechend den Zielsetzungen eines Wissenschaftsnetzes – eine sehr schnelle Gratis-Verbindung zu den anderen ACOnet-Teilnehmern und auch international zu anderen Wissenschaftsnetzen, unabhängig von der Anzahl der HeimbewohnerInnen. Diese unlimitierte (bzw. lediglich durch die Leistungsfähigkeit der lokalen Datenleitung beschränkte) Internet-Verbindung bietet den HeimbewohnerInnen ausgezeichnete Möglichkeiten, vom Studentenheim aus multimedialen Content von Universitätsservern zu beziehen, an eLearning-Projekten teilzunehmen, mit den Angehörigen anderer Forschungs- und Bildungseinrichtungen Videokonferenzen zu veranstalten usw., ohne mit allen MitbewohnerInnen die knappe Bandbreite ins weltweite Internet teilen zu müssen.

Wie kann man sich an den VCampus anschließen?

Voraussetzung für die Kostenübernahme durch das Wissenschaftsministerium ist, dass die Studentenheim-Trägerorganisation mit der Universität Wien eine entsprechende ACOnet-Teilnahmevereinbarung[2)] abschließt. Dem Heimträger entstehen durch den Abschluss einer solchen Vereinbarung keine Kosten, und sie kann von ihm auch jederzeit wieder gekündigt werden. Falls der Heimträger eine höhere vertragliche ACOnet-Bandbreite wünscht, als ihm vom Wissenschaftsministerium finanziert wird, ist das gegen Aufzahlung selbstverständlich möglich. Ein diesbezügliches Informationsschreiben[3)] wurde im Juli 2006 an alle Trägerorganisationen der österreichischen Studentenheime ausgesandt.

Der Heimträger muss in jedem Fall die Kosten für eine entsprechende Leitungsverbindung vom Studentenheim zum nächsten ACOnet-Anschlusspunkt tragen und sich um die technische Infrastruktur im Studentenheim selbst kümmern; der ZID der Universität Wien ist jedoch gerne dabei behilflich, die erforderlichen Schritte in Angriff zu nehmen. Alle weiteren Informationen zum Virtuellen Campus finden Sie unter `www.aco.net/vcampus.html`.

Peter Rastl

---

1) siehe `www.aco.net/standorte.html`

2) siehe `www.aco.net/aconet-vereinbarung-sth.pdf`

3) siehe `www.aco.net/aconet-studentenheime.pdf`

Personalnachrichten

Wie immer sind seit dem Erscheinen des letzten *Comment* einige personelle Veränderungen am Zentralen Informatikdienst zu verzeichnen: In der Abteilung *Universitätsverwaltung* des ZID haben im August 2007 bzw. im September 2007 zwei neue Mitarbeiterinnen, **Tina Kiszner** und **Marlies Bradl**, ihre Tätigkeit in der UNIVIS-Projektkoordination aufgenommen. Die Abteilung *Zentrale Services & Benutzerbetreuung* hat ebenfalls Zuwachs erhalten – **David Schmidt** arbeitet seit Mitte Juli 2007 im Team der Internet-Domainverwaltung, und **Lukas Hönigsberger** verstärkt seit Mitte September 2007 unseren Helpdesk.

Unser langjähriger Mitarbeiter **Aron Vrtala**, der in den letzten beiden Jahren intensiv am Aufbau des PC-Supports der Fakultätsunterstützung mitwirkte, hat hingegen im August 2007 einen einjährigen Karenzurlaub angetreten, und **Margaretha Sylla-Widon**, die seit ihrem sechzehnten Lebensjahr an der Universität Wien als Telefonistin tätig war, genießt seit September 2007 ihren wohlverdienten Ruhestand. Wir wünschen ihr alles Gute für diesen neuen Lebensabschnitt, so wie wir auch allen neuen Mitarbeiterinnen und Mitarbeitern viel Freude und Erfolg bei der Arbeit am ZID wünschen.

Peter Rastl

Ein Konzept bewährt sich:

1000 Instituts-PCs mit Fernwartung

Seit rund drei Jahren betreut der Zentrale Informatikdienst die PCs von Organisationseinheiten der Universität Wien in einem sehr viel größeren Umfang als früher. Der erste Versuch einer solchen umfassenden Unterstützung wurde 2004 an der Rechtswissenschaftlichen Fakultät gestartet, wo er auf große Akzeptanz stieß (siehe Artikel *Anmerkungen zur EDV-Sanierung des Juridicums* in *Comment 05/1*, Seite 3 bzw. unter `http://comment.univie.ac.at/05-1/3/`). Nach Abschluss dieses Projekts wurde das neu geschaffene System zur Ferninstallation und -wartung von Software – vom ZID kurz *Organon* genannt – unter Einbeziehung aller gewonnenen Erfahrungen für einen universitätsweiten Einsatz adaptiert.

Im September 2007 konnte nun ein beachtlicher Teilerfolg gefeiert werden: Mehr als 1000 PCs, verteilt auf 12 Fakultäten und Dienstleistungseinrichtungen der Universität Wien, werden seither über das Organon betreut. Die Teilnahme an diesem System erfolgt auf freiwilliger Basis: Bei Interesse seitens einer Organisationseinheit (OE) startet zunächst ein Prozess der Produktpräsentation und Evaluation. Sofern erwünscht und machbar, folgt dann die eigentliche Umstellung, die sich je nach Rahmenbedingungen und Softwareanforderungen unterschiedlich aufwendig gestaltet.

Die Services der Arbeitsgruppe *Fakultätsunterstützung* (FU) des Zentralen Informatikdienstes sind ausschließlich für Organisationseinheiten der Uni Wien – nicht für einzelne MitarbeiterInnen – verfügbar und gliedern sich in die Bereiche Beratung, Exchange-Service und Organon. Diese werden im Folgenden kurz vorgestellt; alle Details finden Sie im Internet unter `www.univie.ac.at/ZID/fu/`. Grundsätzlich ist zu sagen, dass der ZID nur dann eine derart umfassende Betreuung anbieten kann, wenn die teilnehmende OE eine/n zuständige/n Instituts- bzw. Fakultätsbetreuer/in stellt, der/die alle vor Ort anfallenden Aufgaben erledigt und als Kontaktperson zum ZID fungiert.

Beratung

Im Vorfeld der Umstellung einer Organisationseinheit auf das Exchange- und/oder Organon-Service erfolgt eine ausführliche Beratung der jeweiligen Instituts- oder FakultätsbetreuerInnen. Dabei geht es vor allem darum, wie die PCs ferninstalliert und gewartet werden sollen, d.h. um Hardwareanforderungen, Arbeitsabläufe und Arbeitsaufteilungen. Bei Bedarf ist auch eine Kaufberatung möglich. Zudem ist die Arbeitsgruppe *Fakultätsunterstützung* des ZID bemüht, die EDV-BetreuerInnen in einen ständigen Dialog einzubinden. Dies geschieht insbesondere durch regelmäßige Sitzungen, an denen angesichts der über tausend betreuten PCs bereits eine ansehnliche Zahl von FakultätsbetreuerInnen teilnimmt. In diesen Sitzungen werden offene Probleme und mögliche Verbesserungen besprochen. Durch den Austausch von Wissen und Erfahrungen der FakultätsbetreuerInnen und des ZID kann eine viel bessere Servicequalität für die EndanwenderInnen geboten werden.

Exchange-Service

MS-Exchange ist eine Software, die Arbeitsgruppen eine gemeinsame Nutzung verschiedener Daten wie eMail-Nachrichten, Kalender, Kontakte, Aufgabenlisten etc. erleichtert. Das Exchange-Service des ZID wird üblicherweise in Kombination mit dem Organon in Anspruch genommen, kann aber im Prinzip auch unabhängig davon verwendet werden. MS-Exchange wurde im *Comment* bereits ausführlich vorgestellt; nähere Informationen dazu entnehmen Sie daher bitte dem Artikel *Teamarbeit leicht gemacht – Das Exchange-Service des ZID* in *Comment 07/1*, Seite 29 bzw. unter `http://comment.univie.ac.at/07-1/29/`.

Organon

Unter diesem Namen bietet der ZID eine automatisierte Ferninstallation (auch „Beschickung“ oder „Deployment“ genannt) von Instituts-PCs, verbunden mit einer zentral organisierten, permanenten Softwarewartung. Die betreuten Rechner werden dabei nacheinander mit einer Grundbeschickung, einem Freeware/Shareware-Desktop und bei Bedarf mit Zusatzsoftware ausgestattet.

Grundbeschickung

Diese Phase umfasst die Installation des Betriebssystems (derzeit nur MS-Windows; Linux befindet sich im Testbetrieb) sowie essentieller Komponenten wie Virenscanner, *Windows Server Update Service* (WSUS), Perl-Interpreter und SSH-Server. Die beiden letzteren werden für die Ferninstallation benötigt; über WSUS erfolgt die regelmäßige Aktualisierung der Microsoft-Produkte am PC (z.B. MS-Windows, MS-Office). Der Virenscanner wird vom ebenfalls in dieser Phase installierten *McAfee ePolicy Orchestra Service* (EPO) laufend mit den neuesten Virensignaturen versorgt.

Freeware/Shareware-Desktop

Nach der Grundbeschickung werden die PCs mit einer Palette nicht-kommerzieller (Gratis-)Software versehen. Dieser so genannte Freeware/Shareware-Desktop umfasst zahlreiche Anwendungsprogramme des täglichen Bedarfs, z.B.:

- Mozilla Firefox mit Shockwave-, Flash- und Citrix-Plugin (Webbrowser)
- Mozilla Thunderbird (Mailing)
- 7-Zip, Filezilla, Putty (Dateikompression/-übertragung)

Auszug aus dem Software-Portfolio der Fakultätsunterstützung

(eine vollständige Liste finden Sie unter www.univie.ac.at/ZID/fu-windows/)

Freeware / Shareware / Gratissoftware:

- ActiveSync
- AllwaySync
- Force
- FoxIt
- FreeMind
- iTunes
- OpenOffice.org
- Skype
- VLC Media Player

Kommerzielle Software:

- Adobe Acrobat
- Adobe CS (Photoshop, InDesign, Illustrator, GoLive)
- Adobe Pagemaker
- Adobe Premiere
- Corel Draw
- Corel WordPerfect
- Filemaker
- Macromedia Dreamweaver
- Microsoft Office
- Microsoft OneNote
- Microsoft Project
- Microsoft Visio
- Microsoft Visual Studio .NET Professional
- Nero
- Omnipage
- Reference Manager

Sparten- bzw. Spezialsoftware (teilweise kommerziell):

- Allercalc
- Amos
- APA-Online Manager
- A-Plan
- AutoCAD
- Bibedt
- Convento
- Euklid Dynageo
- Freedom Scientific Jaws
- Freedom Scientific MAGic
- Ghostscript
- Ghostview
- GnuPlot
- i3v
- IDL
- JEdit
- Mathematica
- MATLAB
- MiKTeX
- SAP
- SAS
- SciFinder
- SigmaPlot
- SPSS
- WinEdt
- WinShell
- XNView
- ConTEXT (Editor)
- IrfanView, Gimp, Nvu, Adobe Reader und FreePDF (Erstellen, Bearbeiten und Betrachten von Grafiken, Fotos, Websites und PDF-Dateien)
- Virtual Dub (Abspielen von Videos/DVDs und einfache Videobearbeitung)
- CDBurner XP Pro (CD-/DVD-Brennen)

Zusatzsoftware

Neben dieser auf jedem „FU-PC“ vorhandenen Freeware/Shareware-Ausstattung bietet der ZID noch eine ganze Reihe anderer nicht-kommerzieller und kommerzieller Programme an, die bei Bedarf für eine automatisierte Installation aufbereitet („geskriptet“) werden können. Einen besonderen Fall stellt dabei die so genannte Spartensoftware dar – das sind Programme, die nur von einem eingeschränkten Personenkreis benötigt werden, z.B. nur von einzelnen Fakultäten, Instituten oder Arbeitsgruppen. Im Rahmen der Spartensoftware sind auch die Universitätsverwaltungssoftware i3v, SAP sowie Programme zur Unterstützung von Personen mit eingeschränktem Sehvermögen verfügbar. Der ZID bemüht sich selbstverständlich auch hier, spezielle KundInnenwünsche zu erfüllen. Zur Zeit befinden sich rund 150 fertig geskriptete Programme im Zusatzsoftware-Portfolio der Fakultätsunterstützung. Einen kleinen Auszug daraus finden Sie im nebenstehenden Kasten.

Damit ein bestimmtes Produkt vom ZID geskriptet werden kann, müssen folgende Kriterien erfüllt sein:

- Das Programm muss lizenziert sein, beispielsweise im Rahmen der Standardsoftware (Näheres siehe www.univie.ac.at/ZID/standardsoftware/).
- Sofern es nicht als Standardsoftware am ZID erhältlich ist, muss ein Mindestbedarf von 10 installierten PCs bestehen.
- Das Skripten der Software muss technisch machbar sein, was bisher bei ca. 90% aller Anfragen der Fall war.

Das Erstellen einer solchen automatisierten Software-Installation dauert je nach Komplexität und Umfang zwischen zwei Tagen und zwei Wochen. Die Zeitspanne vom Eintreffen des KundInnenwunsches bis zur Überprüfung der Machbarkeit ist hierbei nicht inkludiert; im Regelfall gelingt es uns jedoch, auch die Machbarkeitsprüfung innerhalb der genannten Frist durchzuführen. Sofern mit einem Produkt ein zusätzlicher Aufwand verbunden ist (z.B. wenn dafür ein eigener Lizenzserver benötigt wird), ist allerdings mit etwas längeren Vorlaufzeiten zu rechnen.

Feedback

Zum Abschluss sollen hier noch einige EDV-BetreuerInnen von Instituten zu Wort kommen, die die Services der Fakultätsunterstützung bereits nutzen:

Unser Institut war das Pilotprojekt bei der Einführung der Fakultätsbetreuung: Zu meiner Überraschung verlief die Umstellung unserer EDV völlig problemlos. Es freut mich, dass ich mich um keine Updates, Sicherungskopien und Ähnliches kümmern muss – das machen unsere PCs beim Herunterfahren ohne uns bei der

Arbeit zu stören „von selber" – meinen herzlichen Dank dem Fakultätsbetreuungsteam / Helpdesk.
Mag. Sybille Krausler (Institut für Staatswissenschaft)

Das Softwaredeployment installiert ein an die Uni angepasstes System. Konfiguration, Programme und Drucker sind schon da, wenn man sich das erste Mal einloggt. Das erleichtert nicht nur den Support für unbedarftere User, sondern verschafft auch die Sicherheit, dass es, wenn was schiefgeht, auch schnell wieder ein lauffähiges System auf meinem Laptop gibt.
Mag. Dr. Rupert Ursin (Quantenoptik, Quantennanophysik und Quanteninformation)

Bevor die Betreuung der PCs an unserem Institut vom ZID übernommen worden ist, war regelmäßig beinahe die Hälfte der Rechner von Trojanern oder/und Viren befallen. Die Hauptursache dafür lag darin, dass es leider nicht möglich war, den Mitarbeitern nachhaltig zu vermitteln, dass sie Betriebssystem und Antivirenprogramm – im Wesentlichen selbstständig – auf dem aktuellen Stand halten müssen. Die zumeist fehlende Firewall und der Umstand, dass alle Mitarbeiter Administratorenrechte besessen haben, hat das Übrige zu der seinerzeitigen Misere beigetragen. Im Ergebnis musste damals ca. alle zwei Wochen ein Rechner (manuell) neu aufgesetzt und ins Netzwerk eingebunden werden, was mir als EDV-Verantwortlichen einen enormen zusätzlichen Zeit- und Betreuungsaufwand verursacht hat. Aber auch die anderen Institutsangehörigen waren aufgrund der häufig vorkommenden Datenverluste in ihrer Arbeit beeinträchtigt. Seit Übernahme der Betreuung durch den ZID sind keine vergleichbaren Missstände mehr aufgetreten, sodass ich die Bemühungen der Fakultätsunterstützung als äußerst erfolgreich und nützlich beurteile. ***Univ.-Ass. Mag. Dr. Wojciech Jaksch-Ratajczak (Institut für Zivilrecht)***

Kurze Einschulungszeit, Reduktion der Wartungszeit, erhöhte Datensicherheit und die Redundanz des Services für die Benutzer(innen) (falls der/die EDV-Verantwortliche gerade nicht anwesend ist – Support durch die FU möglich) sind für mich überzeugende Argumente, für die sich ev. geringfügige Umstellungen des Benutzer(innen)verhaltens (Stichwort „Unart große Daten auf dem Desktop aufzubewahren") auf alle Fälle lohnen. ***Mag. Oliver Strubreither (Institut für Sportwissenschaft)***
Anm.: Dokumente am Desktop zu speichern führt zu längeren Wartezeiten beim Login/Logout.

Dank der intensiven Kooperation mit der FU konnte die Fakultät eine zentral verwaltete Linux-Lösung implementieren. Alle Besonderheiten der IT-Infrastruktur konnten problemlos abgebildet werden.
Andreas Nemeth (Institut für Mathematik)

Rainer Jantscher & Jörg Egger

Neue Standardsoftware

Neue Produkte (Stand 17. 9. 2007)

- Adobe Acrobat Prof. 8 für Windows und Mac
- Adobe After Effects CS3 8.0 für Windows und Mac
- Adobe Dreamweaver CS3 9.0 für Windows und Mac
- Adobe Encore CS3 3.0 für Windows und Mac
- Adobe Fireworks CS3 9.0 für Windows und Mac
- Adobe Flash Prof. CS3 9.0 für Windows und Mac
- Adobe GoLive CS3 9.0 für Windows und Mac
- Adobe Illustrator CS3 13.0 für Windows und Mac
- Adobe InDesign CS3 5.0 für Windows und Mac
- Adobe Photoshop Ext. CS3 10.0 für Windows und Mac
- Adobe Photoshop Lightroom 1.0 für Windows und Mac
- Adobe Premiere Prof. CS3 3.0 für Windows und Mac
- Adobe Soundbooth CS3 für Windows und Mac
- Apple iLife '08 für Mac
- Apple iWork '08 für Mac
- FileMaker Pro 9.0 für Windows und Mac
- MindManager 7 Prof. für Windows und Mac
- MS-Expression Blend für Windows (siehe Seite 18)
- MS-Expression Design für Windows (siehe Seite 18)
- MS-Expression Media für Windows (siehe Seite 18)
- MS-Expression Web für Windows (siehe Seite 18)
- MS-Windows Vista Ultimate
- RSI IDL 6.4 für Windows und Mac
- VMware Fusion 1.0 für Mac
- VMware Workstation 6 für Windows und Linux

Updates (Stand 17. 9. 2007)

- LabVIEW 8.2.1 für Windows, Mac, Linux (bisher 8.2)
- MATLAB R2007b für Win, Mac, Linux (bisher R2007a)

MS-Windows Vista Ultimate

MS-Windows Vista Ultimate ist die am besten ausgestattete Version des neuen Microsoft-Betriebssystems und bietet im Vergleich mit dem bereits bisher als Standardsoftware erhältlichen Vista Enterprise zusätzlich das Media Center. Bei Vista Ultimate muss jede Installation mit einem individuellen *License Key* freigeschaltet werden; aus diesem Grund kostet eine Lizenz EUR 30,– (exkl. Datenträger) statt EUR 21,–.

Neue Software für Studierende

Für Studierende ist nun auch Mathematica 6 für Windows, Mac und Linux um EUR 15,– erhältlich. Wer Mathematica 5.2 über den Webshop (`www.univie.ac.at/ZID/softwareshop/`) bezogen hat, erhält die Version 6 als Gratisupdate; sie muss jedoch wie gewohnt über unseren Webshop bestellt werden.

Informationen zur Standardsoftware:
`www.univie.ac.at/ZID/standardsoftware/`
Informationen zur Software für Studierende:
`www.univie.ac.at/ZID/softwareshop/`

Peter Wienerroither

Als Standardsoftware erhältlich:

Microsoft Expression Studio

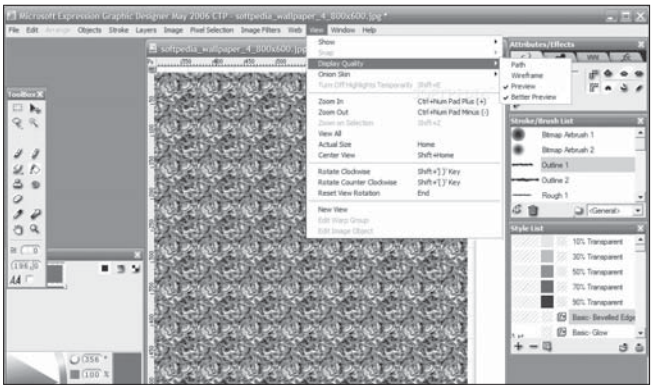
Seit dem Wintersemester 2007/2008 bietet der ZID im Rahmen der Standardsoftware (siehe Seite 17) den Instituten und Dienststellen der Universität Wien das Softwarepaket ***MS Expression Studio*** an. Zu dessen Komponenten zählen die Programme ***Expression Blend***, ***Expression Design***, ***Expression Media*** sowie ***Expression Web***, die separat erhältlich sind.

Expression Blend

Expression Blend ist ein ***Entwickler- und Designwerkzeug für interaktive Benutzeroberflächen und Anwendungen***. Mit dieser Software können Videos, Vektorgrafiken, Schriften, Animationen, Bilder und 3D-Elemente mit interaktiven Bedienelementen kombiniert werden. Diese können entweder aus anderen Programmen importiert (siehe Expression Design) oder mit den in Blend integrierten Vektorgrafik-Tools im Programm selbst erstellt werden.

Expression Design

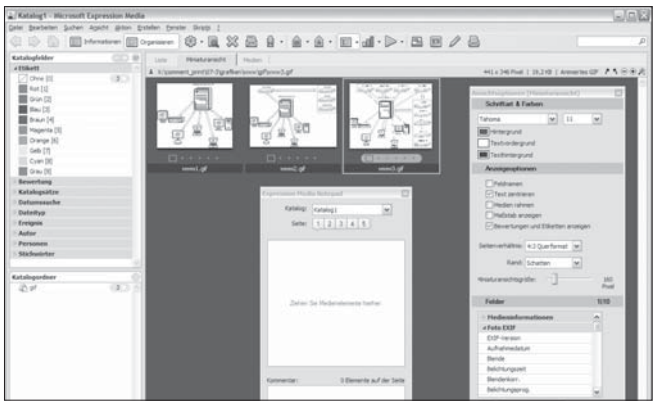
Um grafische Inhalte für Expression Blend selber zu erstellen, steht auch das im Studio-Paket enthaltene ***Vektorgrafik-Zeichenprogramm*** Expression Design zur Verfügung. Mit diesem Programm erstellte Grafiken können nicht nur in die Adobe-eigenen Formate für Photoshop (`.psd`), Illustrator (`.ai`) und Acrobat (`.pdf`) exportiert werden, sondern auch in XAML[1)], welches in Expression Blend Verwendung findet.



Expression Design – Zeichenprogramm

Expression Media

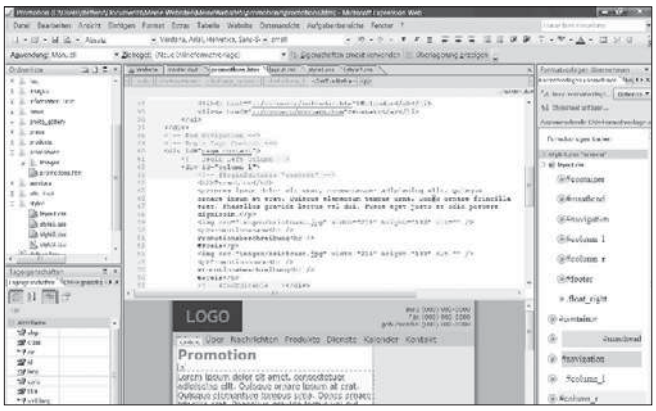
Als ***Verwaltungstool für Bild-, Audio- und Videodaten*** katalogisiert und konvertiert Expression Media viele gängige Formate. Medien können per *Drag & Drop* geordnet werden, Sterne symbolisieren Bewertungen, Farben markieren den Bearbeitungsstatus. Durch die Vergabe von Kategorien, Personennamen und Schlagwörtern sowie beispielsweise die Indexierung mittels Datum lassen sich umfangreiche Suchanfragen durchführen.



Expression Media – Verwaltungstool

Expression Web

Microsoft Expression Web ist ein ***Werkzeug für Webdesigner und Webentwickler***. Der WYSIWYG-Webeditor ist das Nachfolgeprodukt von Microsoft FrontPage auf Basis aktueller Standards wie CSS, XHTML und XML, beherrscht jedoch kein PHP oder Ajax. Wer bereits mit Adobe (vormals Macromedia) Dreamweaver gearbeitet hat, sollte sich in diesem Programm schnell zurechtfinden. Im Gegensatz zu Expression Design und Expression Blend fehlt Expression Web jedoch die XAML-Schnittstelle – und somit der Berührungspunkt zu diesen beiden Komponenten des Studio-Paketes.



Expression Web – Software für Webdesign

Alle vier Programme sind am ZID als Standardsoftware erhältlich bzw. können auch über die Microsoft-Website unter `www.microsoft.com/germany/expression/` einzeln als ***Testversion (bis zu 180 Tagen kostenlos)*** heruntergeladen werden.

Katharina Lüthke

1) *eXtensible Application Markup Language*, eine in XML formulierte Sprache zur Beschreibung und Erstellung von Oberflächen (siehe auch Artikel *Webpublishing mit XML* in *Comment 06/3*, Seite 40 bzw. unter `http://comment.univie.ac.at/06-3/40/`)

Software-Update in den PC-Räumen

In den PC-Räumen der Uni Wien wurde im September 2007 die Software-Ausstattung aktualisiert. Eine vollständige Liste der nun verfügbaren Programme finden Sie im Kasten unten oder unter `www.univie.ac.at/ZID/pcr-ausstattung/`.

Die wichtigsten Änderungen:

- Die Mozilla-Suite wurde durch die Einzelprogramme **Firefox** (Browser), **Thunderbird** (Mailing) und **Nvu** (Web-Editor) ersetzt. Alle bestehenden Benutzereinstellungen für Mozilla wurden dabei automatisch übernommen.

- Im Mailprogramm Thunderbird ist nun die **verschlüsselte Übertragung der Nachrichten** vom Posteingangsserver aktiviert, und zwar mittels TLS, sofern der Benutzer nicht vorher schon SSL verwendet hat. Darüber hinaus wurden in die Konfiguration des Mailprogramms automatisch die **neuen Servernamen** eingetragen (für alle Universitätsangehörigen lautet der Name des Posteingangsservers nun IMAP.UNIVIE.AC.AT, der des Postausgangsservers MAIL.UNIVIE.AC.AT; siehe hierzu auch Seite 25).

- Neu sind **Mathematica** 6.0 sowie **Open Office** 2.2.1 inklusive Wörterbüchern für ca. 30 Sprachen (MS-Office XP bietet nur Wörterbücher für Deutsch, Englisch, Französisch und Italienisch). Bei Office XP wurde das **Compatibility Pack für MS-Office 2007** nachinstalliert – damit kann nun auch das neue Dateiformat gelesen und geschrieben werden.

- Von Adobe Acrobat Professional ist jetzt die Version 8.1 verfügbar. Zusätzlich wurde der **Adobe Reader** 8.1 installiert, der für die Standardanwendungen *PDF Anzeigen* und *Drucken* zu empfehlen ist: Der Adobe Reader kann bestimmte Dokumente schneller drucken als Acrobat Professional. Die beiden Programme sind zwar nicht gleichzeitig verwendbar, das sollte aber kein nennenswertes Problem darstellen.

- WinZip wurde durch das Programm **7-Zip** ersetzt. 7-Zip kann auch `.rar`-Dateien entpacken, was immer wieder gewünscht wurde.

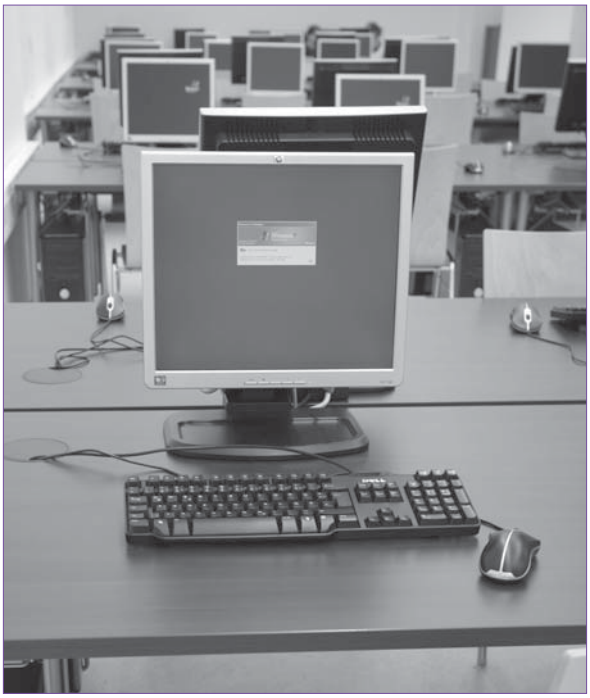
- Im Multimedia-Bereich wurden zahlreiche **Audio- und Video-Codecs** neu oder in neuer Version installiert, sodass nun verschiedenste Formate abgespielt werden können.

Noch eine Neuerung ist mit Beginn des Wintersemesters 2007/2008 in Kraft getreten: Die **PC-Räume des Zentralen Informatikdienstes im NIG** (1010 Wien, Universitätsstraße 7, Stiege I, 1. Stock) sind nun **samstags bis 18:00 Uhr geöffnet**.

Dieter Stampfer

Software in den PC-Räumen der Universität Wien

Mozilla Firefox 2.0	(statt Mozilla-Suite)
Mozilla Thunderbird 2.0	(statt Mozilla-Suite)
Nvu 1.0	(statt Mozilla-Suite)
Microsoft Internet Explorer 7	(Update)
Microsoft Office XP	(wie bisher, aber mit Compatibility Pack)
Open Office 2.2.1	(neu)
Mathematica 6.0	(neu)
Adobe Reader 8.1	(neu)
Adobe Acrobat Professional 8.1	(Update)
Adobe Illustrator 11	(wie bisher)
Adobe Photoshop 8	(wie bisher)
SPSS 15	(Update)
AMOS 7	(Update)
Java JRE 1.5.0.12	(Update)
McAfee VirusScan 8.5	(Update)
Citrix ICA-Client 10.1	(Update)
IrfanView 4.0 mit Plugins	(Update)
Putty 0.60	(Update)
SciTE 1.74	(Update)
7-Zip 4.4.2	(statt WinZip)
WS-FTP LE 6.0	(wie bisher)
WinSSH 3.2.9	(wie bisher)
Exceed 6.1	(wie bisher)



PC-Raum der Universität in 1010 Wien, Schenkenstraße 8–10

WWW.UNIVIE.AC.AT
Alte Adresse, neue Architektur

Ein neuer Webserver?

Seit den Anfängen des Webauftritts der Universität Wien im Jahr 1995 wurde im *Comment* schon mehrmals ein „neuer Webserver" angekündigt.[1)] Diese neuen Webserver waren jedesmal mit einer Erneuerung des Software-Standes und neuen Features verbunden (z.B. die PHP-Unterstützung seit Juni 2005), das Grundkonzept des Servers WWW.UNIVIE.AC.AT wurde aber seit 1995 nicht wesentlich verändert. Im Großen und Ganzen hat sich dieses Konzept auch gut bewährt: Der derzeit verwendete Unix-Server ist sehr leistungsfähig und kann mehrere Millionen Anfragen pro Tag problemlos bewältigen – an Spitzentagen zu Semesterbeginn sind es alles in allem an die 13 Millionen.

Ein Problem dieses „monolithischen" Servers (siehe **Abb. 1**) ist allerdings eine gewisse Anfälligkeit: Der Server beherbergt mehrere Millionen HTML-Dokumente und andere Dateien, zahlreiche CGI-Skripts und PHP-Programme. Jede einzelne Seite kann Ziel einer *Denial of Service*-Attacke werden; Probleme durch ein einziges fehlerhaftes Programm können zu übermäßigem Ressourcenbedarf führen und dadurch den ganzen Server in Mitleidenschaft ziehen. Durch geeignete Maßnahmen kann man solche Probleme zwar eindämmen, aber nicht ganz verhindern. Auch die Software-Wartung ist auf einem so großen und komplexen System schwierig, weil jede Änderung unvorhergesehene Auswirkungen haben kann.

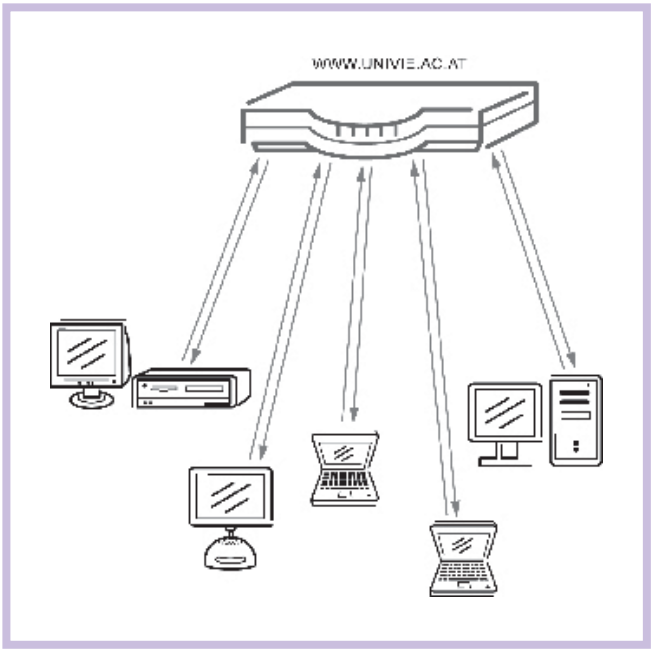


Abb. 1: Das bisherige Konzept des Webservers der Uni Wien: Ein einzelner Server beantwortet alle Anfragen.

Da der aktuelle Server demnächst an die Grenzen seiner Leistungsfähigkeit stoßen wird, ist bald wieder ein „neuer Webserver" erforderlich. Es wäre relativ einfach, die Hardware zu tauschen (es gibt noch wesentlich stärkere Server!), aber um die oben beschriebenen Anfälligkeiten zu beseitigen, hat sich der ZID entschlossen, stattdessen ein radikal neues Konzept von verteilten Servern einzuführen, das im Folgenden näher beschrieben wird.

Das neue Server-Konzept

Es gibt verschiedene Ansätze, ein verteiltes Konzept zu realisieren. Eine Möglichkeit wäre ein Cluster von Servern, die alle unter demselben Hostnamen zu erreichen sind und über ein verteiltes Filesystem alle auf dieselben Daten zugreifen. Ein Vorteil eines solchen Clusters ist die perfekte Lastverteilung (*Load Balancing*) – jede Anfrage kann von jedem beliebigen Server im Cluster beantwortet werden. Wir haben uns jedoch für eine andere Lösung entschieden: Nachdem der Webserver der Universität Wien ein historisch gewachsenes, komplexes System ist, kann eine so weit reichende Umstellung kaum auf einmal durchgeführt werden, sondern muss vielmehr schrittweise und ohne nennenswerte Unterbrechung des laufenden Betriebs erfolgen. Auch sollen möglichst wenige Änderungen von Benutzerseite erforderlich sein – d.h. was bisher funktioniert hat, soll auch weiterhin funktionieren.

Die Hauptbestandteile der neuen verteilten Server-Architektur sind ein *Frontend* und mehrere *Backends*:

- Der **Frontend-Server** ist von außen unter der Adresse WWW.UNIVIE.AC.AT zu erreichen und nimmt alle Anfragen der Klienten (Browser) entgegen. Auch alle virtuellen Hosts (z.B. WWW.UB.UNIVIE.AC.AT) sind auf dem Frontend-Server angesiedelt. Das Frontend beantwortet die Anfragen jedoch nicht selbst, sondern reicht sie unverändert[2)] an den zuständigen Backend-Server weiter, erhält von diesem die Antwort und schickt sie an die Klienten zurück: Das Frontend ist ein so genannter *transparenter Proxy*. Das ist eine wenig anspruchsvolle Aufgabe, die von einem einzigen Server mühelos bewältigt werden kann; als Frontend dient daher bis auf weiteres der bisherige WWW-Server.

- Den Großteil der Arbeit verrichten die **Backend-Server**: Dort befinden sich alle HTML-Dokumente und anderen Daten[3)], dort werden auch alle PHP- und sonstigen Skripts ausgeführt. In der Anfangsphase gibt es nur einen Backend-Server; sobald er ausgelastet ist, können problemlos weitere Server angefügt werden. Dadurch ist

diese Architektur praktisch beliebig skalierbar. Die Backend-Server sind von außen nicht sichtbar und durch eine Firewall vor jeglichem direkten Zugriff geschützt. Auf welchem Backend sich eine Applikation oder ein Dokument befindet, ist vollkommen unerheblich, weil der Hostname des Backend-Servers nirgends aufscheint. Deshalb ist es auch relativ leicht möglich, Applikationen von einem Backend auf ein anderes zu übersiedeln.

Neben dem Frontend und den Backends zählen noch einige andere Server (Datenbank-, Zugangs- und Logserver) zur Server-Farm, die in ihrer Gesamtheit den „neuen Webserver" bildet (siehe **Abb. 2**). Manche dieser Server sind als virtuelle Maschinen unter VMWare implementiert.[4)]

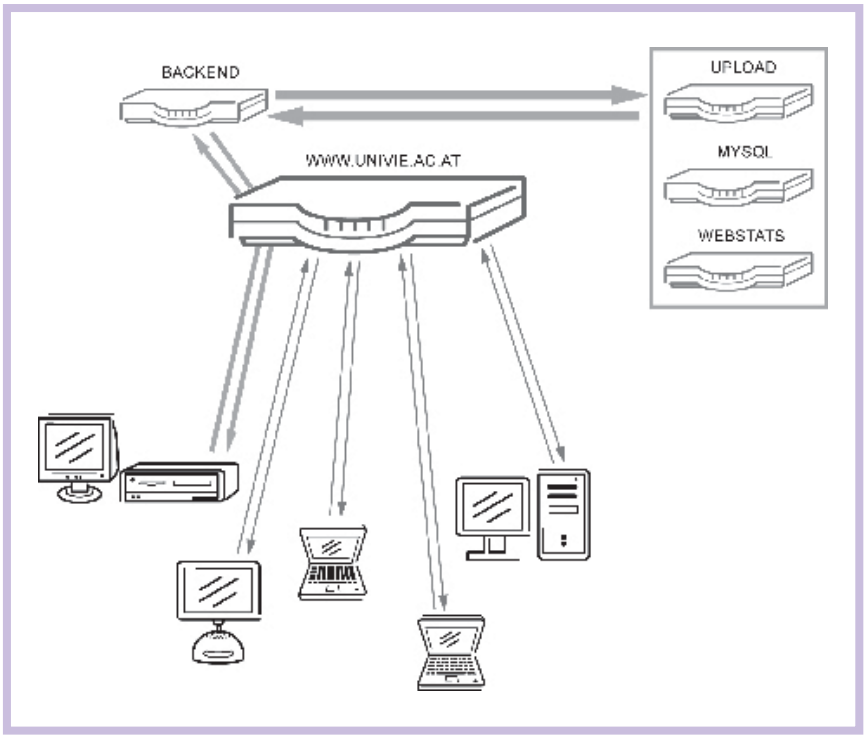


Abb. 2: Der Webserver in der derzeitigen Übergangsphase zu einem verteilten System: Ein Teil der Webseiten ist bereits auf den Backend-Servern angesiedelt; für diese fungiert der Frontend-Server als Proxy. Der Rest befindet sich noch auf dem Frontend-Server.

Software-Ausstattung der Backend-Server

Das neue Konzept mit mehreren Backend-Servern bietet auch den Vorteil, dass auf verschiedenen Servern unterschiedliche Software (Betriebssystem, Webserver, Applikationsserver usw.) installiert werden kann, sodass Applikationen mit beliebigen Anforderungen unterstützt werden könnten. Für einige Anwendungen wird es spezielle Backends geben, die meisten der Backend-Server werden jedoch eine identische Standard-Ausstattung erhalten: eine LAMP-Architektur (*Linux–Apache–MySQL–PHP*), die im Open Source-Bereich häufigste Software-Ausstattung von Webservern.

- **Betriebssystem**: Als Betriebssystem dient Redhat Enterprise Linux Server Release 5 (`www.redhat.com`).

- **Webserver**: Hierfür wird die neueste Version 2.2.4 von Apache eingesetzt (`http://httpd.apache.org/`). Einige lokale Modifikationen der Software sorgen dafür, dass die Backends nichts davon merken, dass sie nicht direkt mit dem Klienten sprechen, sondern mit dem Frontend. Das ermöglicht u.a. eine Zugriffskontrolle auf Basis der IP-Adressen der Klienten, obwohl alle Anfragen eigentlich von der IP-Adresse des Frontends kommen.

- **PHP**: Bisher stand auf dem Webserver der Universität die Version 4.2.2 von PHP (`http://at.php.net/`) zur Verfügung. Mit Ende des Jahres läuft aber der Support für die Version 4 aus. Daher wird empfohlen, PHP-Applikationen möglichst bald auf einen Backend-Server zu übersiedeln (siehe Abschnitt *Migration*), wo die neueste PHP-Version 5.2.4 installiert ist.

- **Perl**: CGI-Skripts in Perl oder anderen Sprachen werden weiterhin unterstützt; Perl (`www.perl.org`) steht in der Version 5.8.8 zur Verfügung.

- **Datenbank**: Auf den Backends ist lediglich ein MySQL-Klient installiert. Die Datenbanken befinden sich auf eigenen Datenbank-Servern, auf denen die Version 5.0 der MySQL-Datenbank (`www.mysql.de`) installiert ist. Auch hier kommen verteilte Server zum Einsatz: Für jeden MySQL-User wird ein virtueller Hostname (*CNAME*) eingerichtet, der beim Öffnen der Datenbankverbindung anzugeben ist; für den User `ihw` lautet dieser beispielsweise IHW.MYSQL.UNIVIE.AC.AT. Dieser *CNAME* ist ein Aliasname für den Datenbank-Server, auf dem die jeweilige Datenbank installiert ist. Dadurch ist es möglich, Datenbanken von einem Server auf einen anderen zu

---

1) siehe Artikel *Ein neuer Webserver für die Uni Wien* in *Comment 01/3*, Seite 16 bzw. unter `http://comment.univie.ac.at/01-3/16/` und Artikel *Gerda geht in Pension* in *Comment 05/2*, Seite 36 bzw. unter `http://comment.univie.ac.at/05-2/36/`

2) Eine Ausnahme bilden nur verschlüsselte Anfragen (HTTPS), die am Frontend entschlüsselt und unverschlüsselt an die Backends weitergereicht werden: Nachdem die unverschlüsselte Übertragung nur in einem geschützten Netz geschieht, stellt sie kein zusätzliches Sicherheitsrisiko dar.

3) Physisch liegen die Daten auf den Speichersystemen des *Storage Area Network* des ZID (siehe Artikel *SAN: Das Storage-Projekt macht Fortschritte* in *Comment 07/1*, Seite 16 bzw. unter `http://comment.univie.ac.at/07-1/16/`), wobei nur die Backend-Server auf die entsprechenden Speicherbereiche (LUNs) zugreifen können.

4) siehe Artikel *Aus eins mach zehn: Der Zauber der Virtualisierung* in *Comment 07/2,* Seite 7 bzw. unter `http://comment.univie.ac.at/07-2/7/`

verschieben (z.B. zwecks gleichmäßigerer Verteilung der Last), ohne dass irgendwelche Änderungen an Applikationen erforderlich werden.

Von minimalen Anpassungen abgesehen ist die Konfiguration des Webservers auf den Backends identisch mit der bisherigen Konfiguration, sodass alle Funktionen wie Authentifizierung mittels u:net- und Mailbox-Passwörtern weiterhin unverändert eingesetzt werden können. Eine kleinere Änderung gibt es bei der „Rechtschreibprüfung" durch das Apache-Modul *mod_speling*: Dieses ist nun so konfiguriert, dass es nur Abweichungen bei der Groß-/Kleinschreibung von URLs stillschweigend ausbessert, aber keinerlei andere Korrekturen (z.B. vertauschte Buchstaben) vornimmt.

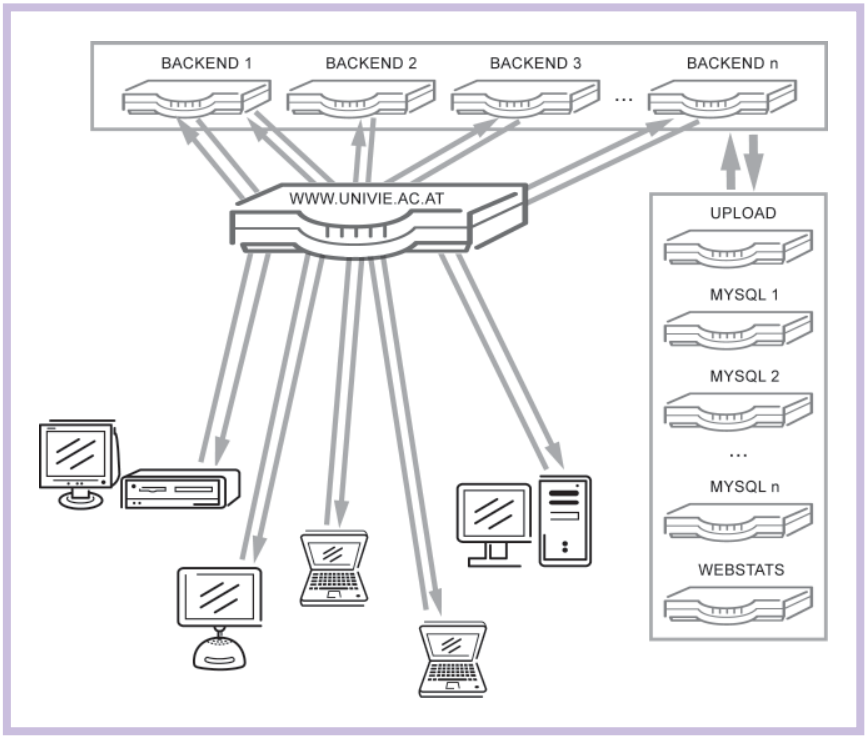


Abb. 3: Endausbau des verteilten Systems: Alle Daten und Anwendungen befinden sich auf den Backends, das Frontend dient nur als Proxy.

Sicherheit und Berechtigungen

Im Abschnitt *Sicherer Multiuser-Betrieb mit PHP und CGI – eine Herausforderung* des eingangs erwähnten *Comment*-Artikels *Gerda geht in Pension* wurde genau beschrieben, welche Schwierigkeiten damit verbunden sind, gleichzeitig PHP- und CGI-Unterstützung anzubieten, den BenutzerInnen möglichst viele Freiheiten zu erlauben und dennoch einen sicheren und stabilen Betrieb aufrecht zu erhalten. Das Hauptproblem ist, dass PHP-Skripts vom Webserver selbst ausgeführt werden und daher mit den (sehr weit reichenden) Rechten des Webservers laufen. Damit die Skripts verschiedener BenutzerInnen einander nicht in die Quere kommen oder gar auf fremde Daten zugreifen können, sind Einschränkungen der Privilegien von PHP-Skripts mittels der PHP-Konfiguration unerlässlich.

Auf den neuen Backends wurde eine andere Lösung implementiert: PHP-Skripts werden nicht vom Apache-Webserver ausgeführt, sondern als externe Prozesse über das CGI-Interface. Das hat folgende Vorteile:

- PHP- und CGI-Skripts laufen ausschließlich mit den Rechten und Privilegien des Eigentümers (*Owner*) des Skripts. Auch Dateien, die von PHP-Skripts angelegt wurden, gehören nunmehr dem Eigentümer des Skripts und nicht mehr dem User `wwwphp`.

- PHP- und CGI-Skripts können in beliebigen Verzeichnissen ausgeführt werden. Das gesonderte Beantragen der PHP-Unterstützung (*nur im Unterverzeichnis php* bzw. *überall*) entfällt.

- Die PHP-Einstellungen *Safe Mode* und *open_basedir* sind damit nicht mehr nötig. Das erleichtert die Installation etlicher Programme, die mit diesen Einstellungen nur schwer zum Laufen gebracht werden können.

Der Nachteil des Ausführens von PHP-Skripts über das CGI-Interface ist eine schlechtere Performance, weil dafür ein eigener Prozess gestartet werden muss. Aus diesem Grund wird die FastCGI-Schnittstelle verwendet, die im Apache-Modul *mod_fcgid* (`http://fastcgi.coremail.cn/`) implementiert ist: Es werden externe Prozesse gestartet, die zahlreiche Skripts abarbeiten können.[5] Zusätzlich sorgt der eAccelerator (`http://eaccelerator.net/`) für eine optimale Performance von PHP-Skripts.

Ein neuer Zugangsserver

Bisher erfolgte die Wartung von Webseiten durch direkten Zugriff bzw. Datenübertragung auf WWW.UNIVIE.AC.AT. Einen solchen Zugriff auf die Backends wird es nicht geben; stattdessen steht dafür ein eigener Zugangsserver namens UPLOAD.UNIVIE.AC.AT zur Verfügung. Die Verzeichnisstruktur ist dieselbe wie auf den Backends.

Anders als bisher sind nun jedoch Dateien im Home-Verzeichnis (z.B. `/u/home/ihw`) für den Webserver nicht mehr sichtbar, daher müssen HTML-Dokumente im Unterverzeichnis `html` abgelegt werden (z.B. in `/u/home/ihw/html`). Will man vermeiden, dass bestimmte Daten via Webbrowser abrufbar sind, müssen sie außerhalb dieses Unterverzeichnisses gespeichert werden. Der bisherige Verzeichnisname `/u/www/username` (z.B. `/u/www/ihw`) funktioniert auch weiterhin.

5) FastCGI steht nur für PHP-Skripts zur Verfügung, für „normale" CGI-Skripts wird weiterhin ein eigener Prozess gestartet.

Der Zugang zum Upload-Server erfolgt auf denselben Wegen wie bisher zum WWW-Server: Die Datenübertragung kann mittels FTP oder (empfohlen) sFTP erfolgen; `\\upload.univie.ac.at\username` kann als Netzlaufwerk verbunden werden; auch Login mittels SSH und interaktives Arbeiten am Server ist möglich. Lediglich Telnet wird aus Sicherheitsgründen nicht mehr unterstützt. Auf dem Upload-Server sind dieselben Versionen von Perl und PHP installiert wie auf den Backends, sodass Applikationen dort interaktiv getestet werden können.

Logfiles und Statistiken

Wer eine Webseite publiziert, will verständlicherweise auch wissen, wie oft und von wem sie gelesen wird. Aus diesem Grund besteht schon seit vielen Jahren die Möglichkeit, die Logdateien einzusehen; sie werden auch automatisch von mehreren Statistikprogrammen ausgewertet.

Dieses beliebte Service ist nun schon etwas in die Jahre gekommen – die verwendeten Statistikprogramme sind nicht mehr die aktuellsten. Die Reorganisation des Webservers wurde daher zum Anlass genommen, auch dieses Service rundum zu erneuern. Dafür wird ein eigener Server eingesetzt, der die Logdateien von diversen Webservern einsammelt und zentral auswertet. Modernere Statistiken werden demnächst unter dem URL `http://webstats.univie.ac.at/` abrufbar sein.

Migration

Wie bereits erwähnt, erfolgt die Inbetriebnahme des neuen verteilten Server-Konzepts schrittweise. Auf dem bisherigen WWW-Server und künftigen Frontend wird der Software-Stand eingefroren, es gibt dort keinerlei Innovationen mehr. Neue Benutzungsberechtigungen werden seit dem 10. September 2007 ausschließlich für das neue System vergeben. Die Migration der bestehenden Accounts (mehr als 1500 Benutzungsberechtigungen, die individuell behandelt werden müssen) wird sich voraussichtlich über mehrere Monate erstrecken, wobei der ZID die jeweils verantwortlichen Subserver-BetreiberInnen rechtzeitig von der bevorstehenden Umstellung ihrer Webseiten verständigt. Im Großen und Ganzen besteht kein Grund zur Eile – mit einigen Ausnahmen:

- Einige Pilot-Anwendungen wurden bereits auf einen Backend-Server übersiedelt. Dabei handelt es sich hauptsächlich um „schwergewichtige" PHP-Applikationen, die hohe Zugriffszahlen aufweisen und den WWW-Server stark belastet haben.

- Wenn Sie schon jetzt umstellen möchten (beispielsweise weil Sie eine neuere PHP-Version brauchen), vereinbaren Sie einfach per eMail an `helpdesk.zid@univie.ac.at` einen Termin für die Migration. Während der Übersiedlung sind die betroffenen Seiten in der Regel nur für wenige Minuten nicht erreichbar: Falls es sich um statische HTML-Seiten handelt, sind keinerlei Änderungen nötig, und auch bei PHP- oder Perl-Skripts sind in den meisten Fällen nur minimale Anpassungen vorzunehmen (in der Regel ändert sich lediglich der Name der MySQL-Datenbank). Gelegentlich sind wegen Inkompatibilitäten zwischen den PHP- und MySQL-Versionen kleinere Code-Modifikationen erforderlich.

- Bei manchen WWW-Accounts gibt es individuelle Sonderlösungen und „Spezialkonstruktionen", die sich nicht automatisch migrieren lassen. Wir werden versuchen, in allen Fällen eine Lösung zu finden, teilweise könnten hier jedoch längere Vorbereitungsarbeiten nötig sein.

Im Endausbau dient der Frontend-Server WWW.UNIVIE.AC.AT nur mehr als reiner Proxy-Server, dessen „Intelligenz" sich darauf beschränkt, zu wissen, welche Webseiten auf welchen Backends liegen (siehe **Abb. 3**). Dann wäre auch der Einsatz eines *Load Balancers* möglich, sodass sich hinter der Adresse WWW.UNIVIE.AC.AT mehrere Frontend-Server verbergen, die sich die Arbeit teilen: Dies würde nicht nur die Skalierbarkeit noch weiter erhöhen, sondern auch für höhere Stabilität sorgen, weil dadurch das Frontend als *Single Point of Failure* wegfällt.

Administration

An der Administration der Benutzungsberechtigungen ändert sich durch das verteilte Server-Konzept nicht viel; Details zur Vergabe und Verwaltung sind unter `www.univie.ac.at/ZID/www-userid/` zu finden. Eine Neuerung ist jedoch, dass WWW-Accounts nunmehr mit einem „Ablaufdatum" versehen werden. Vor dem Zeitpunkt des Ablaufs wird der Verantwortliche kontaktiert und der Account formlos verlängert, sofern er noch benötigt wird. Damit soll u.a. sichergestellt werden, dass die Daten der Kontaktpersonen aktuell bleiben: Zur Zeit gibt es zahlreiche Accounts, die vermutlich nicht mehr benötigt werden, was sich aber kaum verifizieren lässt, da keine Kontaktpersonen mehr bekannt sind. Die Übersiedlung der bestehenden Accounts auf die neuen Backend-Server wird auch zum Anlass genommen, diese Altlasten zu „entsorgen".

Applikationen

Auf dem Webserver stehen mit PHP und Perl mächtige Werkzeuge zur Verfügung, um eigene Anwendungen zu installieren. Dabei hat sich gezeigt, dass etliche populäre Standard-Applikationen oft gewünscht werden und folglich zahlreiche Instanzen dieser Softwareprodukte am Webserver installiert sind: *Content Management Systeme* (CMS), Diskussionsforen, Gästebücher usw. Diese Instanzen unterscheiden sich meist nur marginal voneinander, haben aber oft unterschiedliche Software-Versionen – und manchmal auch unterschiedliche Sicherheitslücken. Hier wäre eine einzige zentrale Installation effizienter, die nur einmal gewartet werden muss, aber allen BenutzerInnen zur Verfü-

gung steht. Wir werden uns daher in Zukunft verstärkt um die Unterstützung solcher Applikationen auf unseren Webservern bemühen, wodurch Programmieren in PHP oder Perl in vielen Fällen überflüssig werden soll.

Ein erster Schritt in diese Richtung wurde mit dem Typo3-Projekt[6] gemacht: Hierbei wird ein leistungsfähiges und flexibles Content Management System zur Verfügung gestellt. Für Institute bzw. Projekte, die ihren Webauftritt im Rahmen des Typo3-Projekts erstellen, sind die in diesem Artikel beschriebenen Details weitgehend irrelevant: Für Typo3 gibt es dedizierte Backend-Server, und die Wartung und Pflege der betreffenden Webseiten erfolgt ausschließlich mit Hilfe von Typo3, sodass man sich um die Eigenschaften des darunterliegenden Webservers nicht zu kümmern braucht.

Erneuerung des Webauftritts der Universität Wien

Nicht nur die Hardware und Architektur des Webservers wird erneuert, auch Inhalt und Form der Webseiten sollen modernisiert werden: Zwar ist auf den verschiedenen Subservern eine Unmenge an Informationen zu finden, jedoch besteht der Webauftritt der Uni Wien aus zahlreichen weitgehend unabhängigen Einzelprojekten, die sich in der Qualität von Inhalt und Form, im Design und in der Organisation stark unterscheiden. Die DLE *Öffentlichkeitsarbeit und Veranstaltungsmanagement* hat den Auftrag, ein Gesamtkonzept für die Erneuerung des Webauftritts der Universität Wien zu erstellen.

Es ist klar, dass ein so umfangreiches Projekt nicht von heute auf morgen verwirklicht werden kann. Als erster Schritt werden daher die Startseite und die in der Hierarchie unmittelbar darunter liegenden Seiten erneuert; die modernisierte Startseite soll in Kürze online sein. Für diese Seiten wird ein eigener Backend-Server zur Verfügung stehen, um höchstmögliche Stabilität zu gewährleisten.

Wie auch immer der neue Webauftritt der Uni Wien im Detail aussehen wird: Mit dem Konzept einer Server-Farm mit Frontend, Backends und Datenbank-Servern steht eine flexible und skalierbare Hardware-Plattform und Software-Architektur zur Verfügung, die auf absehbare Zeit für alle Anforderungen gerüstet ist.

Peter Marksteiner

6) siehe Artikel *Webauftritte leicht gemacht: Typo3 an der Universität Wien* in *Comment 06/3*, Seite 37 bzw. unter `http://comment.univie.ac.at/06-3/37/`

Hochschulschriften-Service der Universitätsbibliothek Wien

Dem internationalen *state of the art* entsprechend können ab sofort Abschlussarbeiten von AbsolventInnen der Universität Wien (Diplomarbeiten, Dissertationen und Masterstheses) als elektronischer Volltext auf dem Server `http://othes.univie.ac.at/` abgerufen werden. AbsolventInnen haben hier die Möglichkeit, ihre Diplomarbeiten und Dissertationen zu veröffentlichen – sofern dadurch keine rechtlichen Bestimmungen verletzt werden – und damit ihre Abschlussarbeit weltweit zur Verfügung zu stellen.

Mit Hilfe strukturierter Metadaten werden die auf diesem Server gespeicherten Dokumente bibliographisch beschrieben und über nationale und internationale Bibliothekskataloge, Suchmaschinen und andere Nachweisinstrumente erschlossen und somit suchbar gemacht. Die Zitierfähigkeit wird durch eine dauerhafte und stabile Internetadresse garantiert. Darüber hinaus trägt die elektronische Veröffentlichung zum Schutz vor Plagiierung bei, da durch die bessere Zugänglichkeit Abschreibende leichter enttarnt werden können. Sollten auch Sie Interesse haben, Ihre Abschlussarbeit in elektronischer Form einer breiten

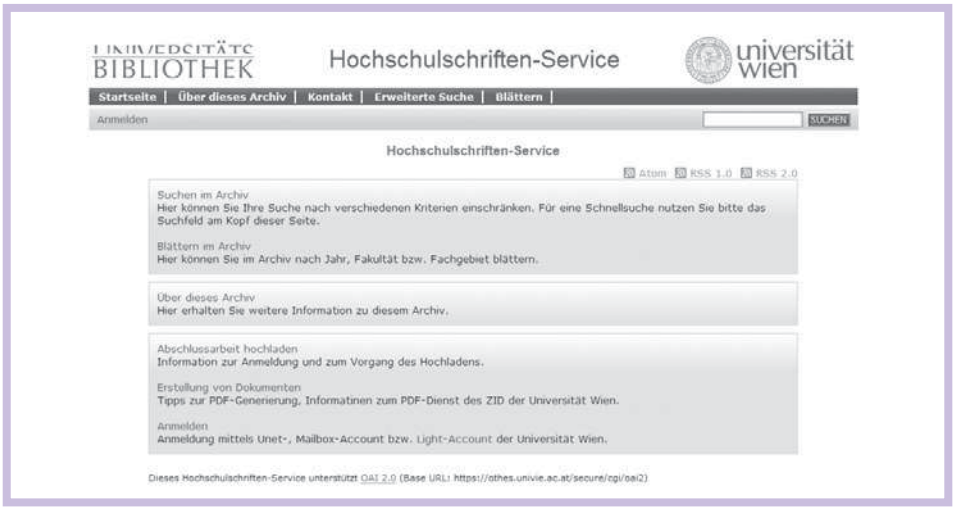


Abb. 1: Startseite des neuen Hochschulschriften-Service (http://othes.univie.ac.at/)

Öffentlichkeit zugänglich zu machen, gehen Sie folgendermaßen vor:

1. Um auf die Eingabe-Seite zu gelangen, müssen Sie sich mit Ihrer u:net- oder Mailbox-UserID anmelden. Sollten Sie keinen gültigen Account der Uni Wien mehr besitzen, können Sie eine befristete Light-UserID per eMail an `thesis-help.ub@univie.ac.at` beantragen.

2. Nach der Anmeldung tragen Sie in die vorgegebenen Felder die Metadaten ein: Autor, Titel etc. Beachten Sie bitte, dass dem internationalen Standard entsprechend ein kurzes Abstract (maximal 250 Worte) anzugeben ist. Die Eingabe-Oberfläche bietet die Möglichkeit, jederzeit abzubrechen und zu einem späteren Zeitpunkt fortzufahren.

3. Die Abschlussarbeit ist als **ein** Dokument im PDF-Format – in der von Adobe spezifizierten Version PDF 1.4. – hochzuladen. Falls Sie keinen Zugang zu einem PDF-Konverter haben, können Sie das PDF-Service des ZID verwenden (siehe `http://othes.univie.ac.at/pdf.html`).

4. Nach Prüfung der Angaben erfolgt die Freigabe durch die Universitätsbibliothek Wien.

Mag. Adelheid Mayer
(DLE Bibliotheks- und Archivwesen)

Umstellungen beim Mailing

Geänderte Servernamen für Studierende

Um das Mailsystem der Uni Wien weiter zu vereinheitlichen, wurden im August 2007 einige Veränderungen vorgenommen. Als Folge davon können nun sowohl Uni-MitarbeiterInnen als auch Studierende den **Posteingangsserver IMAP.UNIVIE.AC.AT** verwenden. Der bisherige Server für Studierende (IMAP.UNET.UNIVIE.AC.AT) funktioniert auch weiterhin; wir empfehlen aber allen Studierenden, den neuen Servernamen in die Konfiguration des eigenen Mailprogramms einzutragen (Details siehe `www.univie.ac.at/ZID/anleitungen-mailing/`). Insbesondere wenn die Datenübertragung vom Server zum PC mittels SSL verschlüsselt werden soll, ist es ratsam, den neuen Servernamen anzugeben: Wenn SSL aktiviert ist und noch der alte Name verwendet wird, erhält man bei jedem Verbindungsaufbau zum Posteingangsserver eine Fehlermeldung bezüglich des Serverzertifikats.

Für den Versand von eMail kommt nach wie vor der **Postausgangsserver MAIL.UNIVIE.AC.AT** zum Einsatz. Auch hier kann die Verbindung vom PC zum Server mittels SSL (über Port 465) verschlüsselt werden. Außerdem empfehlen wir, SMTP-Authentifizierung zu aktivieren, um den Mailversand über unseren Server auch von außerhalb des Uni-Datennetzes – z.B. mit mobilen Geräten – zu ermöglichen.

Die neuen Einstellungen für die Konfiguration Ihres Mailprogramms finden Sie in der Tabelle unten. Noch ein Hinweis: Im Zuge des Software-Updates in den PC-Räumen (siehe Seite 19) wurden dort die Einstellungen des Mailprogramms Thunderbird automatisch richtig gesetzt. Wenn Sie mit Thunderbird in den PC-Räumen der Uni Wien arbeiten, müssen Sie also keinerlei Änderungen vornehmen.

Thomas Riener

	Studierende	MitarbeiterInnen
Mailadresse	a*Matrikelnummer*@unet.univie.ac.at	*vorname.nachname*@univie.ac.at
Protokoll	IMAP (alternativ POP3)	IMAP (alternativ POP3)
	Posteingangsserver	
Servername	**IMAP.UNIVIE.AC.AT**	**IMAP.UNIVIE.AC.AT**
Benutzername	u:net-UserID (a*Matrikelnummer*)	Mailbox-UserID (z.B. zufallr0)
Passwort	u:net-Passwort (5–8 Zeichen)	Mailbox-Passwort (5–8 Zeichen)
SSL	Port 993 (alternativ POP3: 995)	Port 993 (alternativ POP3: 995)
	Postausgangsserver	
Servername	**MAIL.UNIVIE.AC.AT**	**MAIL.UNIVIE.AC.AT**
SMTP-Auth	ja	ja
Benutzername	u:net-UserID (a*Matrikelnummer*)	Mailbox-UserID (z.B. zufallr0)
Passwort	u:net-Passwort (5–8 Zeichen)	Mailbox-Passwort (5–8 Zeichen)
SSL	Port 465	Port 465

Neuer VPN-Server: Bitte verschlüsseln Sie Ihre Verbindung!

Manche Netzwerkdienste der Uni Wien wie z.B. das Datenbank-Service der Universitätsbibliothek sind nur mit einer IP-Adresse der Universität verwendbar – d.h. entweder direkt aus dem Uni-Datennetz, über einen Wählleitungs- oder Breitbandzugang der Universität oder aber über eine VPN-Verbindung (*Virtual Private Network*, Näheres unter `www.univie.ac.at/ZID/vpn/`). Da künftig keine direkten Breitbandanbindungen zum Universitätsdatennetz mehr angeboten werden (siehe Seite 6), ist mit einem entsprechenden Zuwachs bei den VPN-Verbindungen zu rechnen.

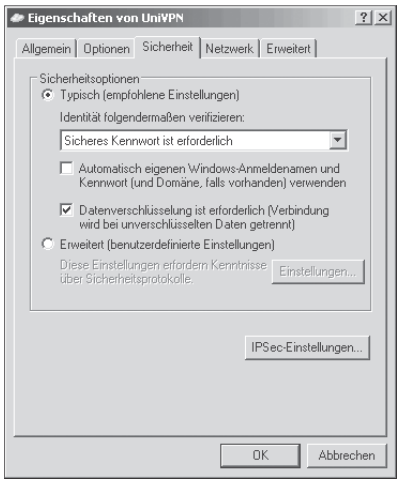


Abb. 1: Umstellen auf verschlüsselte Verbindung (Windows XP)

Um dieser Entwicklung Rechnung zu tragen, wurde der VPN-Server der Uni Wien am 2. Oktober 2007 durch eine neue Maschine ersetzt, die deutlich mehr gleichzeitige VPN-Verbindungen abwickeln kann.

Eine Eigenschaft des neuen Servers ist, dass er nur verschlüsselte Verbindungen zulässt. Diese sind inzwischen aber auch mit den mitgelieferten „Bord-Mitteln" von Windows XP/Windows Vista und Mac OS X 10.4.x/10.5.x leicht zu realisieren. Die dafür nötige Konfigurationsumstellung bereits installierter VPN-Klienten unter Windows ist nicht besonders schwierig:

- Klicken Sie unter ***Systemsteuerung – Netzwerkverbindungen*** mit der *rechten* Maustaste auf das Icon der VPN-Verbindung, wählen Sie im Kontextmenü die Option ***Eigenschaften*** und dann die Registerkarte ***Sicherheit***.
- Wählen Sie hier bei *Sicherheitsoptionen* den Punkt ***Typisch (empfohlene Einstellungen)*** und aktivieren Sie das Kontrollkästchen bei ***Datenverschlüsselung ist erforderlich*** (siehe **Abb. 1**).
- Klicken Sie anschließend auf die Schaltfläche ***IPSec-Einstellungen*** (unter Windows Vista ist diese auf der Registerkarte *Netzwerk* zu finden) und geben Sie als Passwort ***vpnsec*** ein.

Schon funktioniert Ihre VPN-Verbindung zum neuen Server auch mit IPSec-Verschlüsselung. Genaue Anleitungen sind unter `www.univie.ac.at/ZID/anleitungen-vpn/` zu finden.

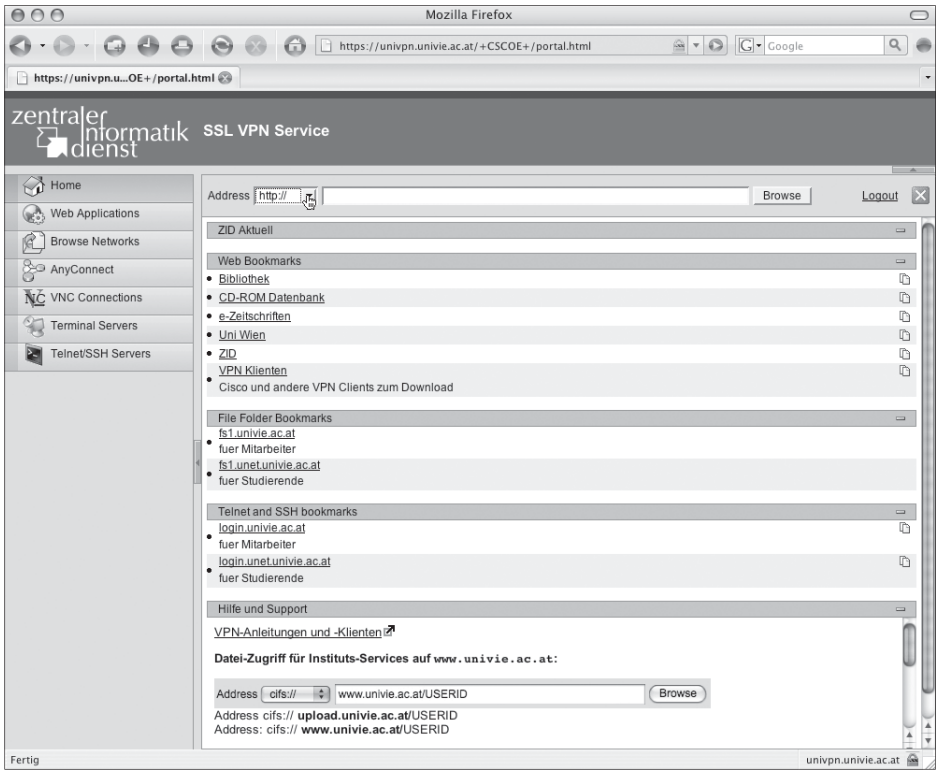


Abb. 2: Startseite des neuen WebVPN-Servers der Universität Wien

Wie bisher ist unter `https://univpn.univie.ac.at/` auch ein VPN-Zugang via Webbrowser möglich. Hier bietet der neue Server ebenfalls zahlreiche neue Optionen – beispielsweise sind jetzt vorkonfigurierte Links zu wichtigen Uni-Servern verfügbar, sodass nun unter anderem auch ein VPN-Zugriff auf die Fileserver der Universität mit einem Mausklick erfolgen kann (siehe **Abb. 2**).

Die Auswahlliste neben dem Punkt *Address* (oben links) enthält eine Reihe von Netzwerkprotokollen, die über die WebVPN-Verbindung verwendet werden können. Weiter unten auf der Startseite des VPN-Servers sind unter dem Punkt *Hilfe und Support* die wichtigsten Daten für den VPN-Zugriff auf Universitätsserver zusammengefasst.

Franz Kaltenbrunner

Gute Seiten – Schlechte Seiten

Die Suche nach Strategien, das Websurfen sicherer zu machen

Feuer ist am Dach, wenn ein Computer, statt seinem Eigentümer (m/w) treu zu dienen, ihn im Auftrag fremder Mächte ausspioniert, ihn ungefragt mit Werbung traktiert oder einfach „nur" unbemerkt kriminellen Nebengeschäften nachgeht – wenn also böse Software, so genannte *Malware*, auf dem Rechner ihr Unwesen treibt. Doch wo kam sie her? Allzu oft lautet die Antwort: Der User hat sie höchstpersönlich aus dem Web heruntergeladen und auf seinem Computer installiert. Nicht ganz absichtlich, aber letztlich eben doch.

Neben Webseiten mit Malware gibt es zum Beispiel auch so genannte *Phishing*-Seiten[1], die dem Anwender z.B. die Bankdaten herauslocken, um sein Konto leer zu räumen, oder Webseiten, die ihm – völlig untechnisch – mit einem Gratis-Service ein überteuertes Abonnement andrehen (siehe **Abb. 1**). Das Spektrum der „bösen Webseiten" ist nur schwer einzugrenzen, und manch einer würde gern in einem Aufwaschen auch gegen Bombenbastelanleitungen, Pornoseiten und vieles mehr vorgehen. Dieser Artikel gibt einen Überblick über die Methoden, mit denen man derzeit der Bedrohung durch böswillige Webseiten zu begegnen versucht. Gleich vorweg: Der Stein der Weisen ist noch nicht gefunden worden.

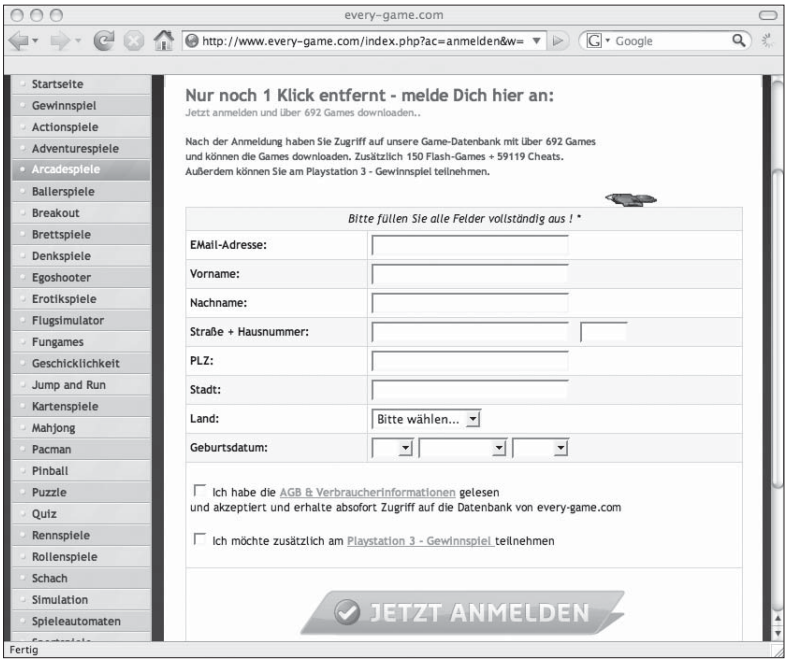


Abb. 1: Ein Dauerbrenner bei Konsumentenschutzorganisationen: Nur wer sich mit dem Scrollbalken bis zum Ende der Seite vorarbeitet, sieht, dass er hier einen Vertrag abschließt und sich zur Zahlung von EUR 59,95 verpflichtet.

Fahrlässige Gemeingefährdung?

Computerzwischenfälle sind wie Wohnungsbrände häufiger auf Fahrlässigkeit als auf technische Gebrechen zurückzuführen. Anders als beim Zündeln neben der Gasflasche ist es in der Computerwelt aber für den Laien oft schwierig oder unmöglich, die drohende Gefahr zu erkennen. Auch wer nicht auf alles klickt, das nicht bei drei auf den Bäumen ist, sondern nur Musik oder Videos von einer Webseite herunterlädt, ein paar nützliche Tools für sein Windows oder Word ausprobiert oder gemäß der eMail-Anleitung von „Administrator" seinen Computer mit dem neuesten Sicherheitsprogramm versieht, kann dadurch böse Software installieren:

- Der **Download von Musik oder Filmen** mag urheberrechtlich nicht immer korrekt sein, sicherheitstechnisch ist das aber irrelevant. Dennoch gelangen die Schadprogramme häufig auf diesem Weg auf den Rechner, weil die angeblichen Musikstücke nicht, oder nicht nur, Musik enthalten. Beispielsweise kann sich die Malware als selbstextrahierendes Archiv tarnen – der User muss also nur doppelklicken und hat sie schon gestartet. Wenn dabei zusätzlich auch noch die gewünschte Musik herauskommt, bemerkt er seinen fatalen Fehler nicht einmal.

- Ähnliches gilt für die nützlichen **Tools**, die zuhauf im Internet zu finden sind. Wer weiß schon so genau, ob sie wirklich nur das tun, was sie zu tun behaupten? Selbst bei Software, die einen guten Ruf hat, kann es sein, dass man auf irgendeiner Webseite eine manipulierte Version davon erwischt – und schon ist das Malheur passiert.

- Auch das gutgläubige **Befolgen von Anweisungen** oder Tipps, die man per eMail erhalten hat, ist gefährlich. Diese stammen nämlich oft von Schwindlern, die sich z.B. als Microsoft, Netzwerkadministrator oder dergleichen ausgeben, um den Anwender dazu zu bringen, höchstpersönlich genau die Software zu installieren, die er lieber nicht auf dem PC haben möchte.

- Für die folgenden Betrachtungen ist es sinnvoll, auch noch ein Szenario aus der Kategorie der technischen Gebrechen einzubeziehen: Der User klickt auf einen

1) Näheres dazu finden Sie im Artikel *Phishing – Bitte nicht anbeißen!* in *Comment 06/2*, Seite 37 bzw. unter `http://comment.univie.ac.at/06-2/37/`.

Link (z.B. aus der Ergebnisliste einer Google-Suche), ruft also nichtsahnend eine Webseite auf, und schwuppdiwupp ist die Malware am Rechner. Dafür müssen drei Voraussetzungen gegeben sein: Es gibt eine Sicherheitslücke im Browser, diese ist noch nicht durch ein Update behoben worden, und die aufgerufene Seite nützt das aus. Hier ist man als Anwender völlig chancenlos, außer durch totale Web-Abstinenz.

Technisch gesehen ist in den geschilderten Szenarien – und in vielen weiteren – der User selbst schuld am Schaden, den er erleidet. Doch was genau hat er falsch gemacht? Nicht jeder kann ein Sicherheitsexperte sein (und selbst diese sind nicht allwissend), daher kann man dem Normalverbraucher nur selten einen Vorwurf machen, wenn er auf solche Tricks hereinfällt. Was beim Zündeln unter fahrlässige Gemeingefährdung fallen würde, ist also in der IT-Welt ein nicht vorwerfbarer Fehlgriff – Freispruch!

Wie kann man sich schützen?

Gegen die Bedrohung durch Malware gibt es vier klassische Gegenstrategien: Virenscanner, regelmäßige Software-Updates, die Verwendung exotischer Software und Misstrauen.

- Der **Virenscanner** am PC ist eine Selbstverständlichkeit und sollte idealerweise einschreiten, sobald der User eine schadensträchtige Datei auf seinen Rechner holt. Allerdings können Virenscanner nur bekannte Malware und hinreichend ähnliche Programme erkennen. Neu geschriebene Malware wird erst erkannt, sobald sie entdeckt wurde, die Antivirus-Hersteller entsprechende Updates bereitgestellt haben und diese auch am PC installiert wurden. Daraus folgt zweierlei: a) Die Virenscanner-Dateien müssen permanent aktualisiert werden, alles andere wäre grob fahrlässig. b) Es gibt stets Malware, die trotz Virenscanner auf den PC gelangen kann.

- Dass Betriebssystem und Anwendungsprogramme regelmäßig mittels **Updates** auf den neuesten Stand gebracht werden müssen, hat ähnliche Gründe: Um zu verhindern, dass manipulierte Webseiten Malware auf einem PC einschleusen, muss jede Sicherheitslücke so rasch wie möglich geschlossen werden. In einigen Fällen kann durch ein Update auch verhindert werden, dass eine Malware ihre volle Wirkung entfaltet. Regelmäßige Updates helfen mit, den Zeitraum, in dem eine Infektion erfolgen kann, kurz zu halten – und senken somit das Risiko.

- Die überwältigende Mehrheit aller Rechner im Internet sind Windows-PCs, die MS-Internet Explorer als Webbrowser verwenden. Für **exotische Software** (und dazu zählt in diesem Zusammenhang schon ein Apple-Rechner mit Safari als Browser) spezielle Malware zu entwickeln bzw. Webseiten zu basteln, die ihre speziellen Sicherheitslücken ausnützen, zahlt sich für die Bösewichte kaum aus. Daher kann auch die Wahl alternativer Software risikominimierend wirken. In der Praxis steht dem allerdings der Nachteil gegenüber, dass manche Webseiten damit nicht funktionieren, weil deren Designer sich statt an Standards an einer spezifischen Version des Internet Explorer orientiert haben.

- Anwendern wird stets ein **gesundes Misstrauen** empfohlen. Eine gute Idee ist, wenn Sie die für Sie zuständigen EDV-Vertrauenspersonen frühzeitig kennenlernen und im Fall von ungewöhnlichen Aufforderungen einfach rückfragen (Kontaktpersonen und -telefonnummern dürfen natürlich nicht der möglicherweise gefälschten Nachricht entnommen, sondern müssen unabhängig davon eruiert werden). In allen anderen Belangen ist Otto Normalverbraucher aber mit dem guten Rat, misstrauisch zu sein, überfordert. Es sind nämlich keineswegs immer Schmuddel- und Raubkopier-Seiten, auf denen Cyberkriminelle auf Opfer lauern – aus der Seriosität eines Anbieters folgt nicht die Sicherheit seiner Webseiten. Ein Klassiker unter den vielen Gründen dafür sind Werbebanner: Der Bösewicht mietet Bannerplatz auf einer Webseite und stellt dort „vergiftete“ Werbebanner ein, und schon sind reihenweise seriöse Seiten zu Hackerseiten geworden. Wie soll man so etwas mit dem Hausmittel des Misstrauens rechtzeitig erkennen?

Diese klassischen Methoden, digitaler Unbill aus dem Weg zu gehen, sind also nach wie vor wirksam und wichtig, gewähren allerdings keinen hundertprozentigen Schutz.

Elektronische Ratgeber

Etwas, das den Anwender davor bewahrt, nichtsahnend böse Webseiten zu betreten, wäre ein großer Fortschritt. Ein solcher Mechanismus müsste allerdings einige Voraussetzungen erfüllen:

- *Benutzerfreundlichkeit*: Die Bedienung des Browsers darf nicht verkompliziert werden – sichere Seiten müssen weiterhin per Mausklick aufgehen, vor unsicheren Seiten muss ohne weiteren Bedienungsschritt gewarnt werden.

- *Transparenz*: Im Falle einer Warnung muss diese so nachvollziehbar sein, dass der Anwender entscheiden kann, ob er die Seite dennoch besuchen will.

- *Privacy*: Es muss gewährleistet sein, dass das Surfverhalten des Users nicht nach außen ausgeplaudert wird.

- *Treffsicherheit*: Es muss zuverlässig vor gefährlichen Seiten, aber möglichst nie vor ungefährlichen Seiten gewarnt werden.

So phantastisch sich das anhören mag, es gibt tatsächlich bereits Ansätze, die User vor dem Bösen zu beschützen. Diese können im Wesentlichen einer von drei Kategorien zugeordnet werden:

- *Maßnahmen bei der Internet-Infrastruktur* (Sperre von Domainnamen oder des Zugangs zu „bösen Seiten"),
- *freiwillige Selbstzensur* von „guten Seiten" (Links auf „böse Seiten" werden nicht angezeigt oder erschwert zugänglich gemacht) oder
- *Filter auf der Seite des Users*, d.h. im Webbrowser[2].

Bevor diese Kategorien näher betrachtet werden, bleibt aber noch eine Frage zu klären: Was ist eigentlich „böse"? Moralische Begriffe umschreiben im IT-Kontext bestenfalls eine Zielrichtung, bedürfen jedoch einer Präzisierung. Die nachfolgend vorgestellten Maßnahmen wenden auch tatsächlich verschiedene Definitionen für „böse Seiten" an, z.B.

- Seiten, die durch Ausnutzung von Sicherheitslücken einen Computer gegen den Willen seines Besitzers manipulieren;
- Seiten, die den Download von Malware anbieten[3];
- Seiten, die sich als Login-Seiten für Online-Banking oder dergleichen ausgeben, um auf betrügerische Weise fremde Zugangsdaten zu erhalten (*Phishing*);
- Seiten, die auf Seiten verweisen, die eines oder mehrere der obigen Kriterien erfüllen;
- ganze Sites, die mindestens eine Seite enthalten, die eines oder mehrere der obigen Kriterien erfüllt. Der Site-Begriff ist allerdings selbst problematisch: Meist wird auf den Domainnamen abgezielt – was z.B. im Falle der Uni Wien die voneinander völlig unabhängigen Websites zahlreicher Institute und Einrichtungen in einen Topf wirft.

Maßnahmen bei der Internet-Infrastruktur: Erst schießen, dann fragen?

Wenn eine „böse Seite" entdeckt wird, wäre es die schnellste Lösung, sie einfach aus dem Verkehr zu ziehen, indem man den Zugang zu ihrem Server sperren lässt; das würde allerdings bedeuten, mit Kanonen auf Spatzen zu schießen. Der logischere und zielführendere – leider aber auch oft vernachlässigte – Weg ist es, den Eigentümer der verseuchten Webseite zu verständigen. Dieser hat die „böse Seite" nur selten selbst bzw. absichtlich installiert und daher in der Regel großes Interesse daran, seinen Webauftritt wieder zu bereinigen. Sollte er nicht kooperieren wollen, kann man sich an seinen Internetprovider wenden: Seriöse Provider haben für den Notfall genügend Handhabe in ihren Geschäftsbedingungen, um Kunden, die das Netz vorsätzlich missbrauchen, wieder loszuwerden.

Hin und wieder kann es vorkommen, dass kurzfristig eine Maßnahme gegen eine „böse Seite" gesetzt werden müsste, dies aber nicht im Einvernehmen mit dem Eigentümer der Seite oder seinem Provider möglich ist – sei es, weil die zuständigen Personen nicht erreichbar bzw. nicht eruierbar sind oder weil sie weder über das notwendige Fachwissen noch über einen kompetenten Dienstleister verfügen. In solchen schwerwiegenden Einzelfällen mag es gerechtfertigt sein, an eine netzweite Sperre zu denken. Dabei muss man sich allerdings einer Reihe kniffliger Fragen stellen:

- Ist die Maßnahme tatsächlich notwendig?
- Ist die Maßnahme tatsächlich ausreichend?
- Ist sie angemessen oder gibt es gelindere Mittel?
- Wie wird sie den Betroffenen (dem, der eine Seite nicht abrufen kann und dem, dessen Seite gesperrt wurde) kommuniziert?
- Wie kann ihre Ursache behoben werden?
- Ist sichergestellt, dass die Maßnahme nach Behebung der Ursache unverzüglich wieder aufgehoben wird?

Jeder Sperre haftet ein Stück Niederlage an, weil das Wichtigste – nämlich das Problem zu analysieren und zu sanieren – nicht gelungen ist. Deshalb sollte sie immer als letztes Mittel angesehen und entsprechend sparsam eingesetzt werden.

Domainsperre

Um im Internet eine Ressource (eine Webseite, eine eMail-Adresse, ...) zu erreichen, bedient man sich meistens eines Domainnamens – beispielsweise `google.at`. Domains sind hierarchisch organisiert, d.h. `google.at` kann nur durch die Verwaltungsinstanz (die so genannte *Registry*) von `.at` eingerichtet werden. In der Hierarchie ganz oben stehen die Länderdomains wie `.at` für Österreich sowie eine Handvoll kategorisierender Domains wie `.com`, `.org` oder `.net`. Der hierarchische Aufbau ist insofern entscheidend, als die übergeordnete Registry (für die österreichischen Domains ist das die *nic.at Internet Verwaltungs- und Betriebsgesellschaft m.b.H.*, siehe `www.nic.at`) rein technisch die Möglichkeit hat, jede Domain in ihrem Bereich aus dem Verkehr zu ziehen – und mit ihr allfällige darunter abrufbare „böse Seiten".

Eine Registry spielt in der virtuellen Welt eine Rolle, die der einer Hoheitsverwaltung gleichkommt – sie allein entscheidet, ob eine Domain und die damit verbundene Firma im Internet existiert oder nicht. Daher muss auch eine Registry Ansprüchen wie Rechtsstaatlichkeit, Unparteilichkeit usw.

---

2) Es gibt auch Filterkomponenten, die ähnlich einer Firewall an der Verbindung zwischen einem Firmennetz und dem Internet installiert werden. Der ZID der Universität Wien setzt keine solchen Geräte ein und für den Privatanwender kommen sie ebenfalls nicht in Betracht, deshalb wird hier nicht näher auf diese Variante eingegangen.

3) Malware umfasst hier neben alten Bekannten wie Viren, Würmern und Trojanischen Pferden auch Software, die den Anwender ausspioniert (*Spyware*), die Fremden den Zugriff auf den Rechner ermöglicht (*Backdoors*), die in penetranter Weise Werbeeinblendungen vornimmt (*Adware*) oder die ihre Existenz verschleiert und sich nicht wieder deinstallieren lässt (*Rootkits*).

genügen: Einem Domaininhaber, der die formalen Erfordernisse erfüllt (korrekte Kontaktdaten, Entrichtung der Gebühren, funktionierende Nameserver, ...), steht seine Domain zu, bis ein ordentliches Gericht anders entscheidet.

Dennoch werden Registries immer wieder aufgefordert, „böse" Domains zu sperren. Groß sind etwa die Begehrlichkeiten diverser Banken, die Domains von Phishing-Sites zügig stillzulegen. Das ist durchaus verständlich, aber aus den geschilderten Gründen nicht einfach so auf Zuruf möglich. Wie wichtig dieses Festhalten der Registries an rechtsstaatlichen Prinzipien ist, zeigt ein Beispiel aus der jüngsten Vergangenheit: Die Antispam-Organisation Spamhaus (`www.spamhaus.org`) beanstandete bei der Firma nic.at bestimmte `.at`-Domains als „Spamschleudern", konnte deren Sperre jedoch mangels hinreichender Argumente nicht durchsetzen. Daraufhin nahm Spamhaus die Mailserver von nic.at in ihre Blacklist[4] auf, was die eMail-Korrespondenz der österreichischen Registry massiv behinderte. Auch der Universität Wien, die die Domainverwaltungs-Technik für nic.at betreibt, wurde mit Blacklisting gedroht. Spamhaus verspielte mit diesem Willkürakt das Vertrauen zahlreicher Mailserver-Betreiber, die sich darauf verlassen hatten, dass auf dieser Blacklist ausschließlich Spamversender aufscheinen. Wenn eine private Organisation wie Spamhaus derart überreagiert und ihren Einfluss als Druckmittel missbraucht, ist Gegenwehr möglich (viele Serverbetreiber entfernten die Spamhaus-Blacklist aus der Konfiguration ihrer Mailserver); nachdem aber österreichische Firmen nicht einfach aus Österreich abwandern können, muss nic.at als nationale Registry höhere Maßstäbe setzen.

Gegen Domainsperren spricht auch, dass diese nicht bloß die Webseiten betreffen, die sich unter dem um `www` ergänzten Domainnamen finden. Zum einen sind oft auch andere abgeleitete Namen für Webserver in Gebrauch – so wie es nicht nur `www.univie.ac.at`, sondern auch `www.unet.univie.ac.at`, `homepage.univie.ac.at` und viele mehr gibt. Zum anderen können zahllose weitere Services – z.B. Mailserver – mit einem Domainnamen verbunden sein, die in keinerlei Zusammenhang mit einer allfälligen „bösen Seite" innerhalb der Domain stehen. Eine Sperre der Domain würde all diese weiteren Services ebenfalls blockieren und einen unabschätzbaren Kollateralschaden verursachen. Es sollte daher selbstverständlich sein, zuerst den Serverbetreiber zu kontaktieren, bevor man weitere Schritte in Erwägung zieht.

Die Befürworter der Domainsperr-Idee haben allerdings auch ein gutes Argument auf ihrer Seite: Insbesondere bei Phishing-Attacken ist häufig zu beobachten, dass eigens dafür verwendete Domainnamen zum Einsatz kommen, die nicht etwa auf „den Server" mit den gefälschten Seiten verweisen, sondern in schnellem Wechsel auf tausende davon. Werden einige dieser Phishing-Server aus dem Verkehr gezogen, ändert das gar nichts, weil es noch zahllose andere gibt. Eine solche Phishing-Attacke lässt sich nur durch Unschädlichmachen der Domain beenden. Registries können zu diesem Zweck durchaus sinnvolle Maßnahmen treffen und tun dies auch in unterschiedlichem Maße: genauere Identitätsprüfung der Domaininhaber, Beschränkung der Zahl der Nameserver für eine Domain, Beschränkung der Häufigkeit, mit der diese gewechselt werden können, usw.

Eine Domain kann zwar nur durch die jeweils zuständige Registry weltweit gesperrt werden, jeder Netzbetreiber kann sie aber natürlich im eigenen Wirkungsbereich blockieren. An der Uni Wien gilt, nicht zuletzt wegen der Zensurnähe solcher Maßnahmen, das Prinzip der vorsichtigen Zurückhaltung: Grundsätzlich wird nichts gesperrt. Sollte wider Erwarten doch einmal ein besonderer Ausnahmefall eintreten, der solche akuten Sofortmaßnahmen erfordert, wird dies auf den ZID-Webseiten und über die Mailingliste `zid-tech` (Näheres dazu siehe `http://lists.univie.ac.at/mailman/listinfo/zid-tech/`) bekannt gemacht.

Sperre von IP-Adressen

Die IP-Adresse (z.B. `131.130.1.78` – nicht zu verwechseln mit dem landläufig als „Internet-Adresse" bezeichneten URL, z.B. `http://www.univie.ac.at/`) ist für den Anwender normalerweise nicht wahrnehmbar und bezeichnet, stark vereinfacht ausgedrückt, die Netzwerkschnittstelle eines bestimmten Rechners im Internet. Indem man allen Datenverkehr mit seiner IP-Adresse unterbindet, könnte man einen Rechner theoretisch ganz vom Netz abkoppeln und so die „bösen Seiten" aus dem Verkehr ziehen. In der Praxis ist das nicht ganz so einfach: Das Internet wurde wegen seiner militärischen Zielsetzungen so entworfen, dass es auch dann noch funktioniert, wenn mehrere zentrale Knoten ausfallen. Eine Folge davon ist, dass es keine einzelne Stelle gibt, an der eine IP-Adresse netzweit blockiert werden könnte. Fragen, wie sie sich bei Domainsperren stellen, lassen sich hier also einfach auf technischer Ebene abschlägig beantworten. Nicht einmal dem Reich der Mitte, das durch die Chinesische Mauer bereits zweieinhalb Jahrtausende Erfahrung im Abschotten hat, ist es gelungen, sein Internet wirksam gegen unerwünschte Einflüsse abzudichten.

Allein der Betreiber des Netzes, in dem sich eine IP-Adresse befindet, kann diese wirksam blockieren[5] – und er hat auch die Möglichkeit, den betroffenen Administrator zu benachrichtigen. Wenn ein Rechner böse Dinge tut und kurzfristig niemand erreichbar ist, der das abstellen könnte, kann es eine sinnvolle Sofortmaßnahme sein, ihn vorübergehend vom Netz zu nehmen.

---

4) Als *Blacklist* bezeichnet man in diesem Zusammenhang eine „schwarze Liste" von bekannten Spamversendern, die Mailserver-Betreiber zur Spambekämpfung heranziehen können.

5) Gerade bei größeren Netzen kann das allerdings zu einem beliebig komplizierten und langwierigen Unterfangen werden. Für den Bereich der Universität Wien wurde einiges an Arbeit investiert, um die notwendigen Werkzeuge und Abläufe für eine praktikable Internet-Notbremse zu entwickeln.

6) siehe `www.heise.de/newsticker/meldung/96100/`

7) siehe `www.stopbadware.org/home/reportsearch`

Umgekehrt kann man als Netzwerk-Administrator auch den Verkehr des eigenen Netzes mit bestimmten IP-Adressen unterbinden. Das ist aber nur in ganz extremen Ausnahmefällen angemessen: Der Betreiber der ausgesperrten Adresse hat ja keine Möglichkeit, von der Sperre zu erfahren und deren Aufhebung zu veranlassen, sobald er sein Problem bereinigt hat. Das Ergebnis ist, dass sich im Laufe der Zeit die gesperrten Adressen häufen und das Internet löchrig wie ein Emmentaler Käse wird. Ähnlich wie bei Domainsperren ist auch hier der mögliche Kollateralschaden gewaltig, da unter einer IP-Adresse mehrere Websites lagern können: Einem deutschen Provider ist es kürzlich gelungen, mit einem Handstreich statt einer einzigen gleich tausende Sites zu sperren.[6] Auch das Sperren von IP-Adressen ist somit kein allgemein brauchbarer Weg, das Internet sicherer zu machen.

Insgesamt betrachtet schneiden die Maßnahmen bei der Internet-Infrastruktur nicht gut ab. An der Benutzerfreundlichkeit gibt es zwar nicht viel zu bemängeln, und auch die Privatsphäre bleibt weitestgehend gewahrt. Die Transparenz fehlt jedoch völlig: Eine Erklärung, warum eine gesperrte Seite nicht erreichbar ist, erhält der Anwender nicht. Er hat auch keine Möglichkeit, die Seite dennoch aufzurufen. Die Treffsicherheit lässt wegen des erwähnten Kollateralschadens ebenfalls zu wünschen übrig.

Freiwillige Selbstzensur: Die weiße Weste beim Verlinken

Wer bei Google sucht, findet meistens auch etwas. Nicht immer ist es das, was er finden wollte, und manchmal ist es sogar eine Webseite, die Google als „böse Webseite“ einstuft. In diesem Fall steht eine kurze Warnung beim Suchergebnis (siehe **Abb. 2**), und ein Klick auf selbiges führt zu einer Warnungsseite, dem so genannten *Interstitial* (siehe **Abb. 3**). Dieses weist den User abermals auf die Gefahr hin und legt ihm nahe, doch lieber anderswo hinzugehen bzw. sich bei StopBadware (`www.stopbadware.org`) näher zu informieren. Nur auf eigenes Risiko dürfe man die betreffende Seite ansurfen. Offenbar will Google also eine weiße Weste wahren und nicht in den Verdacht geraten, auf „böse Seiten“ zu verlinken – das würde ja implizieren, dass Google selbst auch eine böse Site ist.

Bei nach Googles Ansicht ungefährlichen Seiten ist über die Bedienungsfreundlichkeit des Service nicht zu klagen: Alles ist problemlos erreichbar. Bei Seiten, die mit Googles Bann belegt sind, hat jedoch nur derjenige die Zügel in der Hand, der auch firm in *Cut & Paste* und URL-Leisten ist: Die Warnseite enthält keinen anklickbaren Link. Für weniger geübte Anwender stellt das eine Entmündigung dar, die einer Suchmaschine eigentlich nicht zusteht.

Wer versucht, Googles Urteile nachzuvollziehen, gelangt in ein Dickicht von Policies und vagen Andeutungen. Google verweist auf die Webseite von StopBadware; diese arbeitet

Abb. 2: In der Liste der Google-Suchergebnisse ist der Hinweis auf die Gefährlichkeit einzelner Seiten etwas unscheinbar.

Abb. 3: Der Versuch, auf eine als gefährlich eingestufte Seite zu gelangen, führt zu dieser Warnung.

jedoch überdeutlich heraus, dass Google völlig unabhängig von StopBadware entscheide, welche Seiten „gut“ und welche „böse“ seien. Wer aber mit der Einstufung Googles nicht zufrieden sei, solle dennoch bei StopBadware eine Prüfung beantragen, deren Ergebnis Google wohlwollend prüfen werde. Alles klar?

StopBadware dokumentiert die eigenen Kriterien, nach denen Seiten als Malware eingestuft werden, erklärt dabei aber, „auch“ Meldungen von Google und nicht näher genannten *Trusted Third Parties* zu übernehmen. Beim Herumstöbern in StopBadwares Datenbank fiel auf, dass alle 102 dort verzeichneten österreichischen Sites (Stand von Anfang September 2007) von Google gemeldet wurden. Eine gründlichere Suche ergab, dass von den – laut Homepage – 229 735 so genannten *Reported Sites* sage und schreibe 49 eine Einstufung durch StopBadware selbst erhalten hatten.[7] In jedem dieser Fälle ist jedoch in den Erläuterungen zu lesen, die Seite sei nicht von Forschern von StopBadware *reviewed* worden – das verstehe, wer will. Ein Hinweis auf eine andere *Trusted Third Party* als Google war übrigens nicht zu entdecken.

Doch einmal abgesehen von diesem Pingpong-Spiel hinter den Kulissen: Wie sinnvoll und hilfreich ist Googles Selbstzensur für den User?

- Was die *Treffsicherheit* anbelangt, sollte man meinen, dass eine Suchmaschine, die große Teile des Web ohnehin schon vom Indizieren kennt, auch alle darin versteckte Badware aufspüren oder zumindest deren Abwesenheit zweifelsfrei feststellen kann. Doch weit gefehlt: Im Praxisversuch war es nicht sehr schwierig, durch Eingabe von Keywords aus der Schmuddel- oder Raubkopierecke zu Seiten zu gelangen, vor denen Google nicht warnt, die aber sehr wohl Malware enthalten – in erster Linie *Dialer* (das sind Programme, die das Modem dazu überreden, nicht den Provider, sondern teure Mehrwertnummern anzurufen). Andererseits findet man in den StopBadware-Foren immer wieder glaubwürdige Klagen darüber, dass Sites ohne erkennbaren Grund für gefährlich erklärt werden, StopBadware die betroffenen Webmaster lediglich an Google verweist und der Fall dort im Sande verläuft.[8)]

- Ad *Privatsphäre*: Google kennt zwangsläufig die vom User eingegebenen Suchwörter und seine IP-Adresse – dass es durch den Aufruf der Warnungsseite auch noch erfährt, wenn eine „böse Seite" angeklickt wurde, ist da fast schon nebensächlich.

- Zur *Wirksamkeit* des Ganzen ist zu sagen, dass Google zwar seine eigenen Suchergebnisse weißwaschen, aber nicht verhindern kann, dass der User anderswo auf einen Link zur „bösen Seite" klickt. Das Service deckt somit nur ein kleinen Bruchteil der Risiken ab.

Foren-Postings deuten darauf hin, dass Google bzw. StopBadware fallweise die Webmaster jener Sites verständigt, bei denen ein Problem gefunden wird, dass es dafür aber noch keine fixen Prozesse gibt. Es ist bedauerlich, dass hier die Chance vertan wird, Probleme in direkter Zusammenarbeit zu beseitigen und damit echten Nutzen zu stiften. In Summe wundert man sich, dass Google mit einem derart unausgegorenen Flickwerk offiziell in Betrieb gegangen ist, und das schon vor über einem Jahr.

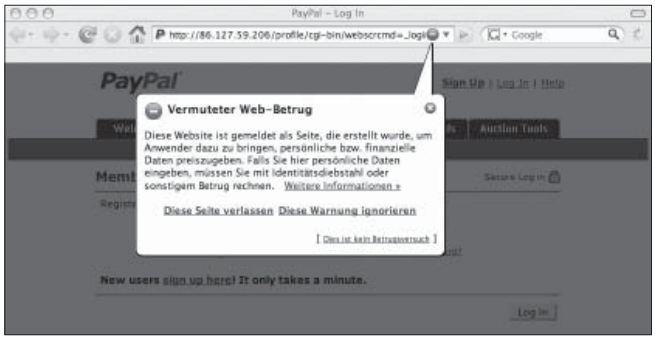


Abb. 4: Firefox-Warnung vor einer Phishing-Seite

Filter auf der Seite des Users: Helferlein im Webbrowser

Sowohl MS-Internet Explorer als auch Mozilla Firefox haben in jüngeren Versionen einen Schutz vor Phishing-Seiten eingebaut. Weiters gibt es einige Plugins, die vor verschiedenen Arten von „bösen Seiten" schützen sollen und unterschiedliche Methoden und Datenquellen nutzen. All diesen Produkten ist gemeinsam, dass sie den URL der Seite, die in den Browser geladen werden soll, mit einer Datenbank abgleichen, die „böse Seiten" verzeichnet. Erweist sich eine Seite als „böse", wechselt zum Beispiel ein Kästchen in einer Menüleiste von grün auf rot oder es wird eine Warnseite eingeblendet.

Die Integration in den Browser hat bestechende Vorteile:

- Der Anwender entscheidet selbst, welche Filter er einsetzen möchte und welche nicht. Diese Freiheit birgt aber auch ein Risiko, das bereits von Virenscannern bekannt ist: Malware, die trotz aller Vorkehrungen einen Weg auf den Computer findet, kann die Filter ebenfalls (und hinterrücks) wieder ausschalten.

- Die Bedienung kann gleichzeitig einfacher und mächtiger gestaltet werden – z.B. durch Popups, die die Gefährlichkeit einer Seite bereits anzeigen, wenn sich der Mauszeiger nur über dem dorthin führenden Link befindet, oder durch ausführliche Hintergrundinformationen in den Werkzeugleisten des Browsers.

- Jede aufgerufene Seite kann individuell überprüft werden. Dies steht im krassen Gegensatz zu Sperren ganzer Domains bzw. Server wegen einer einzelnen Seite, die der Anwender möglicherweise ohnehin nicht besucht hätte. Die Prüfung geht auch über Googles Ansatz hinaus, der nur die Links auf der eigenen Suchergebnis-Seite umfassen kann.

- Sofern die „Böse-Seiten-Datenbank" auf dem PC des Anwenders gespeichert ist und regelmäßig aktualisiert wird, werden keine Informationen über die vom User aufgerufenen Seiten nach außen weitergegeben. Aus technischen Gründen wird allerdings dennoch oft die Online-Abfrage bevorzugt.

---

8) siehe `http://groups.google.com/group/stopbadware/browse_thread/thread/2614b64b3633f34`

9) siehe `www.microsoft.com/germany/windows/products/windowsvista/features/details/ie7antiphishing.mspx`

10) siehe `http://toolbar.live.com/?mkt=de-de`

11) siehe `www.3sharp.com/projects/antiphishing/gone-phishing.pdf`

12) siehe das unter `www.microsoft.com/mscorp/safety/technologies/antiphishing/default.mspx` downloadbare *Anti-Phishing White Paper*

13) siehe `www.codecon.org/2006/program.html#siteadvisor`

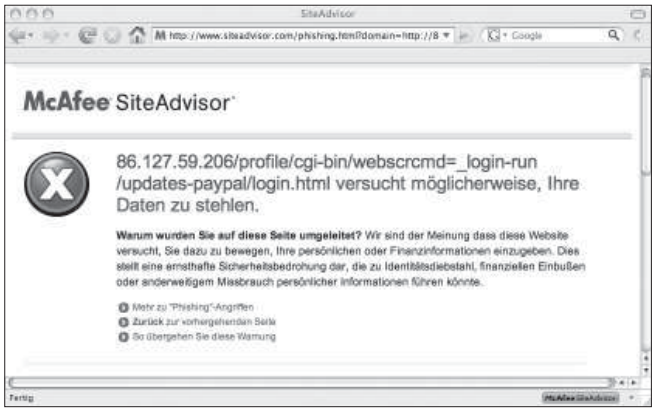


Abb. 5: SiteAdvisor-Warnung vor einer Phishing-Seite

Um die verwendeten Methoden vorzustellen, werden hier vier Anwendungen exemplarisch näher beleuchtet: Microsofts Phishing Filter, der Phishing Filter von Firefox, McAfee SiteAdvisor und WOT.

Microsoft Phishing Filter

In Internet Explorer 7, der bei Windows Vista mitgeliefert wird und auch auf Windows XP ab Service Pack 2 installiert werden kann, ist der Microsoft Phishing Filter bereits enthalten, muss jedoch erst eingeschaltet werden.[9)] Als Kompromiss zwischen Aktualität der Datenbasis und Wahrung der Privatsphäre kombiniert der Filter lokale Listen (sowohl von bekannten „guten" als auch von bekannten „bösen" Websites) und heuristische Seitenanalysen im PC des Anwenders mit einer Online-Abfrage bei den verbleibenden Zweifelsfällen. Eine ganz ähnliche Funktionalität bietet Microsofts *Windows Live Toolbar*.[10)] Diverse von Microsoft in Auftrag gegebene Studien bescheinigen dem Filter hervorragende Trefferraten.[11)]

Woher Microsoft allerdings die Informationen über die Phishing-Seiten bezieht, geht aus der Dokumentation[12)] nicht klar hervor. Naheliegend wäre, bekannte Meldestellen (`www.apwg.org`, `www.phishtank.com` etc.), Microsofts eigene Suchmaschine sowie URLs aus eMails heranzuziehen, die sich in Microsofts Spamfilter bzw. bei Hotmail verfangen haben. Offenbar werden diese Seiten mittels heuristischer Analyse selektiert und zu einer Liste verdächtiger Seiten zusammengestellt. Die weitere Beurteilung erfolgt quasi per Volksabstimmung: Über ein Menü kann jeder Anwender seine Meinung darüber abgeben, ob die dargestellte Seite seiner Meinung nach legitim ist oder nicht. Ob auch eine professionelle Beurteilung seitens Microsoft erfolgt, erschließt sich nicht.

Leider verständigt Microsoft die Betreiber der Sites, die eine Phishing-Seite enthalten, nicht. Damit nicht genug: Die einzige Möglichkeit nachzusehen, ob z.B. die eigenen Seiten als Phishing-Seiten gelistet sind, besteht über den Internet Explorer oder die Windows Live Toolbar. Dasselbe gilt, wenn man mit Microsoft in Kontakt treten will, um Einwände gegen ein irrtümliches Listing zu erheben oder zu melden, dass die Phishing-Seiten entfernt wurden. Damit sind Personen, die kein Betriebssystem von Microsoft verwenden, vom gesamten Verfahren ausgeschlossen. Leider deutet auch nichts auf eine Zusammenarbeit bzw. einen Abgleich mit bereits etablierten Verzeichnissen und Organisationen hin. Wie Google hat auch Microsoft eine immense Chance vertan, wirklich zur Sicherheit im Internet beizutragen.

Firefox Phishing Filter

Ähnlich Microsofts Phishing Filter hat auch Firefox ab Version 2 einen Schutz vor Phishing-Seiten eingebaut (siehe **Abb. 4**). Dieser ist standardmäßig aktiviert und greift nur auf eine lokale Datenbank zu, sodass die Privatsphäre des Anwenders gewahrt bleibt. Um bessere Ergebnisse zu erzielen, wird jedoch empfohlen, die Konfiguration derart zu ändern, dass der URL jeder aufzurufenden Seite online bei Google geprüft wird. Dieser Rat ist schwer nachzuvollziehen: Da die lokale Datenbank laut Dokumentation ohnehin alle 30 bis 60 Minuten aktualisiert wird und es viel länger dauert, bis eine Phishing-Seite gemeldet und überprüft wurde, ist der Zeitgewinn vernachlässigbar. Wenn man bedenkt, dass Firefox bei jeder Online-Abfrage den gesamten URL inklusive allfälliger Parameter übermittelt, wiegt der Verlust an Privatsphäre wohl deutlich schwerer.

Firefox benutzt die Datenbestände von Google, um zu entscheiden, welche Seiten gut und welche böse sind. Daher gilt für seine Zuverlässigkeit das bereits weiter oben über Google und StopBadware Gesagte. Ebenso wie Internet Explorer bietet auch Firefox ein in den Browser integriertes Menü, um Phishing-Seiten zu melden.

In der nächsten Firefox-Version soll der Schutz auch sonstige Malware umfassen. Die zu Redaktionsschluss jüngste Entwicklerversion (Gran Paradiso Alpha 8) hat in einem kurzen Test aber keinerlei Erfolg gezeigt – hier muss man sich wohl noch etwas in Geduld fassen.

McAfee SiteAdvisor

SiteAdvisor ist als kostenloses Plugin für Internet Explorer und Firefox erhältlich. Das Plugin vergleicht die Domainnamen der im Browser aufgerufenen Seiten mit der Datenbank von McAfee und zeigt im Fall eines Treffers eine deutliche Warnung an (siehe **Abb. 5**).

Entscheidend ist naturgemäß die Qualität der abgefragten Datenbank. Hier haben sich die Entwickler – übrigens keine Mitarbeiter von McAfee, sondern frisch gebackene Absolventen des *Massachusetts Institute of Technology* (MIT) – etwas einfallen lassen: So wie es auch die Suchmaschinen tun, lassen sie die Webseiten im World Wide Web automatisch abgrasen und laden die gefundenen Seiten und Dateien in simulierte (virtuelle) PCs. SiteAdvisor schaut quasi mit der Röntgenkamera in diese PCs hinein, und wenn bestimmte Veränderungen am System oder Programm-Merkmale erkannt werden, die für Malware typisch sind, wird die betreffende Website als „böse" markiert.[13)]

So einleuchtend das Konzept klingen mag – in der Praxis erfüllt SiteAdvisor die Erwartungen leider doch nicht. Das konnten wir am eigenen Leib (genauer: an der eigenen Domain) spüren, als `univie.ac.at` als gefährlich eingestuft wurde.

Das Offensichtliche zuerst: Es reicht nicht, lediglich den Domainnamen als Kriterium für die Gefährlichkeit einer Webseite heranzuziehen. Am Beispiel der Universität Wien zeigt sich, dass es völlig überzogen und für den Anwender gar nicht hilfreich ist, alle Webseiten einer Domain über einen Kamm zu scheren und als „böse" zu markieren – selbst wenn sich vielleicht irgendwo in den Tiefen dieses Webspace eine Malware eingeschlichen haben sollte. Um nützlich zu sein, müsste SiteAdvisor einzelne Seiten oder wenigstens Verzeichnisbäume bewerten. Kaum tröstlich, aber doch ein positiver Aspekt: McAfee erfährt nicht, welche Seiten genau vom Anwender aufgerufen wurden, sondern nur deren Domainnamen.

Immerhin kann man bei SiteAdvisor leicht online nachvollziehen, wie eine Bewertung zustande gekommen ist. Hierbei staunten wir nicht schlecht, als wir feststellen mussten, dass Dateien auf unserem FTP-Server (der mit dem Webserver nichts zu tun hat) für McAfees Warnung vor unserer Domain verantwortlich waren.[14)]

Noch größere Augen bekamen wir dann, als wir sahen, warum der FTP-Server der Uni Wien in Verruf geraten war: Ganze zwei Dateien aus der umfassenden und immerhin seit 1995 existierenden Softwaresammlung WinSite, die wir dort als Kopie für unsere User zur Verfügung stellten,[15)] waren vom Automatismus als „böse" eingestuft worden. Der letzte Download, den SiteAdvisor von unserem FTP-Server gemacht hatte, lag allerdings bereits ein Jahr zurück – die Grundlage für das ohnehin höchst zweifelhafte Urteil von SiteAdvisor war also hoffnungslos veraltet.

Noch ein Minus: Selbst die Entwickler solcher automatisierter Tests sind der Meinung, dass diese nicht immer funktionieren, sondern in manchen Fällen ein Mensch zwischen „gut" und „böse" entscheiden muss.[16)] In unserem Beispiel ist die Exaktheit wohl dem Rechenstift zum Opfer gefallen – unsere Bitte an McAfee, die unsinnige Bewertung unserer Domain und die der ebenfalls betroffenen TU Wien zu korrigieren, wurde höflich aber abschlägig beantwortet, mit der Begründung, dass die gesamte Überprüfung automatisiert und daher nicht beeinflussbar sei.

Schließlich bleibt noch zu erwähnen, dass auch McAfee das, was den meisten Nutzen für die Anwender brächte, nicht tut: nämlich die Sitebetreiber von dem (vermeintlichen) Problem in Kenntnis setzen.

Wenn McAfee, einer der traditionsreichsten Hersteller von Antivirus-Produkten, einen in den Browser integrierten Schutz vor „bösen Seiten" herausbringt, kann man ein seriöses Produkt erwarten. Mit dieser halbgaren Bastellösung, so interessant und vielversprechend die technischen Ansätze auch sind, hat sich McAfee aber nicht mit Ruhm bekleckert.

WOT

Wie SiteAdvisor ist WOT ein von frisch gebackenen – diesmal finnischen – Studienabsolventen entwickeltes Bewertungsservice, das sich gegenwärtig jedoch nur mit Firefox nutzen lässt. Auch WOT differenziert nicht die einzelnen Seiten einer Website, sondern gleicht nur den Domainnamen mit einer Datenbank ab.

Das Besondere an WOT ist, dass nicht einfach zwischen „gut" und „böse" unterschieden wird, sondern neben einer Gesamtwertung drei verschiedene Gesichtspunkte beurteilt werden: Vertrauenswürdigkeit als Geschäftspartner, Umgang mit der Privatsphäre und „Kindersicherheit" nach US-amerikanischen Wertmaßstäben (siehe **Abb. 6**).

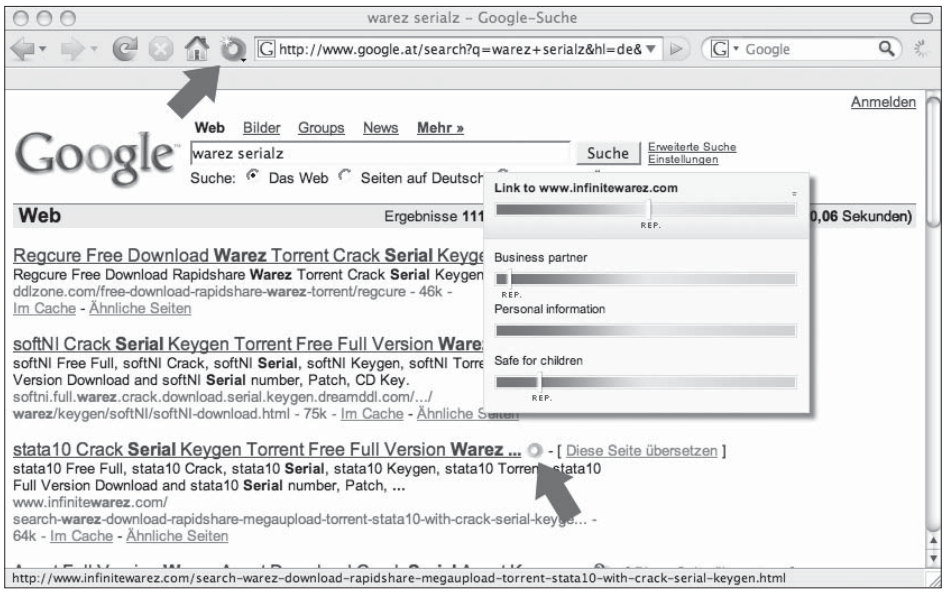


Abb. 6: WOT teilt Seiten nicht nur in „gut" oder „böse" ein, sondern bietet eine differenzierte Beurteilung.

Ganz im Gegensatz zu SiteAdvisor beruht die Beurteilung von Websites hier überhaupt nicht auf technischen Kriterien, sondern ergibt sich vielmehr aus den Bewertungen der WOT-Benutzerschaft. Um speziell bei neuen Seiten (wie es z.B. Phishing-Seiten regelmäßig sind) schnell eine Bewertung anbieten zu können, bezieht WOT auch Informationen von über hundert weiteren Systemen mit ein, beispielsweise vom Phishingseiten-Verzeichnis `phishtank.com`.

Dieser basisdemokratische Ansatz ruft natürlich gerade bei Frage-

stellungen, bei denen Sicherheitsspezialisten gefordert sind, einige Skepsis hervor. Erstaunlicherweise scheint das System aber gar nicht schlecht zu funktionieren, jedenfalls sind im – freilich nicht repräsentativen – Test keine groben Schnitzer aufgefallen. Auch die subjektive Zufriedenheit der Anwender im WOT-Forum scheint recht groß zu sein, gerade im Vergleich zu SiteAdvisor.

Fazit

Obwohl einige der Ansätze, die derzeit verfolgt werden, um den Anwender vor „bösen" Webseiten zu schützen, durchaus vielversprechend scheinen, sind derartigen Werkzeugen einige grundlegende Grenzen gesetzt:

- Eine Schwierigkeit liegt darin, die **Zielsetzung** genau zu definieren. Wenn in diesem Artikel durchgehend die moralinsauer anmutenden Begriffe „gute Seiten" und „böse Seiten" verwendet wurden, dann deshalb, weil es unzählige mögliche Definitionen dafür gibt: Mit diffusen Begriffen kann die Informationstechnologie traditionell sehr schlecht umgehen. Ein Ausweg könnte darin bestehen, den mündigen Anwender im Einzelfall genau und verständlich darüber zu informieren, welche Arten von Gefahren oder Unannehmlichkeiten es gibt, und ihn wählen zu lassen, welche von ihm ferngehalten werden sollen.

- Ein gravierenderes Problem ist das der **Menge**. Derzeit ist nicht absehbar, dass vollautomatische Systeme jemals eine brauchbare Klassifizierung zuwege bringen werden. Eine manuelle Prüfung erfordert aber einen ungeheuren Personaleinsatz, der nur für ein eher enges Anwendungsgebiet – etwa Phishing-Seiten – bezahlbar erscheint. Es muss deshalb damit gerechnet werden, dass alle diese Systeme noch länger ein Problem mit der Treffsicherheit haben werden.

- Eine weitere Komplikation entsteht durch die Möglichkeit, Webseiten **dynamisch** umzugestalten. Bereits jetzt gibt es zahlreiche Webseiten, die sich z.B. den Google-Robots anders präsentieren als dem normalen Anwender. Warum sollten „böse Seiten" nicht ebenfalls eine harmlose Variante vorhalten, die sie den Malware-Fahndern zeigen? Im einfachsten Fall reicht es bereits, ein durch einen Computer nur sehr schwer lösbares Bildrätsel – z.B. ein so genanntes *Captcha*[17] – vor die eigentliche Malware zu setzen, damit diese nicht von Automaten entdeckt werden kann.

- Eine besondere Gefahr ergibt sich aus dem **falschen Sicherheitsgefühl**: Wer sich auf den Ratschlag eines Webseiten-Gutachters verlässt und dabei nicht bedenkt, dass auch dieser nur einen Teil der „bösen" Seiten erkennen kann, gerät möglicherweise in Versuchung, die anderen Sicherheitsmaßnahmen zu vernachlässigen – und fällt den unerkannten Bösewichten dann völlig wehrlos zum Opfer.

- Das Gegenstück zur unerkannten Gefahr ist der **falsche Alarm**. Geschieht dies zu häufig, werden die Anwender (zu Recht) das Vertrauen in das System verlieren und es umgehen. Damit ist die Schutzwirkung dahin.

- Bei den derzeit wohl aussichtsreichsten Kandidaten für gute Schutzsysteme, den Browser-Plugins, sind auch die möglichen **Nebenwirkungen** zu bedenken. Schließlich handelt es sich um Software, die obendrein noch mit anderer Software zusammenarbeiten muss, was das Gesamtsystem noch komplexer macht. Erhöhte Komplexität führt in der Datenverarbeitung traditionellerweise zu erhöhter Fehleranfälligkeit und zu mehr Sicherheitslücken.

- Selbstverständlich ist davon auszugehen, dass alle diese Schutztechnologien auch das Interesse verschiedener **(para)staatlicher Organe** wecken. Diese könnten auf die Idee kommen, ihrer Meinung nach schädliche Inhalte – anfangs z.B. Informationen zur Herstellung von Sprengstoffen – zu unterdrücken. Eine andere Möglichkeit wäre, natürlich nur im begründeten Einzelfall (erst bei Terrorismus und Kinderpornographie, später wohl auch bei illegalem Filesharing), auf die Protokolle der Filter-Datenbanken und damit auf das Surfverhalten des Anwenders zuzugreifen.

Den Anstrengungen, die Anwender zuverlässig vor „bösen Webseiten" zu schützen, weht ein rauer Wind entgegen. Dennoch ist es wichtig, alle verfügbaren Mittel in dieser Richtung auszuschöpfen. Dabei darf auch keinesfalls vergessen werden, dass „böse" Webseiten nur teilweise ein technisches Problem sind. Beispielsweise müssen auch die rechtlichen Rahmenbedingungen geschaffen werden, um mittels Computer verübte Verbrechen international verfolgen zu können. Weiters müssen die Netzbetreiber die logistischen und vertraglichen Voraussetzungen schaffen, um missbräuchlich verwendete Rechner, die sich in ihrem Einflussbereich befinden, rasch aus dem Verkehr ziehen und sanieren zu können.

Die Industrie hat ganz offensichtlich den Bedarf erkannt, das Websurfen sicherer zu gestalten. Die bisher vorliegenden Ergebnisse sind unbefriedigend und noch zu sehr im Bastelstadium, um guten Gewissens empfohlen werden zu können. Man kann gespannt und hoffnungsvoll sein, was die Zukunft bringt.

Alexander Talos

14) Pikanterweise hat SiteAdvisor den FTP-Server nicht auf seine *Rote Liste* gesetzt, wohl aber `www.univie.ac.at` und `univie.ac.at`.

15) siehe Artikel *Softwarearchive auf dem FTP-Server der Universität Wien* in *Comment 97/1*, Seite 29 bzw. unter `http://comment.univie.ac.at/97-1/29/`

16) siehe `www.securityfocus.com/news/11376`

17) siehe `http://de.wikipedia.org/wiki/Captcha`

EDV-Kurse & ECDL-Prüfungen des ZID bis Ende Jänner 2008

Allgemeines

Im Folgenden finden Sie alle Termine der von Ende Oktober 2007 bis Ende Jänner 2008 geplanten **EDV-Kurse**, **Vorträge** und **ECDL-Prüfungen** des Zentralen Informatikdienstes. Genauere Informationen (An-/Abmeldung, Voraussetzungen, Inhalte, Preise, Kursort usw.) finden Sie unter:

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

Da Termine hinzukommen oder entfallen können, beachten Sie bitte die aktuellen Informationen unter den angegebenen Links!

Die aktuellen Kursbelegungen (freie Plätze) können unter dem URL **www.univie.ac.at/ZID/kursbelegung/** abgerufen werden.

Die **Vorträge** sind kostenlos und ohne Anmeldung zugänglich; sie finden im Hörsaal 3 des Neuen Institutsgebäudes statt (NIG, 1010 Wien, Universitätsstraße 7, Stiege I, Erdgeschoss).

Basics

u:net- und PC-Raum-Basics für Studierende

Termin	Zeit	Anmeldung
30.10.2007	09:00 – 12:00 h	bis 30.10.07

Betriebssysteme

Windows – Einführung

Termin	Zeit	Anmeldung
14.11.2007	09:00 – 16:00 h	bis 07.11.07

Textverarbeitung

Word – Einführung (Office XP)

Termin	Zeit	Anmeldung
29.10.2007	09:00 – 16:00 h	bis 22.10.07
23.11.2007	09:00 – 16:00 h	bis 16.11.07

Word – Einführung (Office 2007)

Termin	Zeit	Anmeldung
05.11.2007	09:00 – 16:00 h	bis 29.10.07

Word – Fortsetzung (Office XP)

Termin	Zeit	Anmeldung
31.10.2007	09:00 – 16:00 h	bis 24.10.07
05.12.2007	09:00 – 16:00 h	bis 28.11.07

Word – Fortsetzung (Office 2007)

Termin	Zeit	Anmeldung
08.11.2007	09:00 – 16:00 h	bis 31.10.07

Word – Wissenschaftliches Arbeiten (Office XP)

Termin	Zeit	Anmeldung
09.11.2007	09:00 – 16:00 h	bis 02.11.07

Word – Wissenschaftliches Arbeiten (Office 2007)

Termin	Zeit	Anmeldung
22.11.2007	09:00 – 16:00 h	bis 15.11.07

Tabellenkalkulation

Excel – Einführung (Office XP)

Termin	Zeit	Anmeldung
05.11.2007	09:00 – 16:00 h	bis 29.10.07

Excel – Einführung (Office 2007)

Termin	Zeit	Anmeldung
20.11.2007	09:00 – 16:00 h	bis 13.11.07

Excel – Fortsetzung (Office XP)

Termin	Zeit	Anmeldung
08.11.2007	09:00 – 16:00 h	bis 31.10.07

Excel – Fortsetzung (Office 2007)

Termin	Zeit	Anmeldung
29.11.2007	09:00 – 16:00 h	bis 22.11.07

Datenbanken

Access – Einführung (Office XP)

Termin	Zeit	Anmeldung
12.11. – 13.11.07	09:00 – 16:00 h	bis 05.11.07

Access – Einführung (Office 2007)

Termin	Zeit	Anmeldung
10.12. – 11.12.07	09:00 – 16:00 h	bis 03.12.07

Access – Fortsetzung (Office XP)

Termin	Zeit	Anmeldung
13.12. – 14.12.07	09:00 – 16:00 h	bis 06.12.07

Diverse Applikationen

PowerPoint – Einführung (Office XP)

Termin	Zeit	Anmeldung
03.12.2007	09:00 – 16:00 h	bis 26.11.07

PowerPoint – Einführung (Office 2007)

Termin	Zeit	Anmeldung
12.12.2007	09:00 – 16:00 h	bis 05.12.07

PowerPoint – Fortsetzung (Office XP)

Termin	Zeit	Anmeldung
07.12.2007	09:00 – 16:00 h	bis 30.11.07

PowerPoint – Fortsetzung (Office 2007)

Termin	Zeit	Anmeldung
18.12.2007	09:00 – 16:00 h	bis 11.12.07

Photoshop – Einführung

Termin	Zeit	Anmeldung
05.12.2007	09:00 – 16:00 h	bis 28.11.07

Photoshop & ImageReady – Erstellen von Webgrafiken

Termin	Zeit	Anmeldung
17.12.2007	09:00 – 16:00 h	bis 10.12.07

SPSS – Einführung

Termin	Zeit	Anmeldung
22.11. – 23.11.07	09:00 – 16:00 h	bis 15.11.07

SPSS – Fortsetzung

Termin	Zeit	Anmeldung
10.01. – 11.01.08	09:00 – 16:00 h	bis 03.01.08

Programmierung

Einführung in das Programmieren mit JavaScript

Termin	Zeit	Anmeldung
07.12.07	12:30 – 15:00 h	keine (NIG, HS 3)

Programmieren mit PHP – Teil 1

Termin	Zeit	Anmeldung
16.11.07	12:30 – 15:00 h	keine (NIG, HS 3)

Programmieren mit PHP – Teil 2

Termin	Zeit	Anmeldung
23.11.07	12:30 – 15:00 h	keine (NIG, HS 3)

MySQL-Datenbank mit phpMyAdmin verwalten – Teil 3

Termin	Zeit	Anmeldung
30.11.07	12:30 – 15:00 h	keine (NIG, HS 3)

Internet

HTM-Workshop – Erstellen von Webseiten

Termin	Zeit	Anmeldung
19.11.07	09:00 – 16:00 h	bis 12.11.07
12.12.07	09:00 – 16:00 h	bis 05.12.07

Webdesign – Konzeption und Gestaltung

Termin	Zeit	Anmeldung
15.11. – 16.11.07	09:00 – 16:00 h	bis 09.11.07

Dreamweaver – Einführung

Termin	Zeit	Anmeldung
07.11.07	09:00 – 16:00 h	bis 31.10.07

Flash – Einführung

Termin	Zeit	Anmeldung
12.11.07	09:00 – 16:00 h	bis 05.11.07

HTML 3 – Einführung in Cascading Style Sheets (CSS)

Termin	Zeit	Anmeldung
09.11.07	12:30 – 15:00 h	keine (NIG, HS 3)

ECDL-Prüfungstermine

Termin	Zeit	Anmeldung
30.10.2007	11:00 – 11:45 h	bis 30.10.07
06.11.2007	10:00 – 10:45 h	bis 06.11.07
06.11.2007	11:00 – 11:45 h	bis 06.11.07
16.11.2007	13:00 – 13:45 h	bis 16.11.07
21.11.2007	09:30 – 10:15 h	bis 21.11.07
21.11.2007	10:30 – 11:15 h	bis 21.11.07
29.11.2007	14:00 – 14:45 h	bis 29.11.07
29.11.2007	15:00 – 15:45 h	bis 29.11.07
04.12.2007	10:00 – 10:45 h	bis 04.12.07
04.12.2007	11:00 – 11:45 h	bis 04.12.07
17.12.2007	13:00 – 13:45 h	bis 17.12.07
17.12.2007	14:00 – 14:45 h	bis 17.12.07
08.01.2008	11:00 – 11:45 h	bis 08.01.08
08.01.2008	12:00 – 12:45 h	bis 08.01.08
16.01.2008	15:00 – 15:45 h	bis 16.01.08
18.01.2008	10:00 – 10:45 h	bis 18.01.08
18.01.2008	11:00 – 11:45 h	bis 18.01.08
22.01.2008	13:00 – 13:45 h	bis 22.01.08
22.01.2008	14:00 – 14:45 h	bis 22.01.08
24.01.2008	09:30 – 10:15 h	bis 24.01.08
24.01.2008	10:30 – 11:15 h	bis 24.01.08
30.01.2008	10:00 – 10:45 h	bis 30.01.08

Informationen zu den Kursinhalten und Lernzielen finden Sie auf Seite 38.

EDV-Kursinhalte & Lernziele

Basics

u:net & PC-Raum-Basics für Studierende
Nutzung und sicherer Umgang mit den IT-Services des ZID

Betriebssysteme

Windows – Einführung
grundlegende Funktionen; sicherer Umgang mit Desktopelementen sowie den Windows-Anwendungsprogrammen; Datei- und Ordnerverwaltung

Textverarbeitung

Word – Einführung
Texte selbständig erstellen, modifizieren, speichern und ausdrucken; effiziente Maus- und Tastaturbedienung; Zeichen- und Absatzformatierung sowie Seitengestaltung

Word – Fortsetzung
Verfassen von Serienbriefen; Gestalten umfangreicher Dokumente; Verknüpfung mit anderen Programmen

Word – Wissenschaftliches Arbeiten
Erstellen von Inhalts- und Abbildungsverzeichnissen; Arbeiten mit aktualisierbaren Referenzen sowie effizienter Umgang mit der Gliederungsansicht

Tabellenkalkulation

Excel – Einführung
grundlegende Funktionen; effiziente Maus- und Tastaturbedienung; Zellformatierung und Tabellengestaltung; einfache Berechnungen; grafische Darstellung

Excel – Fortsetzung
Erlernen umfangreicher und komplexer Aufgabenstellungen (verschachtelte Berechnungen, Einsatz komplexer Funktionen) sowie Fehlerbehandlungen

Datenbanken

Access – Einführung
Aufbau und Funktionalität relationaler Datenbank; Datenbanken erstellen und die nötigen Abfragen durchführen

Microsoft Access – Fortsetzung
Vertiefung der Erkenntnisse des Grundkurses

Diverse

PowerPoint – Einführung
Folien mit Grafiken, Texten und Darstellungen erstellen, ausdrucken bzw. als Bildschirmpräsentation vorzuführen

PowerPoint – Fortsetzung
professionelle Präsentationen und Vorträge vorbereiten, gestalten und durchführen; Veröffentlichung im WWW

Photoshop – Einführung
Fotos professionell retuschieren; diverse Ebeneneffekte, Ebenenstile und Filter versiert einsetzen; Fotos und Grafiken für Printmedien sowie für das Internet bearbeiten

Photoshop & ImageReady – Erstellen von Webgrafiken
Entwurf von Layouts und Menüs sowie Export dieser Grafiken in HTML-Seiten; Erstellen von Bild- und Grafikanimationen und Rollovers sowie der Umgang mit Imagemaps

SPSS – Einführung
schrittweise Einführung in die Arbeit mit SPSS anhand praktischer Übungen am PC; Erläuterung des statistischen Hintergrunds

SPSS – Fortsetzung
Vermittlung komplexer statistischer Verfahren (einfache und multiple Regression, Dummy-Variablen, einfaktorielle und mehrfaktorielle Varianzanalyse, Faktorenanalyse oder Clusteranalyse, Erstellen eines Indexes)

Internet

HTML-Workshop – Erstellen von Webseiten
Funktionen und Arbeitstechniken, die zum Aufbau und zur Pflege professioneller Webseiten benötigt werden

Webdesign – Konzeption und Gestaltung
Psychologie, Ergonomie, Technik und Design im Hinblick auf die Gestaltung professioneller Webseiten

Einführung in Cascading Style Sheets – Teil 3
Ergänzungssprache zu HTML; Schrift, Linkfarben, Rahmen oder andere Auszeichnungen mit Hilfe von CSS exakt und in einem Arbeitsgang formatieren

Dreamweaver – Einführung
Planung und Aufbau eines Webprojekts; einfache Möglichkeiten der Textgestaltung mit und ohne CSS sowie weiterführende Funktionen der Software

Flash – Einführung
Grundlagen der Handhabung; Einrichtung der Flash-Arbeitsumgebung; Umgang mit Zeichenwerkzeugen und Ebenen; Erstellen von Animationen und die Anwendung verschiedener Farbeffekte

Programmierung

Programmieren mit PHP – Teil 1
Grundlagen der Skriptsprache PHP (Konfiguration, Strukturelemente, Funktionen und Möglichkeiten zur externen Datenanbindung)

Programmieren mit PHP – Teil 2
weitere Einsatzmöglichkeiten der Skriptsprache PHP; PHP konfigurieren; Überblick über Strukturelemente, Funktionen und Möglichkeiten zur externen Datenanbindung

MySQL-Datenbank mit phpMyAdmin verwalten – Teil 3
Funktionen und Möglichkeiten von MySQL; Administration mittels phpMyAdmin; Datenbanken ins Netz stellen und individuell angepasste Lösungen programmieren

Einführung in das Programmieren mit JavaScript
Einbindung und Verwendung von JavaScript; JavaScript Sprachelemente; Document Object Model (DOM); Manipulation des Browserfensters (Grösse, Inhalt, ...); Reaktion auf Ereignisse (OnClick, OnSubmit etc.); Änderungen der Seite (Farbe, Grafiken, Links, ...)

HANDBÜCHER

Die unten angeführten Handbücher des *Regionalen Rechenzentrums Niedersachsen* (RRZN) können am **Helpdesk** des ZID (`www.univie.ac.at/ZID/helpdesk/`) gegen **Barzahlung** erworben werden. Neben den nachfolgend aufgelisteten Titeln sind auch einige Restexemplare zu älteren Programmversionen (`www.univie.ac.at/ZID/handbuecher/`) erhältlich. RRZN-Handbücher dürfen nur an **Studierende und MitarbeiterInnen der Uni Wien** verkauft werden! Eine Weitergabe an sonstige Privatpersonen, Schulen, Firmen usw. ist ausdrücklich untersagt. Solche InteressentInnen können wir nur auf die Literatur im Buchhandel verweisen, insbesondere auf die des Herdt-Verlags (`www.herdt.de`).

Access 2003 – Grundlagen für Datenbank-Entwickler ..... EUR 5,50
Access 2007 DB – Grundlagen für Datenbank-Entwickler ..... EUR 5,50
Access 2007 DF – Fortgeschrittene Techniken für Datenbank-Entwickler ..... EUR 5,00
Acrobat 5.0 – PDF-Dateien erstellen und publizieren ..... EUR 4,00
Dreamweaver MX 2004 – Grundlagen des technischen Web-Designs ..... EUR 6,00
Effektiver Umstieg auf Windows Vista und Office 2007 ..... EUR 5,50
Excel 2003 – Einführung ..... EUR 5,50
Excel 2003 – Fortgeschrittene Anwendungen ..... EUR 5,50
Excel 2007 – Grundlagen ..... EUR 5,50
Excel 2007 – Fortgeschrittene Anwendungen ..... EUR 5,00
Excel 2007 FF – Formeln und Funktionen clever nutzen ..... EUR 4,00
Flash – ActionScript-Programmierung ..... EUR 5,00
Flash MX 2004 – Grundlagen, Animation für Web-Seiten ..... EUR 6,00
Frontpage 2002 – Grundlagen ..... EUR 5,00
ImageReady 3.0 ..... EUR 5,50
Kleine Windows 2000/XP-Netzwerke – Planung, Aufbau und Support ..... EUR 5,00
Linux – Nutzung mit der grafischen Oberfläche KDE ..... EUR 5,50
Mathematica – Einführung in das Computeralgebrasystem ..... EUR 4,00
Netzwerke – Grundlagen ..... EUR 5,00
Photoshop CS – Einführung ..... EUR 5,50
Photoshop CS3 – Einführung ..... EUR 5,50
PHP, Grundlagen – Erstellung dynamischer Webseiten ..... EUR 5,00
PowerPoint 2003 – Grundlagen ..... EUR 5,50
PowerPoint 2007 – Grundlagen ..... EUR 5,50
PowerPoint 2007 – Fortgeschrittene Techniken ..... EUR 4,50
Publizieren im World Wide Web – Eine Einführung ..... EUR 5,00
SPSS 14 Grundlagen – Eine Einführung ..... EUR 4,00
SPSS für Fortgeschrittene – Durchführung fortg. statistischer Analysen ..... EUR 6,00
StarOffice und OpenOffice.org (inkl. CD) ..... EUR 4,50
Unix – Eine Einführung ..... EUR 4,00
VBA-Programmierung – Integrierte Lösungen mit Office XP ..... EUR 5,00
Windows Server 2003 AuV – Aufbau und Verwaltung eines Netzwerks ..... EUR 6,00
Windows Server 2003 N – Netzwerkadministration ..... EUR 6,00
Windows Vista – Grundlagen für Anwender ..... EUR 5,50
Windows Vista – Systembetreuer ..... EUR 5,50
Windows XP – Systembetreuer Workstation ..... EUR 5,00
Word 2007 – Grundlagen ..... EUR 5,50
Word 2007 – Fortgeschrittene Techniken ..... EUR 5,50

KONTAKTADRESSEN AM ZID

In grundsätzlichen Angelegenheiten wenden Sie sich bitte an den Direktor des Zentralen Informatikdienstes oder an die Abteilungsleiter. **Eine vollständige Personalliste finden Sie unter** `www.univie.ac.at/ZID/staff/`.

Helpdesk

Wenden Sie sich bitte an den Helpdesk des ZID

- als **erste Anlaufstelle** bei EDV-Problemen und technischen Schwierigkeiten sowie für die **Vermittlung zu AnsprechpartnerInnen** bei speziellen Problemen,
- bei **Störungen** im Datennetz und im Telefonsystem der Uni Wien oder an einem Rechnersystem des ZID,
- für Vergabe von **Benutzungsberechtigungen** (UserIDs) für die Rechnersysteme und das Backup-Service,
- für alle Anliegen hinsichtlich Benutzungsberechtigungen – insbesondere Änderung vergessener **Passwörter**,
- für Vermittlung von externen Technikern zur **Unterstützung bei Software-Problemen** (kostenpflichtig!),
- bei Problemen mit dem **Internetzugang von daheim** (*uniADSL, chello student connect, xDSL Uni*, Wählleitungszugänge der Uni Wien),
- für **Anmeldungen zu Kursen und ECDL-Prüfungen**,
- für Ausgabe/Entgegennahme der **Formulare** des ZID,
- für **Verkauf von Handbüchern und Netzwerkzubehör**.

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

bei technischen Fragen zum Thema eLearning:
(`www.univie.ac.at/ZID/elearning/`)
`elearning.zid@univie.ac.at`
Telefon: 4277-14290

bei Fragen zum Telefonsystem der Uni Wien:
`telefon.zid@univie.ac.at`
`handy.zid@univie.ac.at`

bei EDV-Problemen im Bereich der Uni-Verwaltung:
`uvpc.support.zid@univie.ac.at`

bei Fragen zu bzw. Problemen mit i3v:
`support.univis@univie.ac.at`

bei Fragen zur Fakultätsunterstützung:
`fu.zid@univie.ac.at`
Telefon: 4277-14140

bei Fragen zum Datennetz der Uni Wien:
`netzwerk.zid@univie.ac.at`
Telefon: 4277-14042

bei Security-Fragen:
`security.zid@univie.ac.at`

bei Fragen zum Linux-Cluster Schrödinger III:
`schroedinger@univie.ac.at`
Peter Marksteiner 4277-14055

bei Fragen zur Standardsoftware:
`software.zid@univie.ac.at`
Peter Wienerroither 4277-14138

für Öffentlichkeitsarbeit:
`redaktion.zid@univie.ac.at`
`webmaster.zid@univie.ac.at`

ÖFFNUNGSZEITEN

Achtung, eventuell geänderte Ferien-Öffnungszeiten!
Beachten Sie dazu bitte die aktuellen Hinweise unter `www.univie.ac.at/ZID/`.

Helpdesk des ZID
1010 Wien, Universitätsstr. 7 (NIG), Stg. II, 1. Stock
Mo – Fr 9:00 – 18:00

Support Neue Medien (eLearning)
1010 Wien, Universitätsstr. 7 (NIG), Stg. III, Erdgeschoss
Mo, Di, Mi, Fr 9:00 – 16:00
Do 11:00 – 18:00

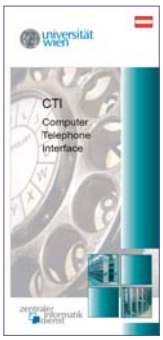
PC-Räume des ZID (NIG, AAKH, UZA)
Mo – Fr 7:30 – 21:30 / Sa 7:30 – 13:00
(NIG: samstags bis 18:00 Uhr geöffnet)

PC-Raum-Betreuung für diese Standorte:
Mo – Fr 9:00 – 20:00

Details: `www.univie.ac.at/ZID/pc-raeume/`

Print-Publikationen des ZID

Die Print-Publikationen sind – nach Verfügbarkeit – kostenlos am Zentralen Informatikdienst der Universität Wien (Neues Institutsgebäude / NIG, 1. Stock, 1010 Wien, Universitätsstraße 7) erhältlich. Alle Informationen finden Sie auch auf den Webseiten des ZID unter `www.univie.ac.at/ZID/`.



CTI – Computer Telephone Interface

Sprache: Deutsch
Folder für MitarbeiterInnen

PC-Räume des ZID

Sprache: Deutsch, Englisch
Folder für Uni-Angehörige

eLearning für Lehrende

Sprache: Deutsch
Folder für MitarbeiterInnen

u:net

Sprache: Deutsch, Englisch
Folder für Studierende

eLearning für Studierende

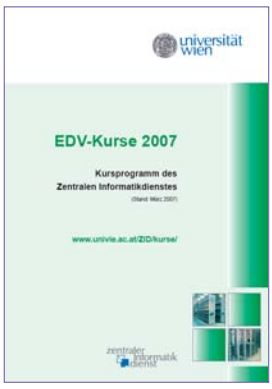
Sprache: Deutsch
Folder für Studierende

Zeitschrift *Comment*

Sprache: Deutsch
Zeitschrift für Uni-Angehörige

Mailbox

Sprache: Deutsch, Englisch
Folder für MitarbeiterInnen



EDV-Kurse

Sprache: Deutsch
Kursprogramm für MitarbeiterInnen, Studierende und Externe

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

COMMENT-WEBSITE

Unter dem Link **http://comment.univie.ac.at/** finden Sie die aktuelle Ausgabe des *Comment* komplett in elektronischer Form – sowohl im HTML- als auch im PDF-Format. Darüber hinaus stehen alle seit dem Jahr 1994 erschienenen *Comment*-Ausgaben im *Archiv* zur Verfügung und lassen sich in der *Comment*-Suche im Volltext durchsuchen. Zudem bietet die Website unter dem Menüpunkt *Abo* die Möglichkeit zur An- und Abmeldung bzw. Änderung eines Print- sowie eines e-Abos an. Um uns zu kontaktieren, schreiben Sie an: **comment.zid@univie.ac.at**