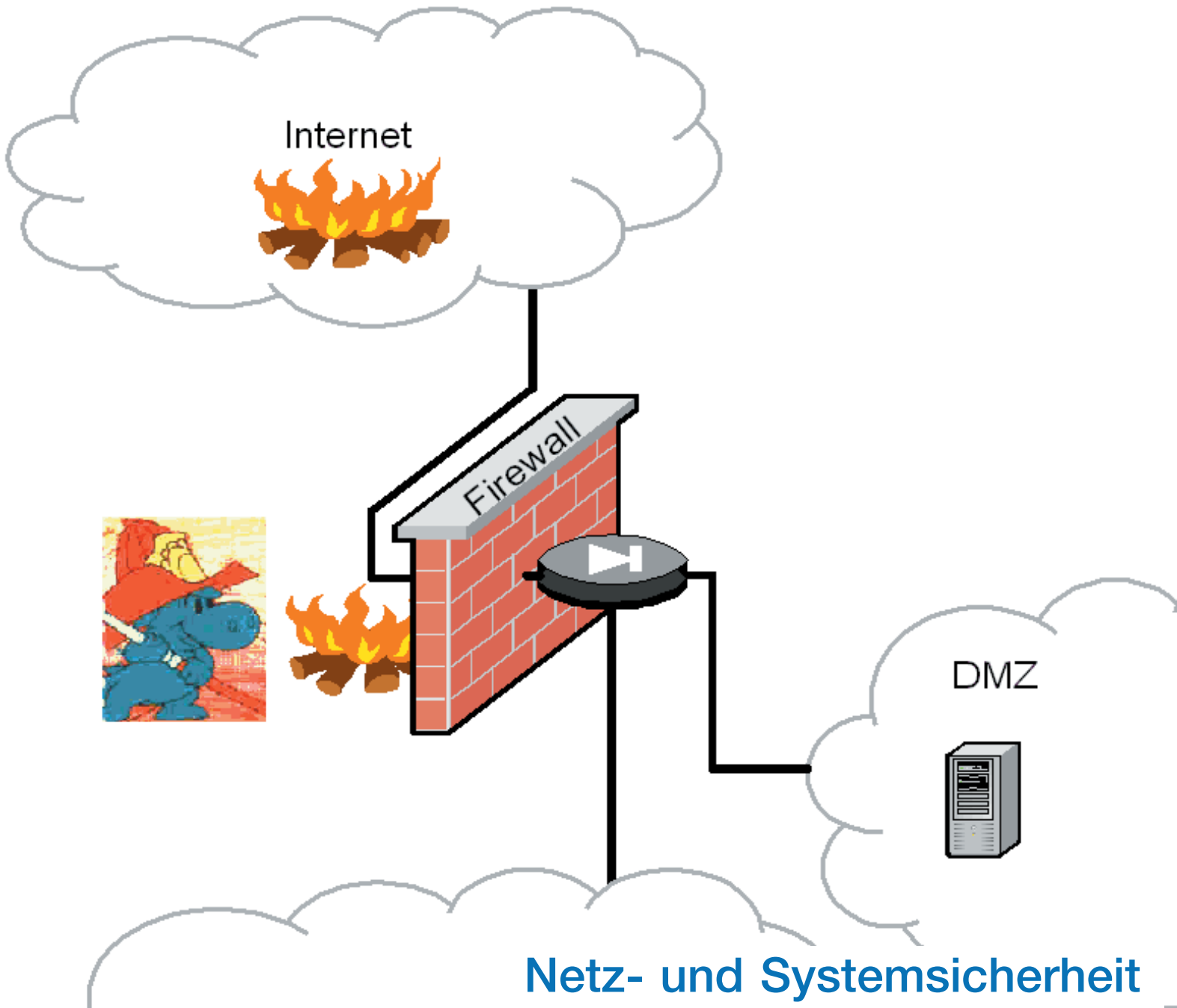


# ZiD-line

INFORMATIONEN DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN



Netz- und Systemsicherheit

Statusbericht Telekommunikationsanlage

Linux – eine Alternative ?

Entwicklung Internet-Service für Studierende

# Inhalt

Netz- und Systemsicherheit . . . . .	3
Firewall und Internet Security an der TU Wien . . . . .	6
Plattformunterstützung durch die Abteilung Standardsoftware . . . . .	9
Statusbericht Telekommunikationsanlage . . . . .	10
Verrechnung der Telefonentgelte . . . . .	14
Erfahrungen mit SGI Origin2000 . . . . .	17
Linux, eine Alternative ? . . . . .	19
Windows 2000 . . . . .	23
10 Jahre Wählleitungen . . . . .	28
Das Internetservice für Studierende der TU Wien . . . . .	35
Wie schnell sind schnelle Fourier-Transformationen ? . . . . .	43
Personelle Veränderungen . . . . .	48
Server-Zertifikate des Zentralen Informatikdienstes . . . . .	49
Wählleitungen / Auskünfte, Störungsmeldungen / Öffnungszeiten . . . . .	50
Personalverzeichnis, Telefonliste, E-Mail-Adressen . . . . .	51

## Impressum / Offenlegung gemäß § 25 Mediengesetz:

*Herausgeber, Medieninhaber:  
Zentraler Informatikdienst  
der Technischen Universität Wien*

*Grundlegende Richtung: Mitteilungen des Zentralen  
Informatikdienstes der Technischen Universität Wien*

*Redaktion: Irmgard Husinsky*

*Adresse: Technische Universität Wien,  
Wiedner Hauptstraße 8-10, A-1040 Wien  
Tel.: (01) 58801-42014, 42001  
Fax: (01) 58801-42099  
E-Mail: [zidline@zid.tuwien.ac.at](mailto:zidline@zid.tuwien.ac.at)  
WWW: <http://www.zid.tuwien.ac.at/zidline/>*

*Druck: HTU Wirtschaftsbetriebe GmbH,  
1040 Wien, Tel.: (01) 5863316*

# Editorial

Sie haben vielleicht die Zeitschrift PIPELINE schon seit längerer Zeit abonniert und die Zusendung einer neuen Ausgabe erwartet. Was Sie nun in Händen halten, ist die erste Ausgabe der **ZIDline**, der Nachfolgezeitschrift der PIPELINE, die nicht mehr fortgesetzt wird. Im Zuge des Inkrafttretens des neuen Universitätsorganisationsgesetzes an der Technischen Universität am 1. 1. 1999 wurde das EDV-Zentrum zum Zentralen Informatikdienst (kurz: ZID). Diese Gelegenheit haben wir ergriffen, unsere traditionsreiche Zeitschrift mit einem neuen Namen und modernisiertem Layout zu versehen.

Ein wesentlicher Punkt der Öffentlichkeitsarbeit des Zentralen Informatikdienstes ist die Präsentation im Web, wo Information zu allen Diensten des ZID sowie News angeboten und laufend aktualisiert werden. Das monatliche Mitteilungsblatt informiert die Institutsvorstände und Funktionäre der TU Wien über das jeweils Neueste in Kürze. Zur Dokumentation der Verwendung der zentralen Applikationsserver des ZID wird alljährlich eine Broschüre mit Berichten über die größten Anwenderprojekte erstellt. Zu aktuellen Themen werden Veranstaltungen organisiert.

Für aktuelle Meldungen, zum Nachschlagen von Informationen, Anleitungen etc. ist das Web das geeignete Medium. In unserer Zeitung, die zweimal jährlich erscheinen wird, wollen wir uns auf Analysen und Hintergrundberichte konzentrieren und Schwerpunkte behandeln. Selbstverständlich gibt es weiterhin auch eine Web-Version.

Wir bemühen uns ab sofort, die neue deutsche Rechtschreibung konsequent anzuwenden.

Kurz zum Inhalt dieser Ausgabe: Ein Schwerpunkt ist die zunehmende Bedeutung von Sicherheitsmechanismen in Rechnernetzen. Das Titelbild zeigt einen Ausschnitt aus der geplanten Lösung mit einem Firewall. Ausführliche Berichte dokumentieren die Entwicklung des Internet-Service für Studierende und des Wählleitungszugangs zur TU Wien. Ferner finden Sie aktuelle Informationen zum Status der Telekommunikationsanlage der TU Wien und der Plattformunterstützung der Abteilung Standardsoftware. Analysen gibt es zu den Themen Linux und Windows 2000.

Die Zusendung dieser *ZIDline* erfolgt an alle Abonnenten der PIPELINE, wobei wir versucht haben, auch den neuen Instituten und Abteilungen an der TU die entsprechenden Personen zuzuordnen. Bitte teilen Sie uns mit, falls Ihre Adresse nicht mehr richtig ist (per E-Mail: [zidline@zid.tuwien.ac.at](mailto:zidline@zid.tuwien.ac.at), per Telefon: 58801-42014 oder über die Web-Seite der *ZIDline*: <http://www.zid.tuwien.ac.at/zidline/>).

Ich würde mich auch über Rückmeldungen freuen, wie Ihnen die neue *ZIDline* gefällt.

*Irmgard Husinsky*

# Netz- und Systemsicherheit

Udo Linauer

Am Zentralen Informatikdienst der Technischen Universität Wien wurde mit Beginn des heurigen Jahres die Position eines Beauftragten für Netz- und Systemsicherheit geschaffen.

Die Beweggründe dafür waren vielfältig, zum Ersten finden wir bei uns durch die vorgegebenen Aufgaben einen besonders intensiven und weit ausgebauten Einsatz von EDV jeglicher Art vor. Dieser Größe zollten **Hacker** wie auch **E-Mail-Spammer** wiederholt Tribut. Die Hackerproblematik schafft tagesaktuell viele Aufgaben für den Sicherheitsbeauftragten: reaktive – das Aufspüren von Hackern und betroffenen Rechnern – wie auch aktive Beratung bei der Installation, **Security-Checks**, **Firewalls** und vieles mehr. Weitere Bedrohungen gehen von **Trojanischen Pferden** und **Viren** aus. Mindestens ebenso wichtig ist aber auch der Bedarf an **Sicherheitskonzepten** im größeren Rahmen, zeitlich wie auch organisatorisch. **Verschlüsselung**, **digitale Signaturen** und **Zertifikate** sind Gesprächsthema für eine breite Öffentlichkeit. Die Adaption für die Technische Universität Wien zählt zu den Agenden des Sicherheitsbeauftragten. Es bleiben zuletzt noch die Bereitstellung von redigierten Informationen und die Organisation von **Informationsveranstaltungen** als weitere interessante Betätigungsfelder zu erwähnen.

## Die Hackerproblematik (UNIX)

Wie bereits erwähnt, kommt es laufend zu Hackerattacken auf Rechner an der TU Wien. Die Attacken treten schubweise auf und konzentrieren sich zur Zeit vorwiegend auf Computer mit dem Betriebssystem Linux. Ein nicht geringer Teil führt zum Erfolg (seit Beginn des Jahres wurden mir ca. 30 Fälle bekannt). Neben dem Verlust der Kontrolle über den eigenen Computer ist das vielleicht größte Ärgernis, dass „gehackte“ Rechner als Basis für weitere Attacken benutzt werden, was zu vielen, teils wütenden E-Mails von Dritten führt. Es zeigte sich, dass auch professionelle Systemadministratoren durch diese neue Problematik vor große Probleme gestellt wurden, denen sie trotz ihrer hohen Fachkompetenz nicht immer gewachsen waren. Mitarbeiter, für die die Betreuung von Rechnern nur eine Nebenbeschäftigung darstellt, haben dementsprechend noch mehr Bedarf an Hilfe, wobei meistens, gleichgültig ob es sich um Vollzeit- oder Teilzeitadministratoren handelte, Problembe-

wusstsein vorhanden war, im gleichen Atemzug aber Zeitmangel als häufigstes Argument für Mängel benannt wurde. Der Aufwand, der getrieben werden muss, um zumindest bei den wichtigsten sicherheitsrelevanten Bereichen am Stand der Technik zu bleiben, ist tatsächlich enorm. Der schnelle Wechsel von Programmversionen und das fast noch schnellere Auffinden von Schwachstellen in neuen Versionen durch Hacker verlangen nach einer steten Beobachtung einschlägiger Informationsquellen. Hierbei kann man davon ausgehen, dass im Allgemeinen Neuigkeiten zuallererst in diversen Foren im Internet publiziert werden (Newsgroups: `news://comp.security.unix`, Web: `http://www.cert.org/` etc.). Man kann sich also nicht darauf verlassen, vom Hersteller oder Servicepartner rechtzeitig informiert zu werden. Bei Freeware und Public Domain ist solche Unterstützung zumeist gar nicht vorgesehen. Die Menge der angebotenen Informationen ist immens und verlangt sehr oft genaue Kenntnis der Betriebssysteme und Applikationen. Da ich natürlich nicht alle Betriebssysteme und Applikationen gleich gut beherrschen kann, sehe ich hier meine Aufgabe in der Vermittlung zwischen hilfesuchenden Mitarbeitern oder auch Studenten und den kompetenten Mitarbeitern am Zentralen Informatikdienst.

Welche Hilfe kann ich Ihnen darüber hinaus anbieten? Zwei wesentliche Merkmale machen einen „sicheren“ Rechner aus: einerseits eine saubere Installation, andererseits die kontinuierliche Wartung und Überprüfung des Systems. **Installation Guides** gibt es jede Menge, Verweise auf ausgewählt gute Informationen können Sie unter `http://www.zid.tuwien.ac.at/security/security.html` für Windows NT und Linux finden. Wartung ist notwendig, Patches müssen eingespielt werden, Zugriffsrechte müssen den Gegebenheiten angepasst werden. Als hilfreich beim Auffinden von Schwachstellen erwiesen sich Programme für **Security Checks**, **Portscans** und dergleichen (z.B. Satan). Um Ihnen bei der Wartung Ihrer Systeme behilflich zu sein, beschlosssen wir, solche Systeme zu evaluieren und ein geeignetes anzuschaffen. Der Evaluationsprozess ist noch nicht abgeschlossen, sehr bald aber werden wir Ihnen eine **kostenlose Sicherheitsüberprüfung** Ihrer Systeme und die dazugehörige Beratung als Service anbieten können.

## Die Hackerproblematik (MS Windows) und Viren

Während auf UNIX-Systemen Hacker primär durch mehr oder weniger brutale Attacken auf Schwächen in der Software (imapd, mountd, ftpd etc.) Zugriff erlangen, gelingt es ihnen bei MS Windows-PCs zumeist durch die Verbreitung manipulierter Software, sogenannter Trojanischer Pferde (z.B. „NetBus“, „Back Orifice“, siehe auch <http://www.symantec.com/avcenter/warn/backorifice.html>). Die Folgen sind dieselben, das Auffinden am besten mittels Port Scanner zu erreichen (s.o.).

Viren sind beinahe ausschließlich auf Rechnern mit Betriebssystemen von Microsoft zu finden. Im Widerspruch zu den häufigen Pressemeldungen über diverse Killerviren steht die geringe Anzahl solcher Meldungen aus dem Bereich der TU Wien, zumindest mir gegenüber. Da ich nicht glaube, dass wir gegen Viren immun sind, empfehle ich, Antivirensoftware in Kombination mit einem den Umständen angepassten **Backupkonzept** flächendeckend einzusetzen. Die Kosten dafür sind gering. (Software z. B. unter <http://swd.tuwien.ac.at/css/angebot.html>). Man unterscheidet zwischen **Scanner** und **Shields**. Virens Scanner durchsuchen neueinzuspielende Software (E-Mail, Web, Disketten) nach bekannten Viren. Klarerweise muss die Datenbank der bekannten Viren immer auf aktuellem Stand gehalten werden. Die Erkennungsrate ist hoch, der Aufwand für das Update der Virendatenbank nicht gering. Um dem Administrator zu entlasten, kommen vermehrt Update-Automatismen zum Einsatz. Virenschilder (Shields) versuchen, typische Symptome von Virenbefall zu erkennen. Es wird also nicht nach fixen Mustern gesucht sondern vielmehr nach allgemeinen, wie etwa die Veränderung der Größe von Dateien. Der Vorteil dieser Methode besteht darin, dass prinzipiell auch brandneue, unbekannte Viren erkannt werden können, zu ihren Schwächen zählt, dass es durchaus auch zu Fehlalarmen kommen kann.

## Firewalls

Aus dem Blickwinkel des Sicherheitsbeauftragten ist die Sicherung eines weitgehend dezentral organisierten Netzes (dazu zähle ich die freie Wahl der Hardware, der Betriebssysteme etc. auf Institutsebene), das möglichst viele Freiheiten gestattet (Betrieb eines Mail-Servers, Proxys u.ä.), eine diffizile Aufgabe. Trotz dieser Vorgaben muss die Anzahl der sicherheitsrelevanten Vorfälle gesenkt werden. Um dies zu erreichen, müssen wir, wie bereits beschrieben, die Qualität der installierten Systeme verbessern. Hilfreich bei der Erhöhung der Systemsicherheit ist der Einsatz von **Firewalls** und ähnlichen Werkzeugen (z. B.: **Packet Filter**). Institutsfirewalls sind bereits auf Eigeninitiative im Einsatz und leisten gute Dienste. Meiner Meinung nach ist das Institut auch die geeignete Organisationseinheit für den Einsatz eines Firewalls. Universitätsweit können nur einige wenige Protokolle oder Services durch einen Firewall gesperrt werden, vor allem das Abblocken von **Denial of Service Attacks** für den ganzen Campus ist auf dieser Ebene sinnvoll. Auf Institutsebene kann viel restriktiver festgelegt wer-

den, was gebraucht wird und was nicht. Ein derartiges Konzept kann aber nur vom Institut selbst implementiert und in Folge gewartet werden. Der Betreiber des TUNET stellt die geeignete Netzstruktur zur Verfügung, der Sicherheitsbeauftragte kann beratend tätig sein.

## Verschlüsselung, digitale Signaturen und Zertifikate

Bei vielen beobachteten Hackerattacken wurden **Password-Sniffer** installiert. Auf diese Weise konnten die Hacker auch Zugang zu an sich „sicheren“ Rechnern erlangen. Unverschlüsselte E-Mails können bei der Übertragung wie auch am Mail-Server auf einfache Weise von Unberechtigten gelesen werden. Es scheint uns daher angebracht, daran zu arbeiten, den Mitarbeitern und Studenten optimale Bedingungen für den Einsatz von Verschlüsselungstechnologien für die sichere Datenkommunikation zu bieten. Da eine abschließende Beurteilung über die Art des Einsatzes von solchen Technologien auf der Technischen Universität Wien noch nicht zur Verfügung steht, möchte ich zur Einstimmung mit einer kleinen Einführung zu gebräuchlichen Kryptoverfahren fortfahren. Ich werde dabei an dieser Stelle nicht im Detail auf spezielle Programme oder Protokolle eingehen (Übersicht Tabelle 1) sondern versuchen, wichtige Begriffe und Problematiken allgemein zu behandeln.

	Login, Filetransfer	Mail	Web	Ecash
Application layer	SSH, Kerberos	PGP, S/MIME, PEM	HTTPS, SHTTP	SET
Transport layer	SSL, TLS			
Internet layer	IPsec, SKIP			
Network layer	Krypto-Boxes, Hardware-Encryption			

Tab.1: vereinfachtes OSI-Schichtenmodell

Verschlüsselung kann auf unterschiedlichen logischen Ebenen des Datenverkehrs zum Einsatz kommen. Vielen der gebräuchlichen Technologien gemeinsam ist die Verwendung von asymmetrischen Verschlüsselungsverfahren.

### Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren basieren auf einem mathematisch zusammenhängenden Schlüssel-paar, wobei der eine Schlüssel zum Verschlüsseln, der andere zum Entschlüsseln verwendet wird. Bei ausreichender Schlüssellänge kann man keinen der beiden Schlüssel aus dem jeweils anderen rechnerisch ermitteln. Beide Schlüssel eignen sich sowohl zum Ver- als auch zum Entschlüsseln, allerdings kann ein mittels eines der beiden Schlüssel erzeugtes **Kryptogramm** (verschlüsselter Text) nur mit dem jeweils anderen wieder entschlüsselt werden. Einer der beiden Schlüssel wird als Chiffrierschlüssel öffentlich bekanntgegeben und als **Public Key (PK)** bezeichnet. Der andere, der zum Entschlüsseln dient, wird von seinem Besitzer geheimgehalten und deshalb auch **Secret Key (SK)** genannt.

Möchte ein Sender S einem Empfänger R eine geheime Nachricht schicken, muss er sich zunächst den Public Key des Empfängers ( $PK_R$ ) verschaffen. Dies kann über E-Mail oder einen **Key Server** geschehen. Der Sender verschlüsselt seine Nachricht mit diesem  $PK_R$  und schickt das Kryptogramm an R. Da nur R den passenden Secret Key  $SK_R$  besitzt, kann auch nur er mit diesem die Nachricht wieder entschlüsseln. Die Übermittlung des Public Keys ( $PK_R$ ) beim Erstkontakt ist unkritisch, da dieser nicht zum Entschlüsseln verwendet werden kann. Dies ist der große Vorteil gegenüber symmetrischen Verfahren, bei denen die Übermittlung des Schlüssels vertraulich sein muss. Es existiert nämlich nur ein Schlüssel, der sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet wird. Fällt allerdings  $SK_R$  in falsche Hände, gilt das Schlüsselpaar als kompromittiert und kann nicht mehr verwendet werden. Ein großer Nachteil gegenüber symmetrischen Verfahren besteht im hohen Rechenaufwand und der damit verbundenen niedrigen Performance. Es werden daher oft kombinierte Verfahren verwendet, bei denen ein einmaliger, mit dem asymmetrischen Schlüssel verschlüsselter, symmetrischer **Session Key** zwischen den beiden Kommunikationspartnern ausgetauscht wird, der in Folge zur Verschlüsselung der Kommunikation dient (z.B. SSL).

symmetrisch	asymmetrisch
DES, TripleDES, IDEA, CAST, Blowfish	RSA, DH/DSS (Diffie Hellmann)
Typische Schlüssellänge: 40, 56, 128, 168	Typische Schlüssellänge: 512, 768, 1024, 2048, 4096

Tab.2: Verschlüsselungsverfahren

Die Schlüssellänge erlaubt keinen direkten Schluss auf die Schlüsselstärke, so ist laut Phil Zimmermann, dem Schöpfer von **PGP**, ein RSA-Schlüssel der Länge 3000 in etwa gleich schwer zu brechen wie ein TripleDES-Schlüssel mit der Länge 168. Bei kombinierten Verfahren ist dieses Faktum zu beachten, da eine falsche Wahl der Schlüssellängen die Sicherheit nicht erhöht, sehr wohl aber die Verschlüsselungsdauer.

## Digitale Signaturen

Einige Public Key-Verfahren eignen sich auch zum Erzeugen sogenannter digitaler Signaturen. Eine digitale Signatur wird an die Nachricht oder Datei angehängt und gewährleistet einerseits deren Unverändertheit (**Integrität**), andererseits die **Identität** des Senders. Damit ist sie der echten Unterschrift insofern überlegen, als diese nicht in solch hohem Grad garantiert, dass der unterzeichnete Text nachträglich nicht mehr manipuliert werden kann. Wie funktioniert die digitale Signatur?

Von der Nachricht wird mittels einer Einweg-Hashfunktion eine Prüfsumme (**Fingerprint**) gebildet. Zu diesen Hash-Funktionen zählen MD5, SHA1 und RIPEMD160. Die Art der Hashfunktion garantiert, dass eine geringfügige Änderung der Nachricht (z.B. Datum) eine markante Änderung des Fingerprints zur Folge hat. Es ist also fast unmöglich, die Nachricht sinnvoll zu verändern, ohne den Fingerprint zu verändern. Der Fingerprint kann als sicheres Siegel für die Unverfälschtheit der Nachricht M angenommen werden. Im nächsten Schritt

wird der Fingerprint mit dem Secret Key  $SK_S$  des Senders S verschlüsselt. Dies stellt sicher, dass M auch wirklich von S signiert wurde. Der Empfänger kann die Signatur nur mit dem passenden Public Key  $PK_S$  des Senders S wieder entschlüsseln. Da aber nur S  $SK_S$  besitzt, ist sichergestellt, dass M auch nur von S signiert worden sein kann.

## Probleme der Public Key-Verfahren

### → Zertifizierung

Noch vor dem bereits erwähnten hohen Rechenaufwand, ist das Hauptproblem die Sicherstellung der Identitäten von R und S. Die meisten Programme erlauben eine lokale Schlüsselgenerierung (z. B.: PGP, OpenSSL (siehe <http://www.openssl.org/>)), wobei die Identifizierung meist über Namen der Person bzw. des Servers und E-Mail-Adresse erfolgt. Es ist also leicht, sich für eine andere Person auszugeben, indem man bei der Schlüsselgenerierung einen fremden Namen verwendet. Analog kann ein fremder Hostname verwendet werden. Ist ein solchermaßen gefälschter Schlüssel einmal akzeptiert, greift die Sicherheit durch den einmaligen Secure Key SK nicht mehr. Es sollten daher zur Gewährleistung der **Authentizität** immer zwei von einander unabhängige Informationskanäle verwendet werden (E-Mail und Telefon, Home Page und FAX etc.). Da der Aufwand dazu mit der Anzahl der Schlüssel zunehmend steigt, wurden zwei unterschiedliche Ansätze zur Lösung dieser Problematik entwickelt.

Der Eine wird **Web of Trust** genannt. Es werden dabei nur Schlüssel persönlich bekannter Personen akzeptiert, bzw. Schlüssel, die von solchen Bekannten akzeptiert werden. Auch dieser Vorgang nennt sich Signieren, da man tatsächlich den fremden Public Key mit seinem eigenen Secret Key unterschreibt. Die bestätigende Unterschrift wird als **Zertifikat** bezeichnet. Dieses dezentrale Netzwerk lebt von der Ehrlichkeit seiner Mitglieder und hat sich beim Einsatz von PGP als gut funktionierend erwiesen.

Beim zweiten Ansatz übernimmt eine zentrale Zertifizierungsstelle – **Certificate Authority (CA)** – die Zertifizierung. Eine (oder mehrere) Registrierungsstellen – **Registration Authority (RA)** – überprüfen die Identität der Teilnehmer und leiten deren Schlüssel an die Certificate Authority zur Zertifizierung weiter, sofern keine Verstöße gegen die **Policy** vorliegen. In dieser Policy werden Rechte und Pflichten von Certificate Authority und Kunden definiert, wie z. B: Bestimmungen zur Qualität der Schlüssel, Sicherheitsvorkehrungen der CA, sowie der Betrieb eines **Key Servers** zur Publikation neuer und Rückruf nicht mehr gültiger Schlüssel.

Certificate Authority und Registration Authority können gegebenenfalls in derselben Institution realisiert werden. Vorteil dieser Methode ist die bessere Überprüfung der Schlüssel, deren Güte auch durch die Definition in der Policy festgelegt und nachlesbar ist, sowie der Umstand, dass man sich nur mehr über die Vertrauenswürdigkeit einer Stelle, nämlich der CA, informieren muss. Da im Rahmen der Kommerzialisierung der Kryptotechniken (**E-Commerce, E-Government**) in nächster Zeit auch bei uns gesetzliche Regelungen zu erwarten sind, kann von einer gewissen Qualität dieser Services ausge-

gangen werden. Der organisatorische Aufwand der Schlüsselverwaltung wandert vom Benutzer zur Zertifizierungsstelle, die in der Regel dafür ein Entgelt verlangen wird. Relativ neu, und durch das strenge deutsche Signaturgesetz (1997) gefördert, ist der technisch an sich vernünftige Einsatz von Chipkarten zur sicheren Speicherung des Secret Keys. Kolportierte Preise von öS 800.-/Jahr für ein Zertifikat auf der Chipkarte exklusive der Kosten für die Chipkartenleser lassen jedoch erwarten, dass der Einsatz vorerst auf gewisse sensitive Bereiche beschränkt bleibt (E-Government). Ein geplanter Einsatzbereich ist der Einsatz von Zertifikaten als Ersatz für die TAN-Briefe im **E-Banking**. Es sollte an dieser Stelle wiederholt werden, dass das Service der Zertifizierungsstelle primär die Überprüfung der Identität einer Person und der eindeuti-

gen Zugehörigkeit eines Schlüssels zu dieser Person ist. Die Korrektheit dieser Angaben bestätigt sie durch ein Zertifikat. Zertifizierung per E-Mail-Anfragen, wie sie in jüngster Zeit immer häufiger angeboten wird, ist daher ein Humbug und gefährdet den Erfolg dieser an sich großartigen Technologie.

## Quellen und Adressen

Security Home Page am ZID:

<http://www.zid.tuwien.ac.at/security/>

E-Mail: [udo.linauer@tuwien.ac.at](mailto:udo.linauer@tuwien.ac.at)  
[security@tuwien.ac.at](mailto:security@tuwien.ac.at)

# Firewall und Internet Security an der TU Wien

Elisabeth Donnaberger, Johann Kainrath

Um die Integrität eines Netzwerkes zu sichern, muss in die Netzwerkinfrastruktur – neben der implizit vorhandenen – zusätzlich Sicherheit etwa in der Form eines Firewalls implementiert werden. Dies kann durch eine eigene dedizierte Hardware oder den Einsatz einer Firewall-Software auf einer Plattform wie Gateway-Maschinen (Router, Rechner mit mehreren Interfaces) geschehen.

Firewalls bieten Sicherheit beim Management und bei der Kontrolle aller Verbindungen zwischen verschiedenen Netzwerkbereichen bzw. Netzwerksegmenten. Typischerweise verfügt ein Firewall über mehrere Interfaces (gleich einem Router), wobei man die innere durch den Firewall abgesicherte Zone das Inside Network (oder auch „Protected Network“) nennt. Im Falle der TU Wien ist dies das TUNET. Die Seite gegenüber, also außerhalb des Firewalls, stellt das Outside Network (oder auch „Unprotected Network“) dar, an der TU Wien im Konkreten der Internet-Anschluss zum AConet bzw. IBM Global Network. Neben diesen Netzwerkbereichen kann ein Firewall auch weitere mehr oder weniger geschützte Segmente (sprich Interfaces) haben, diese nennt man Perimeter Netzwerkbereiche. Hauptaufgaben eines Firewalls sind die Erkennung und der Schutz vor Angriffen auf Netzwerk- bis hin zur Applikationsebene (Abwehr von Denial of Service Attacks, Verhinderung von Mail-Spams und Port Scans). Methoden zur Kontrolle des Datenflusses reichen von einfachen Access-Listen auf Routern („stateless“ Packet Filtering, jedes einzelne Datenpaket muss für sich bestimmte Kriterien erfüllen) bis hin zu sogenannten „Stateful Packet“ Filtering Methoden (kein Paket kann den Firewall passieren, welches

nicht einer Verbindung zuordenbar ist bzw. einen definierten Status hat). Alle Versuche, den Firewall unerlaubt zu durchdringen, werden mit entsprechenden Logging-Mechanismen aufgezeichnet.

Content Filtering und Network Address Translation sind nur einige weitere Möglichkeiten zur Steigerung der Sicherheit im internen Netzwerk-Bereich.

Wie im gesamten Internet traten auch an der TU Wien in der Vergangenheit Vorfälle im Netzwerk auf, die dem Thema Sicherheit in Rechnernetzwerken angehören. Zu den häufigsten Attacks neben echten Einbrüchen in Rechner gehören sogenannte Denial of Service Attacks und Mail-Spamming. Schon alleine um einige dieser gezielten Attacks auf die Verfügbarkeit von Netzwerkdiensten abwehren zu können, muss aus der Sicht des Netzwerkbetreibers mit proaktivem Management auf potentielle Angriffe reagiert werden. State-of-the-Art in heutigen Netzwerken ist der Einsatz von Firewalls.

Die konkrete Implementierung eines Firewalls in ein so komplexes Netz wie das der TU Wien muss jedoch im Vorfeld genau durchdacht sein. So ist eine sogenannte Security Policy für die gesamte TU Wien von der Tech-

nischen Universität selbst zu diskutieren und zu installieren, ohne deren Vorhandensein der sinnvolle Einsatz eines Firewalls in Frage gestellt ist. Dies ist auch die vorherrschende Meinung bei praktisch allen Internet Service-Providern. Eine besondere Komplexität ergibt sich dadurch, dass die TU Wien über eine redundante Internet-Anbindung an zwei Serviceprovider (ACOnet, IBM Global Network) verfügt.

Ein Firewall darf auf keinen Fall die im Netz implementierte Redundanz und somit Service-Qualität für seine Benutzer zunichte machen, und natürlich auch nicht die Performance des Netzes schmälern sondern er sollte ja die von Instituten und Organisationen der TU Wien über das Netz zur Verfügung gestellten Services (Mail, News, WWW und FTP Services, kritische allgemeine Services wie Nameservice und Timeservice) in höchstmöglichem Maße schützen.

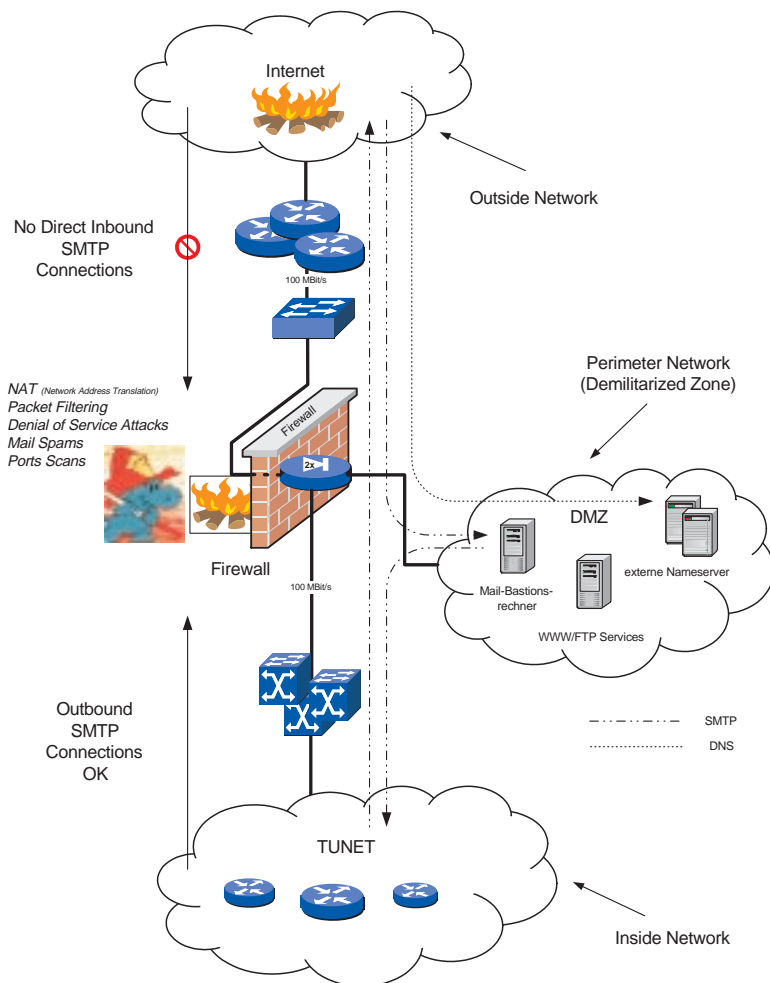
Um diesen Schutz bieten zu können und nicht-authorized Verbindungen zwischen Netzwerkbereichen zu verhindern, muss sämtlicher Verkehr durch den Firewall laufen. Nur dadurch ist eine Kontrolle sicherzustellen. Da bei solch einer richtigen Firewall-Implementierung kein direkter Verkehr von außen nach innen möglich ist, muss eine Zone existieren, wo interne und externe Systeme miteinander kommunizieren können. Dieser neutrale Meeting Point wird durch die sogenannte DMZ

(Demilitarized Zone) realisiert. Typischerweise sind in diesem Perimeter Netzwerkbereich WWW, FTP und Mail-Server für die Outside Internet Services angesiedelt. Man spricht dabei in speziellen Fällen auch von Bastionsrechnern. Hier sind auch die Nameserver für die von außen kommenden (quasi öffentlichen) Anfragen platziert. Dieses sogenannte Perimeter Network kann mit unterschiedlichem Sicherheitslevel konfiguriert werden. Dies ist mit höchster Sicherheitsstufe gleich dem Inside Network bis hin zur geringsten des Outside Network möglich.

Der Verkehrsfluss durch den Firewall teilt sich im Wesentlichen in zwei Arten von Verbindungen (Connections). Bei Outbound Connections sitzt der Client (Initiator einer Verbindung) quasi auf einem Interface mit einer höheren Sicherheitsstufe als der Server (Empfänger). Das Interface mit der höchsten Sicherheitsstufe ist immer das Interface zum Inside Network, das mit der niedrigsten zum Outside Network. Die Demilitarized Zone im Perimeter Netzwerkbereich kann je nach Erfordernissen zwischen diesen Sicherheitsstufen variieren. Inbound Connections (Verbindungen von außen nach innen, i.e. Verbindungen, wo der Initiator in einem Netzwerk mit geringerer Sicherheit sitzt als der Empfänger) sind bis auf explizit erlaubte (sogenannte Conduits) verboten. Im Szenario der TU Wien, wie in der gezeigten Abbildung dargestellt,

handelt es sich beim Outside Network um das Internet (ACOnet, IBM Global Network), das Inside Network umfasst das TUNET. In der DMZ sind vorerst der Mail-Bastionsrechner sowie ein externes Nameserver-Paar (tunamec, tunamed) angesiedelt. Ein weiterer Vorteil dieser DNS Realisierung ist, dass die internen Nameserver von außen nicht mehr direkt erreichbar sind und daher nicht direkt Hackerattacken ausgeliefert sind. Ein weiterer Baustein zur Steigerung der Netzwerksicherheit ist NAT (Network Address Translation). Ursprünglich wurde NAT entwickelt, um der immer größer werdenden Knappheit an IP-Adressen im Internet entgegenzuwirken, damit können interne IP-Adressen in weltweit im Internet gültige Adressen umgewandelt werden. Durch den Einsatz von NAT in Verbindung mit externen Nameservern in der DMZ kann die interne Netzwerktopologie und die IP-Domain versteckt werden und dem Internet gegenüber somit eine komplett andere Sichtweise des Netzes präsentiert (vorgespiegelt) werden. Damit sind Hackerattacken durch Nichtkenntnis der exakten Netzwerkinfrastruktur zusätzliche Barrieren in den Weg gestellt.

Firewall und Internet Security



All diese Maßnahmen sollen neben dem Schutz vor Angriffen aus dem Internet zur Sicherstellung eines reibungslosen Betriebes und stabiler Verfügbarkeit des TUNET und seiner Services beitragen. Das TUNET in seiner wichtigen und längst unabdingbaren Eigenschaft als Produktionsnetz für die Daten- und Telekommunikation der TU Wien muss in Zukunft verstärkt gesichert werden.

## Der Mail-Bastionsrechner

Das sogenannte Mail-Spamming, d. h. das Versenden unerwünschter Mails an eine große Anzahl von Personen, wird seit einiger Zeit immer mehr zu einer starken Belästigung für die Betroffenen und führt zu Überlastungen und Mails-Staus auf Mail-Servern. User und Betreiber mancher Mail-Server sperren ihre Mail-Zugänge gegenüber unerwünschten Sendern, manchmal gleich gegen ganze Domains. Spammer, denen bereits auf vielen Rechnern der Zugang gesperrt wurde, umgehen diese Restriktionen, indem sie ihre Mails über andere Mail-Server „routen“ (Third Party Mail-Relaying. Man spricht von Relaying, wenn Mails von außerhalb der TU Wien über einen Rechner der TU Wien an einen anderen Rechner außerhalb weitergeleitet werden.).

Für die betroffenen Rechner ist SPAM-Relay ist eine extreme Bedrohung der Funktionsfähigkeit, des Ressourcenbedarfs und der Verfügbarkeit. Es kann zu Absturz, Plattenüberlauf und Inoperabilität des Rechners für Mail führen.

Da viele große Provider SPAM-Relaying automatisch erkennen, werden dort auch oft automatisch Aktionen gesetzt. Diese beinhalten z. B., dass keine Mails von den betroffenen Rechnern mehr akzeptiert werden und dass die Rechner an diverse Anti-SPAM Listen gemeldet werden. Solche Listen werden von etlichen Mail-Server-Betreibern (auch einigen Instituten der TU Wien) automatisch verwendet, um ihre Liste der Rechner, von denen sie keine Mails mehr akzeptieren, zu erweitern. Das kann so weit gehen, dass die Rechner an deren Firewall komplett gesperrt werden. Es ist sehr schwer, von solchen Listen in absehbarer Zeit wieder herunterzukommen.

SPAM-Relay ist aber auch eine Bedrohung einer gesamten Organisation wie der TU Wien, da ihre Ressourcen in erheblichem Ausmaß zu illegalen, kommerziellen oder belästigenden Aktionen missbraucht werden. Das Ansehen der TU Wien national und international leidet darunter, weil von ihr solche Mails kommen bzw. weil sie Mail Relaying überhaupt zulässt. Es besteht die Gefahr, dass die gesamte TU Wien auf eine Anti-SPAM Liste gerät.

Es ist daher äußerst wichtig, dass alle Mail-Server am TUNET entsprechend konfiguriert sind, sodass sie nicht als Mail-Relay missbraucht werden können. Weitere ausführliche Informationen über dieses Thema finden Sie in

der PIPELINE Nr. 24 im Artikel „Missbrauch von Mail-Servern an der TU Wien“ von Martin Rathmayer.

Es zeigte sich jedoch, dass an manchen Institutsrechnern das Relaying nicht unterbunden wurde. Unter anderem aus diesem Grund wurde ein neues generelles Konzept für Mail-Routing und Mail-Bearbeitung an der TU Wien erstellt. Dabei wurde eine Lösung erarbeitet, die einen zentralen Mail-Bastionsrechner für die ganze TU Wien vorsieht, mit dessen Hilfe das gesamte TUNET von unerwünschtem Relaying u.ä. abgeschirmt werden kann. Die geplante Lösung hat folgende Struktur:

Eingehende Mails werden über einen sogenannten Mail-Bastionsrechner geleitet, der dazu dienen soll, für den gesamten Mail-Verkehr vom Internet zum TUNET die Relay-Möglichkeit zu unterbinden. Um ihn sowie alle Rechner der TU Wien entsprechend zu schützen, wird ein Firewall-System eingesetzt. Der Bastionsrechner wird in der sogenannten DMZ (de-militarized Zone) aufgestellt, also hinter dem Firewall.

Es wurde für dieses Konzept bereits eine Testkonfiguration aufgebaut und ausführliche Performance Tests wurden durchgeführt. Als Bastionsrechner ist eine Sun Ultra 2/2170 mit 640 MB Memory vorgesehen. Derzeit läuft das System im Testbetrieb, ab Sommer sollen dann die von außen zur TU eingehenden Mails standardmäßig über den Bastionsrechner geleitet werden. In akuten Fällen können auch einzelne Rechner schon früher eingegliedert werden, z. B. wenn ein Mail-Server eines Instituts als SPAM-Relay missbraucht wird und es nicht möglich ist, Relaying über diesen Rechner zu unterbinden.

Neben dem leichteren Umgang mit den derzeit vorliegenden Problemen hat dieses System auch den Vorteil, dass bei zukünftigen neuen Anforderungen nur an wenigen Stellen reagiert werden muss.

### Auswirkungen auf die Benutzer

Außer der gewünschten Unterbindung des Mail-Relays und zusätzlichen Einträgen in den Mail-Headers wird die einzige zu erwartende Auswirkung eine Beschränkung der maximalen Größe von Mails am Bastionsrechner sein.

### Backupmechanismen bei Ausfall des Bastions-Rechners

Da Mail im Internet nach dem „Store and Forward“ Prinzip funktioniert, ist ein kurzer Ausfall des Bastionsrechners nicht weiter tragisch, da die Mails beim letzten Übergaberechner liegen bleiben. Es ist auch ein Backup-Mechanismus in Form der direkten Umgehung des Bastionsrechners möglich, dazu muss bei Ausfall des Bastionsrechners nur die Port-Sperre am Firewall aufgehoben werden. Für diesen kurzen Zeitraum ist dann allerdings der Relay-Schutz aufgehoben.

Bei Fragen betreffend den Mail-Bastionsrechner wenden Sie sich bitte an Elisabeth Donnaberger von der Abteilung Kommunikation.



# Plattformunterstützung durch die Abteilung Standardsoftware

Albert Blauensteiner, Wolfgang Kleinert

Die Abteilung Standardsoftware des Zentralen Informatikdienstes (vormals Abteilung Institutsunterstützung) plant, neben den Bereichen zur Unterstützung der Applikations- und Systemsoftware, den Instituten und Abteilungen an der TU Wien auch in Zukunft eine zeitgemäße Plattformunterstützung anzubieten. Diese Unterstützung soll in ihrer Form und in ihren Inhalten notwendige und nützliche Anpassungen erfahren, um so den Bedürfnissen von etwa 6000 Computersystemen an der TU Wien gerecht zu werden.

Die Abteilung Standardsoftware plant, mit den Betreibern der einzelnen Rechnersysteme eine Art Servicevertrag für das Betriebssystem und die Basis-Software abzuschließen, um einerseits einen quantitativen Überblick über die Anzahl der Kunden zu erhalten und andererseits ein etabliertes Verhältnis zu den Kunden zu gewährleisten, das möglichst bereits mit der Planung und der Analyse von Computersystemen in der Anschaffungsphase beginnen sollte.

Zur Abwicklung der Anfragen ist die Implementierung eines *Call Center Mechanismus* geplant, mit dem alle Anfragen zielgerichtet und optimal innerhalb der Abteilung und deren Partnerfirmen abgewickelt werden können und einer raschen und effizienten Lösung zugeführt werden.

Neben den bisher traditionell unterstützten Plattformen AIX, HP-UX, IRIX, Tru64 UNIX (vormals Digital UNIX) und Solaris werden in Hinkunft auch die Plattformen Linux und Windows NT in gleicher Weise bei Installationen und Problemen unterstützt werden. Ebenso wird man sich wie bisher für die Plattformen OpenVMS und MacOS an die Mitarbeiter der Abteilung Standardsoftware wenden können. Derzeit untersuchen wir auch

die Möglichkeit, die Plattform Windows 95/98 über den *Call Center Mechanismus* gezielt zu unterstützen. Die Unterstützungsleistungen werden wie bisher zum Teil telefonisch, über E-Mail und Remote Login, aber auch bei Bedarf durch direkte Hilfestellung am Institut erfolgen.

Zur Aufrechterhaltung und zum Weiterausbau der unterstützenden Services im Plattformbereich muss vermehrt die Hilfe von externen Firmen und Spezialisten herangezogen werden. Dies nicht zuletzt deshalb, weil sowohl die Anzahl der mit entsprechendem Know-How ausgestatteten, für diese Aufgaben einsetzbaren Mitarbeiter geringer geworden ist, als auch die Zahl der Anforderungen und die Problemstellungen immer umfangreicher werden.

Wir hoffen, die Institute und Mitarbeiter der TU Wien mit diesen neuen Initiativen im Plattformbereich sowie mit der Campussoftware angemessen unterstützen zu können und werden über die geplanten Verbesserungen ausführlich informieren. Weitere Informationen sind über unseren Web Space (<http://sts.tuwien.ac.at/>) sowie bei den zuständigen Mitarbeitern und bei der Service Hotline 42004 erhältlich.

# Statusbericht

# Telekommunikationsanlage

Friedrich Blöser, Johannes Demel

Seit der letzten Ausgabe der PIPELINE wurden weitere wichtige Punkte der Umstellung der Telekommunikationsanlage der TU Wien angegangen. Seit Jänner 1999 ist nun das Chipkartensystem in Betrieb und seit April 1999 können die DECT-Schnurlosapparate an allen Standorten der TU Wien verwendet werden. Bei allen Fortschritten muss aber auch erwähnt werden, dass einige wichtige Punkte immer noch offen sind. Der Stand der einzelnen Teile des Projekts soll im Folgenden dargestellt werden.

## Stand der Installation

Die neue Telekommunikationsanlage der TU Wien, die im Endausbau aus 23 Teilanlagen an insgesamt 16 Standorten der TU Wien bestehen wird, ist bis auf die Standorte Neue Transalpinahalle und Favoritenstraße installiert und in Betrieb. Die Installation der DECT-Sender und der Telefonapparate in der neuen Transalpinahalle erfolgt im Juni 1999.

Beim Gebäude Favoritenstraße wird die Übergabe der Räume an die Institute voraussichtlich im September erfolgen. Vor diesem Zeitpunkt werden von der Fa. Ericsson bereits die Telefonanlagen installiert. Die Telefonapparate in den Institutsbereichen werden erst im Zuge der Übersiedlung installiert. Mit den übersiedelnden Instituten müssen (wieder) Konfigurationsgespräche geführt werden. Diese sind ab dem 16. August 1999 geplant.

Bei der Planung und Ausschreibung der neuen Telekommunikationsanlage wurde großer Wert auf eine ausfallsichere Ausführung gelegt. Für den Betrieb der Anlage unbedingt erforderliche Teile wie der interne Anlagen-Server, der Group Switch, der alle Teilanlagen miteinander verbindet, sowie Vermittlungsarbeitsplätze sollen im Rahmen eines „Dual Homing“-Konzepts sowohl am Standort Freihaus als auch am Karlsplatz existieren. Die vollständige Realisierung dieses Konzepts erfolgt mit der Installation des zweiten Group Switches am Karlsplatz am 10. / 11. Juli 1999. An diesem Wochenende wird es zu einem mehrstündigen Ausfall der Telekommunikationsanlage kommen. Genauere Details werden nach Abklärung mit dem Errichter der Anlage in einer Aussendung an alle Institute folgen.

Aufgrund der Angaben des Betreibers der alten Telefonanlage wurde bei der Planung davon ausgegangen, dass es keine Parallel- und Vorschaltapparate gibt. Dies hat sich leider als falsch herausgestellt. Im Zuge des

Tausches der alten Telefondosen und der Konfigurationsgespräche ergab sich ein Nachverkabelungsaufwand von rund 1000 Nebenstellen. Teilweise mussten nicht nur weitere Leitungen in Räume gezogen werden, sondern auch Steigleitungen verstärkt werden. Diese Nachverkabelungen sind nun abgeschlossen.

## Chipkarten, Verrechnung

Das Chipkarten-System, mit dem das Führen von Dienstgesprächen über die gesetzte Apparateberechtigung hinaus sowie die getrennte Erfassung von Dienst-, Privat- und Drittmittelgesprächen erst möglich wurden, war zum Umschaltzeitpunkt auf die neue Telekommunikationsanlage im September letzten Jahres nicht einsatzbereit, weil alle dafür nötigen Komponenten bis dahin nicht geliefert werden konnten. Beginnend mit Ende Oktober (Umschaltung der Standorte Atominstitut, Theresianumgasse, Floragasse und Aspanggründe) wurden die Telefonapparate mit den Chipkartenlesern ausgestattet. Parallel dazu wurde das Programm zur Programmierung der Chipkarten entwickelt und im Dezember die Produktion der Chipkarten durchgeführt.

Mit Jahresende 1998 konnten die Telefon-Chipkarten von den Instituten in der Telefonvermittlung abgeholt und eingesetzt werden. Nach Behebung der ersten Anlaufschwierigkeiten konnten also nun alle Benutzer einer Chipkarte entsprechend der vergebenen Berechtigung für diese Karte Ferngespräche auch außerhalb Wiens führen. Es wurde daher am 20. Jänner 1999 für alle Telefonapparate, deren Berechtigung in der Zwischenzeit auf Wien Umgebung angehoben worden war, die Berechtigung entsprechend den Konfigurationsgesprächen zurückgesetzt. Das bedeutet, dass von allen Apparaten Telefonate über die Apparateberechtigung hinaus nur mehr mit Chipkarten geführt werden können.

Insbesondere können von all jenen Apparaten, für die nur die Berechtigung H beantragt wurde (hausinterne Nebenstelle), ohne Chipkarte keine Gespräche außerhalb der TU Wien – mit Ausnahme von Notrufen – geführt werden. Ab diesem Zeitpunkt wurden auch von der Vermittlung keine Privat- und Drittmittelgespräche mehr vermittelt, da für diese die Chipkarten zu verwenden sind.

Leider kam es bei der Montage der Chipkartenleser in das Zusatzastengehäuse, das an den Telefonapparat angeschraubt wird, zu Unzulänglichkeiten bei der Zugentlastung des vom Chipkartenleser abgehenden Kabels. Die Folge davon waren dann bei mehreren Apparaten defekte unbrauchbare Chipkartenleser. Im Zuge des im heurigen Frühjahr notwendigen Upgrades der Chipkartenleser-Firmware wird nun systematisch auch dieser Fehler behoben. Um die Beeinträchtigung beim Benutzer vor Ort in Grenzen zu halten, geschieht dieser Upgrade durch kompletten Austausch des Chipkartenlesers. Der vollständige Abschluss dieser Arbeiten wird im Juni erfolgen.

Bis zum gegenwärtigen Zeitpunkt wurden etwa 2900 Chipkarten ausgegeben. Details zu den Apparateberechtigungen, den Chipkarten und zur geplanten Abrechnung finden Sie im Artikel „Verrechnung der Telefonentgelte“ auf Seite 14 in diesem Heft.

## Sprachspeicher

Die Fa. Ericsson hat sich aus verschiedenen Gründen dazu entschlossen, an der TU Wien nicht das bereits an der Universität Wien verwendete Sprachspeichersystem zu installieren, sondern ein neues leistungsstärkeres System einzusetzen. Dieses neue Sprachspeichersystem wurde am 16. November 1998 in Betrieb genommen. Leider erwies sich die Anbindung dieses Systems an die Telekommunikationsanlage als großer Schwachpunkt.

Lange Zeit wurde versucht, die verschiedenen auftretenden Fehler zu lokalisieren und zu beheben. Die Verwendung des Sprachspeichers war dabei zuweilen nur selten bis gar nicht möglich. Da die Schwierigkeiten nur sehr schwer in den Griff zu bekommen waren, wurde im Februar die Anbindung des Sprachspeichersystems an die Telekommunikationsanlage auf ein anderes Protokoll umgestellt. Auch diese Lösung bereitete im Umfeld der TU Wien aufgrund der großen Zahl der eingerichteten Sprachboxen und der Anbindung über 60 Leitungen zu Beginn große Probleme. Allerdings gelang es bei dieser Variante schneller, diese in den Griff zu bekommen, und seit mehreren Wochen funktioniert das Sprachspeichersystem ohne gravierende Probleme.

Wenn für eine Nebenstelle im Zuge der Konfigurationsgespräche oder auch im Nachhinein eine Sprachbox gewünscht wurde, so wurde diese im Sprachspeichersystem eingerichtet. Zur Sprachbox gelangt ein Anrufer immer dann,

- wenn auf dem Apparat die Taste Umleitung Sprachspeicher gedrückt wurde, oder

- wenn für die Nebenstelle der Sprachspeicher als fixes Anrufumleitziel definiert ist. In diesem Fall gelangen ankommende Gespräche zum Sprachspeicher, wenn sich die Nebenstelle nicht meldet oder besetzt ist.
- Weiters gelangt ein Anrufer zur Sprachbox bei folgender Situation: Wenn eine Nebenstelle eine Rufumleitung zu einer anderen Nebenstelle hat (z. B. Sekretariat), diese aber auf die Sprachbox umgeleitet ist, so gelangt der Anrufer ebenfalls zum Sprachspeicher, und zwar zur Sprachbox der ursprünglich angerufenen Nebenstelle.

Bedauerlicherweise haben noch immer viele Benutzer, für deren Nebenstelle eine Sprachbox eingerichtet ist, diese noch nicht aktiviert. Dies muss vom Benutzer der Nebenstelle durchgeführt werden, damit ein Anrufer eine Nachricht hinterlassen kann. Eine Beschreibung, wie dies zu erfolgen hat, findet man im letzten Heft der PIPELINE (Nummer 26, Dezember 1998), in der neuen Telefonfibel sowie auf den Telekom-Webseiten unter <http://www.zid.tuwien.ac.at/telekom/bedienung.html>

Falls eine Sprachbox vom Benutzer der Nebenstelle noch nicht aktiviert wurde, dann kann keine Nachricht hinterlassen werden und der Anrufer wird aufgefordert, die Rautetaste zu drücken, um auf eine Mailbox zuzugreifen, usw. Dies führt zur totalen Verwirrung des Anrufers. Wir ersuchen daher alle Benutzer von Nebenstellen, für die eine Sprachbox eingerichtet wurde, dringend, diese Sprachboxen zu aktivieren. Es ist nicht möglich, solche nicht aktivierten Sprachboxen zur Benutzung freizugeben, da sonst die Vertraulichkeit der Nachrichten nicht gewährleistet wäre. Leider bietet auch das Sprachspeichersystem keine Möglichkeit, mit einem vertretbarem Aufwand nicht aktivierte Sprachboxen herauszufinden.

## Neuaufgabe der Telefonfibel

Die Bedienung des neuen Sprachspeichers unterscheidet sich erheblich von der ursprünglich vorgesehenen. Deshalb war es notwendig, die Telefonfibel insbesondere im Hinblick auf die Bedienung des Sprachspeichers zu überarbeiten. Die neu gedruckte Version der Telefonfibel liegt vor und wurde an alle Institute und Universitätseinrichtungen in einer der jeweiligen Mitarbeiterzahl entsprechenden Stückzahl verschickt. Sollten zu wenig Exemplare der Telefonfibel zur Verfügung gestellt worden sein, so ersuchen wir, dies bei Frau Vojta, Nst. 42054, oder Frau Hanold, Nst. 42062, bekanntzugeben. Es werden dann gerne weitere Exemplare zugesandt.

## DECT-Schnurlostelefonie

Voraussetzung für die Aufnahme des Betriebs der DECT-Endgeräte (Schnurlostelefone) war neben der Montage der DECT-Sender und der Verlegung der zugehörigen Anschlusskabel die neue Software Release BC10 des Telekommunikationssystems. Diese Release stand im September 1998 noch nicht zur Verfügung, wurde aber für November versprochen. Daher wurden die DECT-Endgeräte auch ursprünglich für November

angekündigt. Später wurde dann die geplante Software-Umstellung von der Lieferfirma auf die Zeit der Weihnachtsferien verschoben. Doch auch dieser Termin konnte nicht eingehalten werden, weil die Software noch nicht verfügbar war.

Gegen Ende Jänner konnte endlich das Prozedere der Neuinstallation mit dem Einfrieren der bisherigen Konfiguration und anschließender Adaptierung dieser Konfiguration für die neue Software beginnen. Am Wochenende 13./14. Feber 1999 wurde die neue Software Release BC10 der Telekommunikationsanlage installiert und in Betrieb genommen. Sobald dann auch die nötigen Software-Module für den DECT-Betrieb verfügbar waren, konnte die Fa. Ericsson beginnen, die mittlerweile montierten DECT-Sender (ca. 450 an allen Standorten der TU Wien) an die Anlage anzuschalten.

Aufgrund der langen Zeitspanne zwischen der Bekanntgabe der Benutzerwünsche hinsichtlich der DECT-Schnurlosapparate und der erst im heurigen Frühjahr erfolgten Inbetriebnahme des DECT-Systems wurden die letzten Sommer erhobenen Wünsche für DECT-Endgeräte den Instituten zur Kontrolle und zur Ergänzung vorgelegt. Aufgrund dieser aktualisierten Konfigurationsblätter wurden im März die DECT-Endgeräte mit der endgültigen Firmwareversion programmiert und beginnend nach Ostern an die Benutzer ausgegeben. Die im Auftrag vorgesehenen Reserve-Akkus sowie die in den Konfigurationsblättern angegebenen Freisprecheinrichtungen sind bestellt und sollten noch im Juni ausgegeben werden können.

Als Option wurde von der Lieferfirma auch ein kombiniertes Dualmode-Gerät für DECT und GSM 900 angeboten. Dieses Gerät kommt in Österreich erst auf den Markt und trägt die Bezeichnung TH688. Leider ist es uns noch nicht möglich, das bei der Fa. Ericsson vorhandene Demogerät an der TU Wien zu testen, da dafür erst eine neue Firmware-Version abgewartet werden muss. Nach den derzeitigen Angaben der Herstellerfirma wird es mit diesem Gerät aber nicht möglich sein, sowohl unter seiner TU-Klappe und gleichzeitig unter seiner GSM-Rufnummer erreichbar zu sein. Es kann immer nur ein Empfangsteil aktiv sein. Das bedeutet, dass bei Verwendung des Apparats im DECT-Netz der TU Wien das Gerät mit seiner A1- oder Max-Rufnummer nur über den Weg einer Rufumleitung zur DECT-Nebenstelle der TU angerufen werden kann.

## Neue Funktion „Anrufliste“

Seit der Umstellung der Telekommunikationsanlage auf die Software Release BC10 steht die neue Funktion „Anrufliste“ zur Verfügung. Mit dieser Funktion werden auf einem 3213-Tischapparat (= Standardapparat an der TU Wien, mit Display und zwei Reihen zu je 10 Funktionstasten) die letzten 16 unbeantworteten Anrufe mit Datum und Uhrzeit sowie Nummer und Displayname (falls definiert) gespeichert. Sofern bei externen Anrufen die Telefonnummer mit übertragen wird (Anrufe von ISDN-Anlagen und von Mobiltelefonen), so werden auch diese Anrufe erfasst. Nicht angezeigt werden Anrufe von

externen Analoganschlüssen. Bei mehreren Anrufen von derselben Nebenstelle oder externen Nummer wird jeweils der letzte Anruf in der Liste angezeigt. Nicht erfasst werden Anrufe, die von vornherein wegen aktivierter Anrufumleitung nicht zur Nebenstelle durchgeschaltet wurden.

Für die Anrufliste wird eine Funktionstaste mit LED-Anzeige benötigt, auf die dann diese Funktion programmiert wird. Wenn neue, noch nicht gesichtete Einträge in der Anrufliste vorhanden sind, dann blinkt das LED dieser Taste. Nach Drücken der Funktionstaste kann mit den 4 Softkeys unterhalb des Displays die Anrufliste bedient werden, wobei die Funktion der Keys im Display angezeigt wird. Mit einem dieser Softkeys kann die Liste durchgegangen werden, mit einem weiteren können Einträge gelöscht werden. Durch Drücken des dritten Keys kann ein Rückruf zur eingetragenen Nummer initiiert werden. Der vierte Key dient zum Beenden der Bearbeitung und zur Rückkehr zur normalen Display-Anzeige.

Wenn der Wunsch nach Programmierung dieser Funktion für einzelne Apparate an einem Institut bzw. einer Universitätseinrichtung besteht, so bitten wir um eine E-Mail an die Mail-Adresse `telekom@noc.tuwien.ac.at`. Um die Bearbeitung der Anforderungen zu erleichtern, bitten wir nach Möglichkeit um eine Sammeliste durch den Telekom-Verantwortlichen des Instituts bzw. der Universitätseinrichtung. Die Liste muss zu jeder Nebenstelle auch die gewünschte zu belegende Funktionstaste enthalten. Als mögliche Tasten kommen dafür eigentlich nur die 6 Tasten unterhalb der Menütaste in der rechten Tastenreihe in Frage. Diese Tasten haben, beginnend von oben die Nummern 15, 16, ..., 20. (Die Tasten Drittmittel-, Privat- und Dienstgespräch haben die Nummern 21-23.) Bei Zusatztastenfeldern geht die Nummerierung – wieder beginnend von oben – weiter mit 24, 25, ...

## Abgleich der Daten der TK-Anlage

Bei der installierten Telekommunikationsanlage mit den verschiedenen Servern (wie z.B. für das zentrale Telefonbuch der Vermittlung, das Chipkartensystem, das Billing-System sowie den Sprachspeicher) gibt es eine Vielzahl von Datenbeständen. Ein automatischer Abgleich dieser Daten war daher Teil der Ausschreibung. Ebenso müssen diese Daten aber auch mit den bestehenden Datenbeständen der Universitätsdirektion sowie den White Pages-Daten der TU Wien abgeglichen werden.

Die Komplexität dieser Aufgabe ist vom Auftragnehmer lange Zeit unterschätzt worden. Dies ist auch ein Grund dafür, dass das Personalverzeichnis 1998/99 erst mit beträchtlicher Verspätung und nicht mit allen Nebenstellen gedruckt werden konnte. Aber auch im heurigen Frühjahr verbesserte sich die Situation nicht wesentlich, da mit der Umstellung auf die Software Release BC10 und der Installation der zugehörigen Software für das Anlagentelefonbuch (DNA 4.0) der automatische Datenimport sowie -export nicht mehr funktionierten. Es war daher bis vor kurzem nicht möglich, die aktuellen Tele-

fonnummern der Mitarbeiter aus dem Anlagentelefonbuch für das Personalverzeichnis der Universitätsdirektion zu exportieren. Mit der Installation der endgültigen DNA 4.0 Software Ende Mai soll dies nun wieder möglich sein.

Es hat sich in den letzten Monaten immer mehr gezeigt, dass das Anlagentelefonbuch trotz einer gewissen Flexibilität hinsichtlich zusätzlicher Felder nicht geeignet ist, die Funktion der zentralen Telekommunikationsdatenbank zu übernehmen. Um den wichtigen Punkt des Datenabgleichs endlich in einer befriedigenden Weise durchführen zu können, wurde nun eine umfassende Aufstellung aller Datenbestände angefertigt. Aufgrund dieser Aufstellung soll nun eine allen Anforderungen entsprechende Lösung gefunden werden.

## Computer-Telefonie-Integration

Das Thema CTI (Computer-Telefonie-Integration) war immer ein wichtiges Thema beim Aufbau des neuen Telekommunikationssystems, gerade an einer Technischen Universität. Es war daher zu einem gewissen Grad enttäuschend, dass die vom Auftragnehmer angebotene Variante für die TU Wien nicht praktikabel war. Dabei hätten Clients, die nur für Win95/98 verfügbar waren, auf den einzelnen PCs der TU Wien installiert werden müssen. Vor allem aber war diese Variante im Umfeld der im TUNET gegebenen Netztopologie nicht verwendbar, da im Unterschied zu den zentral vergebenen IP-Namen die historisch gewachsenen Microsoft-eigenen Netzwerknamen nicht eindeutig sind.

Die Hoffnung des ZID lag daher in einer bei Ericsson in Entwicklung befindlichen Web-basierten Lösung. Vor kurzem konnte nun die erste Version des sogenannten Personal Screen Call-Servers demonstriert werden. Dabei können über die üblichen Web-Browser (wie MS Internet Explorer oder Netscape Navigator) verschiedenste Funktionen für eine zugeordnete Nebenstelle ausgeführt werden. So kann etwa vom eigenen Arbeitsplatz auf das zentrale Anlagentelefonbuch der Vermittlung zugegriffen werden, eine Nummer gesucht und gewählt werden. Weiters kann eine Anrufumleitung gesetzt, geändert oder gelöscht werden. Es können auch Vorprogrammierungen für Rufumleitungen gesetzt werden. Weiters gibt es ein Call Log für ankommende Gespräche mit der Möglichkeit des Rückrufs mittels Mausclick.

In den nächsten Wochen wird es am ZID eine Teststellung des PSC-Servers 1.0 geben. Die Release 2 mit weiteren Features (wie Terminruf) soll in einigen Monaten folgen.

## Least Cost Routing

Die vom Planer der Telekommunikationsanlage ausgeschriebene Lösung für die TU Wien sieht eine Anlage vor, die das Least Cost Routing unterstützt. Die derzeit installierten Anbindungen umfassen schon bisher neben den unterschiedlichsten Anschlüssen zur Telekom Austria (ISDN-Multi-Anschlüsse, ISDN-Basisanschlüsse sowie Analogleitungen für Störfälle) auch eine direkte Verbindung zur Telekommunikationsanlage der Universität Wien (Rufnummer 01/42 77-), über die ein Telefonieren ohne Kosten möglich ist. Zur Mobilkom gibt es derzeit eine Standleitung, über die Gespräche immer dann geführt werden, wenn diese Leitung verfügbar und billiger als die Leitung der Telekom ist. Weiters wurde Mitte Mai ein Probetrieb mit je einem „Mobilrouter“ zu den Mobilfunknetzen von max.mobil und one aufgenommen. Zu jedem Netz steht damit ein Kanal zum Tarif von 1,- ATS pro Minute (Abrechnung im 30-Sekunden Takt) zur Verfügung. Wenn der Kanal belegt ist, wird das Gespräch über eine Leitung der Telekom Austria (zu höheren Kosten) geführt. Die Belegung der jeweils günstigsten verfügbaren Leitung erfolgt automatisch, es sind dafür keine besonderen Vorwahlziffern nötig.

Für die Auswahl zusätzlicher Telekom-Provider ist ein gewisser Beobachtungszeitraum notwendig, um basierend auf dem gegebenen Gesprächsverhalten eine Bewertung vornehmen und eine Auswahl treffen zu können. Da nun seit Jahresanfang das Chipkartensystem in Betrieb ist und Statistiken über die abgehenden Ferngespräche angefertigt werden können, wird nun auch die Verwendung zusätzlicher Provider, insbesondere für den Fernverkehr, untersucht. In diesem Zusammenhang soll aber schon jetzt darauf hingewiesen werden, dass die Vorwahl 10xx jener Provider, für die sich die TU Wien entscheiden wird, für die Nebenstellen gesperrt werden muss. Anderenfalls würden sich nämlich Unstimmigkeiten bei der Verrechnung dahingehend ergeben, dass Dienstgespräche der TU Wien einzelner Nebenstellen auf Privatrechnungen von Benutzern verrechnet werden.

## Informationen

Beachten Sie bitte unsere aktuellen Informationen auf den Telekom-Webseiten unter

<http://www.zid.tuwien.ac.at/telekom/>

und die News-Postings in verschiedenen Newsgruppen der TU Wien.

# Verrechnung der Telefonentgelte

Friedrich Blöser

Das Chipkartensystem zur Freischaltung von Nebenstellen für Ferngespräche ist nun seit knapp einem halben Jahr in Betrieb. Endlich sind auch die vom Auftragnehmer zu liefernden Programme zur Erstellung der Gesprächsstatistiken und Rechnungen für die Telefonentgelte nahezu fertig. Es erscheint daher angebracht, noch einmal zusammenfassend den Stand und die Abwicklung der Verrechnung der Telefonentgelte darzustellen.

## Apparateberechtigung und Chipkarten

Jede an die Telekommunikationsanlage der TU Wien angeschlossene Nebenstelle (sowohl Festapparat, DECT-Mobilendgerät, Fax- und Modemanschluss) hat eine bestimmte Grundberechtigung zum Führen von Ferngesprächen. Mögliche Kategorien sind

H	Halbamtlich + Notrufe
WU	Wien und Umgebung
A	Österreich
WW	Weltweit

Die Berechtigung umfasst das Führen von Dienstgesprächen (mit der Amtsholung 02) innerhalb des gesetzlichen Bereichs. Jedes Ferngespräch, das von einer Nebenstelle ohne eine Chipkarte mit Amtsholung 02 geführt wird, ist somit ein Dienstgespräch, das einem Dienstgesprächskonto eines Instituts oder einer Universitätseinrichtung zugeordnet wird.

Für Dienstgespräche über diesen eingeschränkten Bereich hinaus sowie für Drittmittel- und Privatgespräche kann ein Apparat freigeschaltet werden, wenn er über einen Chipkartenleser-Zusatz verfügt (nur bei Digitalapparat 3213 möglich) und der Anrufer eine Chipkarte mit den entsprechenden Berechtigungen besitzt. Chipkarten können beantragt werden mit dem Formular „Anforderung von TU Chipkarten“ (erhältlich am ZID oder über die Telekom-Webseiten).

Nach Einstecken einer Chipkarte in einen Festapparat wird dieser Apparat freigeschaltet für Ferngespräche entsprechend den Berechtigungen der betreffenden Chipkarte. Folgende Berechtigungskombinationen (und nur diese!) sind für die Konfiguration der Chipkarten möglich:

Dienstgespräch	Privatgespräch	Drittmittelgespräch
H	H, A, WW	H, A
H	H, A, WW	H, WW
WU	H	H, A
A	H, A, WW	H, A
A	H, WW	H, WW
WW	H, WW	H, WW

Die Berechtigung H für Drittmittelgespräche wird dabei so realisiert, dass zwar A bzw. WW eingetragen wird, der Chipkarte aber kein Projektcode (für die Verrechnung) zugeordnet wird.

Innerhalb der gesetzten Berechtigung können nun Ferngespräche ohne Inanspruchnahme der Vermittlung geführt werden, d. h. auch zu jenen Tageszeiten, zu denen die Telefonvermittlung nicht besetzt ist. Die Vermittlung vermittelt keine abgehenden Privat- und Drittmittelgespräche mehr. Diese müssen ausschließlich über eine Chipkarte geführt werden. Auch abgehende Dienstgespräche sollen in Hinkunft nur mehr entsprechend der Berechtigung des Apparats bzw. über die Chipkarte geführt werden. In jenen Fällen, in denen Mitarbeiter, Dissertanten, Diplomanden etc. mit ihren Chipkarten gewissen Einschränkungen unterliegen, kann im Einzelfall das Gespräch z. B. über das Sekretariat initiiert und dann übergeben werden.

Da durch die unberechtigte Verwendung einer Chipkarte finanzieller Schaden verursacht werden kann, ist entsprechend sorgsam mit den Chipkarten umzugehen. Der Verlust einer Chipkarte ist unverzüglich bei Frau Hanold, Nst. 42062, und via Fax an 42099 zu melden, damit die Karte gesperrt werden kann. Nicht mehr benö-

tigte Chipkarten sind ebenfalls an Frau Hanold, ZID TU Wien, zu retournieren.

## Telefonentgelte

Die Telekommunikationsanlage der TU Wien ist über verschiedene Außenleitungen der Telekom Austria angeschlossen. Diese Leitungen haben unterschiedliche Tarife, beginnend mit dem Geschäftstarif 3, über Geschäftstarif 2, Geschäftstarif 1 und Standardtarif bis zum Minimumtarif. Durch das Least Cost Routing ist sichergestellt, dass ein abgehendes Gespräch immer über die günstigste freie Leitung geführt wird. Bis auf die Spitzenzeit am späten Vormittag werden somit im Regelfall alle abgehenden Gespräche über den Geschäftstarif 3 mit dem niedrigsten Gesprächsentgelt abgewickelt. Zusätzlich gibt es einen Vertrag zwischen dem Bund, repräsentiert durch das Bundeskanzleramt, und der Telekom Austria bezüglich der Rabattierung der Entgelte auf Basis des Gesamtvolumens des Bundes an Telekom-Leistungen der Telekom Austria. Dieser Rabatt wird selbstverständlich an die Nutzer weitergegeben. Die Höhe der verrechneten Entgelte pro Impuls in Abhängigkeit von der verwendeten Außenleitung kann unter <http://www.zid.tuwien.ac.at/telekom/abrechnung.html> ersehen werden.

Die Telekommunikationsanlage der Universität Wien ist über Glasfaser an die Anlage der TU Wien angeschlossen. Dadurch fallen bei Gesprächen zur Universität Wien unter 01/42 77- ... keine Entgelte an (außer wenn die Leitung ausgefallen ist).

Zu den drei Mobilfunkbetreibern gibt es spezielle Verbindungen: Derzeit gibt es zur Mobilkom eine Standleitung, und zu max.mobil und one wird je ein Mobilrouter eingesetzt. Diese Verbindungen werden immer dann belegt, wenn sie verfügbar und günstiger als die entsprechenden Verbindungen über die Telekom-Leitungen sind.

Die Verwendung von weiteren Providern – insbesondere im Fernbereich – wird derzeit untersucht.

## Verrechnung

Die durch Ferngespräche (über die TU hinaus) anfallenden Gesprächsentgelte werden jeweils den betreffenden Telefonentgeltkonten zugerechnet.

Dienstgespräche (Amtsholung 02) von Apparaten ohne Chipkarte werden jenem Konto zugerechnet, das mittels des Formulars „Einrichtung von Telefonentgeltkonten“ oder „Telefonanschluss“ der Nebenstelle zugeordnet wurde. Dienstgespräche unter Verwendung einer Chipkarte werden jenem Dienstgesprächskonto zugerechnet, das auf dem Formular „Anforderung von TU Chipkarten“ angegeben wurde.

Privatgespräche (Amtsholung 03) werden auf das Privatgesprächskonto des Chipkartenbesitzers verrechnet. Für den Fall, dass jemand mehr als eine Chipkarte (z.B. von verschiedenen Instituten oder für verschiedene Funk-

tionen) besitzt, so werden die Privatgespräche aller Chipkarten auf ein Privatgesprächskonto des Inhabers und nicht auf mehrere getrennte Konten verrechnet.

Drittmittelgespräche mittels Chipkarte (Amtsholung 04 nach vorangegangener Eingabe des Projektcodes) werden dem durch den eingegebenen Projektcode definierten Drittmittelkonto zugeordnet.

Einem DECT-Schnurlosapparat, der ja keinen Chipkartenleser hat, kann ein Privatkonto zugeordnet werden, auf welches die mit 03 initiierten Privatgespräche verbucht werden. Von den DECT-Apparaten sowie von Faxgeräten und Modems können auch Drittmittelgespräche geführt werden (die Amtsholung erfolgt dabei mit 05), allerdings erfolgt die Verrechnung nur auf ein einziges, fest definiertes Drittmittelkonto (Formular „Einrichtung von Telefonentgeltkonten“).

In diesem Zusammenhang soll erwähnt werden, dass eine Chipkarte auf einem beliebigen Chipkartenapparat an der TU Wien eingesetzt werden kann. Die Verrechnung erfolgt immer (auch bei Dienstgesprächen) auf ein der Chipkarte zugeordnetes Entgeltkonto und nicht auf das dem Apparat zugeordnete Konto. Die Chipkarten der TU Wien sind jedoch nicht einsetzbar auf den Telefonapparaten der Universität Wien. Ebenso können die Chipkarten der Universität Wien nicht an der TU Wien verwendet werden.

## Gesprächsstatistiken

Für alle an der TU Wien eingerichteten Telefonentgeltkonten werden rückwirkend ab 1. Jänner 1999 monatliche Verbrauchsstatistiken erstellt.

Für Dienstgespräche werden jeweils alle Gespräche eines Monats gesammelt an das Institut bzw. an die Universitätseinrichtung geschickt. Die Aufstellung ist gegliedert nach den einzelnen Telefonentgeltkonten. Bei den Konten werden jeweils die Summen der Gespräche der Nebenstellen (ohne Chipkarten) sowie der Chipkarten (aufgegliedert nach den Nebenstellen, von denen aus sie geführt wurden) gelistet. Die betreffenden Summen enthalten die Anzahl der Gespräche, die aufgelaufenen Impulse (sofern verfügbar) sowie die Kosten dieser Impulse bzw. Gespräche. Zusätzlich werden vor der jeweiligen Summe für ein bestimmtes Dienstgesprächskonto noch allfällige weitere Entgelte oder Gutschriften angeführt. Dazu zählen etwa die Gesprächsentgelte von nicht umgestellten Standorten ebenso wie Entgelte für telefonisch aufgegebene Telegramme. Außerdem wird für verlorengegangene und daher neu ausgestellte Chipkarten ein Kostenersatz in Rechnung gestellt.

Für jedes einzelne Privatgesprächskonto werden in gleicher Weise Monatsstatistiken erstellt, die an den betreffenden Mitarbeiter persönlich (c/o seine Institutsadresse) verschickt werden. Aus der Aufstellung können die mit der Chipkarte geführten Gespräche, aufgegliedert nach den Nebenstellen, ersehen werden, ebenso natürlich

die Privatgespräche, die von einem persönlichen DECT-Apparat aus geführt wurden.

Für Privatgespräche wurde eine Bagatellgrenze festgelegt: Wenn die Summe der Entgelte eines Monats unter dem Wert von 1,- liegt, so wird dieser Betrag nicht verrechnet. Es wird in einem solchen Fall auch die monatliche Verbrauchsstatistik nicht gedruckt und nicht geschickt.

Bei den Drittmittelgesprächen (UOG Par. 2) wird für jedes einzelne Drittmittelgesprächskonto ebenfalls eine Monatsstatistik erstellt, die alle mittels Chipkarte, von DECT- oder Faxgeräten geführten Drittmittelgespräche für das betreffende Konto enthält. Es gilt auch hier – wie für Privatgespräche – eine Bagatellgrenze von 1,- pro Monat. Statistiken für Drittmittelkonten, die innerhalb des Monats diesen Wert nicht erreichen, werden nicht verschickt.

## **Rechnung über die Telefonentgelte**

Einen Monat nach Versenden der jeweils dritten Verbrauchsstatistik werden für die vorangegangenen drei Monate die Rechnungen erstellt und verschickt. (Innerhalb dieses Monats können etwaige Unklarheiten bei den letzten Statistiken noch geklärt werden.) Diese Rechnun-

gen für die Dienst-, Privat- und Drittmittelgespräche enthalten jeweils die Summe der Entgelte der letzten drei Statistiken. Wurde in einem Monat die Bagatellgrenze für Privat- und Drittmittelgespräche von 1,- nicht erreicht und keine Statistik gedruckt und verschickt, so erscheint für den betreffenden Monat auch kein Betrag in der Quartalsrechnung auf.

Die Rechnungen an die Institute dienen der Information. Die Entgelte werden mittels eines vom Zentralen Informatikdienst der TU Wien ausgestellten und unterzeichneten ZVA aus dem Verfügungsrest (o. Dot.) des Instituts unter 1/14208/6300-901 und der vom Institut genannten Kostenstelle (Formular „Einrichtung von Telefonentgeltkonten“) automatisch abgebucht. Für das erste Quartal 1999 wurde durch den Budgeterlass des Vizerektors für Ressourcen festgelegt, dass die Bezahlung zentral erfolgt. Die Weiterverrechnung an die Institute erfolgt daher ab dem 1. April 1999.

Für die Privat- und Drittmittelkonten werden ebenfalls Quartalsrechnungen (beginnend mit dem 1. Quartal 1999) erstellt, und zwar direkt auf einem Zahlschein mit einer Allonge. Die Entgelte sind mittels dieses Zahlscheins auf das angegebene Konto der TU Wien einzuzahlen.

Für Rückfragen zur Verrechnung wenden Sie sich bitte an die Mailadresse [telekom@noc.tuwien.ac.at](mailto:telekom@noc.tuwien.ac.at) oder telefonisch an DI Friedrich Blöser, Nst. 42041.



# Erfahrungen mit SGI Origin2000

Ernst Haunschmid

Der neue Applikationsserver Freie Programmierung, SGI Origin2000, wurde bereits in der letzten PIPELINE [1] vorgestellt. Die Hardware und die der Origin2000 zugrunde liegende ccNUMA Architektur wurden dort bereits ausführlich beschrieben. Im Mittelpunkt dieses Artikels stehen Software-Aspekte (speziell IRIX-6.5), die Betriebssituation sowie die ersten Erfahrungen mit dem neuen System.

## Das Betriebssystem IRIX-6.5

Zum Zeitpunkt der Lieferung war bereits IRIX-6.5 verfügbar; die neueste Version dieses Betriebssystems bietet neben *Y2K compliance* einige neue und auf anderen UNIX-Plattformen (derzeit) noch nicht verfügbare Features:

- **Checkpoint/Restart** erlaubt es, von einem laufenden Prozess ein *process image* auf einem Plattenspeicher abzulegen. Wird der Prozess (ungewollt) abgebrochen (z.B. durch ein Reboot des Systems), kann dieser Prozess in genau dem Zustand, den er zum Zeitpunkt des Checkpoints hatte, fortgesetzt werden.
- Der **Miser Scheduler** erlaubt es, Ressourcen (CPUs und Hauptspeicher) für eine bestimmte Zeit zur reservieren. In diesem Zeitraum stehen die reservierten Ressourcen den entsprechenden Prozessen exklusiv zur Verfügung; die Anzahl der *context switches* kann dadurch extrem reduziert werden, wodurch die Laufzeit der einzelnen Programme, speziell im Hochlastbereich, deutlich verbessert werden kann.

Checkpoints werden üblicherweise vor einer geplanten System-Abschaltung über das Queuing System angelegt, können aber auch vom Benutzer selbst spezifiziert und durchgeführt werden. Problematisch ist Checkpoint/Restart bei Prozessen, die mit anderen Rechnern kommunizieren; hier ist ein Restart im Allgemeinen nicht möglich.

Der Miser Scheduler verhält sich dem Benutzer gegenüber wie ein rudimentäres Queuing System; daher wurde der Miser Scheduler mit Craysoft NQE kombiniert. Craysoft NQE entspricht in der Funktionalität Sterling NQS, das auf den SGI Power Challenge Systemen eingesetzt wird.

Durch den Einsatz von Miser kann die Laufzeit serieller Jobs um bis zu 15 %, bei parallelen Jobs um bis zu

30 % verbessert werden (abhängig von der jeweiligen Auslastung des Systems). Generell wird durch den Einsatz von Miser ein wesentlich besseres Verhalten im Hochlastbereich gewährleistet; bei voll ausgelastetem System konnte eine Steigerung der Durchsatzleistung von über 15 % beobachtet werden.

Alle Platten der Origin2000 (mit Ausnahme des */tmp*-Filesystems) werden von der Plexing Software gespiegelt. Plattendefekte können damit in den meisten Fällen ohne Beeinträchtigung des Benutzerbetriebes behoben werden, zumal alle Platten im laufenden Betrieb getauscht werden können. Bisher kam es im laufenden Betrieb zu keinen Plattendefekten; in umfangreichen Tests mit simulierten Plattendefekten hat sich die Spiegelung der Platten sehr gut bewährt.

## Leistungsvergleich mit Power Challenge XL

In beiden Systemen werden MIPS R10000 Prozessoren eingesetzt; in den Power Challenge XL Systemen kommt der IP25 zu Einsatz, in der Origin2000 der IP27.

- Der Prozessor ist bei der Origin2000 mit 250 MHz getaktet gegenüber 195 MHz bei den Power Challenge XL Systemen;
- Der *second level cache* wurde von 2 MB auf 4 MB verdoppelt;
- Zudem wird der Cache mit dem vollen Prozessortakt angesteuert (gegenüber zwei Drittel des Prozessortaktes bei den Power Challenge XL Systemen).

Aufgrund dieser Eigenschaften kann man eine Leistungssteigerung von zumindest 30 % erwarten, bei guter Ausnutzung des Cache sollte der Leistungsgewinn deutlich höher sein.

Bei seriellen Applikationen konnten bei den bisher durchgeführten Leistungstest Steigerungen um bis zu 80 % festgestellt werden; bei zusätzlicher Last auf den Systemen ist der Leistungsunterschied noch wesentlich höher (siehe Tabelle 1).

aktive Prozesse	Power Challenge XL	Origin2000
1	1.00	0.56
10	1.47	0.56
20	1.89	0.56
30	–	0.56
60	–	0.61

Tabelle 1: Normierte Laufzeiten für eine numerische Applikation

Die Laufzeit einer Applikation auf der Power Challenge XL hängt sehr stark von der Last auf dem System ab. Da die Hauptspeicherzugriffe aller Prozesse über einen gemeinsamen Systembus erfolgen, kann es hier zu gegenseitigen Behinderungen kommen. Ein wesentlicher Teil der Applikationen auf dem Power Challenge XL Cluster hat hohe Anforderungen an die Speicherbandbreite. Laufen mehrere derartige Applikationen gleichzeitig, kommt es zu entsprechenden Leistungseinbußen. Durch die ccNUMA Architektur tritt dieses Problem bei der Origin2000 nicht oder nur in sehr abgeschwächter Form auf.

Bei einem Lastbenchmark, der in etwa die derzeitige Last auf den Power Challenge Systemen widerspiegelt, erreicht die Origin2000 (64 Prozessoren) die zweieinhalbfache Durchschnittsleistung des Power Challenge XL Clusters (insgesamt 56 Prozessoren).

## Betriebssituation

Der neue Applikationsserver SGI Origin2000 wurde Mitte November geliefert. Aufstellung und Erstinstallation verliefen problemlos, sodass am 4. Dezember 1998 die Abnahme des Systems erfolgen konnte. Nach weite-

ren Installationsarbeiten und entsprechenden Adaptionen an die Betriebserfordernisse an der TU konnte Mitte Dezember der Testbetrieb aufgenommen werden.

Ende Dezember kam es zu den ersten schwerwiegenden Betriebsproblemen; Softwaredefekte führten mehrmals dazu, dass keine neuen Prozesse gestartet werden konnten; in diesen Fällen war ein *Restart* des Systems notwendig. Als Ursache wurden Defekte im Miser Scheduler identifiziert, die teilweise durch *Workarounds* behoben werden konnten. Zusätzlich mussten von einigen Kernel-Komponenten Beta-Versionen installiert werden, um einen Testbetrieb mit dem Miser Scheduler zu gewährleisten.

In den folgenden Wochen traten weitere Hard- und Software-Probleme auf; in den Fällen, in denen eine Fehlerquelle eindeutig identifizierbar war, wurden die entsprechenden Hardware-Komponenten getauscht. Gleichzeitig wurde versucht, das Betriebssystem durch Installation der jeweils neuesten Versionen (teilweise auch Test-Versionen aus den Software-Labors in den USA) ausfallsicherer zu machen.

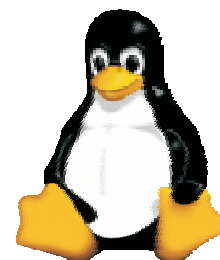
Für einige der Defekte konnte keine eindeutige Ursache festgestellt werden; obwohl diese Defekte auf unserem System wiederholbar waren, konnten sie auf anderen, vergleichbaren Origin2000 Installationen nicht nachvollzogen werden.

Anfang Mai wurde IRIX-6.5.4 installiert. Obwohl es in den folgenden Tagen zu zwei weiteren Systemabstürzen kam (verursacht durch die Hardware-Diagnose Tools), besteht berechtigte Hoffnung, dass sich die Betriebssituation verbessert und stabilisiert und somit die vorhandene und durchaus imposante Rechenleistung der Origin2000 in vollem Umfang den Benutzern zur Verfügung gestellt werden kann.

## Literatur

- [1] P. Berger: Der neue Applikationsserver Freie Programmierung CRAY Origin2000 Hochleistungsserver. PIPELINE 26, pp. 14-15, Wien, 1998.

# Linux, eine Alternative ?



Walter Selos

Schon seit geraumer Zeit steigt der Bekanntheitsgrad des Betriebssystems Linux immer mehr. Nicht nur in Fachzeitschriften schaut einem immer öfter der drollige Pinguin (das Linux-Logo) entgegen, auch in den anderen Medien wird der Name Linux immer öfter erwähnt.

Vor allem die zunehmende Angst vor Monopolisierungstendenzen am Softwaremarkt haben den Ruf nach einer Alternative laut werden lassen, und Linux bietet sich dafür sehr gut an.

Meine Erfahrungen mit Linux gehen schon auf mehrere Jahre zurück, weswegen ich hier einige Worte zu diesem Thema schreiben möchte.

Was hat es nun für eine Bewandnis mit diesem Betriebssystem ? Linux ist ein frei erhältliches UNIX-ähnliches Betriebssystem, welches von Linus Thorwalds unter Mithilfe von Entwicklern, die über die ganze Welt verteilt sind, entwickelt wurde. Diese Projekt konnte nur mittels intensiver Kommunikation zwischen den Entwicklern via Internet realisiert werden. Sowohl die Tatsache, dass das oberste Ziel nicht die Gewinnsteigerung für eine Firma war sondern einfach die technische Qualität, als auch der um vieles größere Entwicklerstab (die musste ja niemand zahlen) spiegelt sich in der Stabilität und Vielseitigkeit dieses Betriebssystems wieder.

Linux ist nicht nur für die Intel-PC-Plattform verfügbar sondern auch für Alpha, Sparc, Mac, PPC, um nur die wichtigsten Portierungen zu nennen.

Linux ist, wie schon erwähnt, freie Software, der Quellcode für das Betriebssystem ist in allen Distributionen enthalten. Die meisten der hunderten mitgelieferten Programme sind nach der GNU/GPL Lizenz lizenziert, d. h. kurz gesagt freie Software, wobei der Quellcode zur Verfügung gestellt werden muss.

## Einsatzbereiche

Das Haupteinsatzgebiet von Linux ist im Moment zweifellos im **Serverbereich**. Die TCP/IP Implementierung gehört zu den größten Stärken diese Betriebssystems. Was damit alles möglich ist, möchte ich in Stichworten erwähnen:

## Als Server

- **Fileserver**

Als NFS-Server für andere UNIXe, als SAMBA-Server für Windows/Windows NT-Clients (sogar als Domaincontroller eingeschränkt verwendbar), auch eine freie Novell-Fileserver-Implementation gibt es (nur Version 3), zum Kaufen gibt es eine Version 4 plus Directory-Service. NFS und SAMBA gibt es ja für alle UNIXe, was besonders für Systemmanager interessant ist, die auch andere UNIX-Plattformen betreuen, die haben keine Umschulung nötig. Die von UNIX-Systemen her bekannte gute Skalierbarkeit trifft auch für Linux zu, was zu einer besseren Leistung bei hoher Belastung führt, verglichen mit manchen anderen Server-Betriebssystemen. Man sollte bei der Interpretation von **Leistungstests** natürlich immer **vorsichtig** sein und mehrere Quellen vergleichen, da es sehr leicht möglich ist, spezielle Testumgebungen zu schaffen, die ein bestimmtes Betriebssystem stark bevorzugen oder benachteiligen können. Zahlen allein sind sicher nicht allzu relevant und oft geht's ja um mehr als die Bekanntmachung technischer Fakten.

- **Printserver**

Das Berkeley Printerprotokoll (lpd) ist standardmäßig bei Linux dabei, über SAMBA kann man Netzwerkdrucker für Windows installieren und auch die Novellserver-Software kann als Printserver dienen.

- **Mailserver**

Es gibt hier die gleichen Möglichkeiten wie bei allen UNIXen: sendmail, smail und was es sonst noch für spezielle Software dafür gibt, inklusive Listserver.

Die Protokolle pop und imap werden standardmäßig unterstützt.

- **Http-Server (Web-Server)**

Auch hier wieder „State-of-the-art“: der bewährte und wohl am meisten verbreitete http-Server „Apache“ leistet auch unter Linux seine guten Dienste.

- **Andere Netzwerkdienste**

Da gibt es praktisch alles, was unter UNIX auch möglich ist. Der Einsatz als **Router** mit IP-Forwarding und ein Route-Daemon, welcher Information mit anderen Routern austauschen kann, ist ebenso möglich wie „**IP-Masquerading**“.

Was ist das ? Nehmen Sie den Fall an, Sie haben ein privates Netzwerk mit vielen Maschinen und einen Anschluss an's Internet (mit einer Adresse). Sie wollen aber von allen Maschinen aus auf externe Netzwerkdienste zugreifen. Dafür gibt's IP-Masquerading. Das hat noch dazu den Vorteil, dass von außen nur auf den Router, nicht aber auf's private Netzwerk zugegriffen werden kann. Durch die Aktivierung von **Packetfiltern** können Sie gleichzeitig noch weitere Zugriffsrestriktionen realisieren. Dabei haben Sie noch keine typische Firewall-Lösung (mit Proxies) eingesetzt, welche es auch dafür gibt. Der eventuelle Nachteil, dass der Quellcode auch Hackern bekannt ist, welche Schwachstellen ausnützen können, wird wieder dadurch wettgemacht, dass diese Lösungen durchschaubarer sind als „Blackboxes“ von Firmen und man dafür mehr Verständnis und eventuell auch individuellere Lösungen entwickeln kann, sowie dadurch, dass durch die große Entwicklergemeinde im Internet meist sehr schnell Schwachstellen erkannt und behoben werden.

Natürlich nützt die beste Firewall-Konfiguration nichts, wenn man erlaubt, dahinter Mail-Attachments durch Anklicken zu aktivieren, oder „Mobile Code“ wie Java oder Active X zulässt.

Sehr angenehm ist es für den Serverbetrieb, dass durch den Zugriff auf die Shell über's Netzwerk eine **Fernwartung** sehr bequem und ohne teure „Third Party“-Produkte möglich ist. Aus Sicherheitsgründen würde ich, vor allem auf einer Universität, die Verschlüsselung via „Secure Shell“ (gibt's am `gd.tuwien.ac.at`) oder „One Time Passwords“ empfehlen.

## Als Desktop-Computer/Workstation

Dieses Einsatzgebiet galt früher als Domäne für „UNIX-Freaks“. Schon seit einigen Jahren unterscheidet sich die Arbeit an einem Linux-Computer kaum von der an einer anderen UNIX-Workstation. Mittlerweile sind die Nachteile einer komplizierten Installationsprozedur sowie das Fehlen von kommerzieller Software wie Officepaketen und Datenbanken nicht mehr wirklich vorhanden (siehe Applixware, StarOffice, Oracle, ...). Die Zahl der kommerziellen Softwareprodukte für Linux steigt ständig.

Auch diesen Artikel schreibe ich mit einem kommerziellen Textsystem auf meinem Linux-Notebook (Linux-

distribution: Mandrake 5.3) und werde ihn dann als MS-Word-kompatibles Attachment zur weiteren Verarbeitung per E-Mail weiterleiten. Es gibt schon sehr schöne, auf X-Windows aufsetzende grafische Oberflächen, ich verweinde hier „KDE“, die Bequemlichkeit ist um nichts geringer als die anderer kommerzieller GUIs, obwohl ich sie nicht ganz ausnütze, da ich nach über zehnjähriger UNIX-Erfahrung immer noch sehr gerne auf eine Shell (Kommandozeile) zurückgreife.

## Die Distributionen und Installationsmöglichkeit auf der TU

Die *auf der TU erhältlichen Distributionen* sind auf 2 Server aufgeteilt:

`linux.edvz.tuwien.ac.at`

(wird in Kürze auf `linux.tuwien.ac.at` umbenannt)

sowie

`gd.tuwien.ac.at`

Auf `linux.edvz` sind die Distributionen **Slackware**, **Debian** und die wichtigsten Teile von **RedHat** gespiegelt und über **NFS** und **anonymous ftp** zugreifbar. Diese Dienste sind im Wesentlichen *auf die TU beschränkt* und dienen zur schnellen Installation über's TU-Netz.

Am `gd.tuwien.ac.at` ist kein NFS-Zugang erlaubt. Außer den oben genannten Distributionen gibt es auch noch **Mandrake** (eine sehr einfach zu installierende, auf RedHat aufsetzende Distribution mit komplett installierter KDE-Oberfläche, als Desktop/Workstation sehr zu empfehlen) und **SuSe** (eine im deutschsprachigen Raum sehr verbreitete Distribution). Da viele dieser Distributionen auch **über anonymous ftp zu installieren** sind, kann man diese auch direkt vom `gd.tuwien.ac.at` installieren (z.B. RedHat, Mandrake). Für einige (Mandrake, SuSe) liegen am `gd` auch **iso-images**, von denen man boot-bare Installations-CDs brennen kann.

## Zu den Distributionen

### Slackware:

Eine schon sehr lange existierende, etwas minimalistische Distribution, sehr geeignet zum Einsatz als Server.

### Debian:

Eine Distribution, die rein auf GNU-Komponenten aufsetzt (d.h. im Wesentlichen frei verfügbare Sources für alle Komponenten). Vielleicht etwas schwieriger zu installieren, aber sehr durchschaubar, reagiert sehr schnell bei der Behebung von Sicherheitslücken, die Bekanntgabe erfolgt über einen eigene Mailing-Liste. Also vielleicht nicht so günstig für Linux-Einsteiger, aber wirklich sehr empfehlenswert für Serverbetreiber.

### RedHat:

Sicher die am meisten verbreitete Distribution, leicht zu installieren, alles in allem ziemlich problemlos.

## Mandrake:

Setzt voll auf RedHat auf, die Installation ist fast identisch, die Konfigurationsdateien und Startup-Skripts sind ebenfalls identisch. Dazu werden die KDE-Oberfläche sowie eine sehr aktuelle Version des X-Window-Systems standardmäßig mitinstalliert. Für Linux-Anfänger sehr zu empfehlen, trotzdem sicher genug für Serveranwendungen (wenn man weiß, was man tut ... sonst sollte man aber von jeder Serverinstallation die Finger lassen, das gilt nicht nur für Linux ...).

## SuSe:

Im deutschsprachigen Raum sehr verbreitet, auch relativ leicht zu installieren. Mir persönlich gefällt das Systemmanagement-Tool „Yast“ nicht besonders gut, speziell in der Version 6.0 habe ich einige unschöne Inkonsistenzen gefunden, aber vielleicht wird's in der nächsten Version besser (es gab ja schon auch bessere Versionen). Probleme gibt's vor allem, wenn man eine spezielle Konfiguration nicht mit Yast bewerkstelligen kann, letzterer aber beim nächsten Aufruf „dazwischen funkt“ und wieder alles eigenmächtig ändert.

Es gibt auch noch weitere Distributionen wie **Caldera** (ich habe Erfahrung mit einer älteren Version und war recht zufrieden damit) und **DLD** (damit habe ich leider keine Erfahrungen).

## Alternative: Ja oder Nein ?

Nachdem Sie nun etwas mehr über Linux wissen, kann ich mir erlauben, die im Titel gestellte Frage genauer zu beleuchten. Sie wird in dieser Weise oft gestellt, es wird aber kaum präzisiert: Alternative wozu ?

### Alternative zu UNIX-Workstations

Meiner Meinung nach grundsätzlich ja. Es sind viele Ausgangssituationen vorhanden, die dafür sprechen:

- Man will die Dienste verwenden, die man auf der Workstation bereits hatte.
- Es sind Systemmanager bzw. Benutzer vorhanden, die sich ohnehin auf UNIX auskennen.
- Die moderne PC-Hardware ist zum Rechnen meist schnell genug, außerdem gibt's Linux ja auch für Alpha- und Sparc-Maschinen.

So gesehen ist Linux sicher die größte Konkurrenz für die klassischen UNIX-Workstations.

Es gibt natürlich immer Ausnahmesituationen, in denen die Workstation eines bestimmten Herstellers inklusive Software nicht ersetzt werden kann.

### Alternative für Server

Da ich selbst schon so manchen Linux-Server installiert habe und auch welche betreibe, kann ich auch diese

Frage positiv beantworten. Allerdings: ich habe langjährige UNIX-Erfahrung. Hier kann ich nicht genug betonen, dass es zum Betrieb eines Servers, egal welches Betriebssystem verwendet wird, nötig ist, sich Kenntnisse anzueignen, um ein sinnvolles, gut überlegtes Systemmanagement zu gewährleisten. Man sollte so weit über die Funktionsweise des Betriebssystems und seiner Komponenten Bescheid wissen, dass es möglich ist, sich anbahnende Fehler und Sicherheitsprobleme zu erkennen und sinngemäß zu reagieren. Oft laufen Server so stabil (speziell auch unter Linux), dass, einmal konfiguriert, für lange Zeit „Zero Administration“ gespielt wird. Umso größer ist dann die Überraschung, wenn Probleme auftreten.

Zum Einsatz in „Mission Critical Systems“ eignet sich Linux, abgesehen von der Komplexität, gut, weil durch Vorhandensein des Quellcodes alle verwendeten Komponenten kontrolliert und verstanden werden können. Das „Einfrieren“ auf eine bestimmte Version, die auch wirklich gut getestet mit den Hardwarekomponenten zusammenspielt, ist bei solchen Anwendungsgebieten oft eine *conditio sine qua non* und durch den vorhandenen Quellcode auch leicht möglich. Ebenso ist die Entwicklung neuer Hardwaretreiber bzw. die Modifikation vorhandener sehr erleichtert.

### Alternative zu anderen Softwaretechnologien

Jetzt kommt's endlich, das politisch brisante Thema. Wie ich anfangs erwähnt habe, wird Linux gerne als Ausweg aus einem zunehmend monopolisierten Softwaremarkt gesehen. Gerade diese Tatsache führt natürlich zu einer Berichterstattung, die sich von einer objektiven, technischen Betrachtung ziemlich weit entfernen kann. Zwar gibt es viele Meinungen zu hören, welche sich sehr wohl in diesem Rahmen bewegen (ich hoffe, ich auch), es spielen jedoch zwei kontrahierende Lager mit und zwar – wie könnte es anders sein – das der potentiellen Monopolisten und das immer stärker werdende derer, die sich von solch einer Monopolisierungstendenz unmittelbar bedroht fühlen.

Zugegeben fühle auch ich mich wohler (welcher Techniker wohl nicht), wenn ich für die Lösung eines technischen Problems mehrere Alternativen zur Verfügung habe, aber wirklich mehrere ...

Auf Grund dieser Polarisierung ist zu erwarten, dass man mit Meinungen konfrontiert wird, in der Linux einerseits hochgelobt wird als das „Non Plus Ultra“, während die andere Partei mit FUD-Kampagnen (Fear, Uncertainty, Doubt) reagiert. Ich könnte mir vorstellen, dass gerade Massenmedien und Glanzpapierprospekte für diese Art von Informationen besonders empfänglich sind. Solche Information kann (bzw. soll) dem Ansehen eines Produktes ziemlich schaden.

Wir können das nicht ändern, sollten es uns aber in Erinnerung rufen, wenn wir uns über Linux (oder eine alternative Lösung) informieren wollen. Wie schon oben erwähnt, gilt das auch für Leistungstests, und es ist empfehlenswert – und dank Internet auch gar nicht schwer –

andere um ihre Erfahrungen mit einer bestimmten Konfiguration zu fragen.

Ein vom **Betriebssystem unabhängiges Problem** spielt bei der Argumentation pro und kontra Linux auch hinein, und meiner Meinung nach ein sehr wesentliches, jedoch oft übersehenes. Es ist der durch Überforderung, Konditionierung und Marketing entstandene Wunsch des Benutzers nach einer einfach zu bedienenden Oberfläche, ohne auf die Vielseitigkeit und Komplexität des Betriebssystems zu verzichten. Die Komplexität ist in dem bestehenden Ausmaß meistens um vieles größer als notwendig, bei der immer höheren Integrationsdichte und den immer niedrigeren Hardwarepreisen aber (leider) verständlich, was dem Benutzer jedoch meist verborgen bleibt. Der wundert sich nur, warum die Version n+1 eines bestimmten Softwareprodukts auf seiner neuen CPU, Version m+1, genauso langsam, wenn nicht langsamer geht als seine alte Hard- und Softwarekonfiguration.

Es ist aber nur bis zu einem gewissen Grad möglich, diese Komplexität hinter einer Oberfläche vollständig zu verstecken. (Würden Sie mit einem viermotorigen Verkehrsflugzeug fliegen, welches als einzige Bedienelemente nur „Eingabe der Zielkoordinaten“, „Start“ und „Not-Aus“ hat – und eine einzige Warnleuchte „allgemeine Flugstörung“? Mir wär's im höchsten Maß suspekt ...) Oft wurde das Problem so gelöst, dass die Komplexität so gründlich hinter der Oberfläche versteckt ist, dass in einem nicht vorgesehen Fehlerfall (allzuviele wurden meist nicht vorgesehen) es selbst einem Experten unmöglich ist, das Problem zu lokalisieren und zu beheben. Wie oft haben wir es schon mit iterativen Neuinstallationen versucht, in der Hoffnung auf Konvergenz dieses Verfahrens? Das ist zwar bei Linux weniger wahrscheinlich, aber es besteht schon heute die Gefahr, dass die Installation so leicht gelingt, dass auch ein blutiger Anfänger ein Linux laufen hat und womöglich an's Netz hängt, ohne die geringste Ahnung, was er da eigentlich hat. Wenn's Probleme gibt, die zwar mit ein wenig Wissen bzw. Erfahrung leicht zu lösen wären, kann er sich nicht helfen, ist enttäuscht und sieht keinen Vorteil im Vergleich zu dem, was er ohnehin schon gewohnt ist.

Also ist das, was sich die Mehrheit wünscht („eierlegende Wollmilchsau“ mit Einknopfbedienung) ein grundlegender Widerspruch, der Designprobleme heraufbeschwört und nur zu einem problematischen Kompromiss führen kann. Was immer für eine „Alternative“ dafür herhalten muss, ohne Enttäuschungen und Unbehagen wird's nicht ganz abgehen.

Wenn auf Grund der (wenig reflektierten) Nachfrage die Entwicklung in diese Richtung ginge, wäre durch Linux keine Alternative entstanden, sondern nur die Nachahmung bereits weitverbreiteter Designfehler. Die Optimierungsaufgabe besteht darin, einen optimalen Kompromiss zwischen dem „Experts only“- und dem „Friss-oder-stirb“-Paradigma zu finden, und der ist wahrscheinlich subjektiv. Man sollte die Entwicklung in dieser Richtung verfolgen.

Ein weitaus größerer Fortschritt für Linux wäre es, wenn sich die einzelnen Distributionen auf einen gemeinsamen Standard in Bezug auf Konfigurationsdateien, Startupscripts usw. einigten, denn wenn alle Linux „gleich eingeräumt“ sind, ist es für Software-Entwickler leichter, ihre Produkte auf Linux zu portieren (nämlich auf „Linux“, nicht auf „RedHat“, „Debian“, „SuSe“ und was es sonst noch alles gibt). Auf diesem Gebiet gibt es noch Einiges zu tun, obwohl es schon Ansätze dafür gibt. Jedoch: die Distributionen definieren sich ja durch den Unterschied.

Je mehr man in dieser Richtung Überlegungen anstellt, umso eher sieht man, dass die Zukunft in viele Richtungen offen ist und dass wesentlich mehr Faktoren als nur technische und wirtschaftliche Überlegungen mitspielen werden. Das ist auch gut so, schließlich soll Technik und Wirtschaft ja dem Menschen dienen und nicht umgekehrt.

Sollten Sie **Fragen** zu Linux haben oder als TU-Mitarbeiter **Unterstützung** dazu benötigen, wenden Sie sich bitte an den Autor dieses Artikels:

Walter Selos, selos@zid.tuwien.ac.at, Kl. 42031 oder an DI Paul Torzicky, torzicky@zid.tuwien.ac.at, Kl. 42035

# Windows 2000

Rudolf Sedlaczek

Die nächste Windows NT Version wird Windows 2000 heißen und soll am 6. Oktober 1999 ausgeliefert werden. Windows 2000 wird nicht nur das technisch signifikanteste Update sein, sondern soll irgendwann im nächsten Jahrtausend die Basis für alle Microsoft Betriebssysteme werden, vom Notebook-PC bis hin zum hochskalierbaren Server-Betriebssystem. Diese zukunftsweisende Ausrichtung soll die Namensänderung von Windows NT 5.0 in Windows 2000 verdeutlichen.

## Überblick

Mitte Mai 1999 konnten sich die Beta-Tester schon über die erfolgte Auslieferung der Beta 3 Version von Windows 2000 freuen. Auf Grund der vielen neuen Features braucht diese Version ca. doppelt so viel Memory und Plattenplatz wie Windows NT 4.0. Die Microsoft Entwickler hoffen aber, dass die Ressourcen-Anforderungen der endgültigen Version auf nur mehr 20% über denen von NT 4.0 zurückgeschraubt werden können. Auch an der Performance soll noch gearbeitet werden, die derzeit teils etwas besser und teils etwas schlechter ist als bei NT 4.0. Auch der Start von Applikationen ist immer noch wesentlich langsamer als bei Windows 98.

Wer diese Beta-Version einsetzt, muss wie üblich bei Microsoft Systemen damit rechnen, nicht auf die endgültige Windows 2000 Version upgraden zu können, sondern frisch installieren zu müssen. Außerdem wurden schon Meinungen bekannt, dass nicht alle technischen Neuerungen der Beta-Versionen auch schon in der ersten Ausgabe der Final Release zu finden wären, da einige Komponenten wie Active Directory und Intellimirror noch nicht ganz ausgereift seien. Microsoft-Vize-Präsident David Cole machte den Mangel an Computerspielen für das neue Windows 2000-System für die Verzögerung verantwortlich.

Windows 2000 wird in vier Versionen für unterschiedliche Einsatzbereiche auf den Markt kommen.

- **Windows 2000 Professional**, das Standard Desktop-Betriebssystem für den kommerziellen Anwendungsbereich.
- **Windows 2000 Server**, durch die Unterstützung von Server-Systemen mit bis zu zwei Prozessoren ist es ideal für kleine und mittelständische Unternehmen.

- **Windows 2000 Advanced Server** ist ein leistungsstarker Abteilungs- und Applikationsserver mit umfangreichen Netzwerk- und Internet-Diensten.
- **Windows 2000 Datacenter Server** unterstützt bis zu 16 Prozessoren und 64 GB Hauptspeicher sowie Server Clustering und Load Balancing. Diese Version wird wahrscheinlich erst einige Monate nach dem Release der obigen Versionen auf den Markt kommen.

## Top Features

- **Administrationsaufwand** für den Desktop wird im Vergleich zu bisherigen Windows-Systemen um mehr als die Hälfte reduziert. Das heißt mit anderen Worten, dass bisher in die Administration von Windows-Systemen mehr als doppelt so viel Zeit investiert werden musste, als eigentlich nötig hätte sein sollen und jetzt auch möglich wird.
- Windows 98 und Windows 2000 werden die gleiche grafische **Benutzeroberfläche** haben.
- Integration modernster (und oft Microsoft-spezifischer) **Internet-Technologie**.
- Microsoft behauptet, Windows 2000 gewährleiste **Datensicherheit**, hohe **Verfügbarkeit**, saubere **Netzwerkintegration** und Ausnutzung moderner Hardware. Vielleicht gelingt es ihnen einmal in dem Ausmaß, das Linux schon heute bietet.

In Windows 2000 werden Technologien integriert sein, die heute schon als Einzelanwendungen verfügbar sind. Ein Beispiel hierfür ist Microsoft **Windows NT Terminal Server Edition**. Dieses Produkt, das Sie heute als eigenständige Applikation kaufen müssen, wird in der Windows 2000 Server Familie als Service integriert sein..

Weitere schon heute verfügbare Technologien sind **Windows NT Load Balancing Services V2.2 (WLBS)**, **Microsoft Scripting Host**, **COM+** und **Microsoft Cluster Server (MSCS)**

## Consumer Windows for 2000

Microsoft will im **Jahr 2000** unter dem Namen „Consumer Windows for 2000“ eine weitere Windows-Version herausbringen, die noch auf der Technik von **Windows 98** basiert. Eigentlich hatte Microsoft geplant, kein neues Betriebssystem mehr auf den Markt zu bringen, das im Kern noch auf der veralteten DOS-Technologie beruht, sondern endlich ein Windows-System für Privatanwender, das auf der Windows NT-Technik aufbaut. Das Erscheinen dieser Consumer Edition von Windows 2000 wird sich laut *WINDOWS Magazine* zumindest bis zum Jahr 2001 verzögern.

## Windows 2000 Desktop

Der folgende Artikel stammt aus der Feder des Autoren-Teams Eric Tierling, Peter Monadjemi und Dirk Jarzyna. Alle drei sind bekannte IT-Experten, die seit vielen Jahren als Journalisten und Buchautoren arbeiten. Sie zählen zu den namhaften Kennern der Szene, wenn es um den Einsatz von Windows in Unternehmen geht. Diesen Artikel und weitere zu den Themen

- **Windows 2000 Setup und Migration**
- **Windows 2000 und Hardware**
- **Active Directory**

finden sie auf dem deutschen Web-Server von Microsoft:  
<http://www.eu.microsoft.com/germany/windows2000/>

## Referenzen

### Microsoft Deutschland:

Windows 2000

<http://www.eu.microsoft.com/germany/windows2000/>

Auswählen der besten Windows-Plattform aus Sicht der Unternehmen

<http://www.eu.microsoft.com/germany/nt5/merkmale/betriebssystem.htm>

Windows NT 5.0 Guide

<http://www.eu.microsoft.com/germany/nt5/serie/default.htm>

### WINDOWS Magazine – Windows 2000

[winmag.com/win2000/](http://winmag.com/win2000/)

Special Report from Tom Henderson: Get Ready for Windows 2000

[http://winmag.com/win2000/special\\_report/](http://winmag.com/win2000/special_report/)

# Desktop von Windows 2000

Durch seine enge Integration mit dem Internet Explorer 5.0 sorgen der Desktop von Windows 2000 einhergehend mit zahlreichen verbesserten und neuen Funktionen für eine spürbare Steigerung der Produktivität.

Gleich beim ersten Start von Windows 2000 fallen optische Unterschiede des Betriebssystems zu früheren Windows-Generationen auf. Bei der Tuchfühlung offenbaren sich dem Anwender noch viele weitere Features.

## Windows 98 Look-and-Feel

Vergleicht man Windows 2000 mit seinem unmittelbaren Vorgänger Windows NT 4.0, sticht ein wesentlicher Unterschied sofort ins Auge: die Benutzerschnittstelle des neuen Betriebssystems. Aufgrund der Integration des Internet Explorer 5.0 in die Arbeitsoberfläche verhält sich der Desktop eher wie ein Web-Browser. Microsoft bezeichnet diese Web-ähnliche Schnittstelle denn auch als Active Desktop.

Die enge Verwandtschaft mit dem Web-Browser erkennt der Anwender zum Beispiel daran, dass Objekte unterstrichen sind, die auf Mausclicks reagieren – genau wie mit Links versehene Objekte einer normalen Web-

Seite. In gleicher Art und Weise reagieren die Objekte der Windows-2000-Benutzerschnittstelle auf einen einfachen Mausclick. Das bedeutet, dass das einfache Anklicken eines Icons das Öffnen des entsprechenden Programms oder Dokuments zur Folge hat. Für Anwender, die direkt von Windows 95 auf Windows 2000 umsteigen, mag das zunächst gewöhnungsbedürftig erscheinen – nicht zuletzt deshalb, weil diese Charakteristik ein anderes Vorgehen zur Mehrfachselektion von Objekten (beispielsweise bei der Markierung mehrerer Einträge im Explorer) oder beim Umbenennen einer Datei erfordert. Anwender, die bereits mit Windows 98 vertraut sind, kennen dieses Vorgehen aber bereits. Die Praxis zeigt zudem, dass gerade Einsteiger das „Single-Click“-Verhalten der neuen Benutzerschnittstelle zu schätzen wissen, denn es stellt tatsächlich eine Vereinfachung dar und, hat man sich erst daran gewöhnt, beschleunigt den Umgang mit dem System.

Das trifft ebenfalls auf zusätzliche kleine Helferlein zu: Zur Taskleiste hat sich eine zusätzliche, direkt neben der Start-Schaltfläche angeordnete Symbolleiste gesellt. In der Standardkonfiguration beinhaltet diese sowohl bei Windows 98 als auch bei Windows 2000 die Schnellstart-Symbolleiste, die ihrerseits mit drei Icons umfasst:



Desktop, Outlook Express und Internet Explorer. Ein einfacher Klick auf das Desktop-Icon zaubert einen „sauberen“ Desktop hervor, indem sämtliche geöffneten Fenster automatisch minimiert werden. Wie bei anderen Schaltflächen auch genügt ein einfacher Mausklick auf eines der anderen Icons, um die entsprechenden Programme zu starten.

Weitere vordefinierte Symbolleisten lassen sich der Taskleiste hinzufügen:

- Adresse: Fügt ein Feld ein, in das der Anwender die Adressen von einer Web-Seiten eingeben kann.
- Links: Zeigt die im Internet Explorer konfigurierten Links an.
- Desktop: Stellt die auf dem Desktop vorhandenen Icons in der Taskleiste dar.

Dem Anwender steht es frei, sich selbst weitere Symbolleisten zu konfigurieren, um beispielsweise seine am häufigsten verwendeten Programme direkt aus der Taskleiste heraus aufrufen zu können.

Der vereinfachte Start von Applikationen ist nicht das einzige Resultat der engen Integration des Internet Explorer 5.0 mit dem Rest des Betriebssystems. Tatsächlich bietet Microsoft damit die echte Web-Integration für sämtliche Aktivitäten. In der einfachsten Form erlaubt der Active Desktop dem Anwender, sowohl Standard-Windows-Icons als auch HTML-Objekte direkt auf dem Desktop zu platzieren, was die Navigation deutlich vereinfacht. Somit besteht für den Anwender keine Notwendigkeit mehr, zunächst seinen Browser zu starten, um Web-Inhalte aus dem Intranet oder Internet abzurufen. Ein Zugriff ist sich vielmehr von nahezu jeder beliebigen Stelle aus möglich, sei es mit der Taskleiste, über den Desktop, aus dem Windows Explorer heraus oder in Applikationen. Web-Seiten, die der Anwender regelmäßig abrufen, kann er einfach zum Ordner „Favoriten“ hinzufügen. Wer es wünscht, kann sämtliche Ordner sehr einfach so konfigurieren, dass sie wie Web-Seiten aussehen und sich genau so verhalten. Ferner lässt sich eine beliebige – komplette – Web-Seite auf dem Desktop ablegen. Der Anwender hat damit zum Beispiel die Homepage seiner Abteilung permanent im Blick.

Augenscheinlich bedeutet es für den Anwender kaum noch einen Unterschied, ob er auf Informationen seiner lokalen Datenträger zugreift oder diese aus dem Intranet des Unternehmens bzw. über das Internet abrufen. Anwendern, die lieber auf die Vorzüge des neuen Desktop-Outfits verzichten möchten, offeriert Windows 2000 die Option, sämtliche Änderungen der Benutzerschnittstelle zu entfernen. Sie kehren damit zur vertrauten Oberfläche von Windows NT 4.0 zurück, so dass wieder Doppelklicks den Ton angeben.



Der Windows 2000-Desktop ist eng mit dem Internet Explorer 5.0 integriert

## Kompatibilität und Stabilität

Eine wichtige Frage dürfte die nach der Kompatibilität sein. Microsoft verfolgt die Intention, Windows 2000 Professionell zum Standard-Unternehmens-Desktop zu machen. Das setzt voraus, dass nahezu alle heute verfügbaren, wichtigen Applikationen vom neuen Betriebssystem unterstützt werden. Der Active Desktop stellt in Bezug auf die Kompatibilität mit sogenannten Legacy-Anwendungen kein besonders kritisches Element dar, denn die bei Windows NT 4.0 unter der Oberfläche existierenden Schnittstellen stehen auch bei Windows 2000 zur Verfügung. Weitere technologische Verbesserungen fließen als überarbeitete oder erweiterte Programmierschnittstellen in das neue Betriebssystem ein. Umfangreiche Tests gewährleisten, dass weit verbreitete Win32- und Win16-Applikationen möglichst reibungslos unter Windows 2000 laufen.

Treiber bilden ein weiteres wesentliches Element zur Nutzung neuer Features. Nachdem Windows NT 4.0 gegenüber seinem kleinen Bruder Windows 95 von vielen Anbietern lange Zeit regelrecht vernachlässigt wurde, hat sich in den vergangenen Monaten bereits für das Vierer-Release von Windows NT die Situation deutlich gebessert. Für den Nachfolger Windows 2000 verspricht Microsoft, wesentlich mehr Geräte zu unterstützen – entweder gleich out-of-the-box oder in Kooperation mit Hardware-Anbietern. Aktuell berücksichtigt Windows 2000 bereits mehr als 6.500 Geräte.

Berichte in diversen Medien und eigene Erfahrungen zeigen, dass Microsoft aber noch manches zu tun hat, um für die erforderliche Kompatibilität zu sorgen, denn mit den bislang kursierenden (frühen) Betas laufen noch nicht alle Anwendungen zufriedenstellend. Die Ursache dafür

ist aber vor allem im Entwicklungs-Charakter dieser Versionen zu suchen. Aus genau demselben Grund macht es derzeit nur wenig Sinn, das noch mit Debug-Code versehene Betriebssystem Performance-Messungen für dieses und jenes Feature zu unterziehen. Bis zum Erscheinen der öffentlichen Beta 3 im Frühjahr und bei der endgültigen Version dürfte das Gros der Kompatibilitätsprobleme ausgemerzt sein, denn einen groben Faux-Pas kann sich heutzutage kein Hersteller mehr leisten.

## Einfache Installation von Anwendungen

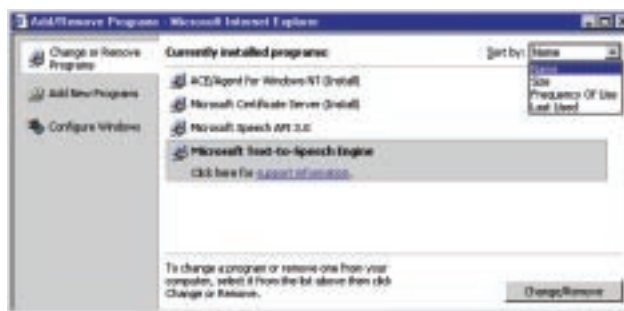
Vor dem Preis, eine funktionstüchtige Applikation auf dem Desktop vorzufinden, haben die Götter den Schweiß gesetzt. In der Vergangenheit haben manche Anwender tatsächlich so einigen Schweiß verlieren können bei Versuchen, eine Applikation ordnungsgemäß zu installieren – und mehr noch, wenn es darum ging, eine Applikation wieder vollständig vom Computer zu entfernen. Installations- und Deinstallationsprobleme lassen sich zwar nicht vollständig beseitigen, doch wartet Windows 2000 von Hause aus mit einigen Erleichterungen auf. Das neue Betriebssystem beinhaltet beispielsweise einen verbesserten und mehr informativen Dialog zum Hinzufügen und Entfernen von Programmen (engl. „Add/Remove Programs“, kurz „ARP“). Die in der Systemsteuerung untergebrachte Komponente gestattet dem Anwender zunächst einmal, genau anzugeben, von welchem Ort aus die neue Applikation zu installieren ist. Zur Auswahl stehen jetzt CD oder Diskette, das Internet und das Unternehmensnetzwerk. Die neue Schnittstelle erlaubt außerdem einen besseren Umgang mit installierten Applikationen etwa mit Hilfe von Sortieroptionen zur Anzeige der installierten oder verfügbaren Applikationen nach Kategorien wie Größe, Nutzungshäufigkeit und Datum der letzten Verwendung. Nach der Installation einer Applikation bietet der neue Windows-Installer Optionen zur nachträglichen Installation weiterer Programmkomponenten, die bei der ursprünglichen Installation noch nicht mit installiert wurden, und zur Entfernung einzelner, nicht mehr benötigter Komponenten. Natürlich gestattet er auch die Deinstallation einer kompletten Anwendung.

Eine deutliche Verbesserung gegenüber entsprechenden Installations-Hilfsprogrammen älterer Windows-Generationen: Erkennen Anwender, dass eine Applikation nicht mehr korrekt zu arbeiten scheint, gestattet ARP eine Reparatur der jeweiligen Installation. ARP ist dabei speziell für Applikationen optimiert, die die neue Windows-Installer-Technologie verwenden, um Installationen, De-installationen, Änderungen und Reparaturen wesentlich zu vereinfachen.

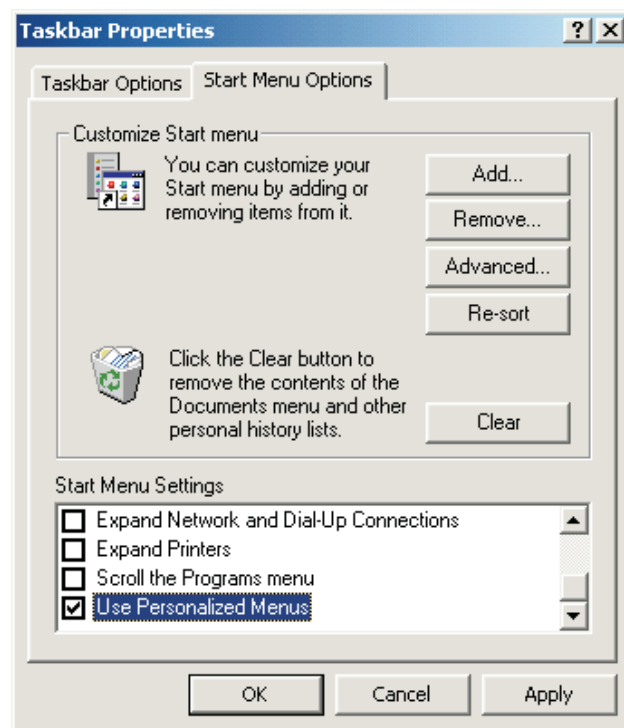
Schlägt die Installation einer neuen Applikation einmal fehl, kann sich der Anwender darauf verlassen, dass sämtliche Änderungen, die der Windows-Installer bis zum Zeitpunkt des Fehlers durchgeführt hat, wieder rückgängig gemacht werden oder dass ein erneuter Installationsversuch genau am Fehlerpunkt beginnt. Die Überwachung der Originalinstallation vereinfacht die Durchführung von Komponenten-Updates.

Der Windows-Installer erzeugt eine kompakte relationale Datenbank in Form einer \*.MSI-Datei, in der sich alle zum Management einer Applikation erforderli-

chen Informationen befinden. Diese Datenbank beinhaltet auch Angaben über die einzelnen Komponenten einer Applikation und darüber, welche Dateien vorhanden sein müssen, damit ein bestimmtes Feature der Applikation funktioniert. Auf diese Weise macht die Windows-Installer-Technologie Schluss zum Beispiel mit DLL-Konflikten, indem sie DLLs in ihre eigenen Verzeichnisse kopiert und so dafür Sorge trägt, dass sich beschädigte Applikationen selbst reparieren. Im Rahmen dieser sogenannten „Selbstheilung“ werden Schlüsseldateien bei jedem Applikationsstart überprüft und gegebenenfalls automatisch ersetzt. Phänomene, dass sich Anwendungen plötzlich nicht mehr starten lassen und das Rätselraten beginnt, welche DLLs dafür verantwortlich sind, dürften damit eine deutliche Reduzierung erfahren.



Der neue Windows-Installer vereinfacht die Installation und Deinstallation von Applikationen deutlich

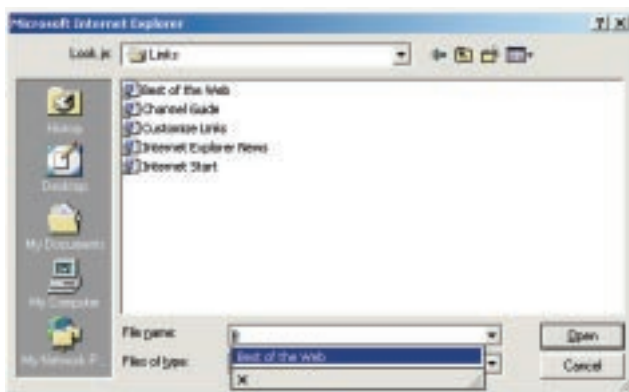


Die sogenannte Personalisierung von Menüs sorgt dafür, dass der Anwender vor allem die für ihn wichtigen Einträge sieht

## Verwaltung von Dokumenten

Windows 2000 bietet viele Verbesserungen für die Arbeit mit beliebigen Dokumenten und Applikationen. Das Feature „Personalisierte Menüs“ (engl. „Personalized Menus“) sorgt beispielsweise für ein aufgeräumtes Startmenü, indem es – auf Wunsch – nur die Einträge darstellt, die der jeweilige Anwender am häufigsten nutzt. Alle anderen Einträge für Programme, Verknüpfungen und Dateien stehen aber sofort wieder zur Verfügung, sobald der Anwender sie benötigt. Die Einträge in den einzelnen Menüs ändern sich automatisch, je nach Häufigkeit der Verwendung einzelner Elemente.

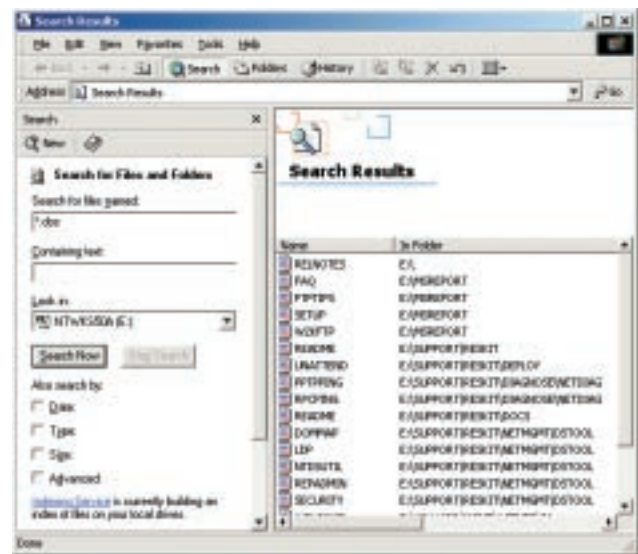
Der neu gestaltete, leistungsfähigere Öffnen-Dialog bietet viele Optionen zum leichten Wiederauffinden von Ordnern und Dateien. Sofort verfügbar sind zum Beispiel die zuletzt verwendeten Dokumente, auf dem Desktop abgelegte Dokumente und Dokumente innerhalb der persönlichen Netzwerkumgebung. Das „AutoComplete“-Feld spart Zeit beim Eintippen von Ordner- und Dateinamen, da es sich kürzlich eingegebene Worte merkt und diese bei einer erneuten Eingabe automatisch vervollständigt.



Der Öffnen-Dialog bietet direkten Zugriff unter anderem auf die zuletzt verwendeten Dokumente und eigene Dokumente

Windows 2000 gestattet eine Konfiguration, in der Applikationen ihre Daten in der Voreinstellung im Ordner „Eigene Dokumente“ (engl. „My Documents“) speichern. Das vereinfacht es natürlich, Dateien zu einem späteren Zeitpunkt wiederzufinden und hilft mit, das Dateisystem sauber zu halten. Hinzugesellt hat sich auch der Ordner „Eigene Bilder“ (engl. „My Pictures“). Der steigenden Bedeutung elektronischer Grafikbearbeitung Rechnung tragend, lassen sich dort von digitalen Kameras oder Scannern erzeugte Bilder übersichtlich ablegen. Bei der Anzeige dieses Ordners im Explorer oder im Öffnen-Dialog ist eine grafische Darstellung der einzelnen Dateien im Kleinformat (engl. „Thumbnails“), während die Schnellansicht über „Image-Preview“ mit Funktionen zum schnellen Zoomen, Drehen und Drucken des Bildes vor dem Aufruf der Datei aufwartet.

Durch die enge Integration des Windows 2000-Desktops mit dem Netzwerk des Unternehmens, dem Intranet sowie dem Internet gestaltet sich auch das Auffinden von Informationen wesentlich flüssiger. Eine Suche mit Hilfe des neuen Suchen-Dialogs über das Startmenü, den Ordner „Arbeitsplatz“ und im Explorer kann auf Wunsch des Anwenders beispielsweise auch das persönliche Adressbuch sowie Internet-Such-Engines in Anspruch nehmen. Dank der im Hintergrund vom optionalen Indexing-Dienstes vorgenommenen Indizierung läuft das Finden von Informationen überdies in vielen Fällen schneller ab als bei früheren Windows-Versionen.



Der Suchen-Dialog hat nicht nur ein Facelifting erfahren, sondern kann jetzt deutlich mehr als bei Windows NT 4.0

## Fazit

Bereits nach den ersten Berührungen mit dem neuen Betriebssystem wird deutlich, dass Microsoft vielfältige Anstrengungen unternommen hat, den Umgang mit Windows 2000 und darüber erreichbaren Ressourcen merklich zu vereinfachen. Anwendern gehen die im Arbeitsalltag anfallenden Aufgaben leichter von der Hand, was der Effizienz zugute kommt. Für viele Unternehmen dürfte Windows 2000 daher zum Kreis der Favoriten bei der Auswahl einer produktiven Desktop-Plattform zählen

Copyright-Informationen von Microsoft für den obigen Artikel: <http://www.microsoft.com/germany/misc/copyright.htm>

# 10 Jahre Wählleitungen

Johann Kainrath

Dieser Artikel gibt einen Überblick von den Anfängen des Wählleitungszugangs zum TUNET bis zu den aktuellen Ausbauten.

## *bis 1989*

### **Wählleitungen bereits als wichtiges Service erkannt**

Der Zugang zum TUNET von externen Bereichen über Modemtechnologie wurde bereits in den Anfängen von TUNET als wichtiges Service erkannt und als solcher unterstützt. Bereits 1986 wurde vom damaligen IEZ (Interuniversitäres EDV-Zentrum) ein Wählleitungszugang mit Geschwindigkeiten von 300 Bit/s zu Services des Rechenzentrums über das PACX betrieben. 1989 stellte das EDV-Zentrum der TU Wien, Abteilung Digitalrechenanlage, den Benutzern 5 Zugänge (300 Bit/s asynchron V.21, 1200/2400 Bit/s asynchron V.22/V.22bis) über Wählleitungen zur Verfügung. Wie sich herauskristallisieren sollte, wurde damit ein Dauerbrenner der Ausbauplanung unter dem Titel „Erweiterung des Wählleitungsservices“ geschaffen.

## *1990*

### **zwei Serien, 9600Bit/s!**

1990 konnte auf 2 der 5 Nummern bereits mit einer Geschwindigkeit von 9600 Bit/s (V.32) vom PACX ins TUNET (cdcnet) interaktiv eingewählt werden. Damals gab es über eine Post-Schaltung zwei Serien mit 3 bzw. 2 Nummern.

## *1991*

### **Umstellung PACX auf Terminalserver**

Als 1991 die Wählleitungen vom bestehenden PACX System auf einen Terminalserver umgestellt wurden, zeigten sich in dieser Phase viele Probleme mit der Instabilität der verwendeten Modems und des erstmals eingesetzten Terminalservers. Auch im Zusammenhang mit dem Benutzerverhalten gab es Probleme, da zu diesem Zeitpunkt die Authentifikation ausschließlich durch das angegebene Passwort und nicht durch eine Kombination aus Usernamen und Passwort bestand.

## *1992*

### **analoge Einzelanschlüsse, Validierung mit Usernamen/Passwort**

Im Jahr 1992 wurden 5 analoge Einzel-Telefonanschlüsse (in zwei Serien organisiert) betrieben. Dabei standen 5 Stück Einzelmodems vom Typ Octocom 8396 in Verwendung (9600 Bit/s mit Fehlerkorrektur und Datenkompressions-Features). Da der bis zu diesem Zeitpunkt eingesetzte Terminalserver vom Typ Bridge Communications nicht ausreichend Sicherheit bot, wurde ein neues Gerät des Herstellers Cisco vom Typ CS516 angeschafft. Der Zugang erlaubte nunmehr die Validierung mit Usernamen und einem zugehörigen Passwort. Des Weiteren bot dieser erstmals die Möglichkeit, nicht nur interaktiv sondern Verbindungen über die Protokolle SLIP und PPP aufzubauen. Eine Ausbaubarkeit der Wählleitungszugänge war bis zu 16 asynchronen Anschlüssen gegeben, denn für 1993 war bereits ein weiterer Ausbau vorgesehen.

Bereits für 1992 war ein Pilotversuch im Hinblick auf einen ISDN-Zugang zur Verbesserung der Wählleitungen geplant. Wie sich herausstellen sollte, konnte von der damaligen Post jedoch erst Ende 1994 eine erste Installation erfolgen. Grund dafür war, dass der Versorgungsgrad mit ISDN-Anschlüssen der Post im Jahr 1992 noch derart gering war, dass der Einsatz an Arbeitszeit und Finanzmitteln nicht zu rechtfertigen gewesen wäre. Verfügbare Geräte waren außerdem zum Teil noch im Prototyp-Stadium.

## *1993/1994*

### **einzelne Modems, SLIP/PPP, V32bis, ISDN, Mail/News/Info-Service**

In den Jahren 1993 und 1994 war ein besonderer Aktivitätsschwerpunkt in der Abteilung Kommunikation des EDV-Zentrums die Erweiterung des Modemzugangs. Da in diesem Zeitraum die Einrichtung des Mail/News/Info-

Services für etwa 5000 Studierende erfolgte, war naturgemäß der Zugang zum TUNET über Wählleitungen eine der Säulen des Konzeptes. Beispielsweise wurden dafür 1994 85.000.- öS für eine Erweiterung/Terminalserver für Modemanschlüsse sowie im Zuge des normalen Netzausbaus (weitere Terminalserver, ISDN-Anschluss) 82.000.- öS investiert. 1993 wurden die 3 Einzelanschlüsse des ZWK (Zentrum für wissenschaftliche Kommunikation, Betreiber des damaligen AConet) in das bestehende Zugangs-Service integriert, und 1994 wurden 4 weitere Außenanschlüsse hinzugenommen. Somit standen insgesamt 12 Modemzugänge zur Verfügung.

Gegen Ende 1994 wurde auch ein ISDN-Basisanschluss von der Post hergestellt (Kapazität 2 x 64kBit/s; 2 B-Kanäle), der in das Dialin-Service zu integrieren war.

Aus den bisherigen Erfahrungen war klar, dass eine weitere Aufstockung alsbald notwendig werden würde (nicht nur um die projektierten 3 Anschlüsse, sondern auf etwa 30 gleichzeitige Zugänge).

Der Zugang über Wählleitungen vom Heimarbeitsplatz, insbesondere im Bereich der Studierenden, gewann immer mehr Bedeutung.

Erstmals ermöglichte der neu angeschaffte Terminalserver nicht mehr nur den interaktiven Zugang über Telnet, sondern mittels SLIP/PPP quasi direkt als Internet-Rechner arbeiten zu können.

SLIP (Serial Line Internet Protocol) erlaubte standardisiert den Transport der IP-Daten über eine serielle Leitung anhand einer sehr einfachen Paket-Struktur. Anstatt sich mit dem Remote Host die Kommunikationsparameter auszuhandeln, verwendete SLIP vordefinierte Werte. Dadurch war SLIP vom Benutzer einfacher aufzusetzen bzw. im Fehlerfall leichter zu analysieren. PPP (Point-to-Point Protocol) hingegen handelt sich beim Verbindungsaufbau die verschiedensten Protokoll-Optionen aus und packt die IP-Daten zur Übertragung über die serielle Leitung in eine detaillierte Paket-Struktur ein.

SLIP und PPP Software (kommerziell und Public Domain) existierte damals bereits für die meisten Betriebssysteme bzw. Rechnerplattformen. Nachdem eine SLIP bzw. PPP Verbindung aufgebaut ist, können via Modemverbindung alle TCP/IP-Netzdienste (telnet, ftp, mail, etc.) in gleicher Weise wie mit direktem Netzwerkanschluss verwendet werden.

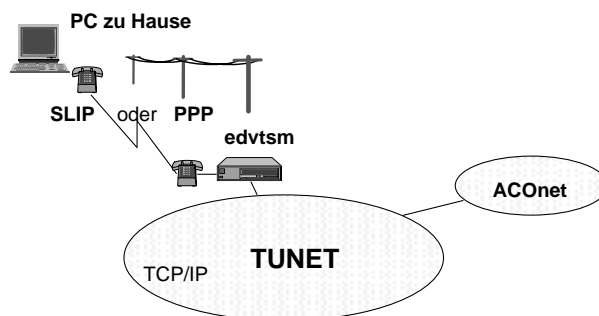
Prinzipiell waren durch diese Einführung

- Filetransfer und Drucken von Dateien,
- Senden und Empfangen von Electronic Mail,
- Einloggen in einen Remote Host mit Terminalemulatoren,
- Ausführen anderer Netzwerkprogramme erst sinnvoll möglich.

Allerdings waren wegen der relativ langsamen Übertragungsgeschwindigkeit (Ethernet: 10.000.000 Bit/s, Modem ca. 14.000 Bit/s) nicht alle Dienste wirklich sinnvoll. Programme im Grafikmodus (z.B. X-Window Oberfläche) konnten nicht vernünftig verwendet werden. Sehr wohl Sinn machten E-Mail-Anwendungen (nur Text-

Dateien) oder Übertragen kleinerer Files mittels ftp (Übertragungsrate ca. 1.000 Byte/sec bei Verwendung eines Modems mit einer Übertragungsrate von 14.400 Bit/s).

Hier ein Bild der damaligen Realisierung im TUNET



Voraussetzungen für die Verwendung dieser neuen Service-Form waren ein PC / eine Workstation mit einem asynchronen Modem (eingebaut oder extern), ein gültiger Account für den Terminalserver (Ansuchen Kommunikations-Services, Wählleitungszugang zum TUNET) sowie SLIP bzw. PPP Software für den Rechner.

Dadurch war die intensive Beratung der Benutzer in Bezug auf Konfigurationseinstellungen ihrer verwendeten Software erforderlich. Auch konnte bereits statt manuellem Login der Loginvorgang mit Scripts automatisiert werden. Hier wurden vom EDV-Zentrum entsprechende Vorlagen zur Verfügung gestellt bzw. entsprechende Informationen in den relevanten Medien veröffentlicht.

Trotz anfänglicher Vorteile von SLIP setzte sich mit zunehmender Verwendung die PPP-Variante beim Dialin-Zugang durch, welches durch einen entsprechenden Artikel in der Informationszeitschrift PIPELINE des EDV-Zentrums näher erklärt wurde.

Einer der wesentlichen Vorteile von PPP lag in der Möglichkeit, dynamische IP-Adressen zwischen den (beiden) Kommunikationspartnern zu verwenden.

PPP wurde auch bereits von an der TU Wien gängigen Betriebssystemen (Unix, Linux, Windows und MacOS) unterstützt, wobei vom EDV-Zentrum neben Empfehlungen für einzusetzende Software auch entsprechende Konfigurationsvorlagen bereitgestellt wurden.

So etwa wurde neben einer im Rahmen der Campuslizenz verfügbaren PC/TCP Software für DOS/Windows auch die Trumpet Winsock für PCs eingesetzt.

Ende 1994 wurden im Rahmen dieses EDV-Zentrums-Services Modem-Übertragungsnormen bis maximal CCITT V32bis (14400 bps) mit MNP4 und V.42 Fehlerkorrektur bzw. MNP5 und V.42bis Datenkompression unterstützt. Das bedeutete eine Geschwindigkeit von 38400 Bit/s zwischen Modem und Terminalserver.

1995

## Mail/News/Info Service für Studierende, Rackmount Modem Lösung

Hohe Anforderungen an das Wählleitungsservice kennzeichneten das Jahr 1995. Gründe waren das sehr gut angenommene Mail/News/Info-Service für Studierende. Viele Studierende wollten und haben dieses Service auch von zu Hause aus genutzt, wodurch die Arbeitsplätze an der TU Wien entlastet wurden. Auch die Mitarbeiter der TU Wien hatten sich verstärkt Modems beschafft, sodass auch von dieser Seite höhere Anforderungen gestellt wurden.

Im Herbst 1994 wurde von der ITU die neue V.34 Norm, die Datenraten (ohne Kompression) von bis zu 28.800 Bit/s über analoge Modems bietet, beschlossen. Die ersten Produkte waren Ende 1994 verfügbar. Der Wunsch der Benutzer nach dieser neuen Technologie wurde daher immer stärker. Viele Benutzer haben beim Kauf eines Modems sinnvollerweise sofort ein – nicht unbedingt viel teureres – V.34 Modem angeschafft. Auf Grund dieser gestiegenen Anforderungen wurde daher ein Ausbau des Wählleitungszugangs auf ca. 30 Anschlüsse mit V.34 Modems geplant.

Da jedoch absehbar war, dass dieses Service sehr viele Personalressourcen bei der Betreuung (Lokalisierung und Behebung von Problemen, Benutzeranfragen) beanspruchen würde, wurde überlegt, das gesamte Service an einen Service-Provider gemeinsam mit anderen Wiener Universitäten (UNI-Wien, WU-Wien) „outzusourcen“. Diese Idee wurde jedoch wegen der relativ hohen Kosten, die bei Gesprächen mit Service-Providern genannt wurden, verworfen.

Zur Erreichung einer entsprechenden Stabilität bei der großen Anzahl von Anschlüssen sollten nicht wie bisher einzelne Modems eingesetzt werden, sondern eine kompakte (Rackmount) Variante (teurere Investitionen, aber billigerer Betreuungsaufwand). Ein weiterer Aspekt bei der Neukonzeption war eine einfachere und kompaktere Verbindung mit der Post und die Zusammenführung der analogen und ISDN-Zugänge. Aus diesen Gründen sollte die neue Lösung über ISDN-Multi-Anschlüsse (30 gleichzeitige Verbindungen über eine Leitung) realisiert werden.

Um die ärgsten Engpässe zu beheben, wurde am Beginn des Jahres eine provisorische Lösung mit einzelnen V.34 Modems installiert. Als weiterer Zwischenschritt wurde der Wählleitungszugang am 14. Juni 1995 um 5 weitere Anschlüsse ausgebaut. Seit 9. Mai waren auf allen Anschlüssen die Protokolle SLIP und PPP konfiguriert. Im Sommer wurde dann eine beschränkte Ausschreibung für ein Rackmount Modem durchgeführt. Dieses System wurde am 23. Oktober 1995 in Betrieb genommen. Ab Anfang Oktober wurden allen Benutzern mit einer gültigen Berechtigung auf einem Fachbereichsrechner (und in der Folge dann auch für weitere zentrale Server wie die Applikationsserver) automatisch eine Berechtigung für die Wählleitungen erteilt.

Um die Anbindung an die Post effizient und flexibel zu realisieren, wurde bei der Post ein ISDN-Multi-

Anschluss bestellt und eine kleine ISDN-Nebenstellenanlage beschafft, die die Umsetzung zwischen dem ISDN Multi-Anschluss und den analogen Modemeingängen durchzuführen hatte (im Jahr 1995 waren noch keine einsetzbaren Produkte, die einen direkten Anschluss des ISDN-Multi-Anschlusses an ein Modemsystem bieten, verfügbar). Der ISDN-Multi-Anschluss wurde von der Post erst sehr verspätet installiert, daher konnte die Erweiterung auf insgesamt 30 Wählleitungszugänge erst am 2. Februar 1996 in Betrieb genommen werden. Schon zu diesem Zeitpunkt war auf Grund der Entwicklung abzusehen, dass auch 1996 ein Ausbau des Services erforderlich war.

Da die Realisierung des ISDN-Zugangs über die vorgesehene SUN von Seiten der Validierung und einem einheitlichen Bild des Zugangs große Probleme bereitete, wurde der ISDN-Zugang vorerst über zwei einzelne ISDN-Terminaladapter in Betrieb genommen. Diese wurden im Zuge der Umstellung auf den ISDN-Multi-Anschluss auch über die Nebenstellenanlage geführt. Dadurch konnte eine einheitliche Hauptnummer für den Zugang zum TUNET realisiert werden. Die Services des analogen bzw. des ISDN-Zugangs werden nur durch eine unterschiedliche Durchwahl unterschieden.

Ende 1995 unterstützten alle Anschlüsse den V.34-Standard, mit dem eine maximale Datenrate von bis zu 28.800 Bit/s auf der Wählleitung erzielt werden konnte (bisher maximal 14.400 Bit/s). Die damals aktuelle Konfiguration der Wählleitungen gestaltete sich in drei Serien mit zweimal 5 bzw. einmal 2 Nummern).

Hier ein interessanter Auszug aus einer Benutzerinformation:

*„... Es kommt immer wieder vor, dass Modems der Serien 1 (5874692) und 3 (5867578) einfach hängen bleiben und nur durch Aus / Einschalten wieder in einen operablen Zustand gebracht werden können. Daher werden alle Modems dieser Serien ab sofort durch eine Zeitschaltung um ca. 4 Uhr Früh kurz aus / eingeschalten. Damit soll die Verfügbarkeit des Wählleitungsservices weiter verbessert werden.“*

Erwähnenswert ist die gegen Ende 1995 einsetzende Verbreitung von Windows 95 auf Home-Computern und damit der verstärkte Bedarf an Benutzerinformationen. Diesem wurde durch den beliebten Artikel „Mit PPP und Windows 95 ins TUNET“ in der PIPELINE Rechnung getragen [1].

1996

## „Internet-Boom“, ISDN Multianschluss, Cisco Terminalserver

Neben den selben Faktoren wie 1995 trug 1996 auch der allgemeine „Internet-Boom“ zu weiter steigendem Ressourcenbedarf bei.

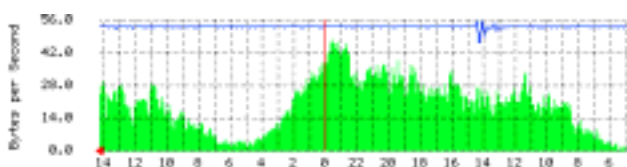
Nachdem am 2. Februar ein ISDN-Multi-Anschluss mit insgesamt 30 Kanälen in Betrieb genommen wurde (das bedeutete zu dieser Zeit fast ein Verdoppeln der Kapazität), war bereits in relativ kurzer Zeit absehbar,

dass der Bedarf weiterhin steigend ist. Es wurde daher ein zweiter ISDN-Multi-Anschluss mit 30 weiteren Kanälen bestellt und von der Post am 19. Juli 1996 installiert.

Auf Grund der existierenden Hardware konnten vorerst nur insgesamt 45 Kanäle in Betrieb genommen werden. Damit wurden kurzfristig Engpässe für die nächste Zeit behoben. Basis für die volle Verfügbarkeit der Leitungskapazität und deren weiterer Ausbau war die Investition in weitere Hardware. Um die Einheitlichkeit und Kontinuität des Benutzer-Interfaces zu erhalten, wurde ein Terminalserver von Cisco (Type AS5200) mit zwei integrierten ISDN-Multi-Anschlüssen und integrierten Analog-Modems nach einem längerem Benutzertestbetrieb beschafft. Damit konnten nun erstmals sowohl Calls von Benutzern mit ISDN-Anschlüssen (ISDN-Karten, ...) als auch analoge Modem Calls in einem Gerät abgewickelt werden – eine sehr kompakte Realisierung des Wählleitungszugangs. Die ISDN-Zugänge waren nun in der Anzahl nur mehr durch die Gesamtanzahl beschränkt (nicht wie bisher mit 2) und gleichzeitig war der ISDN Zugang nun mittels Synchronous PPP realisiert – eine wesentlich schnellere und komfortablere Methode des Verbindungsaufbaus.

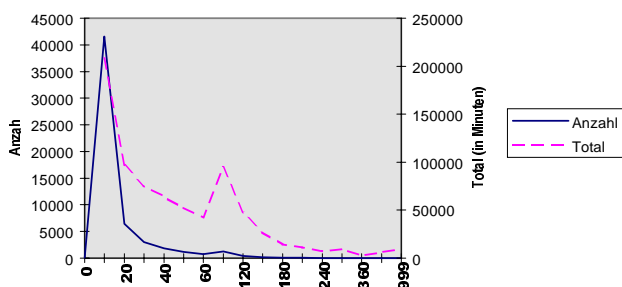
Die neue Hardware wurde nach einem erfolgreichen Testbetrieb am 11. Dezember in Betrieb genommen. Seit diesem Zeitpunkt standen dann max. 52 analoge, gesamt max. 60 Kanäle zur Verfügung (mit der vollständigen Lieferung und Inbetriebnahme der neuen Hardware Anfang 1997 alle 60 Kanäle). Durch die neue Realisierung erfolgte auch eine Änderung der Telefonnummer(n) des Wählleitungszugangs.

Das folgende Bild zeigt die typische Verteilung der Anzahl der belegten Wählleitungskanäle an einem Wochentag. Bytes per Second steht für die Anzahl der Kanäle. Die obere Linie gibt die maximale Anzahl der verfügbaren Kanäle an.



Das nächste Bild zeigt die Verteilung der Dauer einer Session (Anzahl, gesamte Dauer in dieser Kategorie). Es ist klar ersichtlich, dass 73% aller Sessions weniger als 10 Minuten dauern. 90% aller Sessions dauern maximal 30 Minuten.

Connect-Zeit Verteilung



## 1997 „Online-Tarif“, V.34+, K56Flex

Da 1997 der Zugang zum TUNET über Telefonleitungen sowohl aus Gesichtspunkten der Forschung und Lehre als auch als Entlastung der vom EDV-Zentrum betriebenen Benutzerarbeitsplätze hohe Priorität hatte, bestand Handlungsbedarf sowohl beim Ausbau aus Sicht der Performance als auch bei der Anzahl verfügbarer Leitungen. So wurden als erster Schritt am 5. Februar 1997 auf allen Modems erstmals auch die Geschwindigkeiten 31,200 Bit/s und 33,600 Bit/s nach ITU-T Standard V.34 Annex 12 (allgemein bekannt unter V.34+) unterstützt. Aus technischer Sicht wurde am 20. März 1997 eine kleine Verbesserung vorgenommen, denn der Wählleitungszugang wurde von 53 auf 60 gleichzeitig mögliche Verbindungen aufgestockt. Am 7. April 1997 wurde eine tiefgreifende Änderung vorgenommen. Der IP-Adressbereich wurde aus administrativen und technischen Gründen auf das Netz 128.131.35.0 umgestellt, ebenso eine eigene Subdomain eingeführt. Beim ISDN erfolgte eine Änderung der Zugangsprotokolle (Einstellung des Zuganges über ISDN im asynchronous Mode (V.110, X.75, ...); Zugang nur mehr mittels ISDN über Synchronous PPP (manchmal auch als HDLC bezeichnet) und Validierung mit PAP). Am 27. Mai 1997 erfolgte der nächste Schritt, nämlich die Inbetriebnahme eines weiteren ISDN-Multi-Anschlusses (PRI) mit 30 Kanälen. Somit standen ab diesem Zeitpunkt insgesamt 90 gleichzeitige Wählleitungszugänge den Benutzern zur Verfügung.

Ein weiterer Meilenstein war ab 1. November 1997 die Möglichkeit zur Inanspruchnahme des günstigen „Online-Tarifs“ für die TU Wien und somit seine Benutzer unter der Telefonnummer 07189 1 5893. Dadurch konnte einerseits für die Benutzer ein kostengünstigerer Zugang (der Online-Tarif brachte in Summe eine Kostenreduktion auf Benutzerseite von ca. 50 %) geboten werden, für das EDV-Zentrum (stellvertretend für die TU Wien) als „Provider der TU Wien“ brachte dies jedoch erhebliche Probleme im Hinblick auf nicht vorhandene Ressourcen an gleichzeitig verfügbaren Zugängen (hauptsächlich in der Zeit von 18 Uhr bis 2 Uhr Früh; siehe Abbildung: *Aktive Terminal Server-Leitungen*) sowie Hardware im betroffenen Access-Bereich (Modems im Terminalserver).

Daily' Graph (5 Minute Average)



Aktive Terminal Server-Leitungen

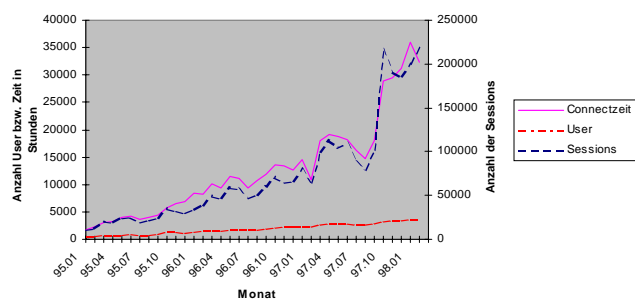
Die dadurch dringend notwendige Bestellung eines weiteren Multi-Anschlusses erfolgte erst zu diesem Zeitpunkt, da die Frage, ob der Online-Tarif überhaupt bzw. dann auch für die Universitäten möglich sein würde, erst kurz vor dessen Einführung / Inbetriebnahme von der PTA entschieden wurde. Außerdem war auf Grund der Auslastungszahlen sowie durchgeführter Modellrechnungen eine Reserve von ca. 30 Kanälen vorhanden.

Neben der zahlenmäßigen Aufstockung wurde auch ein schnellerer Modemzugang gefordert, daher wurden Anfang November 1997 die Modems auf Geschwindigkeiten bis 56 kBit/s aufgerüstet (K56Flex).

Wie aus diesem intensiven Ausbauprogramm ersichtlich, hat die Durchführung von Software Upgrades sowie Tests, Konfigurationsänderungen, Benutzerberatungen, Fehleranalyse und Fehlerbehebung dieses für die TU Wien sehr wichtigen Services viel Arbeitskapazität gebunden. Dieser Aufwand sollte sich, wie sich leider später herausstellte, durch den bereits bestellten weiteren Ausbau (zwei zusätzliche PRI Anschlüsse, ein weiterer Terminalserver) nicht verringern. Vor allem die Koordination mit der PTA war oft ein schwieriges Unterfangen.

In der folgenden Grafik ist die Entwicklung der Verwendung der Wählleitungen in den Jahren 1995-97 dargestellt. Neben den Berechtigungen über die Studenten-Server und die zentralen Server haben ca. 400 Benutzer eine explizite Berechtigung. Etwa 90% der tatsächlichen Sessions stammen von Studierenden im Zuge des Internet-Services. Pro aktivem Modem kann man mit ca. 10 kBit/s ankommenden (download) und ca. 1,4 kBit/s abgehenden (upload) Verkehr rechnen. Zu beachten ist, dass ein Großteil dieses Verkehrs national bzw. international ist und daher die externe Anbindung der TU Wien entsprechend ausgelegt sein muss. 90% aller Verbindungen dauern kürzer als 30 Minuten. Vom Gesichtspunkt der Auslastung der Wählleitungen ist das Benutzerverhalten sehr ungünstig (unter anderem durch die Tarifgestaltung der PTA hervorgerufen). Während tagsüber maximal 30 bis 40 Benutzer gleichzeitig aktiv sind, steigt die Auslastung in der Zeit von 18 bis ca. 1 Uhr auf bis zu 100%. Am Wochenende ist die Auslastung den ganzen Tag über (ab ca. 10 Uhr) sehr hoch, die Spitzen am Abend sind dafür geringer.

Verwendung des Wählleitungszugangs



Ende 1997 verfügte der Wählleitungszugang somit über 3 Multi-Anschlüsse mit insgesamt 90 gleichzeitigen Wählleitungszugängen. Ein weiterer Anschluss war bestellt.

## 1998 weitere ISDN-Multi-Anschlüsse, neue Terminalserver, V.90

Um die weitere Entlastung der vom EDV-Zentrum betriebenen Benutzerarbeitsplätze zu garantieren sowie aus Gesichtspunkten der Forschung und Lehre, bestand natürlich ein Ausbau der Wählleitungszugänge Handlungs-

bedarf. Die stetig steigende Anzahl von Wählleitungsbenutzern bedingt durch die Studentenzahlen mit Heim-PCs erforderte auch 1998 den kontinuierlichen Ausbau an Zugangsleitungen für Benutzer von analogen Modems bzw. ISDN. Natürlich trug dabei auch der kostengünstige Online-Tarif für die Benutzer eine wesentliche Rolle.

Daher wurde am 6. 2. 1998 von der PTA ein weiterer Multi-ISDN-Anschluss (PRI = Primary Rate Interface) in Betrieb genommen. Es standen nun insgesamt 120 gleichzeitige Wählleitungskanäle unter den unveränderten Telefonnummern 01/58932 (Normaltarif) bzw. 07189 1 5893 (Online-Tarif) zur Verfügung. Zu diesem Zeitpunkt war auf allen Kanälen der Zugang über analoge Modems bis 56kbit/s (56KFlex Variante) bzw. ISDN möglich.

Aus Kapazitätsgründen war jedoch nach kurzem Zeitraum am 10. 3. 1998 ein weiterer Ausbau um 30 Kanäle (ein PRI) auf 150 gleichzeitige Kanäle notwendig. Bereits am 7. 5. 1998 erfolgte die weitere Aufstockung mit einem PRI auf 180 Leitungen.

Aufgrund technischer und organisatorischer Gesichtspunkte wurde im Rahmen eines Netzwartungstages am Montag, dem 8. Juni 1998 eine Änderung des IP-Adressbereichs für den Wählleitungszugang vorgenommen (Übersiedlung in das Class-C-Netz 192.35.243.0). Mit Beginn des Wintersemesters wurde nach vielen Tests auch der neue ITU-T Modemstandard V.90 zuerst auf einigen Leitungen in Betrieb genommen und später auf fast alle Modems ausgedehnt. Dieser neue Standard für analoge Modems erlaubt Benutzern unter bestimmten Voraussetzungen Geschwindigkeiten bis zu 56Kbit/s, die jedoch aufgrund der praktisch nie gegebenen idealen Umgebung äußerst selten erreicht werden. Der stabile Zugang mittels ISDN über Synchronous PPP und Validierung mit PAP wurde 1998 von mehr Benutzern verwendet. Dies deutet auf steigende Akzeptanz von ISDN im Heimbereich hin.

Am 3. Dezember 1998 schließlich wurde erneut um einen PRI aufgestockt, somit verfügte die TU Wien über insgesamt 210 gleichzeitige Leitungen.

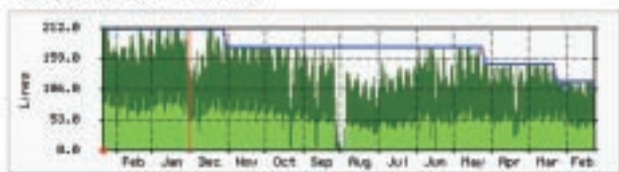
Mit Stand Dezember 1998 verwendeten 4692 verschiedene Benutzer die Wählleitungen. 91,5% aller Connects stammten von Studierenden im Rahmen des Internet-Service für Studierende. Typisch wurden 250.000 bis 270.000 Connects mit insgesamt ca. 53.000 Stunden pro Monat registriert. Im Dezember wurden 255 GByte zu den Benutzern übertragen und 28 Gbyte empfangen. Der 24-Stunden-Schnitt der belegten Leitungen lag bei 73 (von 210). Fast ausschließlich wurde das PPP Protokoll verwendet. Die Benutzer wendeten pro Monat ca. 1 Mio. Schilling für die Telefonkosten auf (Annahme Wien-Umgebung mit Online-Tarif). 74% aller Verbindungen dauerten kürzer als 10 Minuten, 95% weniger als eine Stunde.

Der Online-Tarif brachte zwar auf Benutzerseite durch Kostenreduktion Vorteile, für das EDV-Zentrum brachte dies jedoch erhebliche Probleme im Hinblick auf nicht vorhandene Ressourcen bei gleichzeitig verfügbaren Zugängen (Auslastung des teuren Equipments nur mehr in immer kürzeren Zeiten mit steilen Flanken und tagsüber nur sehr wenig ausgelastete Leitungen). Dieser Entwicklung musste im Herbst durch die Anschaffung eines wei-



teren Terminalserver mit der Anschlussmöglichkeit von 4 PRIs Rechnung getragen werden.

'Yearly' Graph (1 Day Average)



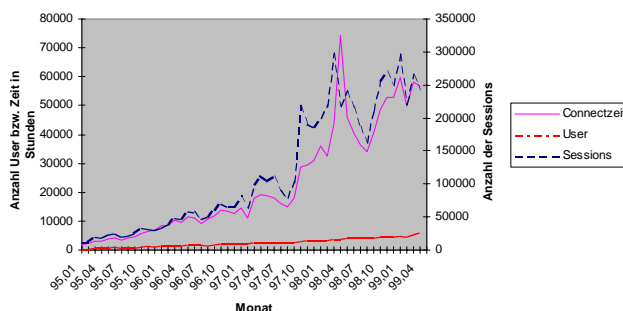
Aktive Terminal Server Leitungen – Jahresgrafik 1998

'Weekly' Graph (30 Minute Average)



Aktive Terminal-Server-Leitungen – wöchentliche Grafik

Unzählige Software-Modemfirmware-Upgrades sowie Tests, Konfigurationsänderungen, Benutzerberatungen, Fehleranalysen und Fehlerbehebungen – besonders im Zusammenhang mit V.90 – forderten einen nennenswerten Teil der Arbeitskapazität in der Abteilung Kommunikation.

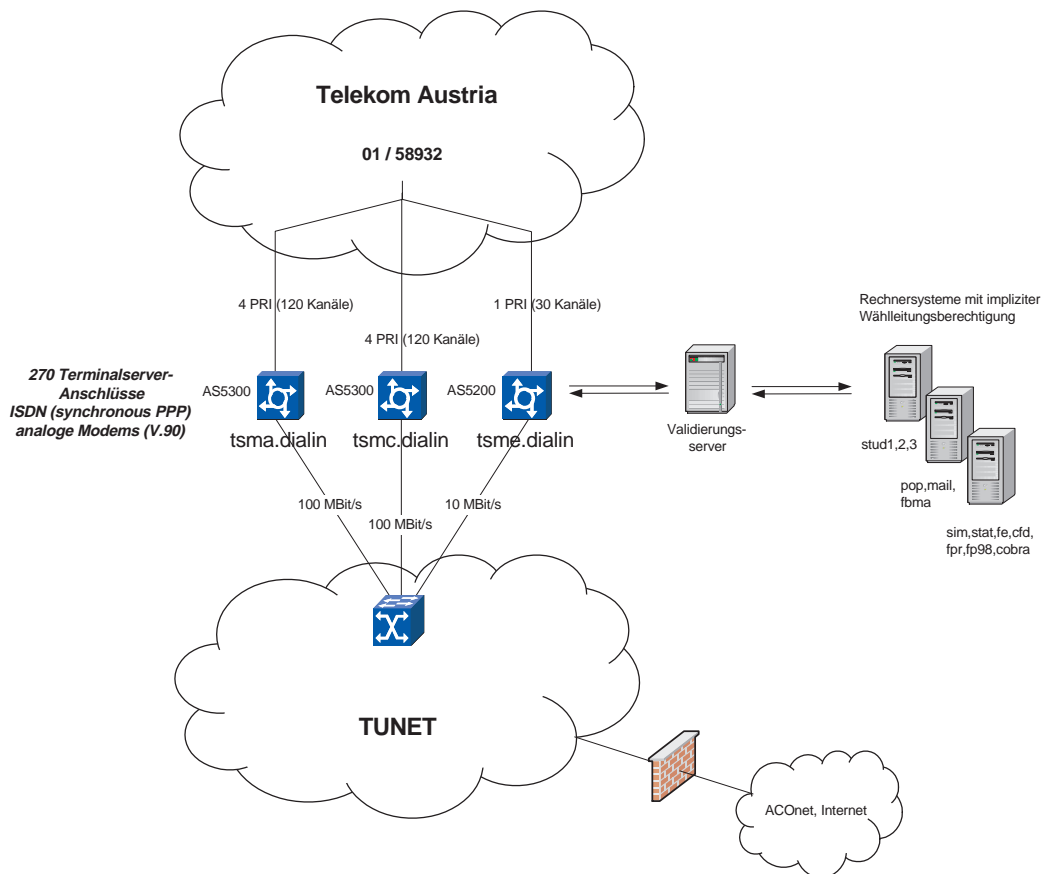


Verwendung des Wählleitungszuganges

## 1999 Übersiedlung der Wählleitungszugänge, OLTE

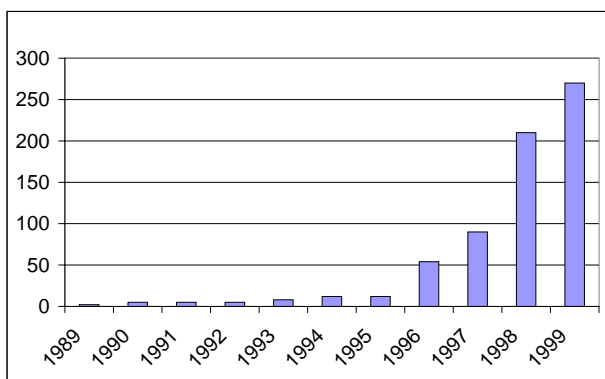
Im Zuge des Telekommunikationsprojektes wurde 1999 eine Änderung in der Wählleitungs-Infrastruktur vorgenommen. Das gesamte Dialin-Equipment übersiedelte aus dem traditionellen Maschinenraum des Zentralen Informatikdienstes (Freihaus 2. Stock) in den zentralen Telekommunikationsraum in den 1. Stock im Freihaus. Dort war bereits bei Inbetriebnahme der neuen Telefonanlage die notwendige Netzinfrastruktur geschaffen worden. Dabei war auch die Telekom Austria gefordert, die einzelnen PRI-Anschlüsse (je Anschluss ein 2 MBit/s Modem über eine Kupferverbindung direkt zum nächsten Ortsamt) ohne größere Unterbrechungen während des Betriebes

Wählleitungszugang Mai 1999



bes an der TU Wien umzuschalten. Dies konnte im Rahmen eines Netzwartungstages im Mai im Wesentlichen ohne Benutzerstörung durchgeführt werden. Alle ISDN-Multi-Anschlüsse (bis auf einen aus Gründen der Ausfallssicherheit) sind nun über Glasfaser über eine sogenannte OLTE (Optical Line Terminator Equipment) geschaltet. Dieses System basiert auf einer Glasfaseranbindung zur Telekom Austria, die an der TU Wien im Freihaus endet, und dort auf einzelne 2 MBit/s Modem-Kupfereinschübe umgesetzt wird. Diese wiederum sind dann direkt mit den entsprechenden Interfaces der Terminalserver verbunden. Damit sollte die Stabilität des gesamten Wählleitungsservices erhöht worden sein.

Weiters ist dieses System leicht auszubauen, was auch bereits 1999 wieder geschehen musste. So wurden zwei weitere ISDN-Multi-Anschlüsse in Betrieb genommen, damit verfügt die TU Wien derzeit über 270 gleichzeitige Kanäle für den Zugang zum TUNET mittels analogen Modems und ISDN. Auf allen Kanälen sind die Zugangsmodalitäten gleich und entsprechen dem Stand der Technik von heute. Die folgende Grafik zeigt den kontinuierlichen Ausbau der Anzahl an Wählleitungen. Damit sollte zumindest bis Ende des Sommersemester 1999 der Bedarf an Leitungskapazität gedeckt sein.



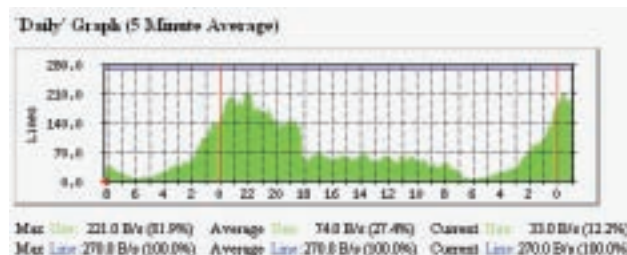
Entwicklung Anzahl der Leitungen

Bedingt durch die Erweiterung musste ein weiteres Class C Netz für dieses Service in Betrieb genommen werden. Der Wählleitungszugang umfasst nun die beiden Class C Netze 192.35.240.0 und 192.35.243.0 (jeweils Maske 255.255.255.0).

Die 270 gleichzeitigen Zugänge sind durch eine Serie von neun Multi-ISDN-Anschlüssen, sogenannten PRIs (Primary Rate Interfaces), realisiert, die auf drei Terminalserver vom Typ Cisco AS5x00 aufgeteilt sind. Alle drei Terminalserver (tsma.dialin.tuwien.ac.at, tsmc.dialin.tuwien.ac.at und tsme.dialin.tuwien.ac.at) unterstützen beim analogen Modemzugang Modulationen bis zu V.90 (56000 Bit/s) bzw. über ISDN (synchronous PPP) 64000 Bit/s.

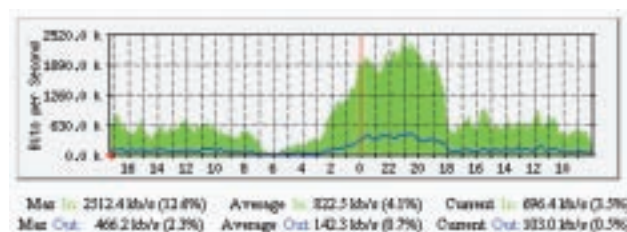
Die Tarifstruktur der Telekom Austria, insbesondere der günstige Online-Tarif führt tagsüber zu einer geringen Auslastung des Wählleitungsservice, ab 18 Uhr jedoch zu einer raschen Zunahme der Anzahl an Logins

(siehe steile Flanken in den folgenden Grafiken). Hier ist auf eine Tarifstruktur-Reform der Telekom Austria zu hoffen, um die Dialin-Ausrüstung effizienter auszulasten. Nichts desto trotz gehört es jedoch auch zu den Aufgaben eines Service Providers, und als solches ist der ZID in diesem Fall zu sehen, in Zeiten mit Spitzenbelastungen weiterhin ein funktionierendes Service zu bieten.



Aktive Terminal-Server-Leitungen – tägliche Grafik

Die Bandbreiten-Ressourcen, die derzeit durch das Wählleitungsservice belegt werden, liegen in etwa bei 2,6 MBit/s (siehe Grafik unten).



Benötigte Bandbreite für Wählleitungen

Beobachtet man die Entwicklung der maximalen Kapazität des Wählleitungsservice von 1989 bis 1999

1989: 5 x 300 Bit/s = 1500 Bit/s  
 1999: 270 x 56000 Bit/s = 15 120 000 Bit/s

ergeben sich folgende Steigerungsfaktoren:

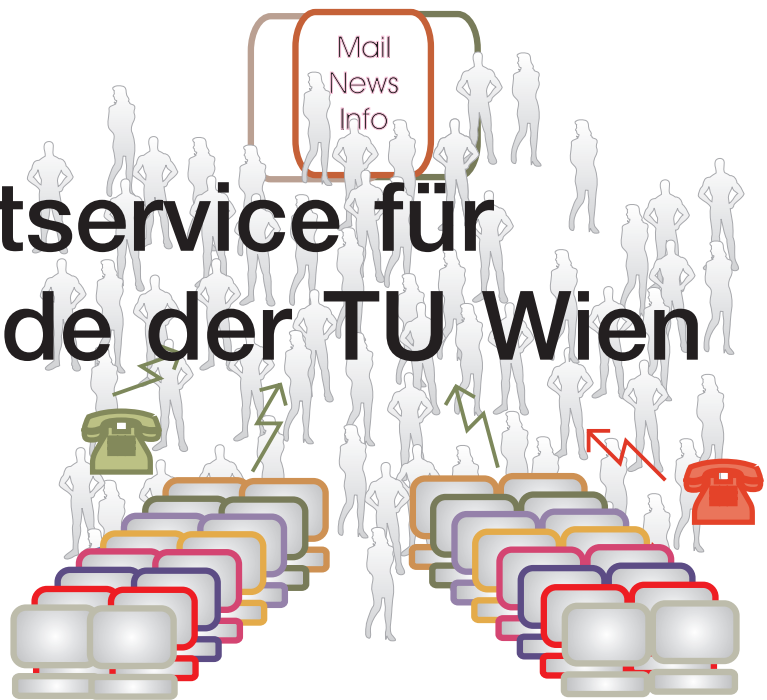
	10 Jahre	pro Jahr
Anzahl Anschlüsse	54	1,5
max. Einzeldatenrate	187	1,7
Gesamtkapazität	10080	2,5

Der zentrale Informatikdienst ist weiterhin bemüht, das Wählleitungsservice den Anforderungen entsprechend auszubauen und damit einen sinnvollen und für die Benutzer befriedigenden Betrieb zu ermöglichen. Dabei gibt es im Zusammenhang mit der analogen Modemtechnologie und der Vielzahl an Fehlerquellen im Bereich der Heimtelefonanschlüsse fast täglich knifflige Problemsituationen zu lösen. Aber auch hier besteht die Zuversicht, diese in der Zukunft meistern zu können.

## Literatur

- [1] J. Kainrath. Mit PPP und Windows 95 ins TUNET. PIPELINE 17, 1995, pp. 13-17
- [2] J. Kainrath. Mit PPP und Windows NT 4.0 ins TUNET. PIPELINE 24, 1998, pp. 7-15

# Das Internetservice für Studierende der TU Wien



Peter Berger

Der folgende Artikel stellt einen „geschichtlichen Rückblick“ über das Projekt „Mail/News/Info-Service für Studierende der TU Wien“ (neuer Name ab 1. 1. 1999: „Internet-Service“) dar, wobei es bis heute keinen definitiven Abschluss gibt. Durch laufende, von den verschiedensten Seiten an das Projektteam herangetragene Wünsche und Änderungsvorschläge und auch durch den rasanten technischen Fortschritt der modernen Informationssysteme und -möglichkeiten war und ist eine Anpassung der technischen Realisierungsstufen notwendig. Alle Änderungen dürfen jedoch nicht das Kernziel des Projektes beschneiden, den (berechtigten) Studierenden der TU Wien einen optimalen Zugang zu modernen Informationstechnologien zu ermöglichen, sondern müssen dazu dienen, das Serviceangebot zu erweitern und zu verbessern.

## Die Realisierungsstufen 1 bis 3 im Rückblick (1994 bis 1998)

Im Frühjahr 1994 wurde vom EDV-Zentrum der TU Wien (ab 1. 1. 1999 Zentraler Informatikdienst, ZID) – basierend auf einem Konzept der Hochschülerschaft der TU Wien – ein Realisierungsprojekt erarbeitet, das den Zugang zu Mail-, News- und Informationsdiensten (Mail/News/Info-Service, neuer Name Internetservice) für Studierende der TU Wien ermöglichen soll. Folgende Anforderung an Services und Nutzungsmöglichkeiten waren vorgegeben:

- persönlicher Username für jeden Studierenden, der bestimmte Berechtigungskriterien erfüllt,
- Electronic Mail (weltweit möglich) mit rechnerunabhängiger Adressierung (d.h. jeder Student hat eine Mail-Adresse der Form e9999999@student.tuwien.ac.at),
- News,
- Info-Dienste,
- permanenter Speicherplatz für Programme und Informationen,

- offener Zugang von den Internet-Räumen (Benutzer-räumen) und von Arbeitsplätzen an der TU Wien,
- Zugang über Wählleitungen.

Eine weitere wichtige Vorgabe war die Sicherstellung der Datenkonsistenz (d. h. die zentrale Speicherung der persönlichen Daten eines Users, gleichgültig von welchen Geräten oder Standorten gearbeitet wird).

Nach einer eingehenden Analyse der Anforderungen und der Prüfung der Kosten verschiedener Realisierungsszenarien wurde ein Konzept gewählt, das neue zentrale UNIX-Studentenserver vorsieht, bestehende Informationssysteme (z. B. News-Server) mit einbindet, die bestehenden Wählleitungszugänge erweitert und PC-Arbeitsplätze in den Internet-Räumen (des ZID und der HTU) vorsieht.

Der Akademische Senat hat am 14. März 1994 dieses Konzept des damaligen EDV-Zentrums zustimmend zur Kenntnis genommen und den Finanzierungsplan genehmigt. Weiters wurde beschlossen, dieses Service jenen aktiven Studierenden der TU Wien zur Verfügung zu stellen, die Prüfungen über mindestens 8 Semesterwochenstunden pro Jahr abgelegt oder den 1. Studienabschnitt abgeschlossen haben.

## Die Realisierungsstufe 1 (1994)

In der ersten Realisierungsstufe im Herbst 1994 wurden der erste UNIX-Studentenserver **stud1.tuwien.ac.at** (IBM RS/6000-380, 128 MB Hauptspeicher, 8 GB Plattenspeicher) und ein „Fachbereichsrechner Mathematik“ **fbma.tuwien.ac.at** (RS/6000-390, 256 MB Hauptspeicher, 6 GB Plattenspeicher) angekauft. Auf diesem wurden neben Accounts für Mitarbeiter der Fachgruppe Mathematik auch Accounts für Studenten der Fachrichtung Mathematik eingerichtet.

Weiters hatte sich die Fakultät für Bauingenieurwesen bereit erklärt, für Studierende der Fachrichtungen Bauingenieurwesen und Maschinenbau einen Rechner **studbimb.tuwien.ac.at** (HP 835, 96 MB Hauptspeicher, 6 GB Plattenspeicher) zur Verfügung zu stellen.

An Software standen auf diesen Systemen das UNIX-Betriebssystem (IBM bzw. HP), C und perl, Kommunikationssoftware (telnet, ftp, X11), Editoren (vi, pico, emacs, axe), Programme für Mail (mail, elm, pine), Newsreader (tin, pine, xrn), Info-Software (gopher, mosaic, netscape, lynx) und ein WWW-Server zur Verfügung.

Jedem User wurden 5 MB permanenter Massenspeicher als Home-Directory zur Verfügung gestellt. Weiters konnten unter „public.html“ selbst entwickelte WWW-Seiten auf jedem Studentenrechner angeboten werden.

### Das Anmeldesystem

Die Anmeldung zur Nutzung dieser Services erfolgt über eine WWW-Maske, die von jedem Rechner im Internet aufgerufen werden kann. Als Username wird die Matrikelnummer des Studenten mit einem „e“ davor genommen. Die Feststellung der Erfüllung der Berechtigungskriterien erfolgt durch die ADV-Abteilung der Universitätsdirektion, die Überprüfung erfolgt bei der Anmeldung. Nach der (erfolgreichen) Anmeldung wird von einem Tutor im Internet-Raum Freihaus eine Bestätigung (mit dem Initial Passwort und der Information, auf welchem UNIX-Studentenrechner sein Home-Directory liegt) ausgedruckt und dem User gegen Unterschrift übergeben.

Gleichzeitig wird mit der Einrichtung des Usernamens auf einem Studentenserver (auf welchem entscheidet das Anmelde-Script auf Grund der Lastsituation und der Studienrichtungen) eine Eintragung des Users in den White Pages (X500 Datenbank) der TU Wien vorgenommen, sodass die Adressierung in der Form e9999999@student.tuwien.ac.at erfolgen kann.

Für Studien, die auf der TU Wien und/oder auf anderen Universitäten absolviert werden können (z. B. Wirtschaftsinformatik), wird die Vergabe der Usernamen im Sekretariat des ZID durchgeführt (wobei die Regelung gilt, dass von den geforderten Prüfungen über mindestens 8 Semesterwochenstunden mindestens 4 Stunden an der TU Wien abgelegt wurden).

Diese Usernamen sind für Studierende im ersten Studienabschnitt ab dem Vergabezeitpunkt 12 Monate gültig, dann wird eine Überprüfung gemäß den Kriterien durchgeführt. Sind diese erfüllt, so wird der User auto-

matisch um ein weiteres Jahr verlängert, wenn nicht, werden die Berechtigungen und alle Daten nach 2 Mahnungen gelöscht. Für Studierende im zweiten Studienabschnitt werden die Berechtigungen gelöscht, wenn sie dieses Service länger als 15 Monate nicht verwenden. Die Eintragungen in den White Pages bleiben erhalten. Ist eine entsprechende Mail-Adresse dort angegeben, so werden Mails bei der Adressierung e9999999@student.tuwien.ac.at an diese Mail-Adresse weitergeleitet.

Dieses Anmeldesystem hat sich sehr gut bewährt. Bereits in der ersten Woche (24. - 30. 10. 1994) hatten sich 1110 Studenten angemeldet, zum Jahreswechsel 1994/95 hielten wir bei 2170 Anmeldungen, verteilt auf die drei Server stud1, fbma und studbimb.

### Internet-Räume

Die Schaffung von PC-Arbeitsplätzen war eine entscheidende Voraussetzung für die Realisierung des Gesamtprojektes.

Dazu wurden an den bestehenden Arbeitsplätzen im Bereich Freihaus (Erdgeschoss und 2. Stock) wesentliche Erweiterungen der Hardwareausstattung vorgenommen. Alle 42 PC-Arbeitsplätze wurden mit 17-Zoll Bildschirmen ausgestattet, zwei weitere Laserdrucker (HP Laserjet 4 und Epson Stylus Color) wurden sowohl im Erdgeschoss als auch im 2. Stock installiert. Diese PCs liefen unter Windows 3.1, als Boot-Server dienten Novell-Server. Die Vergabe der Usernummern, die Überprüfung der Hardware und die Beratung der Studenten werden von Tutoren des EDV-Zentrums durchgeführt, die täglich anwesend sind.

Jeder Student mit einem gültigen Usernamen konnte diese Arbeitsplätze benutzen. Es wurde ein User STUDENT eingerichtet, der nach einer entsprechenden Überprüfung des Usernamens und des Passwortes auf „seinem“ UNIX-Rechner eine für Mail/News- und Infodienste geeignete Softwareumgebung am PC zur Verfügung stellt. Die notwendigen Konfigurationsdateien (INI-Files) der Windows-Software wurden auf dem UNIX-Rechner im eigenen Home-Directory gespeichert und bei jedem Login an den Novell-Servern von dort geladen. Damit ist eine weitgehende Datenkonsistenz erreicht, d. h. von allen PCs in den Internet-Räumen und in den HTU-Fachschaften konnte mit der zuletzt aktuellen, eigenen Softwareeinstellung gearbeitet werden.

Nach Abschluss eines Kooperationsvertrages zwischen dem EDV-Zentrum und der HTU wurden in den Räumen der Fachschaft Elektrotechnik (Gußhausstraße 27-29, 1. Stock) und Informatik (Treitlstraße 3, Hochparterre) 4 bzw. 6 PCs installiert. Weiters wurden leistungsfähige Novell-Server gekauft, um eine Vernetzung der Geräte zu ermöglichen. Die Betreuung der PCs wird von Tutoren der HTU durchgeführt, die Novellserver-Betreuung und die Basisinstallation wurde vom EDV-Zentrum vorgenommen.

Zusätzlich wurden 8 asynchrone Terminals (VT 220), die vom Institut für Mikroelektronik zur Verfügung gestellt wurden, in der Treitlstraße installiert. Obwohl damit nur in „Linemode“ gearbeitet werden kann, werden diese Geräte zum Lesen von Mails und News intensiv genutzt.

## Software auf den PC-Arbeitsplätzen

Folgende Softwarekomponenten standen in den Internet-Räumen zur Verfügung:

PC-DOS 6.3 mit Windows 3.1
MS Fortran/Basic/C++/Pascal/F90
TCP/IP (telnet, ftp)
Pmail / Eudora
MS Winword/Excel/PowerPoint/Access
Mosaic / Hgopher
CorelDraw
PageMaker
HCL-eXceed

## Wählleitungszugänge

Die Berechtigung zur Nutzung der Wählleitungszugänge ist durch die Vergabe des Usernamens am UNIX-Server gegeben, d. h. jeder Student mit einem gültigen Usernamen der Form e9999999 kann über Telefon und Terminalserver die Services nutzen. Nach Aufbau der Verbindung über ein Telefon und ein gängiges Terminal-Emulationsprogramm meldet sich ein Terminalserver mit der Aufforderung, Usernamen und Passwort einzugeben. Als Username ist nun z. B. e9999999@stud1 anzugeben, als Passwort jenes am UNIX-Rechner.

Ende 1994 standen in Summe 12 Wählleitungszugänge zur Verfügung.

## Die Realisierungsstufe 2 (1995 und 1996)

In der ersten Realisierungsphase nutzten bereits 3566 Studierende dieses Service (Stichtag 2. Mai 1995), wobei eine Verteilung der Usernummern von ca. 70% : 14% : 16% auf die Studentenserver (stud1 : fbma : studbimb) zu beobachten war.

Einige Hardware-Änderungen wie z. B. Ausbau des Hauptspeichers und der Platten sowie Softwareanpassungen wurden vorgenommen.

Auf dem System stud1 waren im Mai 1995 über 2500 Usernummern vergeben. Dies führte zu einer sehr hohen Belastung dieses Rechners und zu entsprechend hohen Lastsituationen und Antwortzeiten. Trotz der schwierigen Budgetsituation konnte mit der zweiten Phase des Projektes begonnen werden, wobei die hohe Stabilität der eingesetzten Hard- und Software wesentlich zur hohen Akzeptanz bei den Studenten beitrug.

## Die neuen UNIX-Server stud2 und stud3

Am 27. Mai 1995 wurde der neue Studentenserver **stud2.tuwien.ac.at** (IBM RS/6000-380, 128 MB Hauptspeicher, 12 GB Plattenspeicher) in Betrieb genommen. Dieses System verfügt über eine fast gleiche Hard- und Softwareausstattung wie das System stud1, um Objekt- und Binärcode-Kompatibilität sowie gleiche Softwareoberflächen zu bieten. Auf dem System stud1 wurden zusätzlich 128 MB Hauptspeicher installiert.

Für Studierende der Fachrichtung Raumplanung und Architektur wurde die Anmeldung auf einem „Aliasrechner stud2“ vorgezogen, nachdem vom EDV-Labor der Fakultät für Raumplanung und Architektur SCSI-Platten (2x 2GB f/w) zur Verfügung gestellt wurden.

Im Mai 1996 waren über 7000 User auf den drei Systemen aktiv. Vor allem das über 10 Jahre alte System studbimb war dieser Belastung nicht mehr gewachsen. Als Ersatz für dieses System wurde im Mai 1996 ein System **stud3.tuwien.ac.at** (HP 9000-D350, 160 MB Hauptspeicher, 12 GB Plattenspeicher) installiert, das alle User des Systems studbimb übernahm.

## Organisatorische Änderungen

Bereits nach einigen Monaten im praktischen Betrieb zeigte sich, dass die Berechtigungskriterien nicht ausreichend genau formuliert waren. In Zusammenarbeit mit der ADV-Abteilung der Universitätsdirektion der TU Wien wurden diese Kriterien neu formuliert und veröffentlicht. Eine wesentliche Änderung gegenüber der Erstversion ist die dynamische Definition des Beobachtungszeitraumes von mindestens 12 Monaten, die eine gerechte Überprüfung der abgelegten Prüfungen ermöglicht.

## Die neuen Berechtigungskriterien

(Auszug aus einem Schreiben des EDV-Zentrums an die ADV-Abteilung der Universitätsdirektion)

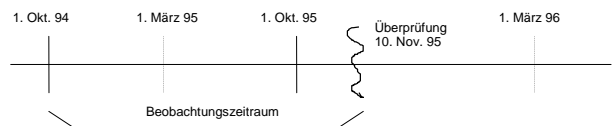
Diese Überprüfung erfolgt für alle Studierenden der TU-Wien, die ein „offenes Studium“ betreiben nach folgenden Kriterien:

1. Berechtigt sind alle Studierenden im ersten Studienabschnitt mit Stammhochschule TU-Wien, die in einem Beobachtungszeitraum Prüfungen im Ausmaß von 8 oder mehr Semesterwochenstunden an der TU-Wien abgelegt haben und an der TU-Wien inskribiert sind.

Dieser Beobachtungszeitraum ist die Zeitspanne zwischen der Überprüfung (am 10. Werktag jedes Monats), und den vorletzten Stichtagen 1. Oktober oder 1. März, je nachdem welcher dieser Zeitpunkte später eintrifft. Der Beobachtungszeitraum ist daher immer größer als 12 Monate.

Beispiel:

Überprüfung der Studierenden am 10. November 1995  
Beobachtungszeitraum (ob Prüfungen über 8 Stunden oder mehr abgelegt wurden) ist der 1.10.94 bis 6.11.95



2. Berechtigt sind alle Studierenden mit Stammhochschule TU-Wien, die sich im 2. Studienabschnitt befinden (1. Diplomprüfung abgelegt), die ein Studium abgeschlossen (2. Diplomprüfung) und ein anderes Studium inskribiert haben oder die ein Doktoratsstudium oder Aufbaustudium betreiben und an der TU-Wien inskribiert sind.
3. Studierende mit anderer Stammhochschule sind berechtigt, wenn die Prüfungskriterien an der TU-Wien entsprechend dem Punkt 1 erfüllt sind.

4. Für Studierende, die ein mit anderen Universitäten gemeinsam eingerichtetes Studium betreiben (z. B. Betriebs- und Wirtschaftsinformatik, Technischer Umweltschutz usw.), gelten die Zulassungskriterien wie in den Punkten 1 und 2; die geforderten Prüfungen können aber auf den anderen Universitäten abgelegt werden. Die Überprüfung dieser Daten wird vom EDV-Zentrum durchgeführt.

## Dauer der Berechtigung

Die Überprüfung entsprechend den Berechtigungskriterien werden von der ADV-Abteilung der TU Wien an jedem 10. Werktag jedes Monats durchgeführt.

Erfüllt ein Student die Kriterien nicht mehr, wird er aus dem Datensatz, der dem EDV-Zentrum übermittelt wird, gestrichen. Vom EDV-Zentrum wird daraufhin eine Mail mit einer entsprechenden Information an den User gesendet (1. Mahnung), nach einem Monat wird eine 2. Mahnung versendet und nach einem weiteren Monat wird die Usernummer mit allen Daten gelöscht.

Studierende, die nach den Kriterien nach Punkt 2 (z. B. im 2. Studienabschnitt) geprüft werden, werden dann gelöscht (nach entsprechenden Mahnungen), wenn sie 12 Monate lang kein Login durchgeführt haben. Diese Vorgangsweise kann vom EDV-Zentrum nur dann durchgeführt werden, wenn im Datensatz der ADV-Abteilung ein Feld „erste Diplomprüfung abgelegt“ vorhanden ist.

## Das Projekt „Umstellung Novell – Windows NT“

### Ausgangssituation

Anfang 1996 waren in den Internet-Räumen des EDV-Zentrums etwa 120 *diskless* PCs aufgestellt. Die PCs liefen mit dem Betriebssystem DOS und der Benutzeroberfläche Windows 3.1. Als Boot- und Software-Server wurden 7 Novell-Server mit dem Betriebssystem Novell NetWare 4.10 eingesetzt. Als File-Server (und für die Benutzervalidierung) wurden die Studenten-UNIX-Server verwendet. Das Drucken erfolgte von Queues auf den Novell-Servern über einen Consol-PC auf die entsprechenden Drucker. Die Arbeitsplatzrechner waren jeweils zu Gruppen mit etwa 12 PCs zusammengefasst, die am zugehörigen Novell-Server angeschlossen waren, der für diese PCs auch als Router fungierte.

Diverse technische und organisatorische Probleme – vor allem im Zusammenhang mit Novell 4.1 – und die mangelnde Sicherheit von Bus-Netzen und Repeatern gegenüber dem Abhören von TCP/IP-Verbindungen machten Ende 1995 Überlegungen für eine Neukonfiguration notwendig. Folgende grundsätzliche Entscheidungen wurden getroffen:

- Trennung der Router-Funktionalität von den Servern.
- Ersatz der Bus-Verkabelung durch eine strukturierte Sternverkabelung mit Switches.
- Einsatz von Windows NT als Server-Betriebssystem und von Windows 95 als Client-Betriebssystem.
- Reduktion des Softwareangebotes in den Internet-Räumen gegenüber der Situation unter Novell/Windows 3.1.

- Da die Kombination Win95/WNT das Netzwerk deutlich stärker belastet als die Win3.1/Novell Konfiguration, ist eine Anbindung der Server mit 100 Mbit/s erforderlich.
- Validierung direkt unter WNT mit dem unter UNIX vergebenen Usernamen.

Im Zuge der Evaluierung der Leistungsfähigkeit dieser Konfiguration mit WNT 3.51 stellte sich heraus, dass für einen Produktionsbetrieb WNT 4.0 eingesetzt werden muss. 1996 wurde die Umstellung der Verkabelung und der Netzstruktur durchgeführt, im Herbst 1996 wurde mit der Umstellung auf WNT 4.0 und Win95 begonnen, diese Umstellung war im Sommer 1997 abgeschlossen.

### Umstellung der Server

Mit dem (verspäteten) Einlangen der Release-Version von Windows NT Ende August 1996 wurde der erste tatsächlich für den endgültigen Betrieb vorgesehene Windows NT Server aufgesetzt. Als Hardware wurde ein neu angeschaffter Dual Pentium PC mit 128 MByte Hauptspeicher (DEC Prioris), 8 GByte SCSI Platten, einem CD-ROM Laufwerk und einem Streamer-Tape verwendet. Probleme traten lediglich beim Versuch auf, die vorgesehene Ethernetkarte mit 100 Mbit/s zu betreiben. Erst der Austausch der Karte gegen ein neueres Modell – Anfang Jänner 1997 – brachte den benötigten Netzwerkdurchsatz.

In weiterer Folge wurden schrittweise die drei neueren Novell-Server außer Betrieb genommen. Zuerst wurde der Server für das Gußhaus abgebaut. Die dort aufgestellten PCs wurden über die bereits bestehende 100 Mbit/s Verbindung auf einen der Server im Freihaus umgestellt. Das war wegen des reduzierten Bedarfes in den Ferienmonaten möglich. Der freigewordene Rechner wurde als Server für die Internet-Räume im Freihaus 2. Stock eingesetzt. Jeweils mit einigen Wochen Verzögerung wurden auch die beiden anderen „größeren“ Novell-Server auf Windows NT umgestellt.

Für jeden „großen“ Internet-Raum steht somit ein eigener Boot-Server zur Verfügung, von dem die PC-Arbeitsplätze booten. Ein Fileserver wurde installiert, um den einzelnen Benutzern – unabhängig vom verwendeten Arbeitsplatz – ihre individuelle Arbeitsoberfläche (Desktop) zur Verfügung zu stellen. Jeder Student hat auf diesem Fileserver für seine Initialisierungs- und Konfigurationsdateien einen Datenbereich mit 1,8 GB Kapazität. Für alle anderen Daten des Benutzers wird über Samba auf einen der UNIX-Studenten-Server zugegriffen.

Die wesentlich effizientere Verwaltung der Usernamen (gleicher Username wie auf den UNIX-Studentenservern) mit eigenem Passwort ermöglicht es, den Zugang zu den PC-Arbeitsplätzen in einer vergleichbaren (hohen) Sicherheitsstufe wie unter UNIX zu realisieren. Die Vergabe dieser Berechtigungen, die Einrichtung der User und der Home-Directories, die Passwortvergabe u. dgl. erfolgen durch dafür entwickelte Programme gleichzeitig mit der Einrichtung des Users unter UNIX, von Seiten der Studenten sind keine Aktionen erforderlich (die Einrichtung der Berechtigung erfolgt automatisch bei der Anmeldung).

## Netzwerkumstellung

Ziel der Netzwerkumstellung war es, leistungsfähige und abhörsichere Verbindungen zwischen den PCs in den Internet-Räumen und den diversen Servern zu schaffen. Dazu wurde einerseits die bestehende Verkabelung (größtenteils Thinwire) durch eine strukturierte Verkabelung (TwistedPair mit Switches) ersetzt. Soweit bereits TwistedPair Verkabelungen bestanden, wurden die Repeater durch leistungsfähige Switches ersetzt. Gleichzeitig sollten auch die Server nicht mehr als Router verwendet werden. Besonders stark genutzte Verbindungen (zu den Windows NT Servern, zwischen den Switches und in's TUNET hinaus) wurden auf 100 Mbit/s aufgerüstet. Dadurch ist ein flaches Netz entstanden, in dem alle lokalen Verbindungen direkt – d. h. ohne einen Router zu belasten – aufgebaut werden können.

Diese Umstellung betraf einerseits alle PCs in den Internet-Räumen und andererseits alle Studentenserver (stud1, stud2, stud3 u. ä.) sowie die Netzwerk-Server (mr, proxy, info), die nun mit mindestens einem Interface direkt im Netz der Internet-Räume hängen.

Wegen der zentralen Bedeutung dieser Umstellung wurde diese zu Beginn der Sommerferien 1996 begonnen. Auf Grund von Verzögerungen bei der Hardware-Anlieferung und insbesondere bei den Verkabelungsarbeiten wurden diese Umstellungen erst Mitte Jänner 1997 abgeschlossen, wobei folgende Ethernet-Switches installiert waren: 2 Stück Cisco Catalyst 5000, 5 Stück Cisco Catalyst 3000.

Die Uplink-Verbindung der Switches erfolgt über mindestens 100 Mbit/s, später wurden 3 Switches über ATM mit dem TUNET gekoppelt.

## Das Softwareangebot in den Internet-Räumen

Nach dem Boot-Vorgang von Windows 95 stehen folgende Softwarekomponenten lokal am PC zur Verfügung (s. <http://www.ben.tuwien.ac.at/ben/software.html>):

Hilfsprogramme von Windows 95 (inkl. telnet, ftp u.dgl.)
MS Office (Word, Excel, PowerPoint)
Eudora
Netscape
Internet Explorer
HCLeXceed
Java

## Die PC-Arbeitsplätze

Der Ausbau und die Verbesserung der Hardware der PC-Arbeitsplätze waren wichtige Komponenten bei der Schaffung einer neuen, modernen Struktur der Internet-Räume. In der Gußhausstraße wurde ein weiterer Internet-Raum eingerichtet (Erweiterung der bestehenden Räume um 2 Fensterachsen). Nach intensiven Verhandlungen mit der Hochschülerschaft der TU Wien konnte mit der Fachschaft Physik ein Abkommen getroffen wer-

den, in dem ein Teil des Lernraumes im Freihaus, 2. Stock (gelber Bereich) als PC-Raum (12 PCs) umgestaltet wurde. Weiters konnte nach Gesprächen mit der Fachschaft Bauingenieurwesen auch im Bereich Karlsplatz 13 ein PC-Raum (BIZ, 11 Arbeitsplätze) geschaffen werden.

1996 standen 140 PC-Arbeitsplätze des EDV-Zentrums für das Internet-Service zur Verfügung.

## Linux in den Internet-Räumen

Gegen Ende des Sommersemesters 1996 konnte der Grundstein zu einem lang ersehnten Wunsch vieler Studenten gelegt werden, nämlich auch Linux auf den Arbeitsplatzrechnern in den Internet-Räumen verwenden zu können.

Das EDV-Zentrum hat bei der Umsetzung dieses Wunsches neue Wege beschritten. Das Projektteam bestand zum großen Teil aus engagierten Informatik-Studenten, allen voran Herwig Wittmann, Richard Kail und Raimund Bauer, die in Abstimmung mit dem EDV-Zentrum, vertreten durch Peter Hoffmann, tatkräftig an der Realisierung gearbeitet haben.

So war es auch möglich, nach knapp einem Monat an Brainstorming, Installation und Konfiguration von Hard- und Softwarekomponenten im Internet-Raum Informatik (Institutsgebäude Treitlstraße) Anfang Wintersemester 1996/97 einen Testbetrieb zu beginnen.

## Wählleitungszugänge

Die Anzahl der Wählleitungszugänge wurde bis Ende 1996 Schritt für Schritt ausgebaut auf 54 gleichzeitige Anschlüsse (asynchron, max. 14.400 V.32bis) und 2 ISDN-Anschlüsse.

## Die Realisierungsstufe 3 (1997 - 1998)

Die dritte Phase des Projektes kann als Konsolidierungsphase bezeichnet werden. In allen Teilbereichen wurden Verbesserungen (Kapazitätserweiterungen, Security-Maßnahmen usw.) sowie Detail-Änderungen vorgenommen. Ende 1998 nutzten 11.453 Studierende der TU Wien dieses Service.

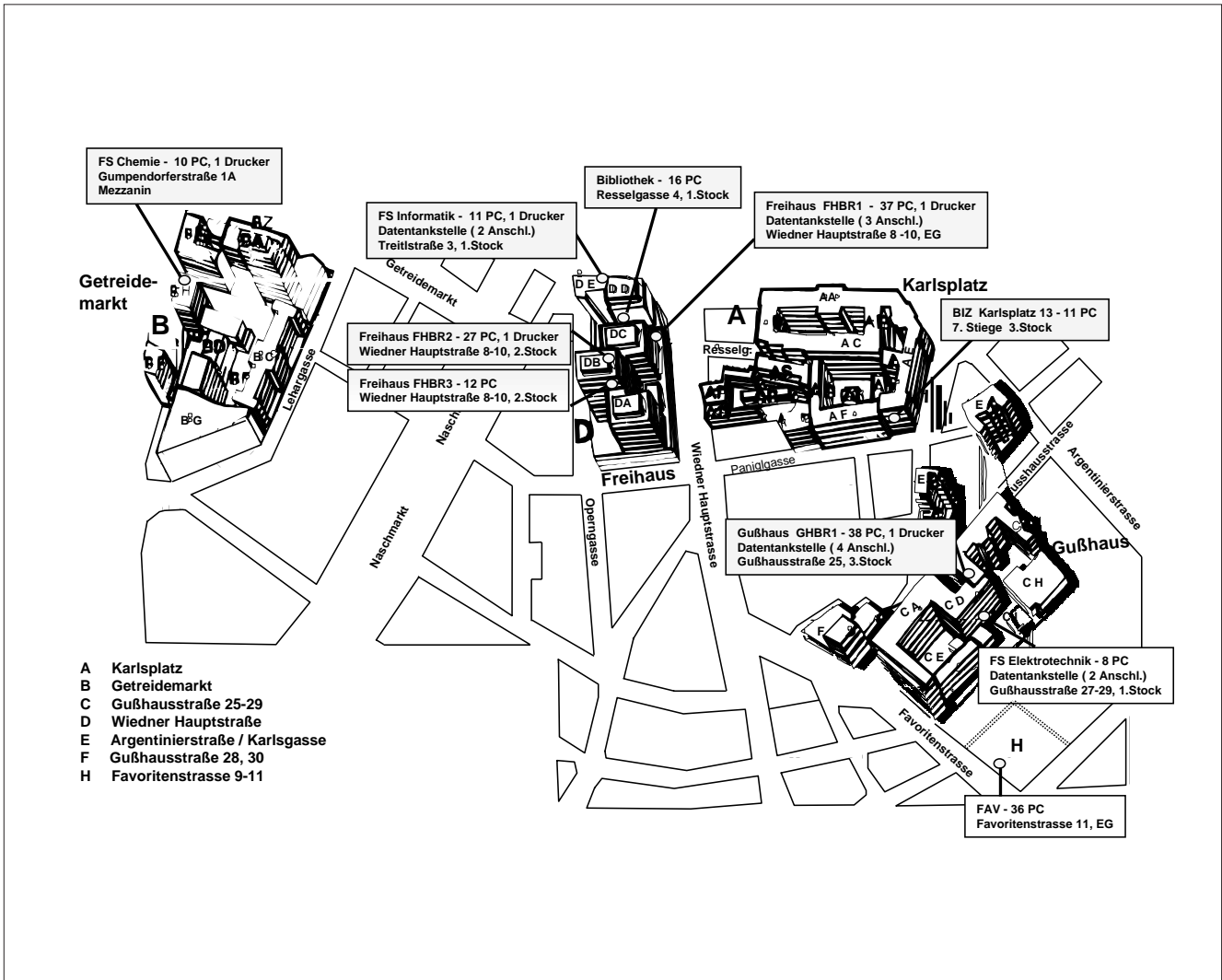
## UNIX-Studentenserver

stud1, stud2 und fbma: Vergrößerung der Home-Filesysteme durch Austausch der 4GB Platten auf 9GB Platten.

stud3: Systemtausch auf eine HP K260 (1 CPU PA 8000, 180 MHz) mit 256 MB Hauptspeicher, 16 GB Hauptspeicher für /home, 4 GB für das Mail-Filesystem.

Eine wesentliche Erweiterung des permanenten Plattenplatzes pro User (Disk-Quotas) wurde auf allen UNIX-Studentenservern vorgenommen, es stehen jedem User zur Verfügung:

Soft/Hardlimit im Home-Filesystem: 10/15MB pro User  
Soft/Hardlimit im Mail-Filesystem: 2/4MB pro User



## Internet-Räume

Anfang 1997 wurde die Umstellung auf WNT 4 abgeschlossen, weiters wurden die letzten Detail-Änderungen an der neuen Netzstruktur in den Internet-Räumen fertiggestellt. Soweit es die Verkabelung erlaubt hat, wurde eine Erhöhung der Verbindungs-Bandbreite zwischen den Switches untereinander vorgenommen (Einsatz von Cisco Fast Ether Channel Ende 1998).

Anfang 1998 wurde auf Grund der hohen Studentenzahlen die „Kernzeitbeschränkung“ eingeführt, d. h. jeder User hat in der Kernzeit (Montag bis Freitag in der Zeit von 10:00 bis 18:00 Uhr) maximal 5 Stunden Connect-Zeit auf den PCs in den Internet-Räumen zur Verfügung (egal, ob unter Windows oder Linux gearbeitet wird). Die Einführung dieser Maßnahme führte zu einer deutlichen Reduktion der Wartezeiten auf einen freien PC. Außerhalb der Kernzeit können die PC-Arbeitsplätze ohne Zeitbeschränkung genutzt werden.

Im Bereich Security wurde die Übertragung vom Passwort im Klartext durch die Validierungsmethode SECURITY = SERVER (bei der Laufwerksverbindung mit dem UNIX-Studentenserver mit samba) unterbunden.

Weiters wird durch die Überwachung der MAC-Adressen der PCs in den Internet-Räumen sichergestellt, dass keine „fremden“ PCs angeschlossen werden können.

## PC-Arbeitsplätze

Mitte 1997 waren alle PC-Arbeitsplätze mit 17" Farbbildschirmen ausgestattet, auf allen PCs wurde der Hauptspeicher auf 16 MB (teilweise auf 32 MB) aufgestockt. Die Erneuerung der Arbeitsplätze wird nach Möglichkeit in einem Dreijahreszyklus vorgenommen.

Im Herbst 1997 wurde in den Räumen der HTU Fachschaft Chemie (Gumpendorferstraße 1a) ein kleiner PC-Raum mit 10 Arbeitsplätzen eingerichtet. Mitte 1998 wurden im Leseraum der Hauptbibliothek (1. Stock) weitere 16 PC-Arbeitsplätze aufgestellt und jeweils über einen ATM-Uplink in das Netzwerk der Internet-Räume eingebunden.

Damit stehen insgesamt 181 PC-Arbeitsplätze und 16 (line-orientierte) Terminals in den Internet-Räumen zur Verfügung.



### Zusammenstellung der PC-Arbeitsplätze in den Internet-Räumen (Summe 181 PCs, 16 Terminals)

BR Freihaus (EG, FHBR1)	37 PC-Arbeitsplätze 1 Laserdrucker 1 Terminal
BR Freihaus (EG, FHBR1)	13 PC-Arbeitsplätze
Eingangsbereich Freihaus (snake)	6 Terminals
BR Freihaus (2. Stock, FHBR2)	27 PC-Arbeitsplätze 1 Laserdrucker
BR Gußhausstr. (3. Stock, GHBR1)	36 PC-Arbeitsplätze 1 Laserdrucker
Bibliothek TUW (1. Stock, BIB)	16 PC-Arbeitsplätze
HTU Fachschaft Elektrotechnik Gußhausstr. (1. Stock)	8 PC Arbeitsplätze
HTU Fachschaft Informatik (INF) Treitlstraße 3 (1. Stock)	11 PC-Arbeitsplätze 9 VT 320 Terminals
HTU Fachschaft Physik (FH 2. Stock)	12 PC-Arbeitsplätze
HTU Fachschaft Bauingenieure (BIZ)	11 PC-Arbeitsplätze
HTU Fachschaft Chemie (FCH) Gumpendorferstr. 1a	10 PC-Arbeitsplätze 1 Laserdrucker

Im Eingangsbereich Freihaus wurde ein „INFO-CORNER“ eingerichtet, 6 Stück (line-orientierte) Terminals, die an einen Terminalserver angeschlossen sind, ermöglichen den einfachen und raschen Zugang zu den UNIX-Studentenservern und eignen sich gut zum raschen Mail- oder News-Lesen.

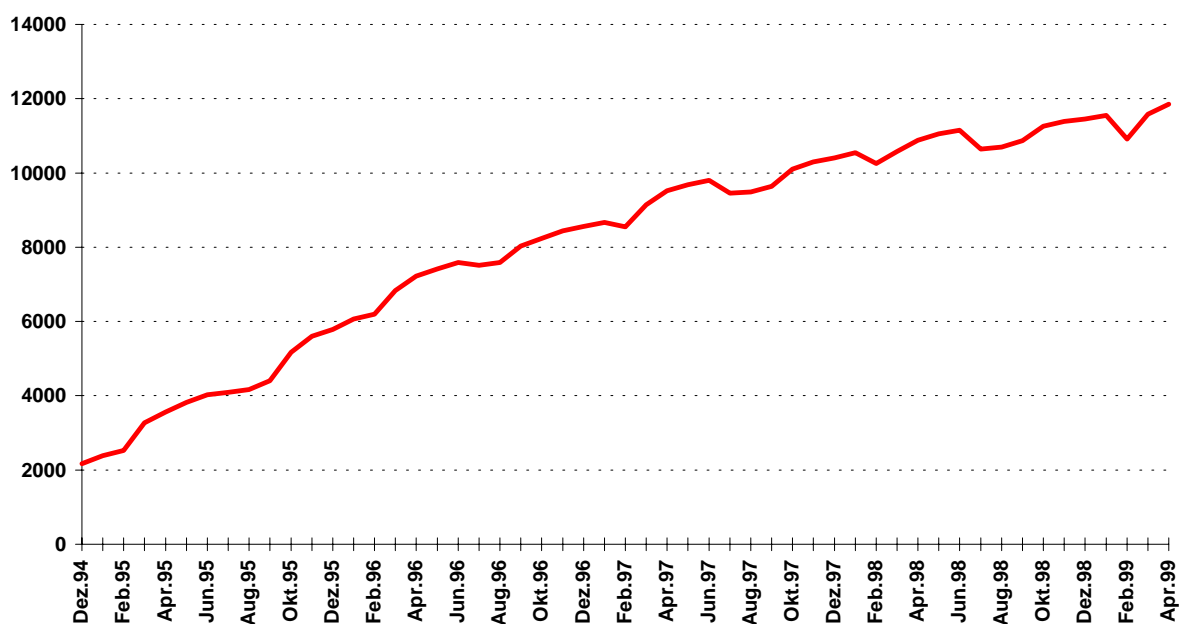


### Linux in den Internet-Räumen

Nach dem (positiven) Abschluss des Probetriebes im WS 1996/97 wurde Linux voll in den Boot-Vorgang der PCs eingebunden, über einen eigenen Menüpunkt konnte W95 oder Linux gebootet werden. Mitte 1997 wurde ein eigener Boot-Server (Pentium 200, 128 MB Hauptspeicher, 10 GB Platten) für Linux (mars.zserv) aufgebaut, der mit 100 Mbit/s an das Internet-Raum-Netzwerk angeschlossen ist.

Linux läuft zufriedenstellend und stabil. Dieses Betriebssystem wird vor allem in den Fachschaftsräumen Informatik und Elektrotechnik verwendet, ca. 20% der PCs werden unter Linux gebootet.

Studenten-Usernummern (Summe) auf den Servern stud1, stud2, fbma und stud3



## Wählleitungszugang

Seit 1. November 1997 kann der Wählleitungsanschluss der TU Wien auch über den sogenannten „Online-Tarif“ der PTA erreicht werden. Mitte 1998 wurde die Anzahl der gleichzeitig verfügbaren Wählleitungszugänge auf 180 Kanäle aufgestockt (analog und ISDN), Geschwindigkeit bis 56 kbit/s.

## Online-Zugang über TeleWeb

Mitte 1998 wurde ein Vertrag zwischen der TU Wien und der Firma Telekabel abgeschlossen, der für Mitarbeiter und Studierende der TU Wien (die berechtigt sind, das Internet-Service zu nutzen) ein TeleWeb Privatpaket zu einem monatlichen Fixpreis von öS 390.- enthält. Damit ist ein zeitlich und mengenmäßig unbegrenzter Zugang zum Internet über den TU Proxy gegeben.

## Zusammenfassung und Ausblick

Die Nutzung des Internet-Service durch Studierende der TU Wien steigt laufend, eine Anpassung der Serverkomponenten ist daher laufend notwendig. Für 1999 ist der Ersatz der über 4 Jahre alten IBM-Systeme stud1 und stud2 geplant, beide Systeme werden durch ein System HP 390 mit 2 Prozessoren (HP PA-8200, 240 MHz) und 512 MB Hauptspeicher (stud4.tuwien.ac.at) ersetzt.

Das System stud3 wird um einen weiteren Prozessor und zusätzlich 256 MB erweitert, sodass ab Herbst 1999 auch dieses System mit 2 Prozessoren (HP PA-8000, 180 MHz) und 512 MB Hauptspeicher ausgestattet ist. Weiters ist eine Erweiterung der Plattenkapazitäten geplant, sodass nach der Installation der neuen Hardware eine Erhöhung der Disk-Quoten im Mail-Bereich wie im Home-Bereich erfolgen wird.

Ein offenes Problem stellt die Zugangsmöglichkeit zu diesem Service für Studierende im ersten Semester dar. Nach den geltenden Berechtigungskriterien kann dieses Service frühestens im 2. Semester (wenn entsprechende Prüfungen abgelegt wurden) genutzt werden. Nach der Entwicklung des Softwarepaketes SIDES-4mi (personalisiertes Informations- und Kommunikationssystem für die Lehre) steigt der Wunsch nach der Zulassung von Erstsemestrigen zum Internet-Service. Für die UNIX-Studentenserver ist das ohne Probleme realisierbar, ein großes Problem stellt die Raumsituation für die PC-Arbeitsplätze dar. Von Seiten des Zentralen Informatikdienstes kann einer Ausweitung um ca. 2.000 Studierende nur dann zugestimmt werden, wenn zumindest ein weiterer Internet-Raum mit ausreichenden PC-Arbeitsplätzen geschaffen wird. Nur so kann verhindert werden, dass eine Verschlechterung der Services eintritt.

Anfang Mai 1999 hatten 11.864 Studenten eine Usernummer, die Anzahl der berechtigten Studenten, die nach

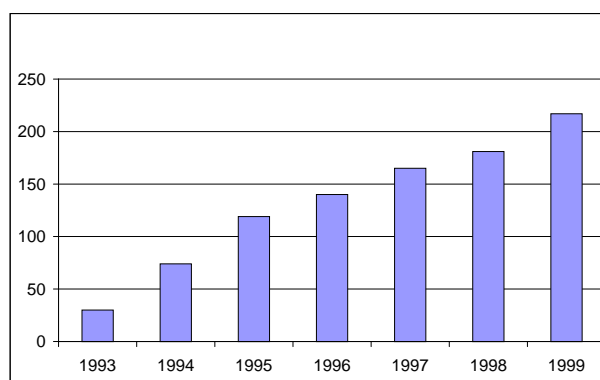
den Berechtigungskriterien das Service nutzen könnten, betrug nach den Daten der ADV-Abteilung der TU Wien 14.465.

## Internet-Räume

Im April 1999 wurden als Ersatz für die über 3 Jahre alten Windows NT Server neue Serversysteme gekauft. Nach einer intensiven Testphase wurde die Entscheidung getroffen, jeden der drei „großen“ Boot-Server durch einen NT-Cluster – bestehend aus 2 Rechnern (Intel Pentium II mit 400 MHz, 384 MB Hauptspeicher, 4 GB Systemplatte) und einem RAID-System (3 x 4 GB) und je einer 100 MB Netzwerkkarte – zu ersetzen. Diese Konfiguration verfügt über eine deutlich höhere Netz-Durchsatzleistung und über eine höhere Ausfallsicherheit als ein Einfach-Serversystem. Der schrittweise Ersatz der alten NT-Server ist bis Mitte 1999 geplant.

Um die schwierige Situation bei den Arbeitsplätzen zu verbessern, wurden in einem eigenen Projekt „**Datentankstelle**“ die Möglichkeiten untersucht, an verschiedenen Standorten in der TU Wien Ethernet-Steckdosen zu installieren, um einen privaten Laptop an das lokale Netzwerk der TU Wien anschließen zu können. Aus Sicherheitsgründen musste gewährleistet sein, dass nur Studenten mit einer gültigen Usernummer für das Internet-Service diese Anschlüsse nutzen dürfen (volle Validierung mit Usernummer und Passwort). Nach umfangreichen Tests wurde eine Lösung für Laptops unter Windows 95/98 und WNT entwickelt, für Rechner unter Linux ist eine Lösung in Arbeit. Diese Datentankstellen stehen zur Zeit am INFO-Corner (Freihaus), in der Fachschaft Informatik und Elektrotechnik und im Internet-Raum Gußhausstraße zur Verfügung.

Eine deutliche Verbesserung der Situation bei den PC-Arbeitsplätzen ist der geplante **Internet-Raum in der Favoritenstraße 11** (Erdgeschoss), in dem 33 PCs und ein Drucker aufgestellt werden. Die Inbetriebnahme ist für Oktober 1999 geplant. Im folgenden Diagramm ist die Entwicklung der PC-Arbeitsplätze in den Internet-Räumen beginnend mit 1993 zu sehen.



PC-Arbeitsplätze 1994 -1999

Im Bereich der Wählleitungen sind weitere Aufstockungen vorgesehen (siehe auch Artikel auf Seite 28).

# Wie schnell sind schnelle Fourier-Transformationen ?

Herbert Karner

karner@titania.tuwien.ac.at

Christoph W. Überhuber

christof@uranus.tuwien.ac.at

Institut für Angewandte und Numerische Mathematik, Technische Universität Wien

Die Erfindung immer leistungsfähigerer Algorithmen hat die Problemlösungskapazität moderner Computersysteme mindestens genauso stark vorangetrieben wie die Fortschritte der Computertechnologie in den letzten Jahrzehnten. Ein Meilenstein war die Erfindung der „schnellen Fourier-Transformation“ (FFT). Dieser Algorithmus wurde in Dutzenden Programmen in höchst unterschiedlicher Qualität implementiert. Die Geschwindigkeit der verschiedenen FFT-Programme kann – je nach Problemgröße und Computertyp – um mehr als das Zehnfache divergieren. Im folgenden Beitrag wird der Frage nachgegangen, welche Softwareprodukte sich für wirklich schnelle Fourier-Transformationen eignen.

Diskrete Fourier-Transformationen (DFTs) finden vielfältige Anwendungen im Bereich der Natur- und Ingenieurwissenschaften, sei es bei der Filterung gestörter Signale oder im Rahmen der numerischen Lösung von partiellen Differentialgleichungen. Andere – „alltägliche“ – Anwendungen der DFT findet man z. B. in Computertomographen oder bei der Kompression von Audio- und Video-Daten (MP3 bzw. MPEG) zur Übermittlung im Internet.

Kern der DFT ist eine spezielle Matrix-Vektor-Multiplikation. Für einen Datenvektor der Länge  $N$  erfordert eine solche Berechnung der DFT – größenordnungsmäßig –  $N^2$  (komplexe) Additionen und Multiplikationen. 1965 publizierten Cooley und Tukey [3] einen Algorithmus, die „schnelle Fourier-Transformation“ (engl. *fast Fourier transform* – FFT), der die Berechnungskomplexität der DFT von  $O(N^2)$  auf  $O(N \log N)$  reduziert.

Durch diese drastische Reduktion der arithmetischen Berechnungskomplexität nahm die Bedeutung von DFT-Methoden enorm zu. FFT-Routinen sind zu einem wichtigen Bestandteil aller wissenschaftlichen Programmbibliotheken, wie z.B. IMSL, NAG und ESSL, geworden. Darüber hinaus gibt es eine Vielzahl von frei erhältlichen – *public domain* – FFT-Paketen und Routinen, die über das Internet verfügbar sind.

Dieser Beitrag widmet sich dem Leistungspotential von frei verfügbaren FFT-Programmen und einigen weit verbreiteten FFT-Programmen, die in kommerziellen wissenschaftlichen Programmbibliotheken enthalten sind.

Im Rahmen eines FWF-Spezialforschungsbereichs (SFB 011 „AURORA“), der sich mit Themen des Hochleistungsrechnens beschäftigt, wurde eine umfangreiche Vergleichsuntersuchung an 24 FFT-Programmen auf 6 Computersystemen (siehe Tabelle 2) durchgeführt (Auer et al. [2]). Dabei standen zwei Fragen im Mittelpunkt:

- Welche FFT-Programme erbringen die besten Leistungen (Laufzeit und Gleitpunktleistung), d. h., wie ist der State-of-the-art (Stand der Technik) bei FFT-Algorithmen und Programmen ?
- Welche Computersysteme (an UNI und TU Wien) eignen sich besonders gut für FFT-Berechnungen und warum, d. h., welche Beziehungen bestehen zwischen bestimmten Eigenschaften der Hardware und der Leistung von FFT-Programmen ?

## Die schnellsten FFT-Programme

Die folgenden fünf FFT-Programme erzielten die besten Laufzeiten:

**FFTPACK** von Paul Swarztrauber (National Center for Atmospheric Research, Boulder, Colorado) kann als „Klassiker“ unter den FFT-Programmpaketen betrachtet werden. Die erste Version des in Fortran 77 geschriebenen Pakets wurde bereits 1973 veröffentlicht. FFTPACK-Routinen dienen als Basis für die in der IMSL-Bibliothek enthaltenen FFT-Programme. FFTPACK Version 4.1 (Nov. 1988) ist über NETLIB (<http://www.netlib.org/fftpack/index.html>) erhältlich.

**FFTW** („Fastest Fourier Transform in the West“) von Matteo Frigo und Stephen Johnson (MIT Laboratory for Computer Science) ist das zur Zeit „innovativste“ FFT-Programmpaket. In FFTW sind erste Ansätze zu einer architekturadaptiven FFT-Berechnung realisiert. In einer – zeitaufwendigen – Initialisierungsphase wird ein „Berechnungsplan“ ermittelt, der die FFT-Algorithmen an die Speicherhierarchie des Rechners anpasst. Das in ANSI C geschriebene Programmpaket ist über <http://theory.lcs.mit.edu/~fftw/> erhältlich.

**Green:** Sammlung von in C geschriebenen FFT Programmen von J. Green (Naval Undersea Warfare Center, New London, CT). Die Programme sind über <http://hyperarchive.lcs.mit.edu/HyperArchive/Archive/dev/src/ffts-for-risc-2-c.hqx> erhältlich.

**Ooura:** Sammlung von in C geschriebenen FFT-Programmen von T. Ooura (Research Institute for Mathematical Sciences, Kyoto University). Die Programme sind über <http://momonga.t.u-tokyo.ac.jp/~ooura/fft.html> erhältlich.

**Sorensen:** Sammlung von in Fortran 77 geschriebenen FFT-Programmen von H. V. Sorensen (University of Pennsylvania). Das Programm ist über <http://www.jjjj.de/fxt/sorensen.tgz> erhältlich.

## Kommerzielle FFT-Programme

Zusätzlich zu den fünf besten, frei verfügbaren FFT-Programmen werden in diesem Beitrag auch die am häufigsten benutzten kommerziellen FFT-Programme einer Bewertung unterzogen.

**IMSL Fortran 77 Bibliothek:** Detaillierte Informationen zu den IMSL-Programmbibliotheken der Visual Numerics Inc. sind über <http://www.vni.com/products/ims1/> erhältlich.

**NAG Fortran 77 Bibliothek:** Detaillierte Informationen zu den numerischen Programmbibliotheken der NAG Ltd. sind über <http://www.nag.co.uk/> erhältlich.

**„Numerical Recipes“ Software:** Die in der Buchreihe *Numerical Recipes – The Art of Scientific Programming* (Press et al. [6]) in den Programmiersprachen Fortran 90, Fortran 77, Pascal, C und BASIC veröffentlichten FFT-Programme sind über den Buchhandel oder über <http://www.nr.com/com/storefront.html> zu erwerben.

Tabelle 1 gibt eine Übersicht über die wichtigsten Merkmale der untersuchten FFT-Software. Dabei zeichnen sich die frei verfügbaren FFT-Programme durch die (teils wesentlich) bessere Leistung und die kommerziellen FFT-Programme durch die (meist) größere Funktionalität aus.

	Länge $N$	Dimension(en)	Leistung
FFTPACK	beliebig	1-D	sehr gut
FFTW	beliebig	1-D, 2-D, ...	sehr gut
Green	$2^n$	1-D	sehr gut
Ooura	$2^n$	1-D	sehr gut
Sorensen	$2^n$	1-D	gut
Num. Recipes	$2^n$	1-D, 2-D, 3-D	befriedigend
IMSL F77	beliebig	1-D, 2-D, 3-D	gut
NAG F77	beliebig	1-D, 2-D, ...	genügend

Tabelle 1: FFT-Software, die in diesem Beitrag behandelt wird.

## Leistungsbeurteilung

Für den Benutzer eines Computersystems, der auf die Lösung einer konkreten Aufgabenstellung wartet, ist vor allem die dafür erforderliche Zeit von Interesse, die von zwei Einflussgrößen – Arbeit und Leistung – abhängt:

$$\text{Zeit} = \frac{\text{Arbeit}}{\text{Leistung}_{\text{effektiv}}} = \frac{\text{Arbeit}}{\text{Leistung}_{\text{maximal}} \cdot \text{Wirkungsgrad}}$$

Für den Anwender sind daher folgende Kenngrößen von Interesse:

1. Die zu verrichtende *Arbeitsmenge*, die sowohl von der Art und Komplexität der Problemstellung als auch von Eigenschaften des Lösungsalgorithmus abhängt. Die Arbeitsmenge und damit der Zeitbedarf für die Problemlösung kann durch algorithmische Verbesserungen reduziert werden. So reduzieren z. B. FFT-Algorithmen die erforderliche Arbeitsmenge für eine diskrete Fourier-Transformation (eines Datenvektors der Länge  $N$ ) von  $2N^2$  auf ungefähr  $5N \log N$  arithmetische Operationen.
2. Die *Maximalleistung* ist ein Hardware-Charakteristikum des eingesetzten Computersystems, das von speziellen Anwendungsproblemen unabhängig ist. Die Anschaffung neuer Hardware mit größerer Maximalleistung führt (fast) immer zu einer Verringerung des Zeitbedarfs der Problemlösung.
3. Der *Wirkungsgrad* ist der Prozentsatz der Maximalleistung, der bei der Ausführung einer bestimmten Arbeitsmenge erreicht wird. Er bringt zum Ausdruck, in welchem Ausmaß die potentiellen Möglichkeiten des Computersystems von einem Programm genutzt werden. Er ist also eine Maßzahl dafür, wie gut die Implementierung, also die Umsetzung des Algorithmus in ein Computerprogramm, gelungen ist. Eine Erhöhung des Wirkungsgrades lässt sich durch Optimieren der Programme herbeiführen (siehe Überhuber [7]).

Die Rechenzeit der verschiedenen FFT-Programme kann – je nach Problemgröße und Computertyp – um mehr als das Zehnfache divergieren. Diese extremen Rechen-

zeitunterschiede sind größtenteils auf Implementierungs- und damit auf Wirkungsgradunterschiede zurückzuführen.

**Maximale Gleitpunktleistung:** Eine wichtige Hardware-Kennzahl ist die *Maximalleistung* (*peak performance*)  $P_{\max}$  eines Computers. Sie entspricht der theoretisch möglichen Maximalanzahl von Gleitpunkt-Operationen, die von diesem Computer pro Zeiteinheit durchgeführt werden können. Falls sich  $P_{\max}$  auf die pro Sekunde ausführbaren Gleitpunktoperationen bezieht, so erhält man die *maximale Gleitpunktleistung* mit der Einheit **flop/s** (*floating-point operations per second*) bzw. Mflop/s ( $10^6$  flop/s) oder Gflop/s ( $10^9$  flop/s).

Tabelle 2 zeigt die maximalen Gleitpunktleistungen der in der Studie verwendeten Computersysteme.

Computersystem	Maximalleistung
DEC AlphaServer 8200 5/440	880 Mflop/s
HP 9000/K460-XP	720 Mflop/s
IBM RS/6000-397	640 Mflop/s
SGI Cray Origin 2000	500 Mflop/s
Compaq PowerMate 8100e PC	400 Mflop/s
SGI Power Challenge XL	390 Mflop/s

Tabelle 2: Maximale Gleitpunktleistung (eines einzelnen Prozessors) der verwendeten Computersysteme.

**Empirische Gleitpunktleistung:** Wenn man die in einem Zeitraum  $T$  verrichtete Arbeit durch die Anzahl  $W_F$  der in  $T$  ausgeführten Gleitpunktoperationen charakterisiert, so erhält man die *Gleitpunktleistung* (*floating-point performance*)

$$P_F[\text{flop/s}] = \frac{W_F}{T} = \frac{\text{Anzahl der ausgeführten Gleitpunktoperationen}}{\text{Zeitdauer in Sekunden}}$$

Im Gegensatz zu der rechnerisch ermittelten Maximalleistung gewinnt man diesen empirischen Wert durch Messungen an laufenden Programmen. Zahlenangaben erfolgen wie bei der analytischen Leistungsbewertung in Mflop/s oder Gflop/s. Für diesen Beitrag wurden nur die Ergebnisse der komplexen FFT-Programme bei Transformationslängen  $N = 2^n$ ,  $n \in \{5, 6, \dots, 21\}$  verwendet.

**Zeitmessung:** Die Tabellen 3 und 4 zeigen gemessene Rechenzeiten von acht verschiedenen FFT-Programmen. In Tabelle 4 sind die Slow-down-Faktoren (relativen Rechenzeiten bezogen auf den jeweils schnellsten Fall) dargestellt. Bemerkenswert ist vor allem das schlechte Abschneiden des NAG-Programms, das durchschnittlich sechsmal mehr Rechenzeit benötigt als die jeweils schnellsten Programme.

FFT-Programm	Transformationslänge $N$			
	$2^5$	$2^{10}$	$2^{15}$	$2^{20}$
FFTPACK / <i>cfft</i>	7 $\mu$ s	239 $\mu$ s	47,5 ms	32,8 s
FFTW	5 $\mu$ s	261 $\mu$ s	24,5 ms	8,3 s
Green	8 $\mu$ s	254 $\mu$ s	22,3 ms	—
Ooura	5 $\mu$ s	233 $\mu$ s	28,0 ms	13,0 s
Sorensen	10 $\mu$ s	286 $\mu$ s	50,9 ms	—
Num. Recipes	13 $\mu$ s	483 $\mu$ s	50,0 ms	32,6 s
IMSL / <i>dfftc</i>	10 $\mu$ s	398 $\mu$ s	60,0 ms	32,3 s
NAG / <i>c06fc</i>	58 $\mu$ s	1400 $\mu$ s	73,5 ms	21,5 s

Tabelle 3: Absolute Laufzeiten komplexer FFT-Programme auf einem Prozessor des ZID-Servers SGI Power Challenge XL.

FFT-Programm	Transformationslänge $N$			
	$2^5$	$2^{10}$	$2^{15}$	$2^{20}$
FFTPACK / <i>cfft</i>	1,4	<b>1,0</b>	2,1	4,0
FFTW	<b>1,0</b>	1,1	1,1	<b>1,0</b>
Green	1,6	1,1	<b>1,0</b>	—
Ooura	<b>1,0</b>	<b>1,0</b>	1,3	1,6
Sorensen	2,0	1,2	2,3	—
Num. Recipes / <i>four1</i>	2,6	2,1	2,2	3,9
IMSL / <i>dfftc</i>	2,0	1,7	2,7	3,9
NAG / <i>c06fc</i>	11,6	6,0	3,3	2,6

Tabelle 4: Slow-down-Faktoren (relative Rechenzeiten bezogen auf den jeweils schnellsten Fall) auf dem ZID-Server SGI Power Challenge XL.

**Flop-count:** Für eine exakte Bestimmung der empirischen Gleitpunktleistung muss die genaue Anzahl der ausgeführten Gleitpunktoperationen (z. B. mit Hilfe von PMCs<sup>1</sup>) bestimmt werden. Wie man aus Abb. 1 erkennen kann, ist die in der Literatur oft verwendete Näherungsformel  $W_F = 5N \log N$  für die arithmetische Komplexität von FFT-Algorithmen nur sehr ungenau. Würde diese Formel stimmen, dann müsste die normalisierte arithmetische Komplexität  $W_F / N \log N$  für alle  $N$  den konstanten Wert 5 haben. Der Grund für die niedrigeren Werte und für das nichtkonstante Verhalten liegt darin, dass verschiedene FFT-Implementierungen Multiplikationen mit den trivialen Einheitswurzeln 1,  $-1$ ,  $i$  und  $-i$  unterschiedlich behandeln (zu vermeiden suchen).

**Wirkungsgrad:** In Abb. 2 ist die gemessene (empirische) Gleitpunktleistung der fünf leistungsfähigsten FFT-Programme auf dem ZID-Server SGI Cray Origin 2000 in einer Wirkungsgrad-Darstellung zu sehen.

<sup>1</sup> PMCs (*performance monitor counter*) sind spezielle Prozessor-Register, die in der Lage sind, verschiedene Arten von Ereignissen, wie z. B. Cache-Misses oder die Anzahl der ausgeführten Gleitpunktoperationen, zu zählen. Die meisten modernen RISC-Prozessoren enthalten PMCs (Auer et al. [1]).

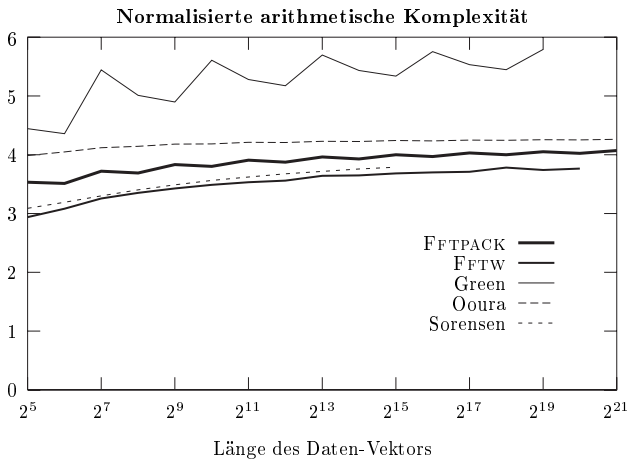


Abbildung 1: Normalisierter Flop-count ( $W_F / N \log_2 N$ ) von FFT-Programmen.

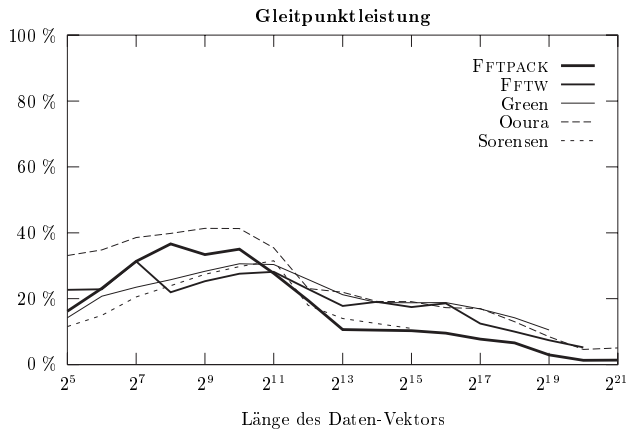


Abbildung 2: Empirische Gleitpunktleistung (Wirkungsgrad) von FFT-Programmen auf einem Prozessor des ZID-Servers SGI Cray Origin 2000 (100 % entsprechen der theoretischen Maximalleistung von 500 Mflop/s.)

## Vergleich der verwendeten Computersysteme

Den Tabellen 5 und 6 können absolute Rechenzeiten und Slow-down-Faktoren (relative Rechenzeiten bezogen auf den jeweils schnellsten Fall) des Programmpakets FFTW entnommen werden. Trotz der unterschiedlichen Maximalleistungen (siehe Tabelle 2) weisen die Workstations (von DEC, IBM und HP) ein relativ ähnliches Leistungsverhalten auf. Die SGI-Server mit ihren relativ niedrigen Maximalleistungen (pro Prozessor) benötigen durchschnittlich 2–3mal so viel Rechenzeit wie die schnellsten Workstations. Bemerkenswert ist das gute Abschneiden des PCs, der bei großen Transformationslängen – wo hohe Leistung besonders wichtig ist – mit den ZID-Servern mithalten kann bzw. die SGI Power Challenge sogar deutlich überholt.

Computersystem	Transformationslänge $N$			
	$2^5$	$2^{10}$	$2^{15}$	$2^{20}$
DEC AlphaServer 8200	4 $\mu$ s	130 $\mu$ s	16,4 ms	1,90 s
HP 9000/K460-XP	5 $\mu$ s	172 $\mu$ s	13,5 ms	1,96 s
IBM RS/6000-397	3 $\mu$ s	190 $\mu$ s	19,4 ms	1,20 s
SGI Cray Origin 2000	4 $\mu$ s	234 $\mu$ s	18,6 ms	2,65 s
SGI Power Challenge XL	5 $\mu$ s	261 $\mu$ s	24,5 ms	8,25 s
Compaq PowerMate PC	13 $\mu$ s	758 $\mu$ s	49,1 ms	2,53 s

Tabelle 5: Absolute Laufzeiten von FFTW auf verschiedenen Computersystemen.

Computersystem	Transformationslänge $N$			
	$2^5$	$2^{10}$	$2^{15}$	$2^{20}$
DEC AlphaServer 8200 5/440	1,3	<b>1,0</b>	1,2	1,6
HP 9000/K460-XP	1,7	1,3	<b>1,0</b>	1,6
IBM RS/6000-397	<b>1,0</b>	1,5	1,4	<b>1,0</b>
SGI Cray Origin 2000	1,3	1,8	1,4	2,2
SGI Power Challenge XL	1,7	2,0	1,8	6,9
Compaq PowerMate 8100e PC	4,3	5,8	3,6	2,1

Tabelle 6: Slow-down-Faktoren (relative Rechenzeiten bezogen auf den jeweils schnellsten Fall) von FFTW auf verschiedenen Computersystemen.

**SGI Cray Origin 2000 vs. SGI Power Challenge XL:** In Abb. 3 sind die normalisierten Laufzeiten der fünf leistungsfähigsten FFT-Programme auf der SGI Cray Origin 2000 dargestellt. Die normalisierten Laufzeiten dieser fünf FFT-Programme auf der SGI Power Challenge XL kann man Abb. 4 entnehmen.

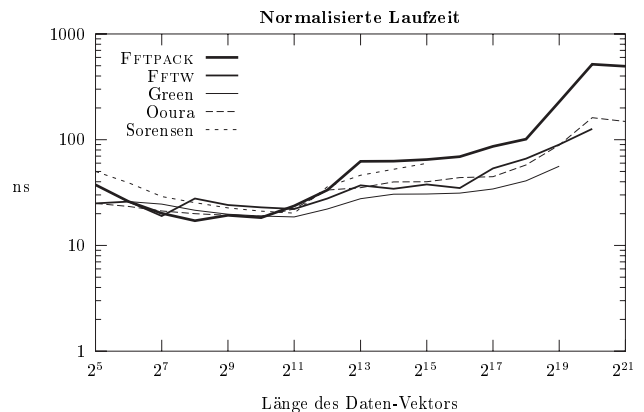


Abbildung 3: Normalisierte Laufzeit ( $T / N \log_2 N$ ) von FFT-Programmen auf einem Prozessor des ZID-Servers SGI Cray Origin 2000.

Die MIPS R10000-Prozessoren der SGI Power Challenge werden mit einer Taktfrequenz von 195 MHz betrieben, während die Prozessoren der SGI Cray Origin 2000 mit 250 MHz betrieben werden (Speed-up von 28,2 %).

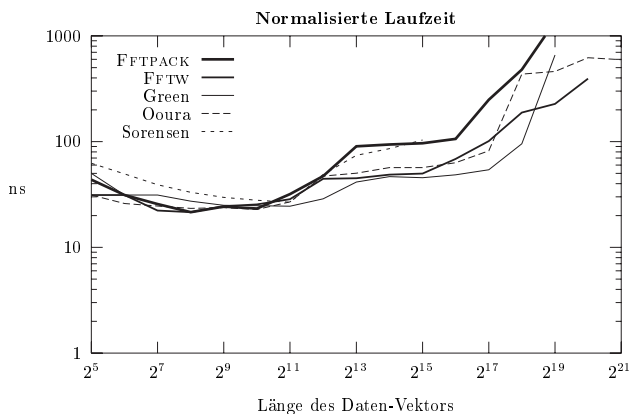


Abbildung 4: Normalisierte Laufzeit ( $T/N \log_2 N$ ) von FFT-Programmen auf einem Prozessor des ZID-Servers SGI Power Challenge XL.

Solange die FFT-Berechnung lokal im L1-Cache ausgeführt werden kann, spiegelt sich diese Relation auch in den gemessenen Laufzeiten wider. So benötigt z. B. die FFTPACK-Routine für die Transformation eines Vektors der Länge  $N=2^{10}$  auf der SGI Power Challenge 0,239 ms; auf der SGI Cray Origin werden 0,187 ms benötigt, was einem Speed-up von 28,3 % entspricht.

Aufgrund des nur 2 MB großen L2-Daten-Caches der SGI Power Challenge weisen dort sämtliche FFT-Routinen deutlich ausgeprägtere Performance-Einbrüche auf als auf der SGI Cray Origin (mit einem L2-Daten-Cache von 4 MB). So hat z. B. die getestete FFTPACK-Routine für Transformationslängen  $N \geq 2^{17}$ , aufgrund von L2-Cache-Misses, einen dramatischen Leistungsabfall auf der SGI Power Challenge XL. Für die Transformation eines Vektors der Länge  $N=2^{18}$  benötigt die Power Challenge ungefähr fünfmal so viel Rechenzeit wie die Cray Origin.

## Multiply-Add-Optimierte FFT-Programme

Zusätzlich zu den „üblichen“ Gleitpunktoperationen, wie Addition, Subtraktion, Multiplikation und Division, besitzen moderne RISC-Prozessoren auch eine Instruktion, die eine Multiplikation und eine davon abhängige Addition – die Operation  $(a \cdot b) + c$  (Multiply-Add) – in derselben Zeit wie eine einzelne Gleitpunkt-Multiplikation oder Addition ausführen kann.

Multiply-Add-Operationen haben einen großen Einfluss auf die Gleitpunktleistung. So hat z.B. der Hochleistungsrechner Cray Origin 2000 von SGI eine Zykluszeit von  $T_c = 4$  ns. In einem Taktzyklus können maximal zwei Gleitpunktoperationen – eine Multiply-Add-Instruktion – ausgeführt werden. Als maximale Gleitpunktleistung ergibt sich damit:

$$P_{\max} = \frac{N_c}{T_c} = \frac{2 \text{ Operationen}}{4 \cdot 10^{-9} \text{ Sekunden}} = 500 \text{ Mflop/s.}$$

Je geringer der Anteil der Multiply-Add-Instruktionen an der Gesamtzahl der konkret auszuführenden Gleitpunktoperationen eines Programmes ist, desto weiter entfernt sich die reale Leistung des Rechners von seiner theoretischen Maximalleistung.

In konventionellen FFT-Algorithmen ist die Anzahl der Additionen stets größer als die Anzahl der auszuführenden Multiplikationen. Es ist daher unmöglich, eine Instruktionsanordnung zu finden, die es erlaubt, alle auftretenden Additionen im Rahmen von Multiply-Add-Instruktionen auszuführen. Darüber hinaus ist es nicht einmal möglich, alle Multiplikationen im Rahmen von Multiply-Add-Instruktionen auszuführen. Eine schlechte Ausnutzung der Multiply-Add-Instruktionen (ein schlechter Wirkungsgrad) ist daher bei konventionellen FFT-Implementierungen unvermeidlich. So nutzen z. B. die in diesem Beitrag erwähnten FFT-Routinen die Multiply-Add-Instruktionen nur zu einem Prozentsatz von 20 - 25 % aus.

Den Autoren dieses Beitrags ist es gelungen, zwei völlig neue Klassen von FFT-Algorithmen zu entwickeln, die Multiply-Add-Instruktionen zu 100 % ausnutzen (Karner, Auer, Überhuber [4]):

- Eine Klasse von FFT-Algorithmen mit reduzierter arithmetischer Komplexität, und
- eine Klasse von FFT-Algorithmen, bei der die Anzahl an Speicherzugriffen auf die zur Berechnung benötigten Einheitswurzeln von  $O(N)$  auf  $O(\sqrt{N})$  reduziert wird.

## Ausblick

Die Autoren werden ihre Arbeit an der Entwicklung hocheffizienter FFT-Algorithmen und deren Implementierung auf modernen Computersystemen im Rahmen des Spezialforschungsbereiches „AURORA“ (SFB 011) unter Förderung durch den FWF fortsetzen. Interessierte Leser sind herzlich eingeladen, mit den Autoren Kontakt aufzunehmen.

## Literatur

- [1] M. Auer, F. Franchetti, H. Karner, C. W. Ueberhuber: *Performance Evaluation of FFT Algorithms Using Performance Counters*. AURORA Tech. Report TR1998-20, Inst. für Angew. und Num. Math., TU Wien, 1998.
- [2] M. Auer, R. Benedik, F. Franchetti, H. Karner, P. Kristöfel, R. Schachinger, A. Slateff, C. W. Ueberhuber: *Performance Evaluation of FFT Routines – Machine Independent Serial Programs*. AURORA Tech. Report TR1999-05, Inst. für Angew. und Num. Math., TU Wien, 1999.
- [3] J. W. Cooley, J. W. Tukey: *An Algorithm for the Machine Calculation of Complex Fourier Series*. Math. Comp. 19 (1965), pp. 297-301.
- [4] H. Karner, M. Auer, C. W. Ueberhuber: *Multiply-Add Optimized FFT Kernels*. Math. Models Methods Appl. Sci., erscheint 1999.
- [5] H. J. Nussbaumer: *Fast Fourier Transform and Convolution Algorithms*. Springer-Verlag, Heidelberg, 1981.
- [6] W. H. Press, B. P. Flannery, S. A. Teukolsky, W. T. Vetterling: *Numerical Recipes in C: The Art of Scientific Computing*. Cambridge University Press, Cambridge, 1992.
- [7] C. W. Ueberhuber: *Numerical Computation*. Springer-Verlag, Heidelberg, 1997.
- [8] C. F. Van Loan: *Computational Frameworks for the Fast Fourier Transform*. SIAM Press, Philadelphia, 1992.

AURORA-Reports sind über das Internet erhältlich: <http://www.vcpc.univie.ac.at/aurora/publications/>

# Personelle Veränderungen



Mit 1. März 1999 hat Herr **Dipl.-Ing. Wolfgang Meyer** (E-Mail: meyer@zid.tuwien.ac.at, Nebenstelle 42050) seine Tätigkeit als neuer Referatsleiter Netz-Hardware in der Abteilung Kommunikation aufgenommen. Zu seinen Aufgaben zählt unter anderem die Planung und die Koordination des Ausbaus bzw. der Erneuerung sowie Wartung der TUNET Infrastruktur (Verkabelung, Switches, Repeater) im Instituts- und Gebäudebereich. Er ist daher Ansprechpartner der Institute bei Änderungs-/Erweiterungswünschen der Institute in diesem Bereich.



Herr **Dipl.-Ing. Johann Klasek** (E-Mail: klasek@zid.tuwien.ac.at, Nebenstelle 42049), bisher am Institut für Rechnergestützte Automation tätig, übernimmt die Agenden von Herrn Dipl.-Ing. Rathmayer, der in der Abteilung Zentrale Services neue Aufgaben übernommen hat. Zu seinen Aufgaben zählen die Betreuung des News-Services sowie gemeinsam mit Frau Dipl.-Ing. Donnaberg die Betreuung der Services White Pages, Mail Router und POP.

Frau **Anna Tarkus**, bisher in der Vermittlung tätig, wechselte mit 1. Juni 1999 in die Poststelle. Wir wünschen ihr auf ihrem weiteren Weg viel Erfolg und alles Gute.

Herr **Dieter Preiner**, der uns seit Sommer vorigen Jahres bei der Bewältigung der Telefoninstallation tatkräftig unterstützte, verlässt uns, um sich wieder voll dem Abschluss seines Studiums zu widmen. Wir wünschen ihm dabei und bei seinem zukünftigen Weg viel Erfolg und alles Gute.

Herr **Michael Krausz** und Herr **Wolfgang Leithner** haben Anfang des Jahres auf eigenen Wunsch den Zentralen Informatikdienst verlassen und sind in der Privatwirtschaft tätig. Wir wünschen ihnen viel Erfolg in ihrer weiteren beruflichen Laufbahn.

Völlig unerwartet ist am 1. April 1999 Herr **Anton Roza** im 59. Lebensjahr verstorben. Er begann im Jahre 1968 als Operator am Institut für Numerische Mathematik, hat dann an der Digitalrechenanlage und am IEZ verschiedene organisatorische Aufgaben wahrgenommen und war zuletzt für die Administration der Betriebsmittelanfragen und der Betriebsstatistiken für die zentralen Applikationsserver zuständig. Wir haben ihm am 21. April am Alt-Simmeringer Friedhof das letzte Geleit gegeben.

Frau **Elli Widmann** hat am 1. April 1999 den wohlverdienten Ruhestand angetreten. Sie war uns seit 1981, anfangs an der Prozeßrechenanlage, dann im reorganisierten EDV-Zentrum, eine wertvolle Kraft in der Administration und Buchhaltung. Wir wünschen ihr alles Gute und viel Lebensfreude.



Seit 26. April 1999 ist Herr **Klaus Peter Egler** halbtags am ZID angestellt (E-Mail: egler@zid.tuwien.ac.at, Nebenstelle 42094). Er ist im Bereich Internet-Räume für Hard- und Software der PC-Clientsysteme zuständig.



Herr **Stefan Gombar** ist seit 3. Mai 1999 halbtags am ZID angestellt (E-Mail: gombar@zid.tuwien.ac.at, Nebenstelle 42081). Sein Aufgabengebiet ist die Mitarbeit bei der Betreuung des Servers des neuen lokalen Bibliothekssystems der TU Wien.

Allen neuen Mitarbeitern wünschen wir viel Freude und Erfolg bei ihrer jeweiligen Tätigkeit.



# Server-Zertifikate des Zentralen Informatikdienstes



Die sichere Kommunikation zwischen Client und Server umfasst Vertraulichkeit, Integrität und Authentizität. Die ersten beiden Punkte werden durch Verschlüsselung abgedeckt, der letzte durch Passworte (dem Server gegenüber) und Serverzertifikate (dem Benutzer gegenüber). Ein – anhand der Fingerprints geprüftes – Zertifikat gibt also dem Benutzer die Gewissheit, mit dem richtigen Server zu kommunizieren.

Der Netscape Communicator und der Internet Explorer Version 5 können Serverzertifikate beim ersten Zugriff auf den jeweiligen Server laden. Mit älteren Versionen des Internet Explorers muss das Zertifikat explizit geladen werden.

## Fingerprints

info.tuwien.ac.at (Informationsserver für die TU Wien)

4D:EB:13:25:06:B8:A1:9A:5E:89:7D:8D:C5:2F:A2:DD

iu.zid.tuwien.ac.at (Campussoftware Verwaltung)

A0:FF:97:E3:25:5D:07:B9:20:CC:84:D6:88:05:EB:0F

swd.tuwien.ac.at (Campussoftware Verteilung)

1F:DD:05:AA:92:20:81:29:97:BD:07:09:02:68:16:7D

# Wählleitungen

01 / 589 32

**Normaltarif**

07189 15893

**Online-Tarif**  
(50 km um Wien)

Datenformate:

300 - 56000 Bit/s (V.90)

MNP5/V.42bis

PPP

ISDN

Synchronous PPP

---

## Auskünfte, Störungsmeldungen

### Sekretariat

Tel.: 58801-42001  
E-Mail: sekretariat@zid.tuwien.ac.at

### TUNET

Störungen  
Tel.: 58801-42003  
E-Mail: trouble@noc.tuwien.ac.at

Rechneranmeldung  
E-Mail: hostmaster@noc.tuwien.ac.at

### Standardsoftware Service-Line

Tel.: 58801-42004  
E-Mail: campus@zid.tuwien.ac.at

### Zentrale Server, Operating

Tel.: 58801-42005  
E-Mail: operator@zid.tuwien.ac.at

### Internet-Räume

Tel.: 58801-42006  
E-Mail: studhelp@zid.tuwien.ac.at

### Telekom

Hotline: 08 (nur innerhalb der TU)  
E-Mail: telekom@noc.tuwien.ac.at  
Chipkarten: 58801-42062

### Netz- und Systemsicherheit

E-Mail: security@tuwien.ac.at

---

## Öffnungszeiten

### Sekretariat

Freihaus, 2. Stock, gelber Bereich

Montag bis Freitag  
8 Uhr bis 13 Uhr

- Ausgabe und Entgegennahme von Formularen für Benutzungsbewilligungen für Rechner des ZID,
- Internet-Service für Studierende: Vergabe von Benutzungsbewilligungen, die nicht automatisch erteilt werden können,
- allgemeine Beantwortung von Benutzeranfragen, Weiterleitung an fachkundige Mitarbeiter.

Telefonische Anfragen: 58801-42001

### Internet-Räume

Die Internet-Räume (in den Gebäuden Hauptgebäude, Freihaus, Gußhausstraße, Treitlstraße, Gumpendorferstraße,

Hauptbibliothek) sind im Regelfall entsprechend den Öffnungszeiten des jeweiligen Gebäudes geöffnet. An Sonn- und Feiertagen ist kein Betrieb. Genauere Information unter <http://www.ben.tuwien.ac.at/ben/Zeiten.html>

### Operator-Ausgabe

Freihaus, 2. Stock, roter Bereich

Montag bis Freitag  
7 Uhr 30 bis 20 Uhr

- Ausgabe für Farbdrucker, Diaservice.
- Passwortvergabe für das Internet-Service für Studierende.
- Ausgabe diverser Informationen für Studierende, Weiterleitung von Anfragen an fachkundige Mitarbeiter.

# Personalverzeichnis

## Telefonliste, E-Mail-Adressen

Zentraler Informatikdienst (ZID)  
der Technischen Universität Wien  
Wiedner Hauptstraße 8-10 / E020  
A - 1040 Wien  
Tel.: (01) 58801-42000 (Leitung)  
Tel.: (01) 58801-42001 (Sekretariat)  
Fax: (01) 58801-42099  
WWW: <http://www.zid.tuwien.ac.at/>

### Leiter des Zentralen Informatikdienstes:

W. Kleinert 42010 [kleinert@zid.tuwien.ac.at](mailto:kleinert@zid.tuwien.ac.at)

### Administration:

A. Müller 42015 [mueller@zid.tuwien.ac.at](mailto:mueller@zid.tuwien.ac.at)  
M. Haas 42018 [haas@zid.tuwien.ac.at](mailto:haas@zid.tuwien.ac.at)

### Öffentlichkeitsarbeit

I. Husinsky 42014 [husinsky@zid.tuwien.ac.at](mailto:husinsky@zid.tuwien.ac.at)

### Netz- und Systemsicherheit

U. Linauer 42026 [linauer@zid.tuwien.ac.at](mailto:linauer@zid.tuwien.ac.at)

## Abteilung Zentrale Services

<http://www.zid.tuwien.ac.at/zserv/>

### Leitung

P. Berger 42070 [berger@zid.tuwien.ac.at](mailto:berger@zid.tuwien.ac.at)  
W. Altfahrt 42072 [altfahrt@zid.tuwien.ac.at](mailto:altfahrt@zid.tuwien.ac.at)  
J. Beiglböck 42071 [beiglboeck@zid.tuwien.ac.at](mailto:beiglboeck@zid.tuwien.ac.at)  
P. Deinlein 42074 [deinlein@zid.tuwien.ac.at](mailto:deinlein@zid.tuwien.ac.at)  
P. Egler 42094 [egler@zid.tuwien.ac.at](mailto:egler@zid.tuwien.ac.at)  
H. Eigenberger 42075 [eigenberger@zid.tuwien.ac.at](mailto:eigenberger@zid.tuwien.ac.at)  
H. Fichtinger 42091 [fichtinger@zid.tuwien.ac.at](mailto:fichtinger@zid.tuwien.ac.at)  
H. Flamm 42092 [flamm@zid.tuwien.ac.at](mailto:flamm@zid.tuwien.ac.at)  
S. Gombar 42081 [gombar@zid.tuwien.ac.at](mailto:gombar@zid.tuwien.ac.at)  
W. Haider 42078 [haider@zid.tuwien.ac.at](mailto:haider@zid.tuwien.ac.at)  
E. Haunschmid 42080 [haunschmid@zid.tuwien.ac.at](mailto:haunschmid@zid.tuwien.ac.at)  
F. Mayer 42082 [fmayer@zid.tuwien.ac.at](mailto:fmayer@zid.tuwien.ac.at)  
J. Pfennig 42076 [pfennig@zid.tuwien.ac.at](mailto:pfennig@zid.tuwien.ac.at)  
M. Rathmayer 42086 [rathmayer@zid.tuwien.ac.at](mailto:rathmayer@zid.tuwien.ac.at)  
J. Sadovsky 42073 [sadovsky@zid.tuwien.ac.at](mailto:sadovsky@zid.tuwien.ac.at)  
G. Schmitt 42090 [schmitt@zid.tuwien.ac.at](mailto:schmitt@zid.tuwien.ac.at)  
E. Srubar 42084 [srubar@zid.tuwien.ac.at](mailto:srubar@zid.tuwien.ac.at)  
G. Vollmann 42085 [vollmann@zid.tuwien.ac.at](mailto:vollmann@zid.tuwien.ac.at)  
Werner Weiss 42077 [weisswer@zid.tuwien.ac.at](mailto:weisswer@zid.tuwien.ac.at)

## Abteilung Kommunikation

<http://nic.tuwien.ac.at/>

### Leitung

J. Demel 42040 [demel@zid.tuwien.ac.at](mailto:demel@zid.tuwien.ac.at)  
S. Beer 42061 [beer@zid.tuwien.ac.at](mailto:beer@zid.tuwien.ac.at)  
F. Blöser 42041 [bloeser@zid.tuwien.ac.at](mailto:bloeser@zid.tuwien.ac.at)  
S. Dangel 42066 [dangel@zid.tuwien.ac.at](mailto:dangel@zid.tuwien.ac.at)  
E. Donnaberger 42042 [donnaberger@zid.tuwien.ac.at](mailto:donnaberger@zid.tuwien.ac.at)  
S. Geringer 42065 [geringer@zid.tuwien.ac.at](mailto:geringer@zid.tuwien.ac.at)  
J. Haider 42043 [jhaider@zid.tuwien.ac.at](mailto:jhaider@zid.tuwien.ac.at)  
M. Hanold 42062 [hanold@zid.tuwien.ac.at](mailto:hanold@zid.tuwien.ac.at)  
P. Hasler 42044 [hasler@zid.tuwien.ac.at](mailto:hasler@zid.tuwien.ac.at)  
S. Helmlinger 42063 [helmlinger@zid.tuwien.ac.at](mailto:helmlinger@zid.tuwien.ac.at)  
H. Kainrath 42045 [kainrath@zid.tuwien.ac.at](mailto:kainrath@zid.tuwien.ac.at)  
J. Klasek 42049 [klasek@zid.tuwien.ac.at](mailto:klasek@zid.tuwien.ac.at)  
W. Koch 42053 [koch@zid.tuwien.ac.at](mailto:koch@zid.tuwien.ac.at)  
J. Kondraschew 42046 [kondraschew@zid.tuwien.ac.at](mailto:kondraschew@zid.tuwien.ac.at)  
I. Macsek 42047 [macsek@zid.tuwien.ac.at](mailto:macsek@zid.tuwien.ac.at)  
F. Matasovic 42048 [matasovic@zid.tuwien.ac.at](mailto:matasovic@zid.tuwien.ac.at)  
W. Meyer 42050 [meyer@zid.tuwien.ac.at](mailto:meyer@zid.tuwien.ac.at)  
R. Ringhofer 42060 [ringhofer@zid.tuwien.ac.at](mailto:ringhofer@zid.tuwien.ac.at)  
R. Vojta 42054 [vojta@zid.tuwien.ac.at](mailto:vojta@zid.tuwien.ac.at)  
Walter Weiss 42051 [weiss@zid.tuwien.ac.at](mailto:weiss@zid.tuwien.ac.at)

## Abteilung Standardsoftware

<http://sts.tuwien.ac.at/>

### Leitung

A. Blauensteiner 42020 [blauensteiner@zid.tuwien.ac.at](mailto:blauensteiner@zid.tuwien.ac.at)  
C. Beisteiner 42021 [beisteiner@zid.tuwien.ac.at](mailto:beisteiner@zid.tuwien.ac.at)  
E. Donnaberger 42036 [donnaberger@zid.tuwien.ac.at](mailto:donnaberger@zid.tuwien.ac.at)  
G. Gollmann 42022 [gollmann@zid.tuwien.ac.at](mailto:gollmann@zid.tuwien.ac.at)  
A. Klauda 42024 [klauda@zid.tuwien.ac.at](mailto:klauda@zid.tuwien.ac.at)  
M. Klug 42025 [klug@zid.tuwien.ac.at](mailto:klug@zid.tuwien.ac.at)  
H. Mastal 42079 [mastal@zid.tuwien.ac.at](mailto:mastal@zid.tuwien.ac.at)  
H. Mayer 42027 [mayer@zid.tuwien.ac.at](mailto:mayer@zid.tuwien.ac.at)  
J. Peez-Donatowicz 42028 [peez-donatowicz@zid.tuwien.ac.at](mailto:peez-donatowicz@zid.tuwien.ac.at)  
E. Schörg 42029 [schoerg@zid.tuwien.ac.at](mailto:schoerg@zid.tuwien.ac.at)  
R. Sedlaczek 42030 [sedlaczek@zid.tuwien.ac.at](mailto:sedlaczek@zid.tuwien.ac.at)  
W. Selos 42031 [selos@zid.tuwien.ac.at](mailto:selos@zid.tuwien.ac.at)  
B. Simon 42032 [simon@zid.tuwien.ac.at](mailto:simon@zid.tuwien.ac.at)  
A. Sprinzl 42033 [sprinzl@zid.tuwien.ac.at](mailto:sprinzl@zid.tuwien.ac.at)  
P. Torzicky 42035 [torzicky@zid.tuwien.ac.at](mailto:torzicky@zid.tuwien.ac.at)

Anzeige der Firma Adobe