

Einführung in die Nutzung des SchunterNet

2. Auflage – Oktober 2000

SchunterNet e.V. Braunschweig
Bienroder Weg 54 38108 Braunschweig Telefon/Fax: (0531) 2 35 14 59 www.schunternet.de

➤ ... Erläuterung im Glossar

MS-DOS, Windows, Windows 95/98, Windows NT sind eingetragene Warenzeichen der Microsoft Corporation. Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen.

Impressum:

Herausgeber: SchunterNet e.V.

Bienroder Weg 54

38108 Braunschweig

Autoren: Ronny Heidenreich, Uwe Greßhake unter Verwendung der „Wohnheimnetz FAQ“ des Studentenwohnheimes Schützenweg 42 in Oldenburg (<http://www.Fortytwo.Uni-Oldenburg.de/~waterman/FAQ/>) sowie der „Technischen Hinweise für Informationsanbieter im World Wide Web“ des Rechenzentrums der Technischen Universität Braunschweig (http://www.tu-bs.de/www/techn_hinweise/)

Dank an Andreas Lübbecke für zahlreiche Korrekturen und Ergänzungen sowie an Oliver Böhnke für die Informationen zum Macintosh.

Satz: L^AT_EX

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Der Verein SchunterNet e.V. | 5 |
| 2 | Anmeldung und Netzanschluß | 5 |
| 2.1 | Nutzervertrag | 5 |
| 2.2 | Rechner und Betriebssystem | 6 |
| 2.3 | Netzwerkkarte und MAC-Adresse | 6 |
| 2.4 | IP-Adressen und Namen | 7 |
| 2.5 | Kosten | 7 |
| 2.6 | Minimale Netzkonfiguration | 8 |
| 2.6.1 | Windows95/98 | 8 |
| 2.6.2 | WindowsNT | 11 |
| 2.6.3 | UNIX (Linux) | 16 |
| 2.6.4 | OS/2 | 17 |
| 2.6.5 | Macintosh | 17 |
| 2.7 | Abmeldung | 18 |
| 3 | Netzdienste | 18 |
| 3.1 | Electronic Mail | 18 |
| 3.2 | WWW und HTTP-Proxy | 19 |
| 3.3 | Usenet News | 20 |
| 3.4 | ICQ (I Seek You) | 22 |
| 3.5 | FTP | 23 |
| 3.6 | NTP — Time Service | 23 |
| 4 | Benutzerserver (jupiter.schunter.etc.tu-bs.de) | 23 |
| 4.1 | Zugriff auf das Homedirectory | 23 |
| 4.1.1 | ... per ftp (File Transfer Protocol) | 23 |
| 4.1.2 | ... durch Einloggen auf dem Server | 23 |
| 4.1.3 | ... per SMB-Mount | 24 |
| 4.1.4 | ... per NFS-Mount | 24 |
| 4.2 | Private Homepages | 24 |
| 5 | Sicherheit | 25 |
| 5.1 | Viren, Trojaner, Bugs | 25 |
| 5.1.1 | Computerviren | 26 |
| 5.1.2 | Trojanische Pferde (Trojan Horses) | 26 |
| 5.1.3 | Bugs | 26 |
| 5.2 | Paßwörter | 27 |
| 5.3 | ssh — Die Secure Shell | 29 |
| A | Satzung des Vereins SchunterNet e.V. | 30 |
| B | Benutzerordnung des SchunterNet e.V. | 34 |

| | | |
|----------|---|-----------|
| C | Gebührenordnung des SchunterNet e.V. | 39 |
| D | RZ-Benutzungsordnung der TU Braunschweig | 40 |
| E | Richtlinien für das TUBS-Net | 47 |
| F | WWW-Richtlinien an der TU Braunschweig | 50 |
| G | DFN-Benutzungsordnung | 54 |
| H | Glossar | 59 |

1 Der Verein SchunterNet e.V.

Um die Realisierung der Vernetzung des Studentenwohnheims An der Schunter voranzutreiben, wurde am 28. August 1997 der Verein *SchunterNet e. V.* gegründet. In diesem Rahmen wurde in Zusammenarbeit mit dem Studentenwerk, dem Rechenzentrum und nicht zuletzt verschiedenen IT-Unternehmen ein Konzept für ein Wohnheimnetz erarbeitet. Im November 1997 erhielt der Verein vom Studentenwerk ein Darlehen und den Auftrag, das Netz zu realisieren.

Am 1. Juli 1998 waren die Kabel im Haus 1 verlegt und die aktiven Komponenten angeschlossen, so daß der Probetrieb beginnen konnte. Seit September 1998 ist auch die Funkanbindung an das Rechenzentrum funktionsfähig und das *SchunterNet* offiziell in Betrieb. Im Sommersemester 1999 wurden schließlich auch die übrigen Gebäude an das Netzwerk angeschlossen.

Der *SchunterNet e. V.* betreibt das Netz, stellt die ➤Systemadministration und verwaltet die Teilnehmerdaten.

Wöchentlich wird eine Sprechstunde im Datenraum im Keller des Hauses 1 (dort wo das Logo an der Tür hängt) angeboten. Hier können Probleme beim Netzbetrieb besprochen oder der Netzantrag abgeholt und eingereicht werden. Mindestens zweimal jährlich findet zudem eine Mitgliederversammlung statt.

Da all dies von den Bewohnern neben ihrem Studium erledigt wird und die zu investierende Zeit daher begrenzt ist, sind weitere helfende Hände natürlich immer willkommen. Der *SchunterNet e. V.* ist dabei nicht als ein außenstehender Anbieter eines Netzzugangs zu betrachten, sondern vielmehr als eine rechtlich notwendige Organisationsform aller Netzteilnehmer, respektive Teil der Bewohnerschaft des Wohnheims. Jedem sollte bewußt sein, daß ohne die aktive Mitarbeit *jedes* Nutzers dieses Netz nicht entstanden wäre und in Zukunft auch nicht weiter betrieben werden kann.

2 Anmeldung und Netzanschluß

2.1 Nutzervertrag

Um einen Zugang zum *SchunterNet* zu erhalten, muß zunächst ein Antrag gestellt werden. Dieser dient zum einen der Registrierung der persönlichen und technischen Daten der Nutzer bzw. deren Computer im *SchunterNet e. V.* und im Rechenzentrum der TU zum Zwecke der ➤Administration und zum anderen als Nutzervertrag der Anerkennung der Teilnahmeregeln durch den Nutzer. Gleichzeitig erfolgt die Aufnahme in den *SchunterNet e. V.* als passives Mitglied.

Der Antrag kann den Prospektständern entnommen werden, welche sich in jedem Haus neben den Briefkästen befinden, und ist vollständig ausgefüllt und unterschrieben in

den Briefkasten des Vereins in Haus 3 einzuwerfen. Eine Postscriptversion ist auch unter <http://www.schunternet.de/SchunterNet/Verein/Dokumente/> zu finden.

Es folgen einige Hinweise zum Ausfüllen des Antrags und zu den Hintergründen.

2.2 Rechner und Betriebssystem

Rechner-Typ PC, Mac, Atari, Amiga, Sun, Cray, ...

Betriebssystem Linux, WfW 3.11, Win95/98, Win NT, MS-DOS, OS/2, MacOS, AmigaOS etc.
hier können auch mehrere angegeben werden

2.3 Netzwerkkarte und MAC-Adresse

In jedem Zimmer befindet sich eine Anschlußdose, in der Regel über der Pinwand neben der Kofferklappe. Zum Anschluß ist ein Netzwerkadapter (Ethernet-Karte) mit RJ45-Buchse und ein Anschlußkabel (Twisted Pair, RJ45, **nicht** crossed over) der benötigten Länge erforderlich. Die Bandbreite der Netzkarte bzw. der Netzanbindung kann 10 MBit/s (10BaseT) oder in stark begrenzter Anzahl 100 MBit/s (100BaseT) betragen. Macs haben seit 1996 10BaseT sowie seit 1999 10/100BaseT Ethernet eingebaut, das gilt auch für iMacs/iBooks/PowerBooks.

Jede Ethernet-Karte bzw. -Chip hat eine weltweit eindeutige Hardware-(oder ↗MAC-)Adresse, die fest in der Karte eingestellt ist. Bei älteren Ethernet-Karten ist sie auf einen der Chips aufgeklebt, bei neueren erfährt man sie entweder aus der mitgelieferten Dokumentation, oder durch ein Service-Programm, welches auf der mitgelieferten Diskette zu finden ist. Dazu wird der Rechner im MS-DOS-Mode gestartet (echtes DOS ist wichtig, also keine MS-DOS-Eingabeaufforderung oder DOS-Box unter Windows!) und das Programm `A:\setup` aufgerufen. Unter „View Configuration“ steht die Hardwareadresse (6 Byte, hexadezimal, jeweils durch Doppelpunkt getrennt). Die Adresse kann z.B. so aussehen: `00:12:6b:9f:20:cc`

Benutzer von Windows 95/98 haben noch eine weitere recht einfache Möglichkeit. Das Programm `winipcfg.exe` im Windows-Verzeichnis (meist `C:\WINDOWS`) zeigt Informationen über den Netzwerkanschluß an, unter anderem auch die Hardwareadresse. Wichtig ist hierbei, daß im entsprechenden Auswahlfeld die Ethernet-Netzwerkkarte angewählt ist (die PPP-Adresse `44:45:53:54:00:00` ist **nicht** die gesuchte). Unter ↗UNIX/Linux kann die Adresse z.B. mit dem Programm `ifconfig` abgefragt werden. Unter Windows NT findet sich das dazu nötige Programm im Startmenü unter Programme/Verwaltung (Allgemein)/Windows NT-Diagnose. Hier steht die MAC-Adresse auf der Seite „Netzwerk“ und da über den Button „Transporte“.

Beim Macintosh kann die MAC-Adresse ermittelt werden, indem man das Kontrollfeld „TCP/IP“ aufruft und dessen INFO-Button anwählt. Die hier angegebene „Hardware

Adresse“ ist die MAC-Adresse. Alternativ kann die MAC-Adresse auch mit dem „Apple System Profiler“ im Apple-Menü ermittelt werden.

2.4 IP-Adressen und Namen

Damit ein Rechner im Internet identifiziert werden kann, benötigt er eine weltweit eindeutige IP-Adresse, die euch von der ↗ Netzadministration zugeteilt wird. Für das SchunterNet stehen Adressen in den Bereichen 134.169.136.xxx und 134.169.137.xxx zur Verfügung.

Da diese Zahlenkolonnen recht unhandlich sind, erhält jeder Rechner im Wohnheim zusätzlich einen eindeutigen Namen, welcher aus einem Host- und einem Domain-Teil besteht. Die Domain unseres Wohnheims ist `schunter.etc.tu-bs.de`. Der Hostname kann frei gewählt werden und darf aus Kleinbuchstaben (keine Umlaute) und Zahlen bestehen, muß aber mit einem Buchstaben beginnen. Natürlich darf er im Wohnheim auch nur höchstens einmal vorkommen. (Bsp.: `scotty logan5 ...`). Falls es euren gewählten Rechnernamen schon gibt, müßt ihr einen anderen Namen wählen.

Aus Gründen der Handhabbarkeit wird eine Bezeichnung empfohlen, die übersichtlich, reproduzier- und merkbar ist. Überlange Zeichenfolgen, die keinen Sinn ergeben, sind das zum Beispiel nicht.

Um einen Zugang auf den Benutzerserver (Linux-PC) zu erhalten (z.B. um dort eine ↗ Homepage einzurichten oder die eingegangene ↗ E-Mail abzuholen), benötigt ihr noch einen Loginnamen. Auch dieser kann relativ frei gewählt werden, darf jedoch nicht mehr als 8 Zeichen enthalten und sollte in einem gewissen Zusammenhang mit dem zugehörigen Benutzer stehen (Vorname, Spitzname etc.) Bei der Wahl des Loginnamens sollte man beachten, daß dieser außerdem den ersten Teil der E-Mail-Adresse darstellen wird, also `loginname@schunter.etc.tu-bs.de`. Daher gilt hier die obige Empfehlung für die Zeichenfolge des Rechnernamens besonders.

2.5 Kosten

Das *SchunterNet* wurde mit einem zinsfreien Kredit des Studentenwerks finanziert, welcher im Zeitraum von fünf Jahren in monatlichen Raten zurückzuzahlen ist. Diese Kosten werden auf eine monatliche Nutzungsgebühr nach der Gebührenordnung [Anhang ??] umgelegt.

Um den Aufwand für den Kassenwart in Grenzen zu halten, ist die Zahlung nur durch Einzugsermächtigung möglich, ein Vordruck befindet sich am Netzantrag. Bitte beachtet, daß die Banken bei nicht gedecktem Konto oder aus anderen Gründen nicht ausgeführten Lastschriften Bearbeitungsgebühren erheben, die bis zu 10,- € betragen können und euch durch den Verein in voller Höhe belastet werden.

2.6 Minimale Netzkonfiguration

Bei fast allen Betriebssystemen müssen während der Installation ein paar Angaben gemacht werden, die überall gleichartig sind:

TCP/IP-Adresse bzw. Host-Adresse hier muß die sogenannte IP-Adresse des eigenen Rechners eingegeben werden, z.B. 134.169.136.255.

Jeder Computer im Wohnheim hat eine eigene IP-Adresse. Dies sind vier Zahlen von 0 bis 255 die jeweils durch einen Punkt getrennt werden. Die ersten beiden Zahlen sind innerhalb des Wohnheims (und innerhalb der TU) immer gleich und zwar 134.169. Die dritte Zahl ist im Wohnheim entweder 136 oder 137. Die IP-Adresse identifiziert genau einen Computer, also hat jeder Rechner eine andere IP-Adresse. Diese wird euch bei Annahme des Antrags von der ↗Administration mitgeteilt.

Hier wurde von dem Beispiel 134.169.136.255 ausgegangen. Anstatt der 255 muß dann die passende/richtige Endung eingesetzt werden.

Subnet mask Hier muß korrekterweise 255.255.254.0 eingegeben werden.

Netzadresse, Broadcast Wenn danach gefragt wird, muß als Netzadresse 134.169.136.0 und als Broadcastadresse 134.169.137.255 eingetragen werden.

DNS/Name Server, Router, Gateway Hier muß immer die IP-Adresse 134.169.136.1 eingegeben werden.

TCP/IP Domain Name Hier muß `schunter.etc.tu-bs.de` eingegeben werden.

Host Name oder Rechnername Hier muß der im Antrag angegebene Rechnername (siehe auch ??) eingetragen werden.

DHCP, BOOTP und DDNS Falls hiernach gefragt wird, dann sollte dies nicht ausgewählt bzw. mit nein beantwortet werden.

Ansonsten folgen hier noch ein paar Hinweise, die betriebssystemspezifisch sind:

2.6.1 Windows95/98

Damit also auf zur Maus-Klick-Orgie: Es wird davon ausgegangen, daß das Fenster „Systemsteuerung“ geöffnet ist (zu finden über das Menü Start unter Einstellungen).

Zunächst zur Netzwerkkarte und damit zum schwierigsten Teil: Wann die Karte konfliktfrei läuft und Windows95 auch überzeugt davon ist, ist nur sehr schwer festzustellen. Das hier sind einige Anhaltspunkte.

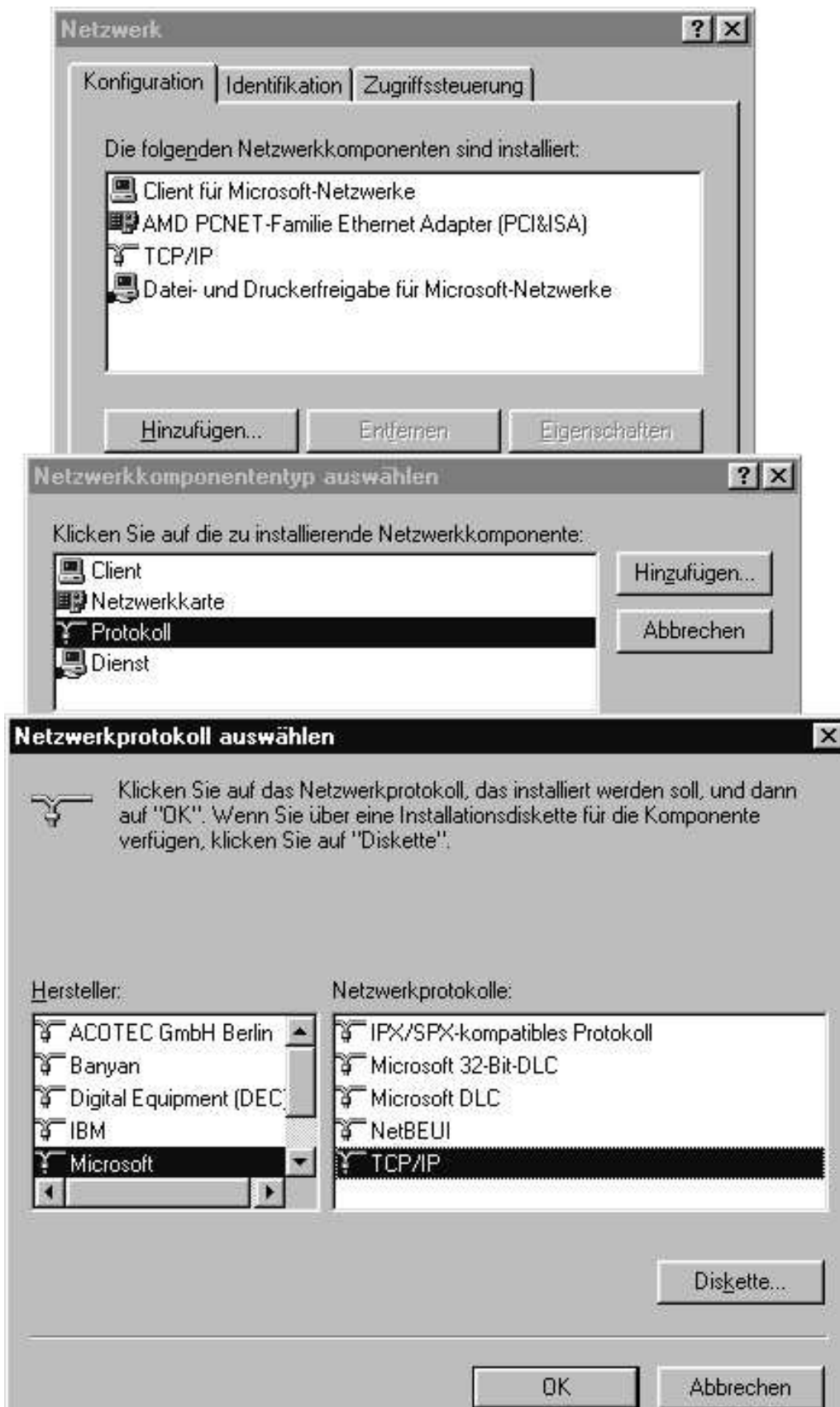


Die Karte funktioniert mit Sicherheit noch nicht, wenn

- sie unter **System** ⇒ **Geräte-Manager** ⇒ **Netzwerkkarten** gar nicht auftaucht oder
- das Netzwerkkartensymbol an besagter Stelle mit einem gelb unterlegten Rufzeichen ! versehen ist.

Die Karte funktioniert mit sehr großer Wahrscheinlichkeit, wenn

- sie unter **System** ⇒ **Geräte-Manager** ⇒ **Netzwerkkarten** auftaucht und
- nicht mit dem gelben Symbol versehen ist und
- sie unter **System** ⇒ **Geräte-Manager** ⇒ **Computer** ⇒ **Eigenschaften** nicht mit dem kleinen runden ⓘ-Symbol (blau auf weißem Grund) versehen ist.



Falls alle Bedingungen bis auf die letzte erfüllt sind, kann die Karte möglicherweise auch funktionieren. In dem Fall hilft nur Ausprobieren. Aus meinen Erfahrungen kann ich leider keine zielgerichtete Anleitung zusammenstricken, wie auftretende Konflikte beseitigt werden, aber funktioniert hat es letztendlich doch immer irgendwie. Oft ist auch Glück bzw. Willkür seitens des Betriebssystemherstellers dabei. Wenn die Karte einmal installiert ist, ist der Rest ein Kinderspiel.

Unter wird durch \Rightarrow \Rightarrow \Rightarrow \Rightarrow \Rightarrow das TCP/IP-Protokoll installiert. Über \Rightarrow werden die oben genannten Einstellungen (IP-Adresse, \nearrow Subnetmask, Gateway, \nearrow DNS-Server, Host- und Domain-Name) vorgenommen. Alle anderen Felder bleiben zunächst leer. Das NETBEUI-Protokoll sollte entfernt werden, ebenso IPX, wenn es nicht aus bestimmten Gründen ganz unbedingt benötigt wird. Der „ \nearrow Client für Netware-Netzwerke“ ist ebenfalls fürs Wohnheim ohne Bedeutung und kann entfernt werden. Wichtig ist der „ \nearrow Client für Microsoft-Netzwerke“, dieser sollte auch unter „Primäre Netzanmeldung“ (oder so ähnlich) gewählt werden. In der Registerkarte „Identifikation“ sollte nochmals der Rechnername und als Arbeitsgruppe „**schunter**“ angegeben werden.

Abgeschlossen wird jeweils mit . Dazwischen liegen beliebig viele Reboot-(= Rechnerneustart-)Vorgänge, je nachdem, wie Windows sich gerade fühlt. Wenn Windows dann zum ersten Mal nach Benutzernamen und Kennwort fragt, ist es ratsam, als Benutzernamen den Loginnamen (siehe ??) für den Wohnheimserver zu wählen. Das Paßwort ist an dieser Stelle egal und kann getrost auch weggelassen werden.

Bei der gesamten Installation ist es extrem ratsam, die Windows95/98-Installations-CD in greifbarer Nähe zu haben, da von dieser CD die Netzwerktreiber installiert werden.

2.6.2 WindowsNT

Bei der Installation des Betriebssystems ist darauf zu achten, daß der ganze Netzwerkkram mitinstalliert wird (ich weiß auch nicht, wie man das nachinstalliert, wenn es nicht schon da ist...). Zumindest sollte dann der Ordner „Netzwerkumgebung“ auf dem Desktop vorhanden sein.

Wenn man dort (mit rechter Maustaste) auswählt, erscheint ein Requester, aus dem der Computer-Name und die Arbeitsgruppe/Domäne hervorgeht. Durch kommt man in folgende Eingabemaske:

Identifikationsänderungen ? X

Anhand der folgenden Informationen wird Ihr Computer im Netzwerk identifiziert. Sie können den Computer-Namen und auch die Arbeitsgruppe oder Domäne, in der der Computer erscheinen wird, ändern. Falls angegeben, können Sie dann ein Computer-Konto in der Domäne erstellen.

Computer-Name:

Mitglied von:

☒ Arbeitsgruppe:

☐ Domäne:

☐ Computerkonto in der Domäne erstellen

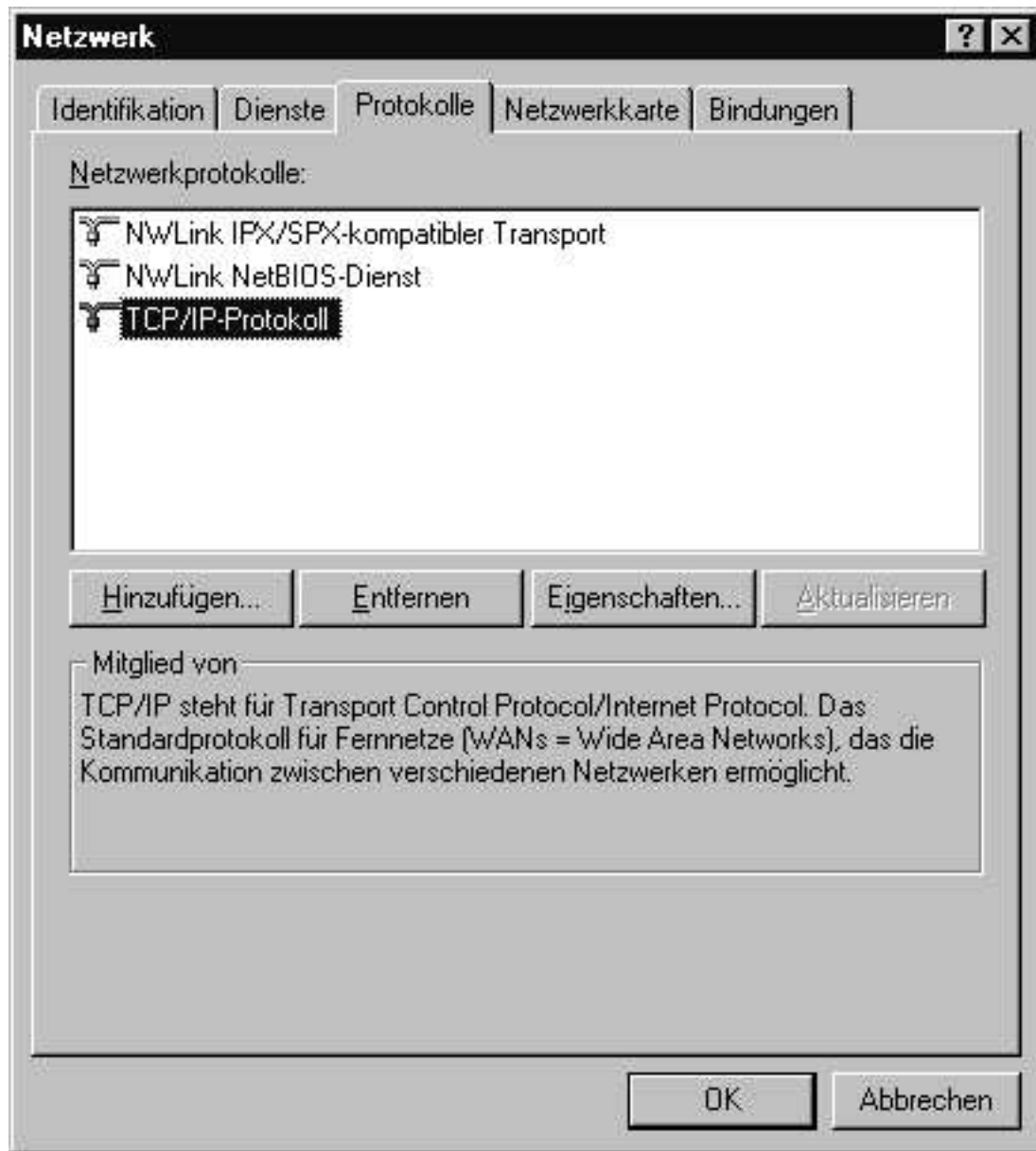
Mit dieser Option wird ein Konto in der Domäne für diesen Computer erstellt. Geben Sie ein Benutzerkonto an, mit dem Arbeitsstationen zur angegebenen Domäne hinzugefügt werden können.

Benutzername:

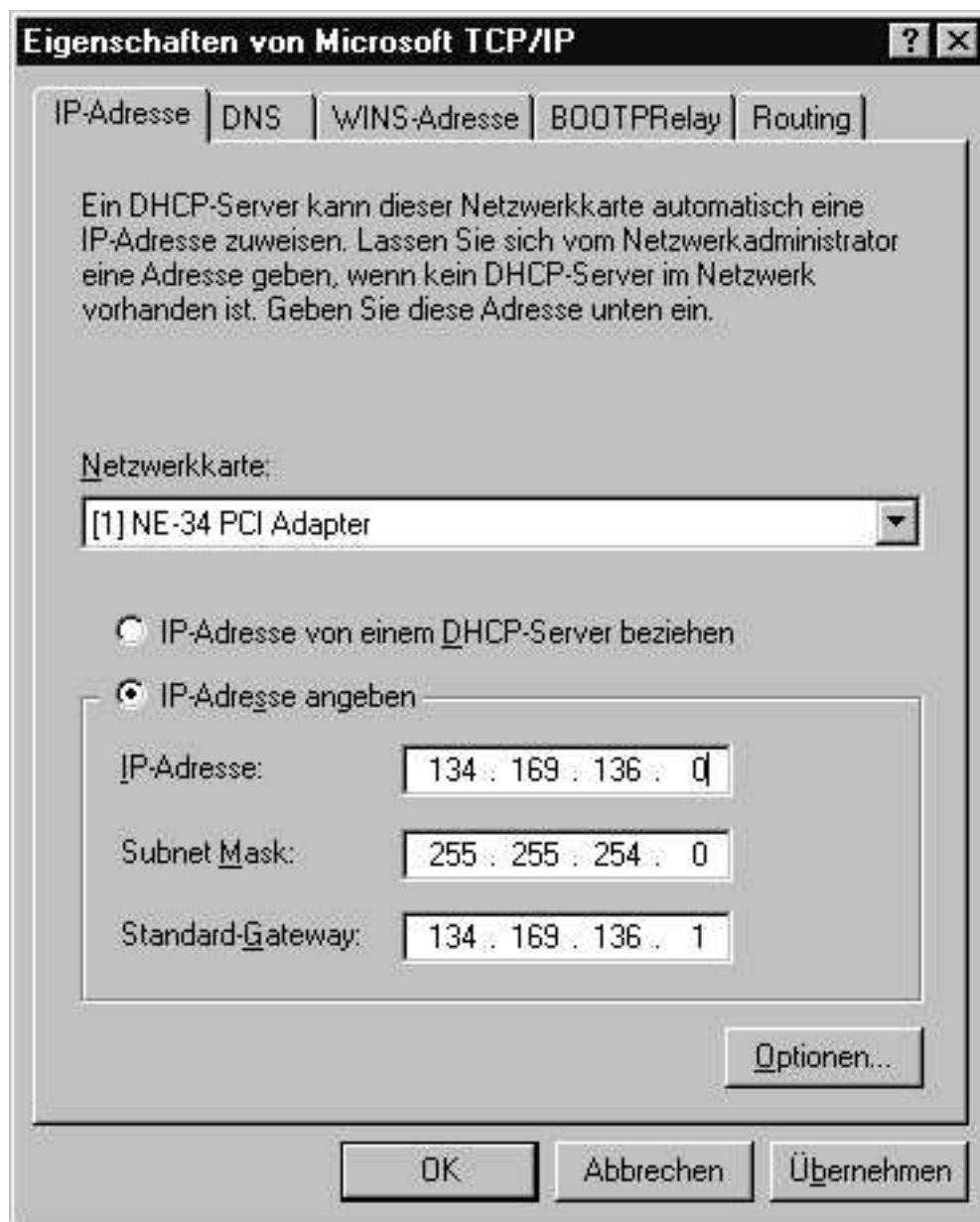
Kennwort:

OK Abbrechen

Dort ist nun der richtige Rechnername einzutragen. Des weiteren ist der Knopf für Arbeitsgruppe wichtig (eine Domäne ist nach Windows-Nomenklatur nicht das, was man darunter normalerweise versteht – und setzt einen Domänencontroller voraus, den es im SchunterNet nicht gibt). Welche Arbeitsgruppe man einträgt ist an sich egal, allerdings bekommt man später nur die Rechner sofort zu sehen, die in der selben Arbeitsgruppe sind. Im SchunterNet sind die meisten Rechner in der Gruppe **SCHUNTER** (ein paar auch in **Arbeitsgruppe** :-), zumindest ist der Server **Jupiter** dort zu finden). Das kann man jetzt mit **OK** bestätigen.



Als nächstes ist die Seite „Protokolle“ anzuwählen (s.o.). Hier sollte zumindest „TCP/IP-Protokoll“ aufgeführt sein. Wenn nicht, kann man es über „Hinzufügen“ dto. Andere Protokolle wie zu Beispiel NetBIOS oder IPX/SPX sind auch noch üblich und werden hauptsächlich von Spielen verwendet (sprich: ganz wichtig, aber nicht für diese Broschüre). Sodann wählt man „TCP/IP“ aus und geht auf Eigenschaften.... Jetzt sollte sich folgendes Bild zeigen:



Im SchunterNet gibt es keinen DHCP-Server, sprich automatische Zuteilung von IP-Adressen, also den Radiobutton „IP-Adresse angeben“ wählen. Nun trägt man nun die vom SchunterNet zugeteilte IP-Adresse, SubNetMask und Standard Gateway (=Default-Gateway) ein. Unter **Optionen...** finden sich noch verschiedene Dinge, die man braucht, wenn man selbst einen Gateway einrichten will, aber das soll hier nicht das Thema sein (genauer gesagt, ich hab es auch noch nicht probiert) – also da braucht man nichts extra eintragen. Weiter oben ist auch immer die Netzwerkkarte genannt – wiederum nur von Interesse, wenn man mehrere davon haben sollte.

Als nächstes ist noch der Nameserver einzutragen. Das geschieht auf der Seite „DNS“.



Hier ist nochmals der Host (=Rechnername) erwähnt. Die Domäne muß noch eingetragen werden: `schunter.etc.tu-bs` Bei „Suchreihenfolge für DNS“ ist noch mittels `Hinzufügen...` die IP-Adresse des Nameserver einzutragen, also im SchunterNet die 134.169.136.1 (ja, ja, das ist der selbe Rechner wie das Gateway)

Die Einstellungen für die WINS-Adresse auf der folgenden Seite bleiben leer. Der beim Bestätigen der Änderungen der Netzwerkeigenschaften erfolgende Warnhinweis, daß keine primäre WINS-Adresse eingegeben wurde, kann getrost ignoriert werden.

2.6.3 UNIX (Linux)

Zunächst muß die Netzwerkkarte vom Betriebssystemkernel erkannt werden. Angenommen, die eigene IP-Adresse lautet 134.169.136.255, und die Netzwerkkarte wurde als Interface eth0 erkannt. Dann sollten die drei Zeilen

```
root@erde:~ # ifconfig eth0 134.169.136.255 netmask 255.255.254.0 \
              broadcast 134.169.137.255
root@erde:~ # route add 134.169.136.0
root@erde:~ # route add default gw 134.169.136.1
```

ausreichen, um den Netzwerkzugriff zu erhalten. Praktischerweise werden diese Zeilen in einem der Boot-Startup-Skripte untergebracht. Abhängig von der vorliegenden ↗ UNIX-Version müssen noch die Dateien `/etc/hosts`, `/etc/host.conf` und `/etc/resolv.conf` angepaßt werden, um fremde Rechner auch über Namen und nicht nur über IP-Adressen ansprechen zu können.

So sollte das zum Beispiel aussehen:

```
# /etc/hosts
127.0.0.1      localhost
134.169.136.255 erde.schunter.etc.tu-bs.de      erde
# end of /etc/hosts

# /etc/host.conf
order hosts bind
multi on
# end of /etc/host.conf

# /etc/resolv.conf
search schunter.etc.tu-bs.de tu-bs.de
nameserver 134.169.136.1
# end of /etc/resolv.conf
```

Der Vollständigkeit halber: Ein Loopback-Device muß ebenfalls konfiguriert sein. Bei den meisten ↗ UNIX-Systemen sollte dieser Vorgang aber bereits in der Standardinstallation integriert sein. Ansonsten helfen die Manual-Pages zu `ifconfig(8)` und `route(8)` weiter.

Bei aktuellen Linux-Distributionen vereinfacht sich noch einiges. Kernel mit den notwendigen eingepackten Treibern sind meist vorhanden. Falls die Netzwerkkarte dennoch nicht gefunden wird, kann mit dem Bootparameter `ether` bzw. mit den jeweiligen Modul-Parametern nachgeholfen werden (siehe Handbuch der Distribution). Die Interface- und Routingkonfiguration sowie die ↗ DNS-Einstellungen werden von den Administrations-

und Installationswerkzeugen (z.B. YaST von S.u.S.E) weitestgehend automatisch vorgenommen. Falls Probleme auftauchen, sollte die umfangreiche Dokumentation von Linux so ziemlich alle Fragen beantworten. Wenn das zur Distribution gehörige Handbuch nicht reicht, sind die Linux-HOWTOs die nächste Anlaufstelle. Bei jeder guten Distribution liegen diese Dokumente nach der Installation irgendwo unter /usr/doc.

2.6.4 OS/2

Bei der Installation von OS/2 muß die Installation von TCP/IP-Diensten ausgewählt werden. Falls OS/2 bereits installiert ist, können die TCP/IP-Dienste auch nachinstalliert werden, indem nacheinander der Ordner „System“, der Ordner „Systemkonfiguration“ und schließlich der Ordner „Installieren/Entfernen“ geöffnet werden. Im letzteren findet sich das Programm „Netzwerkinstallation anpassen“ (oder so ähnlich). Mit diesem können die TCP/IP-Dienste nachinstalliert werden. Bei der Installation wird der Benutzer dann nach den oben genannten und folgenden Angaben gefragt:

(Netzwerk-)Adapter hier findet die Auswahl des Hardwaretreibers für die Netzwerkkarte statt. Falls eine NE2000-kompatible Netzkarte eingebaut werden soll, kann hier der Treiber für Eagle-Technology NE2000plus Ethernet Adapter ausgewählt werden. Allerdings kann dieser Treiber scheinbar keine Plug and Play-Karten automatisch erkennen. Deswegen muß eine solche Karte vor der Installation auf manuell eingestellt werden, siehe dazu Benutzeranleitung der Karte. Über Einstellungen gibt es die Möglichkeit die sogenannte Unterbrechungsebene (IRQ) und Basisadresse zu kontrollieren (wovon unbedingt Gebrauch gemacht werden sollte) oder gar zu verändern (durch Auswahl/Anklicken der Einstellung IRQ oder Basisadresse und Anklicken von Ändern). Normalerweise ist für eine Netzwerkkarte auch nur ein Hardwaretreiber erforderlich und kein weiterer.

Protokoll hier sollte einfach TCP/IP ausgewählt werden. Normalerweise ist nur dieses eine ↗ Protokoll erforderlich und kein anderes und weitere Einstellungen sind ebenfalls nicht nötig.

Eigentlich sollte beim Installieren von OS/2 bzw. den Hardware- und Netzwerktreibern alles automatisch geschehen. Der Benutzer muß bei Aufforderung nur die richtigen Daten eingeben.

2.6.5 Macintosh

Die Konfiguration des Macintosh erfolgt analog zu der für Windows 95/98 usw. beschriebenen. Die dazu aufzurufenden Kontrollfelder (Apfel-Menü ⇒ Kontrollfelder) heißen: „TCP/IP“ und „Internet“. Alternativ kann der „Internet Assistent“ (im Ordner „Internet“ auf der Bootplatte) benutzt werden, der Schritt für Schritt durch die Konfiguration führt. Die Netzwerkeinstellungen können jederzeit geändert werden und sind ohne Neustart/Reboot sofort gültig.

2.7 Abmeldung

Damit die Beendigung der Mitgliedschaft reibungslos vonstatten geht und nicht zu viele Nutzungsgebühren eingezogen werden, sollte die Abmeldung mindestens sechs Wochen im voraus, spätestens bis zum 15. des vorletzten Monats der Teilnahme, bei der Netzverwaltung eingereicht werden. Dies kann formlos (mit Unterschrift), mittels des beim Verein erhältlichen oder auf dem Webserver (<http://www.schunter.etc.tu-bs.de/SchunterNet/Verein/Dokumente/Abmeldung.ps>) zu findenden Vordrucks oder durch die auf dem Webserver zu findende Eingabemaske <http://www.schunter.etc.tu-bs.de/SchunterNet/abmeldung.html> erfolgen. Dort kann dann auch eine neue ↗E-Mail-Adresse und/oder die URL einer neuen ↗Homepage angegeben werden, auf welche dann in den auf den Austritt folgenden sechs Monaten eingehende Nachrichten oder Anfragen weitergeleitet werden. Eine Abmeldung per ↗E-Mail ist nicht ratsam, da nicht gesichert ist, daß diese auch vom vorgeblichen Absender stammt.

3 Netzdienste

3.1 Electronic Mail

Der Loginname des Benutzerservers bildet den ersten Teil der ↗E-Mail-Adresse, welche dann folgendermaßen aussieht: `loginname@schunter.etc.tu-bs.de` Um die Merkbarkeit zu vereinfachen, wird außerdem ein Mail-Alias der Form `Vorname.Nachname@schunter.etc.tu-bs.de` eingerichtet. Umlaute werden zu ae, oe, ue usw.

Zum Senden und Empfang von E-Mail im SchunterNet sind z.B. unter Netscape folgende Einstellungen notwendig:

Bearbeiten ⇒ Einstellungen ⇒ Mail & Diskussionsforen ⇒ Mail-Server: ⇒
Server für eingehende Mail: `pop.schunter.etc.tu-bs.de`

Unter Bearbeiten... kann der Benutzername und das Paßwort gespeichert werden (siehe dazu auch ?? und ??).

Server für ausgehende Mail: `mail.schunter.etc.tu-bs.de`

Wie komme ich an meine E-Mail in der Uni?

Mehrere E-Mail-Adressen bei verschiedenen Service-Providern zu haben, ist keine Seltenheit mehr. Daraus erwächst die Frage, wie es möglich ist, alle ↗E-Mails von einem einzigen Arbeitsplatz aus abzurufen und zu bearbeiten. Dabei gibt es grundsätzlich zwei Strategien.

1. Sämtliche ↗E-Mail wird zunächst automatisch an eine einzige Adresse weitergeleitet und auf dem empfangenden ↗Server gesammelt zwischengelagert. Von dort kann sie auf einmal abgerufen werden.
2. Die ↗E-Mail bleibt auf dem ↗Server, der zu der jeweiligen Adresse gehört. Der Arbeitsplatzrechner muß dann immer von mehreren ↗Servern die ↗E-Mail abholen.

Die erste Methode kann dadurch eingeschränkt werden, daß man als normaler Benutzer nicht auf allen ↗Serversystemen die Möglichkeit hat, eine automatische Weiterleitung der ↗E-Mail zu veranlassen. Die zweite Möglichkeit bereitet Probleme, wenn die Software auf dem Arbeitsplatzrechner nicht darauf ausgerichtet ist, von mehr als einem ↗Server ↗E-Mail abzurufen. Folgende Beispiele sollen helfen, das richtige Verfahren zu wählen. Die Mail-Adresse im Wohnheim sei `loginname@schunter.etc.tu-bs.de`.

Forwarding ins Wohnheim (1.Strategie) Angenommen, es besteht ein zweiter ↗Account auf den ↗UNIX-Systemen im Hochschulnetz (Institute etc.). Dann kann auf den dortigen ↗UNIX-Systemen eine Datei mit Namen „`.forward`“ angelegt werden, die die Adresse im Wohnheim enthält (z.B. mit dem Kommando: `# echo loginname@schunter.etc.tu-bs.de > .forward`). Sämtliche ↗E-Mail an die Hochschul-Adresse wird dann an das Wohnheim weitergeleitet und kann dort zusammen mit der restlichen ↗E-Mail abgerufen werden. Leider funktioniert das seit der Umstellung auf das Filesystem `afs` im Rechenzentrum nicht mehr.

Der an der TU vergebene Mailalias der Form `V.Nachname@tu-bs.de` kann aber direkt auf den Wohnheimserver umgeleitet werden. Dies kann jeder über den Benutzerdatendienst des RZ der TU-Braunschweig (<https://www2.tu-bs.de/rz/benutzerservice/>) selbst erledigen.

Zunächst meldet man sich über den Link „LOGIN“ mit dem RZ-login (üblicherweise eine `y`-Nummer) an. Dann führt ein Klick auf den gelben Button im Feld „Mailbox“ zu einem Änderungsformular für die Mailadresse. Dort wird z.B. die Mail-Adresse „`loginname@schunter.etc.tu-bs.de`“ eingegeben und mit abschicken bestätigt.

Abruf von mehreren Servern (2. Strategie) Hier bleibt die Organisation ganz dem Arbeitsplatzrechner überlassen. Die jeweilige Mail-Software muß so eingestellt werden, daß von allen Mail-Servern, bei denen ein Zugang besteht, die ↗E-Mail abgeholt wird. Zu jedem Mail-Zugang gehört ein POP3-Server mit Benutzerkennung und Paßwort. Nicht jedes Mail-Programm bietet diese Möglichkeit.

3.2 WWW und HTTP-Proxy

Im *SchunterNet e.V.* wird ein eigener ↗Server für das ↗World Wide Web betrieben. Dieser dient unter anderem der Information über das Wohnheim An der Schunter,

vorhandene Möglichkeiten zum Arbeiten und Leben sowie die dort stattfindenden Veranstaltungen. Die Website ist unter dem URL <http://www.schunternet.de/> zu erreichen.

Um den Datenverkehr über die Funkbridge zum RZ gering zu halten und den Zugriff auf häufig genutzte Informationsquellen im Internet zu beschleunigen, sollten alle Zugriffe auf ↗WWW- und ↗FTP-Server über den lokalen ↗Proxy-Cache erfolgen. Dazu muß dieser im verwendeten Browser eingestellt werden, z.B.:

Netscape Communicator:

⇒ ⇒ ⇒ ⇒
 ⇒
 FTP Proxy, Gopher Proxy und HTTP Proxy: proxy.schunter.etc.tu-bs.de
 Port: 3128
 No proxy for: schunter.etc.tu-bs.de schunternet.de schuntille.de
schunterkino.de

MS Internet Explorer:

⇒ ⇒ ⇒
 ⇒
 Adresse des Proxy-Servers: proxy.schunter.etc.tu-bs.de
 Anschluß: 3128
 Ausnahmen: schunter.etc.tu-bs.de schunternet.de schuntille.de
schunterkino.de

Wer sich von der steigenden Anzahl an Werbebannern im Web gestört fühlt, kann auch den Port/Anschluß 8000 eintragen und sich von dem dort hörenden Junkbuster einen Großteil der Banner ausfiltern lassen.

3.3 Usenet News

Zur Teilnahme am weltweiten Informationsaustausch über das ↗Usenet kann im *SchunterNet e. V.* der ↗Server¹ news.schunter.etc.tu-bs.de genutzt werden (Standard-Port ist 119). Dieser stellt neben den im Rechenzentrum (news.tu-bs.de) aufliegenden Newsgruppen auch die Hierarchien *corel.**, *intel.**, *linux.**, *microsoft.**, *netscape.**, *star-office.** und *schunter.** zur Verfügung.

Letztere ist die lokale Hierarchie unseres Wohnheims mit den Gruppen

¹Tatsächlich läuft im lokalen Netz gar kein Newsserver im eigentlichen Sinne (abgesehen von dem für die lokalen Gruppen), sondern lediglich ein ↗Proxy (*nntpcache*). Das bedeutet, dem ↗Client wird ein vollwertiger Newsserver suggeriert, aber die Daten werden von verschiedenen ↗Servern geladen und an den Client weitergereicht sowie lokal gecached. Vorteil dieser Methode ist, daß weniger Festplattenplatz vorgehalten werden muß und dennoch eine große Auswahl an Newsgruppen angeboten werden kann, wobei zweite und folgende Zugriffe auf dieselben Nachrichten beschleunigt erfolgen. Nachteilig sind fehlender Einfluß auf die Haltezeiten und langsamerer Erstzugriff auf die Informationen.

| | |
|-------------------------------|--|
| <code>schunter.general</code> | Allgemeines im Wohnheim an der Schunter. |
| <code>schunter.net</code> | Das Netzwerk. |
| <code>schunter.test</code> | Tests nur hier!. |

Im Usenet herrschen andere Gepflogenheiten als in Chatrooms oder auf WWW-Boards. Empfohlen wird, zunächst

`de.newusers.infos` Infos und periodische Postings fuer neue User. (Moderated)

aufzusuchen und sich die dort ständig neu geposteten 15 Artikel für Einsteiger durchzulesen. Fragen dazu kann man in

`de.newusers.questions` Neue Benutzer im Netz fragen, Experten antworten.

stellen, dort wird einem von kompetenten Leuten geholfen. Diese Informationen und die Einhaltung der dortigen Empfehlungen können eine Menge Ärger ersparen und halten so zumindest den deutschsprachigen Teil des Usenets (de.*) nutzbar.

Zwingend erforderlich ist die Verwendung einer gültigen E-Mail-Adresse nach ↗ RfC 1036. Um sich vor unerwünschter Werbemail (Bulk E-Mail, SPAM) zu schützen ist es eine sehr gute Idee, sich z.B. entweder

- a) eine kostenlose Extra-Mailadresse für das Usenet einzurichten (www.hotmail.com) die man dann gar nicht weiter nutzt, oder aber
- b) sich eine kostenlose E-Mail-Adresse bei www.gmx.de für Mail & News zu besorgen.

Auf gar keinen Fall darf mit einer ungültigen bzw. nicht erreichbaren E-Mail-Adresse gearbeitet werden.

Eine GMX-Adresse (mit automatischer Weiterleitung nach `schunter.etc.tu-bs.de`) hat die Vorteile, daß

1. Man nicht ständig das „Konto“ wechseln bzw. beim Mailen statt News posten die Mail-Adresse nicht ändern muß.
2. sehr effektive automatische Filter bei GMX vor SPAM schützen, und
3. beim Auszug aus dem Wohnheim bzw. Kündigung des Netzzugangs die Mails an GMX auf den künftigen Server umgeleitet werden können oder aber bei GMX verbleiben können, diese Adresse also stets gültig ist und nicht ständig umgeändert werden muß.

3.4 ICQ (I Seek You)

Was ist ICQ?

ICQ ist ein kleines nützliches Internet Tool, welches dich darüber informiert, wer gerade online ist und es einem ermöglicht, mit denjenigen in Kontakt zu treten. ICQ übernimmt für dich die Internetsuche nach einem Bekannten und informiert dich, wenn der Betreffende gerade online ist. Man kann mit ICQ Chatten, Mitteilungen, Dateien und URL's schicken oder einfach nur mit Bekannten rumhängen, während man durchs WWW surft.

Wie funktioniert es?

Wenn du ICQ installierst (nachdem du es von <http://www.icq.com/download/step-by-step.html> heruntergeladen hast), fragt dich das Programm danach, dich auf einem Server zu registrieren, welcher mit dem weltumspannenden ICQ-Netzwerk verbunden ist. Zum Zeitpunkt der Registrierung erhältst du eine eindeutige ICQ-Nummer (die UIN – Universal Internet Number – am besten irgendwo notieren!), weiterhin gibt dir ICQ die Möglichkeit, persönlich Informationen unter deiner ICQ# zu speichern. Dies ermöglicht anderen ICQ-Nutzern, dich eindeutig zu erkennen, wenn du dich einloggst.

Wenn du dich einmal registriert hast, kannst du eine Liste über Freunde und Bekannte für dich erstellen, welche ICQ dann dazu benutzt, diese Bekannten für dich zu suchen. Währenddessen läuft ICQ im Hintergrund, ohne andere laufende Anwendungen zu unterbrechen. Sobald du dich im Internet einloggst, informiert ICQ alle Bekannten, daß du anwesend bist, und informiert dich darüber, wenn Bekannte sich ein- oder ausloggen. Sobald du weißt, wer online ist, reicht ein Rechtsklick auf den Namen des Betreffenden um einen Chat zu starten, eine Mitteilung zu schicken, Dateien auszutauschen, oder andere peer-to-peer Anwendungen zu starten.

Weitere Tips gibt es unter <http://www.icq.com/icqtour/>

Firewall/Router-Einstellungen

Auf den Button klicken. Danach das Feld auswählen. Nun auf , weiterhin ⇒ . Nun wählen, nun ⇒ ⇒ . Wenn bei „Status“ „Success“ steht, läuft alles. Herzlichen Glückwunsch! Nur noch auf den Button unten rechts (das Blümchen!) klicken. Ist es grün, seid ihr online.

Falls nicht, wendet euch doch bitte an die Newsgroup `schunter.general` auf dem Server `news.schunter.etc.tu-bs.de`.

© by EWU (ICQ# 37759570)

3.5 FTP

Auf dem lokalen ↗ftp-Server `ftp://ftp.schunter.etc.tu-bs.de/` kann frei nutzbare Software zur Verfügung gestellt werden.

3.6 NTP — Time Service

Zur Synchronisation der Rechneruhren im SchunterNet mittels des Network Time Protocol (NTP) kann der ↗Server `time.schunter.etc.tu-bs.de` verwendet werden, welcher seinerseits mit primären Timeservern im Internet abgeglichen wird. Zur Einrichtung sei auf die Dokumentation der erforderlichen ↗Client-Software verwiesen.

4 Benutzerserver (*jupiter.schunter.etc.tu-bs.de*)

4.1 Zugriff auf das Homedirectory

Wie so oft gibt es auch hier mehrere Möglichkeiten:

4.1.1 ... per ftp (File Transfer Protocol)

Mit einem beliebigen ↗ftp-Programm können Dateien in das ↗Home-Directory eingespielt werden. Auch die meisten anderen Dateioperationen wie Löschen, Verzeichnisse anlegen usw. können im allgemeinen mit solchen Programmen durchgeführt werden.

Beim Einlogprozeß müssen Benutzerkennung und Paßwort angegeben werden, ein Zugriff auf die ↗Home-Directories per anonymous-ftp ist nicht möglich. Aus diesem Grund ist der Netscape Navigator für diese Zugriffsart nicht so gut geeignet.

4.1.2 ... durch Einloggen auf dem Server

Mit `rlogin` oder einem beliebigen Terminalprogramm (vorzugsweise ↗telnet) kann man sich direkt auf dem ↗Server (Name: „jupiter“) einloggen und in einer ↗UNIX-Shell-Umgebung (`bash`) arbeiten. Als Texteditoren stehen z.B. `vi` (bzw. `vim`, `elvis`) und `joe` sowie `emacs` zur Verfügung.

4.1.3 ... per SMB-Mount

Für Windows95/98-Benutzer ist diese Variante vermutlich die komfortabelste Zugriffsmöglichkeit. Dies funktioniert folgendermaßen:

Unter `Systemsteuerung` ⇒ `Netzwerk` wird über `Hinzufügen...` ⇒ `Dienst` „Datei und Druckerfreigabe für Windows-Netzwerke“ installiert, falls dies nicht schon zuvor geschehen ist. Dann kann mit dem Windows-Explorer über `Extras` ⇒ `Netzlaufwerk verbinden` mit der Angabe „\\jupiter\<username>“ das ↗ Homedirectory auf einen neuen Laufwerksbuchstaben abgebildet werden. Es ist sinnvoll, die Option „Verbindung beim Start wiederherstellen“ zu aktivieren. Das Paßwort ist in diesem Fall das Server-Paßwort. Der Datei- und Druckerfreigabedienst kann übrigens später wieder entfernt werden. Wenn er allerdings nie installiert wurde, klappt auch der ↗ SMB-Zugriff auf fremde Laufwerke nicht (eine Windows-Kuriosität).

Auch für Linux-Benutzer besteht die Möglichkeit, mit Hilfe von `smbmount` diese Zugriffsmethode zu benutzen. Ein Nachteil dabei ist, daß normalerweise bei jedem Mount-Vorgang das Paßwort eingegeben werden muß. Man kann sich zwar leicht ein Skript schreiben, das diese Aufgabe übernimmt, aber dann muß man auch das Paßwort im Klartext in dem Skript unterbringen, was eine potentielle Sicherheitslücke darstellt.

4.1.4 ... per NFS-Mount

Für Linux und alle anderen ↗ UNIX-Varianten ist dies die richtige Lösung. Da sie im Wohnheim relativ selten genutzt wird, ist eine Freigabe des ↗ Home-Directorys per ↗ NFS nicht initial für alle Benutzer eingerichtet. Wer hiervon Gebrauch machen möchte, sollte eine kurze Mitteilung an `admin@jupiter` mit Angabe des Loginnamens und der eigenen IP-Adresse schicken.

Ein Tip: Wer sein Server-Home-Directory in den Home-Directory-Bereich eines normalen Benutzers auf der eigenen Maschine mounten möchte, sollte dafür sorgen, daß die UID und GID auf beiden Rechnern übereinstimmen. Das vermeidet Probleme mit File-Permissions.

4.2 Private Homepages

Jeder Benutzer kann in seinem HOME-Bereich auf dem Benutzerserver ein Unterverzeichnis mit dem Namen `public_html` anlegen (auf `jupiter.schunter.etc.tu-bs.de` sollte dieses bereits existieren), das der ↗ WWW-Server als Dokumenten-Verzeichnis für persönliche ↗ WWW-Seiten interpretiert. Eine dort liegende Datei mit dem Namen `index.html` wird als ↗ Homepage interpretiert (alternativ ist auch `index.htm` möglich). Der URL dieser ↗ Homepage besteht aus dem Namen des ↗ WWW-Servers, dem Tilde-Zeichen (`~`) und dem Login des Benutzers (Beispiel: `http://www.schunter.`

`etc.tu-bs.de/~user/`). Es sollte euch bewußt sein, daß dieses Verzeichnis mittels ↗ WWW-Server weltweit eingesehen werden kann.

Das Erzeugen eines Unterverzeichnisses `public_html` geht (unter Linux) so:

- Einloggen auf `jupiter.schunter.etc.tu-bs.de` mittels Kommando: `telnet jupiter` oder: `ftp jupiter` und anschließender ↗ Authentifizierung
- Kommando: `mkdir ~/public_html` zur Erzeugung des Unterverzeichnisses, in dem die ↗ WWW-Seiten liegen sollen
- Kommando: `chmod 755 ~/public_html`, damit jedermann (!) dieses Verzeichnis lesen kann
- Kommando: `chmod 711 ~`, damit jedermann ein vorhandenes Verzeichnis im HOME-Bereich finden kann

Das Verzeichnis kann aber auch vom PC unter Windows per ↗ ftp mit graphischer Oberfläche angelegt werden, z.B. mit WS_FTP. Auch dazu müßt ihr euch auf `jupiter` einloggen. Ein Verzeichnis könnt ihr dort per Knopfdruck anlegen.

Legt im Verzeichnis `public_html` eine Datei mit dem Namen `index.html` an (absoluter Pfad: `~/public_html/index.html`). Diese Datei findet man mit dem URL: `http://www.schunter.etc.tu-bs.de/~user/`

Natürlich müssen auch alle Dateien in diesem Verzeichnis zum Lesen freigegeben werden:

- Kommando: `chmod 644 ~/public_html/*`

Zusätzlich kann im selben Verzeichnis (`~/public_html/`) eine Datei `description.txt` mit einer kurzen Beschreibung des Inhalts der ↗ Homepage (eine Zeile, maximal 50 Zeichen) angelegt werden. Diese wird dann auf der Übersichtsseite der privaten ↗ Homepages im SchunterNet mit angezeigt.

5 Sicherheit

5.1 Viren, Trojaner, Bugs

„The degree to which you take security seriously and invest in it should be proportional to the value and sensitivity of your system and its data.“ (aus <http://www.nwi.net/~pchelp/security/advice.htm>)

Dank Computer-BILD weiß es jede/r: Im Internet warten Tausende von Kriminellen nur darauf, daß du deinen Computer an das Netz anschließt. Wenn du also vermeiden willst, daß diese bösen Jungs und Mädchen sich an deinem Home-Banking-Account, deiner Diplomarbeit oder gar deinen Quake-Spielständen zu schaffen machen, solltest Du einige Sachen beachten.

Damit die Angreifer (fälschlicherweise oft auch Hacker genannt) auf deinen Computer bzw. deine Daten zugreifen können, muß ein bestimmtes Programm auf deinem Computer laufen. Dabei gibt es mehrere Möglichkeiten:

5.1.1 Computerviren

Ein Computervirus ist eine Sequenz von Programmcode, welche in anderen, nützlichen Code eingefügt ist und mit diesem ausgeführt wird. Dabei versucht sich der Code in andere Programme zu kopieren, d.h. dieses zu infizieren. Viren befinden sich also immer in einem „Wirtsprogramm“. Bootsektor-Viren setzen sich in den Bootsektor von Disketten oder Festplatten fest. Dieser Programmcode wird nach dem Booten des Rechners direkt gestartet. Damit ein Virus von einer geliehenen Diskette nicht gleich gestartet wird, stelle im BIOS die Boot-Sequenz zuerst auf Laufwerk C. Weiterhin kann sich ein Virus in einem Anwendungsprogramm (z.B. MS-Word) oder in einem Spiel verstecken. Allerdings können auch andere Dateien ausführbaren Code enthalten: MIME-encoded Mail, WWW-Seiten mit JavaScript oder VBScript, Postscript Dateien, Word-Dateien, ... Gegen Viren hilft ein (besser zwei) gutes und aktuelles Virenkiller-Programm und seine häufige Anwendung.

5.1.2 Trojanische Pferde (Trojan Horses)

Analog zur griechischen Mythologie wird hier ein Köder ausgelegt. Neben diesem erhält man jedoch unerwünschten Programmcode. Trojaner können sich prinzipiell in den gleichen Dateitypen wie Viren aufhalten. Starte daher niemals (!) Programme unbekannter Herkunft auf deinem Computer. Gleiches gilt natürlich auch für den Crack von www.evilhacker.org (gibt's die wirklich?) oder Programme die du auf einem Rechner hier im lokalen Netz gefunden hast. Wenn Dich Dein Mailprogramm fragt, ob es ein Programm ausführen soll, und du bist dir nicht absolut sicher, warum, antworte mit nein! Eines der ausgereiftesten Trojaner ist z.Z. SubSeven: mehr Infos dazu unter <http://home.t-online.de/home/TschiTschi/subseven.htm>.

5.1.3 Bugs

Fehlerhafte Programme die du bereits installiert hast, können offene Angriffspunkte enthalten. Softwarehersteller bringen häufig Updates zu ihren Betriebssystemen oder

Anwendungsprogrammen heraus. Halte dich auf den Laufendem und aktualisiere auf neuere Versionen, insbesondere, wenn Sicherheitslücken bekannt geworden sind.

Sicherheit im Computerbereich ist ein Katz-und-Maus-Spiel. Informiere dich deshalb laufend über die aktuellen Entwicklungen. Sicherheit ist kein Produkt was man fertig installieren kann, sondern ein ständiger Prozeß. Sei skeptisch, wenn Dir jemand sagt, mit seinem Produkt bist Du sicher. Auch unsere Firewall bietet nur begrenzten Schutz gegen Angriffe von „außen“, gegen Angriffe aus dem Wohnheim ist sie völlig nutzlos.

Infos zum Thema Sicherheit findet man z.B. unter <http://www.insecure.org/> im Internet.

Zum Schluß noch eine Bitte: Wenn ihr eine Email erhaltet, in der vor einer anderen mit dem Betreff: XYZ gewarnt wird und man euch auffordert, diese an möglichst viele Leute weiter zu senden, dann leitet diese NICHT weiter! Solange man Emails nur liest und nicht ausführt, können sie niemals Schaden anrichten!

© by Richard Karsch

5.2 Paßwörter

Wie ändere ich das Paßwort?

Um das Paßwort zu ändern, muß zunächst ein Terminalprogramm gestartet werden, z.B. `➤ telnet`. Als Zieladresse wird der Rechner jupiter angegeben (IP-Adresse ist 134.169.136.3, falls der `➤ DNS`-Server nicht benutzt werden kann). Man erhält dann folgende (oder ähnliche) Begrüßungsmeldung:

```
Welcome to S.u.S.E. Linux 5.3 (i386) - Kernel 2.0.36 (ttyp5).
```

```
jupiter login:
```

Es folgt die Eingabe der Benutzerkennung und des (alten) Paßworts. Bei der Eingabe des Paßworts erfolgt kein Echo auf dem Bildschirm, auch nicht symbolisch (z.B. durch *). Danach erscheint folgende (oder eine ähnliche) Meldung:

```
Last login: Thu Mar 20 15:30:06 on ttyp1 from erde.schunter.et  
No mail.  
loginname@jupiter:/home/users/loginname >
```

Man befindet sich nun in einer `➤ UNIX`-Shell-Umgebung. Zum Ändern des Paßworts reicht es, das Kommando `passwd` zu kennen. Nach dessen Aufruf wird man zunächst nach dem alten, und dann zweimal nach dem neuen Paßwort gefragt. Falls bei der Frage nach

dem neuen Paßwort zwei unterschiedliche Zeichenketten angegeben wurden (Tippfehler), erscheint die Meldung

`They don't match; try again.`

und man darf noch mal ein neues Paßwort angeben (wiederum zweimal). Wichtig: In der ↗ UNIX-Welt wird grundsätzlich zwischen Groß- und Kleinschreibung unterschieden, also auch beim Paßwort. Wenn alles geklappt hat, kann man die Umgebung mit dem Kommando `exit` wieder verlassen. Auf spezielle deutsche Sonderzeichen (Umlaute und Esszett) sollte beim Paßwort verzichtet werden. Auch wenn die ↗ UNIX-Anmeldung und das ↗ E-Mail abholen noch klappt, so gibt es doch spätestens bei ↗ SMB-Zugriffen (↗ Homedirectory abbilden, Drucken übers Netz) Schwierigkeiten.

Das Terminalprogramm ↗ telnet gehört zum Lieferumfang von sämtlichen ↗ UNIX-Clones, Windows95/98 und Windows NT. Für andere Betriebssysteme muß es gegebenenfalls noch nachinstalliert werden. Prinzipiell kann man auch jedes andere Terminalprogramm verwenden, das eine DEC-vt100 Terminalemulation beherrscht.

Wie sicher ist das Paßwort? Wie sicher sollte es sein?

Die Sicherheit des Paßworts sollte nicht unterschätzt werden. Erstens sind manche Paßwörter leichter zu knacken als andere, und zweitens kann mit einem geklauten oder geknackten Paßwort weitaus mehr Unfug getrieben werden als nur fremde ↗ E-Mails zu lesen.

Wer eine Vorstellung davon bekommen möchte, wozu ein unbefugter Zugang mißbraucht werden kann, dem sei das Buch „Kuckucksei“ von Clifford Stoll empfohlen. Es handelt sich dabei übrigens nicht um ein Informatik-Fachbuch, sondern um einen tatsachenbasierten Roman. Man erfährt auf sehr humorvolle und auch für Laien verständliche Weise, wie Computersysteme angegriffen und mißbraucht werden können.

Das Paßwort sollte also möglichst schwer zu knacken sein. Gegen systematische alphabetische Angriffe (Ausprobieren aller Kombinationen aller verfügbaren Zeichen) ist im Grunde kein Kraut gewachsen. Allerdings ist der Zeitaufwand derart hoch, daß diese Angriffsart kaum praktikabel ist. Die Wahrscheinlichkeit, das richtige Paßwort zu erwischen, ist geringer als die, daß das Paßwort inzwischen geändert wurde. Häufiger sind dagegen die sogenannten Wörterbuchattacken, bei denen nur solche Paßwörter ausprobiert werden, die auch sinnvolle Wörter ergeben, wie sie eben in Wörterbüchern einer beliebigen Sprache stehen (deutsch oder englisch zum Beispiel). Auch Namenslisten (menschliche Vornamen, Firmennamen, etc.) werden oft als Grundlage benutzt.

Und wie wähle ich nun mein Paßwort?

In der letzten Frage wurde geklärt, welche Zeichenketten nicht als Paßwörter benutzt werden sollen (Echte deutsche oder englische Wörter, Eigennamen, Firmennamen usw).

Es gibt mehrere Regeln, die ein Paßwort gegenüber den üblichen Attacks praktisch immun machen:

1. Groß- und Kleinschreibung gemischt verwenden (wird unterschieden)
2. Zahlen mit einbauen
3. Sonderzeichen mit einbauen (allerdings keine speziellen deutschen Sonderzeichen, siehe oben)
4. Paßwort nicht zu kurz wählen (8 Zeichen sind optimal)

Als nächstes stellt sich möglicherweise die Frage, wie man sich ein solches sicheres Paßwort noch merken können soll. Es gibt verschiedene Eselsbrücken und der Phantasie sind keine Grenzen gesetzt. Eine Möglichkeit: Man nimmt sich eine Zeile aus seinem Lieblingsgedicht, -song, oder was auch immer und greift sich die Anfangsbuchstaben heraus. Aus „We don’t need no Education“ ergibt sich beispielsweise das Paßwort „WdnnE“ — leicht zu merken und schwer zu erraten bzw. zu knacken.

5.3 ssh — Die Secure Shell

Bei konventionellen Methoden des Arbeitens auf entfernten Rechnern (↗ `telnet`, `rlogin`, `rsh`) werden Eingaben und Ausgaben unverschlüsselt über das Netz übertragen. Das schließt bereits die ↗ Authentifizierung ein, d.h. das Paßwort wird im Klartext übertragen und erst auf dem Zielrechner verschlüsselt und verifiziert. Dadurch hat jeder, der sich auf einem System befindet, welches auf die Übertragungswege zugreifen kann, die Möglichkeit, diese Daten mitzuhören und bspw. Paßwörter auszufiltern. Auch wenn dies innerhalb unseres Wohnheimnetzes aufgrund der physikalischen Struktur nicht möglich ist, sollte es dennoch berücksichtigt werden.

Eine Möglichkeit, die Kommunikation sicherer zu machen, ist die Secure Shell, ein Programm zum Login und zur Ausführung von Kommandos auf entfernten Maschinen. Es soll `rlogin` und `rsh` ersetzen und stellt einen sicheren verschlüsselten Kommunikationsweg zwischen zwei Rechnern über ein unsicheres Netzwerk zur Verfügung. Auch X11-Ausgaben und beliebige TCP/IP-Verbindungen können über den verschlüsselten Kanal übertragen werden.

A Satzung des Vereins SchunterNet e.V.

Stand: 05. August 1997

§1 Name und Sitz

1. Der Verein führt den Namen „*SchunterNet e.V.*“
2. Der Verein hat seinen Sitz in Braunschweig.
3. Der Verein ist eingetragener Verein im Vereinsregister beim Amtsgericht Braunschweig.

§2 Vereinszweck

1. Zweck des Vereins *SchunterNet e.V.* ist die Planung, der Aufbau und der Betrieb eines Computernetzwerkes im „Studentenwohnheim An der Schunter“ einschließlich dessen Anbindung an das Netz der Technischen Universität Braunschweig, sowie die Förderung der Kommunikation von Studenten im nationalen und internationalen Rahmen.
2. Der Verein verfolgt ausschließlich gemeinnützige Zwecke und ist nicht eigenwirtschaftlich tätig.

§3 Mitgliedschaft

1. Mitglied kann jeder Bewohner der Wohnheimanlage „Studentenwohnheim An der Schunter“ werden.
2. Der Verein besteht aus aktiven und passiven Mitgliedern.
3. Passives Mitglied kann werden, wer einen Antrag auf einen SchunterNet-Anschluß gestellt hat und die Satzung sowie deren Ergänzungsordnungen anerkennt.
4. Aktives Mitglied kann werden, wer einen Antrag auf einen SchunterNet-Anschluß gestellt hat, die Satzung und deren Ergänzungsordnungen anerkennt und aktiv am Aufbau und Betrieb des Netzes mitarbeitet.
5. Über die Aufnahme aktiver Mitglieder entscheidet die Mitgliederversammlung mit einfacher Mehrheit. Die Mitgliedschaft beginnt mit der Aufnahme durch die Mitgliederversammlung.
6. Ein passives Mitglied kann in jeder Mitgliederversammlung einen Antrag auf aktive Mitgliedschaft stellen. Die Aufnahme erfolgt entsprechend Ziffer ??.
7. Die Mitgliedschaft endet durch Verlust der Geschäftsfähigkeit, Auszug aus dem „Studentenwohnheim An der Schunter“ oder Austrittserklärung.

8. Der Austritt ist schriftlich gegenüber dem Vorstand zu erklären und wird einen Monat nach Eingang der schriftlichen Austrittserklärung bei dem Vorstand wirksam.
9. Mitglieder, die dem Zweck und Ansehen des Vereins zuwider handeln oder gegen Bestimmungen der gültigen Satzung oder der Ergänzungsordnungen verstoßen, können durch Beschluß des Vorstandes aus dem Verein ausgeschlossen werden. Widerspricht der Betroffene innerhalb eines Monats, entscheidet die Mitgliederversammlung über den Ausschluß mit 2/3 Mehrheit. Bis zur Entscheidung der Mitgliederversammlung ruhen die Mitgliedschaftsrechte des betroffenen Mitglieds.

§4 Beiträge

Von den Mitgliedern werden keine Beiträge erhoben.

§5 Organe

Die Organe des Vereins sind:

- a) die Mitgliederversammlung
- b) der Vorstand

§6 Mitgliederversammlung

Die Mitgliederversammlung bestimmt auf der Grundlage des Vereinszwecks die Richtlinien für die Tätigkeit des Vereins.

Sie ist im übrigen insbesondere zuständig für:

- a) Die Entgegennahme des Jahresberichtes des Vorstandes
- b) Die Erteilung von Entlastungen
- c) Die Wahl des Vorstandes
- d) Die Wahl der Systemverwaltung
- e) Satzungsänderungen und Auflösung des Vereins
- f) Aufnahme von Mitgliedern und, im Falle des Widerspruchs gegen den den Ausschluß aussprechenden Vorstandsbeschluß, für den Ausschluß von Mitgliedern.

§7 Einberufung der Mitgliederversammlung

1. Die ordentliche Mitgliederversammlung muß mindestens einmal im Semester stattfinden. Der Termin der Mitgliederversammlung ist mindestens eine Woche vorher bekannt zu geben. Die Bekanntgabe des Termins erfolgt durch Aushang am Anschlagbrett der Heimselbstverwaltung oder E-Mail.

2. Außerordentliche Mitgliederversammlungen finden statt:

- a) auf Beschluß des Vorstandes oder
- b) wenn dies 10% der Mitglieder unter Angabe des Zwecks verlangen.

Die Versammlung wird vom Vorstand durch Aushang am schwarzen Brett oder E-Mail mit einer Ladungsfrist von einer Woche unter Mitteilung der Tagesordnung einberufen.

3. Die Mitgliederversammlung beschließt mit einfacher Mehrheit der Stimmen. Stimmberechtigt ist jedes aktive Mitglied.

Satzungsänderungen, die vorzeitige Abwahl des Vorstandes und die Entscheidung über den Ausschluß von Mitgliedern nach §3 Ziffer ?? dieser Satzung erfordern eine Mehrheit von 2/3 der abgegebenen Stimmen.

4. Jedes aktive und passive Mitglied hat in der Mitgliederversammlung Rederecht und darf Anträge stellen. Werden gegen einen Beschluß die Unterschriften von mehr als der Hälfte aller aktiven und passiven Mitglieder vorgelegt, so gilt dieser als nicht gefaßt.

§8 Beschlußfähigkeit der Mitgliederversammlung

- 1. Jede ordnungsgemäß einberufene Mitgliederversammlung ist beschlußfähig, wenn mindestens 2/3 der aktiven Mitglieder anwesend sind.
- 2. Im Falle der Beschlußunfähigkeit ist die Mitgliederversammlung innerhalb eines Monats erneut einzuberufen. Diese ist dann ohne Rücksicht auf die Anzahl der erschienenen Mitglieder beschlußfähig.

§9 Vorstand

- 1. Die Zahl der Vorstandsmitglieder bestimmt die Mitgliederversammlung. Der Vorstand besteht jedoch mindestens aus drei Mitgliedern, nämlich dem Vorsitzenden, dem stellvertretenden Vorsitzenden und dem Kassenwart.
- 2. Je zwei Vorstandsmitglieder vertreten den Verein gemeinsam.
- 3. Die Vorstandsmitglieder werden von der Mitgliederversammlung einzeln und auf die Dauer von zwei Studiensemestern gewählt.

Jedes Vorstandsmitglied bleibt im Amt, bis die Amtszeit des neugewählten Nachfolgers beginnt oder die Mitgliederversammlung beschlossen hat, sein Amt nicht wieder zu besetzen. Eine Wiederwahl ist möglich.

Die vorzeitige Abwahl eines Vorstandsmitgliedes kann nur mit 2/3 Mehrheit der ordnungsgemäß einberufenen Mitgliederversammlung erfolgen. Die Abwahl eines

Vorstandsmitgliedes wird erst wirksam, wenn sich die Mitgliederversammlung zugleich auf einen Nachfolger geeinigt oder beschlossen hat, sein Amt nicht wieder zu besetzen.

§10 Aufgaben des Vorstandes

Der Vorstand sorgt für die Durchführung der Beschlüsse der Mitgliederversammlung und für die Information der Mitglieder.

§11 Beurkundung von Beschlüssen

Der Schriftführer fertigt über Beschlüsse der Mitgliederversammlung Protokolle an, die vom Versammlungsleiter und ihm unterschrieben werden.

§12 Schlußbestimmungen

1. Im Falle einer Auflösung des Vereins fällt das Vereinsvermögen der Heimkasse des Wohnheims „An der Schunter“ zu.
2. Diese Satzung tritt mit dem Beschluß der Gründungsversammlung vom 23. April 1997 in Kraft.

B Benutzerordnung des SchunterNet e.V.

Stand: 16. Februar 2000

Präambel

Das im Studentenwohnheim *An der Schunter* durch den *SchunterNet e.V.* betriebene Netzwerk soll allen Mietern die Möglichkeit bieten, mit ihren Heimrechnern (Mac, PC, etc.) einfach und kostengünstig an moderner Datenkommunikation zu partizipieren. Die gemeinsame Nutzung von Ressourcen steht dabei im lokalen Netz im Mittelpunkt. Dazu gehören der Datenaustausch über das Netz, die Nutzung zentraler oder privater Peripheriegeräte (Drucker, Scanner, Streamer, etc.) sowie die Bereitstellung nichtkommerzieller Software auf File-Servern.

Mit der Anbindung an das Hochschulnetz erhält der Teilnehmer die Möglichkeit, seinen PC als Terminal für eine UNIX-Workstation einzusetzen. Durch die Verbindung mit dem weltweiten Internet bieten sich den Studenten letztendlich ganz neue Wege der Recherche und Informationsbeschaffung vom eigenen Schreibtisch aus. Zentraler Punkt ist hierbei das World Wide Web, welches in den letzten Jahren die Popularität des Internet erst begründet hat.

§1 Gültigkeit

1. Die folgenden Regelungen gelten für alle Benutzer des Netzes des *SchunterNet e.V.* im Studentenwohnheim *An der Schunter*, Braunschweig. Sie ergänzen die Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig. [Anhang ??]
2. Diese Ordnung tritt mit ihrer Veröffentlichung in Kraft. Sie verliert ihre Gültigkeit bei Inkrafttreten einer neuen Benutzerordnung.

§2 Allgemeine Bestimmung

1. Die Teilnahme an Datennetzen verlangt von jedem einzelnen einen verantwortungsvollen Umgang mit diesem Medium. Die Benutzerordnung wurde geschaffen, um die Funktionsfähigkeit des Netzwerkes und ein geregeltes Miteinander der Teilnehmer zu gewährleisten.
2. Jeder Benutzer verpflichtet sich, diese Ordnung anzuerkennen.
3. Für die Nutzung der Ressourcen des Hochschulnetzes (TUBS-Net und Zugang zum Internet) ist darüber hinaus die Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig [Anhang ??] verbindlich.

4. Betriebs- und Hardwarekosten werden entsprechend der Gebührenordnung [Anhang ??] des *SchunterNet e.V.* auf die Nutzer umgelegt.

§3 Zulassung der Benutzer

1. Grundsätzlich ist jeder Bewohner des Studentenwohnheims *An der Schunter* berechtigt, sich an das Wohnheimnetz anzuschließen, sofern er sich mit den hier aufgeführten Regelungen einverstanden erklärt und dem *SchunterNet e.V.* beitrifft.
2. Einschränkungen werden im Einzelfall durch den *SchunterNet e.V.* ausgesprochen.

§4 An- und Abmeldung

1. Zur Anmeldung ist der Antrag auf Netzanschluß sowie Mitgliedschaft im *SchunterNet e.V.* auszufüllen und unterschrieben beim Vorstand des *SchunterNet e.V.* einzureichen. Dieser stellt einen Nutzervertrag des Teilnehmers mit dem Betreiber dar.
2. Änderungen der Benutzerdaten sind dem Verein unverzüglich mitzuteilen.
3. Die Teilnahme kann durch Auszug aus dem Wohnheim, Abmeldung oder Ausschluß (s. §8) beendet werden. Auszug oder Abmeldung sind dem Verein mindestens sechs Wochen im voraus anzukündigen.

§5 Rechte des Benutzers

1. Jeder Benutzer hat das Recht, den ihm zur Verfügung gestellten Netzanschluß zu jeder Zeit im Rahmen dieser Benutzerordnung zu nutzen.
2. Grundsätzlich kann jeder Benutzer alle zur Verfügung gestellten Dienste des Netzes in Anspruch nehmen.
3. Der Benutzer wird im Rahmen der Möglichkeiten durch die Vertreter des *SchunterNet e.V.* beraten und betreut. Dies ist zu den festgelegten Sprechstunden in den Räumlichkeiten des Vereins möglich.

§6 Bereitgestellte Dienste des Netzes

Primärer Anschluß Der primäre Anschluß an der im Zimmer des Benutzers vorhandenen Netzwerkdose wird zur Verfügung gestellt und auf Antrag freigeschaltet. Der *SchunterNet e.V.* ist stets um einen sicheren und unterbrechungsfreien Betrieb des Wohnheimnetzes bemüht, soweit dies beim Stand der Technik und im zeitlichen Rahmen der Mitglieder möglich ist.

Sekundärer Anschluß Auf gesonderten Antrag kann bei ausreichenden Ressourcen der in der Dose vorhandene Zweitanschluß für Netzwerknutzung zusätzlich freigeschaltet werden.

Protokoll des Anschlusses Der Anschluß erfolgt über 10 MBit/s Ethernet (10BaseT) und ermöglicht je nach Netzwerkadapter des Benutzers Half- bzw. Full-Duplex-Betrieb.

MAC Adressen der Netzwerkadapter Jedem Anschluß werden aus Gründen der Sicherheit bis maximal vier vom Benutzer angegebene MAC-Adressen (Media Access Control, eindeutige Identifizierungsnummer eines Netzwerkadapters) fest zugeordnet.

Protokolle Im internen Netz wird grundsätzlich jedes Protokoll (TCP/IP, IPX/ODITM, NetBIOSTM, appletalkTM, etc.) durchgeschaltet. Die Verbindung zum Hochschulnetz erfolgt ausschließlich über das Internetprotokoll (IP).

IP-Adresse Jedem Anschluß wird eine statische IP-Adresse zur Verfügung gestellt, die den Rechner im gesamten Internet eindeutig identifiziert. Hierdurch wird es grundsätzlich möglich, die Dienste des Internet in Anspruch zu nehmen und von außen (z.B. vom Rechenzentrum aus) auf die Ressourcen des eigenen Rechners zuzugreifen. Einschränkungen oder Erweiterungen dieser Zugriffsmöglichkeiten können nach den Wünschen des Benutzers vom Administrator eingestellt werden.

E-Mail Jeder Benutzer erhält eine eigene Mailbox mit Adresse, auf die er über POP3 oder Imap zugreifen kann.

WWW- und FTP-Zugang Der Zugang zum World Wide Web und zu FTP-Servern wird über einen Proxyserver gewährleistet.

Usenet News Je nach vorhandenen Ressourcen werden Newsgroups nach den Wünschen der Benutzer lokal zur Verfügung gestellt.

lokaler NTP Service Es wird eine zeitgenaue Synchronisierung der Systemuhren der eigenen Rechner ermöglicht.

Benutzerserver Jedem Teilnehmer wird ein Arbeitsverzeichnis auf dem Benutzerserver (Linux-Workstation) zur Verfügung gestellt. Nach Wunsch können projektbezogene Benutzergruppen eingerichtet werden. Jeder Benutzer darf bis zu neun weitere Accounts mit eingeschränkten Möglichkeiten beantragen.

private WWW-Homepages Jeder Benutzer kann im Rahmen des zur Verfügung gestellten Speicherplatzes eigene ➤ Homepages erstellen und veröffentlichen.

weitere Dienste Der Verein kann darüber hinaus weitere Dienste zur Verfügung stellen.

§7 Pflichten des Benutzers

Jeder Teilnehmer ist für seinen Rechner und den Netzzugang über selbigen voll verantwortlich. Das bedeutet:

1. Der Teilnehmer hat die ihm zur Verfügung gestellten Betriebsmittel und Dienste sorgfältig und ihren Bestimmungen entsprechend zu benutzen.
2. Jeder Teilnehmer hat Maßnahmen zum Schutz vor unbefugter Nutzung seines Anschlusses und der zur Verfügung gestellten Dienste durch Dritte zu ergreifen.
3. Jeder Verdacht auf Mißbrauch von Ressourcen ist der Netzverwaltung unverzüglich zu melden.
4. Bauliche Veränderungen an der Netzwerkinstallation dürfen nur mit schriftlicher Genehmigung des *SchunterNet e.V.* vorgenommen werden.
5. Die Störung oder Beeinträchtigung des Netzbetriebs durch unsachgemäßen Einsatz von Hard- und Software ist zu vermeiden. Störungen jeder Art sind unverzüglich dem *SchunterNet e.V.* zu melden.
6. Es ist dem Teilnehmer verboten, eine andere als die ihm zugewiesene IP-Adresse im Netz zu benutzen (Address-Spoofing) oder Masquerading zu betreiben.
7. Der am Netz angeschlossene Rechner darf grundsätzlich nicht für Routingzwecke verwendet werden. Ausnahmen bedürfen der schriftlichen Genehmigung des *SchunterNet e.V.*
8. Jede Art des Mithörens von Datenübertragungen, des unberechtigten Zugriffs auf fremde Daten oder des unberechtigten Zugangs zu fremden Rechnern ist zu unterlassen. Schon der Versuch ist strafbar.
9. Die Bereitstellung und Nutzung von Software und Dokumentationen ist nur im Rahmen der maßgeblichen Lizenzbestimmungen zulässig.
10. Das Beziehen oder Verbreiten strafrechtlich relevanter Daten ist zu unterlassen.
11. Der Teilnehmer ist dazu verpflichtet regelmäßig, nach Möglichkeit täglich, seine SchunterNet-EMails zu lesen. Er hat weiterhin dafür zu sorgen, dass er die EMail auch korrekt empfangen kann. Dabei ist es unerheblich, ob die EMail direkt vom SchunterNet-Mailserver oder über eine Weiterleitung bezogen werden.

§8 Verfahren bei Verstößen gegen die Benutzerordnung

1. Benutzer, die gegen die Benutzerordnung verstoßen, werden von den Vertretern des *SchunterNet e.V.* auf den Verstoß hingewiesen.

2. Bei schweren oder wiederholten Verstößen gegen die Bestimmungen der Benutzerordnung wird der betreffende Teilnehmer von der weiteren Nutzung ausgeschlossen. Werden Belange des Zusammenlebens im Wohnheim berührt, kann zusätzlich ein Heimratsverfahren angestrengt werden.
3. Die Geräte und Anlagen werden in funktionsfähigem Zustand übergeben. Durch unsachgemäße Behandlung eingetretene Schäden hat der Nutzer in vollem Umfang zu tragen. Bei Beendigung der Nutzung, spätestens beim Auszug, wird von Vertretern des *SchunterNet e.V.* der Zustand kontrolliert und ein Abnahmeprotokoll erstellt. Der Nutzer bleibt für entstehende Schäden haftbar, solange er diese Abnahme nicht durchführen lassen hat.
4. Wird durch Verstöße zusätzlicher administrativer Aufwand zur Wiederherstellung oder Bewahrung der Funktion und Sicherheit des Systems notwendig, so hat der Verursacher die entstehenden Kosten sowie die Arbeitsleistung entsprechend den in der Gebührenordnung [Anhang ??] festgelegten Tarifen zu tragen.
5. Wer über diese Bestimmungen hinaus gegen die Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig [Anhang ??], Interessen dritter, nationales oder internationales Recht verstößt, hat mit Meldung an die zuständigen Stellen bis hin zur Anzeige zu rechnen.

§9 Haftungsausschluß

1. Ein Anspruch auf ununterbrochene Funktion des Netzes besteht nicht. Schadenersatzansprüche des Benutzers gegenüber den Betreibern können nicht geltend gemacht werden.
2. Für Schäden an Hardware, Software oder Daten des Benutzers, die durch die Teilnahme am Netzbetrieb entstehen, übernimmt der Betreiber keine Haftung.

C Gebührenordnung des SchunterNet e.V.

Stand: 1. November 1999

1. Eine Anschlußgebühr wird nicht erhoben.
2. Die Nutzungsgebühr (Monatsgebühr) wird dynamisch erhoben. Sie wird abhängig vom Finanzbedarf des Vereins sowie der Anzahl der Nutzer angepaßt und sollte einen Betrag von 20 DM (in Worten: zwanzig Deutsche Mark) nicht überschreiten. Derzeit ist die Gebühr auf 10,-€ (in Worten: zehn Euro) festgelegt.
3. Bei der Freischaltung des Zugangs wird für den laufenden Monat eine volle Monatsgebühr erhoben. Gleichzeitig ist die Nutzungsgebühr für den folgenden Monat im Voraus zu entrichten. Zur Absicherung eventueller durch den Nutzer verursachter Forderungen Dritter an den Verein, ist eine Kautions von 10,-€ zu hinterlegen.
4. Alle Folgezahlungen sind bis 15. des Vormonats für den entsprechenden Monat einzuzahlen (jeweils eine Monatsgebühr).
5. Die Zahlung der Nutzungsgebühr erfolgt ausschließlich per Lastschriftinzugsverfahren.
6. Bei nicht gedecktem Konto kann die Kündigung fristlos zum Ende des laufenden Monats erfolgen.
7. Nach jeder Kündigung beträgt die Wiederanschlußgebühr drei Monatsgebühren.
8. Die Nutzungsgebühren werden in erster Linie zur Rückzahlung des Kredits des Studentenwerkes verwendet. Eventuelle Überschüsse werden für Reparaturen und weitere Investitionen genutzt.
9. Wird ein Zweitanschluß beantragt, so sind die Kosten der Umrüstung von Anschlußdose und Patchfeld (2xTP/TP-Einsatz) durch den Antragsteller zu tragen.
10. Durch Benutzer verursachter zusätzlicher Arbeitsaufwand im Sinne §8, Absatz 4 der Benutzerordnung [Anhang ??] wird zu einem Stundensatz von 12,80 € in Rechnung gestellt.
11. Schäden an vereinseigener Hardware, die durch unsachgemäßen Umgang fahrlässig oder vorsätzlich entstanden sind, gehen in vollem Umfang zu Lasten des Verursachers.
12. Änderungen dieser Gebührenordnung sind in den halbjährlichen Mitgliederversammlungen möglich.

D Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig

Stand: Dezember 1994

I Allgemeines

§1 Aufgaben des Rechenzentrums

Das Rechenzentrum ist eine zentrale Einrichtung der Technischen Universität Braunschweig, der alle Datenverarbeitungsanlagen und Datenkommunikationsnetze innerhalb der Universität zugeordnet sind. Dem Rechenzentrum obliegen folgende Aufgaben:

1. Der Betrieb der Datenverarbeitungsanlagen und des Datenkommunikationsnetzes zur Erfüllung von Aufgaben der Universität in Forschung, Lehre und Studium sowie zur Erledigung von Verwaltungsaufgaben.
2. die Beratung und Unterstützung für die Nutzung der Datenverarbeitungsanlagen, des Datenkommunikationsnetzes und der Rechnerprogramme,
3. die Betreuung aller der Hochschule verfügbaren Datenverarbeitungskapazitäten und Datenkommunikationsnetze sowie die betriebsfachliche Aufsicht über alle Datenverarbeitungsanlagen der Hochschule,
4. die Koordination der Beschaffung und Ergänzung von Datenverarbeitungsanlagen, Datenkommunikationsnetzen und Rechnerprogrammen.

§2 Leistungen und Inanspruchnahme des Rechenzentrums

(1) Das Leistungsangebot des Rechenzentrums umfaßt insbesondere:

1. Die Bereitstellung von DV-Geräten,
2. die Bereitstellung einer allgemeinen Datenkommunikation, insbesondere über das Hochschulnetz,
3. Zugang zu Informationsdiensten,
4. Dienstleistungen im Zusammenhang mit der DV-Versorgung.

Das Leistungsangebot des Rechenzentrums im einzelnen wird in Online-Dokumentationen, Handbüchern und Mitteilungen des Rechenzentrums gesondert bekanntgegeben.

(2) Die Inanspruchnahme des Rechenzentrums bedarf der Zulassung und erfolgt nach Maßgabe dieser Benutzungsordnung und ihrer Anlagen:

- Richtlinien für das Hochschulnetz (Anlage 1 [Anhang ??]).
- Richtlinien zur Kontingentierung der DV-Kapazitäten der zentralen Anlagen (Anlage 2).
- Richtlinien zum Betrieb von www-Servern und zur Nutzung von www-Diensten (Anlage 3 [Anhang ??]).

§3 Nutzungsberechtigte

Folgende Personen bzw. Institutionen können auf Antrag die Leistungen des Rechenzentrums in Anspruch nehmen:

1. Die Mitglieder und Angehörigen der Universität, alle Fachbereiche, wissenschaftliche Einrichtungen, Betriebseinheiten usw., die im Ausstattungsplan, im Organisationsplan oder im Haushaltsplan einer niedersächsischen Hochschule oder einer Hochschule außerhalb des Landes geführt sind.
2. Andere wissenschaftliche Einrichtungen, die ganz oder überwiegend aus öffentlichen Mitteln finanziert werden.
3. Sonstige Einrichtungen und Personen, die nicht unter Ziffer ?? oder Ziffer ?? fallen.

§4 DV-Benutzer und DV-Beauftragte

Benutzerinnen bzw. Benutzer sind diejenigen Personen, die die Leistungen des Rechenzentrums unmittelbar in Anspruch nehmen. Die von den Einrichtungen der Hochschule mit der Abwicklung ihrer Datenverarbeitungsvorhaben beauftragten Mitarbeiter/-innen heißen DV-Beauftragte.

II Benutzungserlaubnis

§5 Zulassungsverfahren

- (1) Wer die Leistungen des Rechenzentrums in Anspruch nehmen will, bedarf der Zulassung (Benutzungserlaubnis). Mit der Zulassung wird das Benutzungsverhältnis begründet. Die Benutzer haben die Benutzungsordnung und deren Anlagen zu beachten.
- (2) Die Benutzungserlaubnis ist — einschließlich der erforderlichen Benutzeridentifikation — schriftlich zu beantragen. Der Antrag soll auf den Vordrucken des Rechenzentrums gestellt werden und hat folgende Angaben zu enthalten:
 1. Angaben zur beantragenden Person oder Einrichtung,

2. Angaben, die eine Zuordnung zu Rangstufen der Bearbeitung gemäß § 8 ermöglichen,
 3. Angaben zu Art, Umfang und Zweck der beabsichtigten Nutzung,
 4. Abgabe der verlangten Erklärungen.
- (3) Nutzungsberechtigte, die die Genehmigung erhalten, eigene Rechner bzw. Subnetze am Hochschulnetz anzuschließen und zu betreiben, können Mitgliedern und Angehörigen der TU Braunschweig unter Beachtung der „Richtlinien für das Hochschulnetz“ [Anhang ??] Zugang zum Hochschulnetz gewähren.

§6 Erlaubniserteilung

- (1) Die Benutzungserlaubnis, mit der auch die Benutzeridentifikation vergeben wird, wird vom Leiter des Rechenzentrums schriftlich erteilt. Sie ist auf die beantragte und bewilligte Nutzungsart beschränkt. Mit der Erlaubniserteilung erfolgt die Einstufung in die jeweilige Rangstufe (§ 8) und Kostengruppe. Die Erlaubnis kann zeitlich befristet, eingeschränkt und unter Auflagen und Bedingungen erteilt werden. Die Benutzungserlaubnis ist nicht übertragbar.
- (2) Die Berechtigung zur Nutzung bestimmter Leistungen kann vom Rechenzentrum insbesondere mit Bezug auf folgende Gesichtspunkte eingeschränkt oder versagt werden:
 - Rangstufenfolge gemäß § 8 (Nutzungspriorität),
 - Vorrang von Arbeiten in Lehre und Forschung der Universitätseinrichtungen,
 - Zweckbestimmung der betreffenden Geräte bzw. Rechnersysteme,
 - Lizenzbestimmungen,
 - Wirtschaftlichkeit bzw. Verhältnismäßigkeit der Verfahren,
 - Leistungsvermögen und Auslastung der betreffenden Geräte bzw. Rechnersysteme.
- (3) Der/die Nutzungsberechtigte hat wesentliche Änderungen seiner im Antrag gemachten Angaben unverzüglich dem Rechenzentrum mitzuteilen; insbesondere ist er/sie verpflichtet, die Beendigung der Nutzung unverzüglich bekanntzugeben.

§7 Beendigung des Benutzungsverhältnisses

- (1) Die Benutzungserlaubnis erlischt mit Beendigung des Benutzungsverhältnisses:
 - Nach Ablauf der erteilten Frist.

- Aufgrund einer entsprechenden Mitteilung des Nutzungsberechtigten oder der/des DV–Beauftragten.
 - Sobald der Nutzungsberechtigte aus der TU Braunschweig bzw. aus derjenigen Einrichtung ausscheidet, die die Benutzungserlaubnis beantragt hat.
 - Durch Ausschluß gemäß § 12 (2).
- (2) Der Nutzungsberechtigte verpflichtet sich, bei Beendigung des Benutzungsverhältnisses:
- alle ihn betreffenden bzw. von ihm genutzten Datenbereiche und Adressen freizugeben,
 - die vom Rechenzentrum zur Verfügung gestellten Arbeitsmittel zurückzugeben,
 - alle sonstigen Ansprüche des Rechenzentrums, die aus dem Benutzungsverhältnis entstanden sind, zu erfüllen.

§8 Rangstufen

Die Datenverarbeitungsvorhaben werden nach der Zugehörigkeit der sie durchführenden Nutzungsberechtigten (siehe § 3) in Gruppen gegliedert, denen Rangstufen zugeordnet sind. Die Rangstufenzuordnung legt die jeweilige Nutzungspriorität fest und richtet sich nach den vorläufigen Grundsätzen für die Errichtung und den Betrieb von Hochschulrechenzentren in Niedersachsen — bekanntgegeben mit RdErl. d. MWK vom 19.9.1978 – 1053 – 02 804 – GültL MWK 60/55 —.

III Benutzungsregeln

§9 Rechte und Pflichten der Benutzer

- (1) Benutzerinnen und Benutzer sind verpflichtet, diese Benutzungsregeln einzuhalten. Für die Nutzung des Hochschulnetzes gelten zusätzlich die speziellen, in den „Richtlinien für das Hochschulnetz“ (Anlage 1 [Anhang ??]) aufgeführten Regelungen.
- (2) Die Nutzungsberechtigten können diejenigen Leistungen des Rechenzentrums in Anspruch nehmen, für die sie eine Benutzungserlaubnis haben. Die bereitgestellten Ressourcen, die durch Kontingente (gemäß § 14) begrenzt sein können, sind in wirtschaftlicher und dem Nutzungszweck angemessener Weise zu nutzen. Im übrigen haben die Benutzer darauf zu achten, daß sie die Nutzungsmöglichkeiten anderer nicht in unangemessener Weise beeinträchtigen.
- (3) Die Nutzung der DV–Einrichtungen für kommerzielle oder private Zwecke ist nur mit schriftlicher Zustimmung des Rechenzentrums und nach Festlegung der Entgelte zulässig.

- (4) Der Nutzungsberechtigte hat dafür Sorge zu tragen, daß die ihm zugeteilten Benutzeridentifikationen nicht an andere weitergegeben oder in sonstiger Weise mißbräuchlich verwendet werden.
- (5) Bei der Nutzung von Räumen bzw. Geräten des Rechenzentrums sind die Bedienungsanleitungen, allgemeinen Sicherheitsvorschriften und die Vorschriften der Hausordnung zu beachten. Beim Umgang mit Einrichtungen und Geräten des Rechenzentrums ist die gebotene Sorgfalt aufzuwenden.
- (6) Benutzerinnen und Benutzer dürfen Software und Dokumentationen, die ihnen vom Rechenzentrum direkt oder indirekt zur Verfügung gestellt werden, nicht ohne Genehmigung des Rechenzentrums kopieren, an Dritte weitergeben oder Dritten zugänglich machen oder an anderen Prozessoren als denen verwenden, für die das Rechenzentrum die Software bestimmt hat. Im übrigen sind die für die zur Verfügung gestellte Software maßgeblichen Lizenzbestimmungen einzuhalten.
- (7) Es ist untersagt, Manipulationen an der Betriebssystem-Software und an Benutzerverzeichnissen vorzunehmen oder Zugriff auf Benutzerbereiche auszuführen, für die keine Berechtigung vorliegt.
- (8) Nach Aufforderung durch das Rechenzentrum ist der Nutzungsberechtigte verpflichtet, einen Bericht über die Benutzung der Rechanlagen und die dabei gewonnenen Erfahrungen abzugeben.

§10 Sicherheit des Datenmaterials

- (1) Das Rechenzentrum sorgt im allgemein üblichen Rahmen für die Sicherung der Daten, die die Benutzer-/innen auf elektronischen Datenträgern des Rechenzentrums speichern.
- (2) Das Rechenzentrum bewahrt Medien, die mit Daten von Benutzern beschrieben sind, während einer festgelegten Frist auf. Die innerhalb dieser Frist nicht abgeholten Medien können vom Rechenzentrum vernichtet werden.

§11 Verarbeitung schutzwürdiger Daten

Die Verarbeitung und Übertragung von Daten, die schutzbedürftig im Sinne der Datenschutzbestimmungen sind, ist nur nach vorheriger Rücksprache mit dem Rechenzentrum und nur unter Einhaltung der vorgeschriebenen Sicherheitsmaßnahmen gestattet.

§12 Ordnungsmaßnahmen

- (1) Verstößt ein Nutzungsberechtigter gegen diese Benutzungsordnung und deren Anlagen, insbesondere gegen die sich aus § 9 ergebenden Pflichten, kann der Leiter des Rechenzentrums die Benutzungserlaubnis vorübergehend einschränken bzw.

in wiederholten oder schwerwiegenden Fällen die Benutzung für einen bestimmten Zeitraum untersagen. Der betreffende Benutzer muß davon unter Angabe der Gründe in Kenntnis gesetzt werden.

- (2) In besonders schwerwiegenden Fällen kann dem betreffenden Benutzer nach vorheriger Anhörung und mit Zustimmung der „Senatskommission für die elektronische Datenverarbeitung“ die Benutzungserlaubnis entzogen werden. Bei einem schwerwiegenden Verstoß wird der Leiter des Rechenzentrums prüfen, ob strafrechtliche oder zivilrechtliche Schritte einzuleiten sind.
- (3) Der Leiter des Rechenzentrums übt das Hausrecht aus und ist weisungsberechtigt.

§13 Haftung

- (1) Die Benutzer haften für die von ihnen schuldhaft verursachten Schäden sowie für Verluste und Veränderungen der Daten des Rechenzentrums oder Dritter. Sie stellen das Rechenzentrum (bzw. die Universität) vor Ansprüchen Dritter frei, sofern etwaige Schäden auf Verstöße gegen diese Benutzungsordnung, insbesondere gegen Lizenzbestimmungen Dritter zurückzuführen sind.
- (2) Das Rechenzentrum haftet für die von seinen Mitarbeiterinnen und Mitarbeitern in Ausübung ihrer Dienstpflichten vorsätzlich oder grob fahrlässig verursachten Schäden. Eine Haftung des Rechenzentrums für fehlerhafte Rechenergebnisse, für die Zerstörung von Daten und die Beschädigung von Datenträgern sowie für Terminüberschreitungen bei Rechenarbeiten ist — soweit rechtlich zulässig — ausgeschlossen.

IV Bewirtschaftung von Betriebsmitteln

§14 Kontingentierung

- (1) Da Rechenzeiten und Betriebsmittel in beschränktem Umfang zur Verfügung stehen, werden sie gegebenenfalls in Form von Kontingenten an die Benutzer verteilt. Betriebsmittel im Sinne dieser Ordnung sind insbesondere Speicherbereiche, Drucker, Übertragungswege auf Datenleitungen und Rechner-Arbeitsplätze.
- (2) Die Zuteilung der Kontingente erfolgt gemäß einem Verteilungsschlüssel, der die Zugehörigkeit der Nutzungsberechtigten (gemäß § 8) sowie den Aufgabenbezug, insbesondere den Vorrang von Lehre und Forschung, berücksichtigt. Die jeweiligen Kontingente setzen sich aus einem festen Sockelbetrag und einem bedarfsbezogenen Anteil zusammen. Die Kontingente werden in der Regel jeweils zu Beginn eines Quartals neu berechnet.

- (3) Die Regelungen zur Kontingentierung im einzelnen werden durch Senatsbeschluß festgelegt.
- (4) Die Verteilung der Rechenzeiten der zentralen Rechenanlagen geschieht im einzelnen nach Maßgabe der „Richtlinien zur Kontingentierung der DV-Kapazität der zentralen Anlagen der TU Braunschweig“ (Anlage 2).

§15 Entgelte und Kostenermittlung

- (1) Für die Inanspruchnahme der Leistungen des Rechenzentrums sind je nach Rangstufe folgende Entgelte zu entrichten:

| | | |
|-----------------|---|-------------------|
| Rangstufen 1, 2 | Angehörige von Hochschulen des Landes | unentgeltlich |
| Rangstufe 3 | Angehörige von Hochschulen außerhalb des Landes | Selbstkosten Land |
| Rangstufe 4 | Hochschulbedienstete bei Nebentätigkeit und sonstige Nutzer | Marktpreise. |

Die Nutzung von Rangstufe 1 und 2 erfolgt grundsätzlich unentgeltlich; Aufwendungen im Sinne von § 61 Abs. 1 Satz 2 LHO (Landeshaushaltsordnung) sind zu erstatten. In den Rangstufen 3 und 4 werden Entgelte erhoben.

- (2) Für Leistungen, die den im Rechenzentrum üblichen Rahmen überschreiten, können zusätzliche Entgelte erhoben werden. Diese legt das Rechenzentrum fest und teilt sie auf Anfrage mit.
- (3) Grundlage für die Bemessung der in Anspruch genommenen Leistungen sind die Betriebsunterlagen des Rechenzentrums. An Hand dieser Unterlagen ermittelt das Rechenzentrum die zu zahlenden Entgelte. Den Nutzungsberechtigten werden regelmäßig Nachweise über die entstandenen Kosten zugestellt und, falls nach der Landeshaushaltsordnung Kosten zu erheben sind, diese in Rechnung gestellt.
- (4) Benutzungsentgelte sind auch dann zu entrichten, wenn Programme ergebnislos oder fehlerhaft durchgeführt werden, es sei denn, der Fehler ist nachweislich und aufgrund grober Fahrlässigkeit vom Rechenzentrum zu vertreten und das Benutzungsentgelt ist erheblich. Bei Inanspruchnahme sonstiger Leistungen des Rechenzentrums gilt Satz 1 entsprechend.
- (5) Das Nähere zu den Entgelten einschließlich der Sonderleistungen und der Kostenermittlung ist in der „Entgeltordnung“ geregelt. Es gelten die jeweils vom Präsidenten genehmigten Sätze für die Kategorien „Selbstkosten Land“ und „Marktpreise“.

§16 Inkrafttreten

Diese Benutzungsordnung tritt am Tage nach ihrer hochschulöffentlichen Bekanntmachung in Kraft. Gleichzeitig treten frühere Benutzungsordnungen außer Kraft.

E Richtlinien für das Hochschulnetz der Technischen Universität Braunschweig

Stand: Dezember 1994

1 Allgemeines

- 1.1 Hochschulnetz im Sinne der „Benutzungsordnung für das Rechenzentrum“ [Anhang ??] ist das allgemeine Datenkommunikationsnetz der TU Braunschweig. Für den Betrieb des Hochschulnetzes gelten die nachfolgend aufgeführten Bestimmungen.
- 1.2 Die Verantwortung für den Betrieb des Hochschulnetzes als logisches System liegt beim Rechenzentrum, das die dem Netzbetrieb (Netzmanagement, Einstellung intelligenter Netzkomponenten) zugrundeliegenden Programme betreibt.
- 1.3 Die Verantwortung für die Leitungen und Übergabepunkte des Hochschulnetzes liegt bei der Abteilung Betriebstechnik der TU Braunschweig.
- 1.4 Die verfügbaren Netzdienste und Anschlußtypen (Kopplungselemente) werden in Publikationen des Rechenzentrums bekanntgemacht.
- 1.5 Der Zugang zum Hochschulnetz ist über Rechner des Rechenzentrums oder über Rechner bzw. Rechnernetze (kurz: „Rechner“) der Nutzungsberechtigten möglich, für die geeignete Anschlüsse bereitgestellt werden.
- 1.6 Betreiber von nutzeigenen „Rechnern“ am Hochschulnetz („Rechnerbetreiber“) können alle Nutzungsberechtigten gemäß §3 der Benutzungsordnung [Anhang ??] sein.
- 1.7 Für jeden an das Hochschulnetz angeschlossenen „Rechner“ gibt es einen Übergabepunkt, in der Regel ein Kopplungselement, mit dem die betriebstechnische Verantwortung für das Netz endet. Die Kommunikation auf der Nutzerseite, d.h. bis zum Übergabepunkt, liegt in der Verantwortung des „Rechnerbetreibers“.

2 Aufgaben und Pflichten des Rechenzentrums

- 2.1 Das Rechenzentrum ist stets um einen sicheren und ununterbrochenen Betrieb des Hochschulnetzes bemüht, soweit dies beim Stand der Technik möglich ist. Ein störungsfreier Betrieb kann aber angesichts des Entwicklungsstandes und des offenen Charakters der derzeitigen Netze nicht garantiert werden.

- 2.2 Das Rechenzentrum vergibt und verwaltet die Netzadressen und berät die „Rechnerbetreiber“ in Fragen der Nutzung des Hochschulnetzes. Soweit höhere Netzdienste zu koordinieren sind, übernimmt das Rechenzentrum diese Aufgabe.
- 2.3 Das Rechenzentrum übernimmt keine Verantwortung für über das Hochschulnetz herangetragene Beeinträchtigungen des Betriebs der angeschlossenen „Rechner“.
- 2.4 Das Rechenzentrum hat das Recht, Teile des Hochschulnetzes zeitweilig stillzulegen, wenn diese Maßnahme erforderlich ist, um bei Störungen die Funktionsfähigkeit des übrigen Netzes zu erhalten.

3 Aufgaben und Pflichten der Benutzer des Hochschulnetzes

- 3.1 Die Benutzung des Hochschulnetzes besteht darin, über ein an das Hochschulnetz angeschlossenes Rechnersystem Daten in das Hochschulnetz zu senden oder daraus zu empfangen. Als solche unterliegt sie der „Benutzungsordnung für das Rechenzentrum der TU Braunschweig“. [Anhang ??] Benutzerinnen und Benutzer des Hochschulnetzes sind somit neben den im Rechenzentrum registrierten Benutzern auch Personen, die als Mitglieder und Angehörige der TU Braunschweig unter der Verantwortlichkeit eines „Rechnerbetreibers“ tätig sind. (Siehe Benutzungsordnung §5 [hier: Anhang ??])
- 3.2 Der Benutzerin oder dem Benutzer ist es untersagt, Änderungen an den Übergabepunkten vorzunehmen. Soweit sie geeignet sind, den Betrieb des Hochschulnetzes zu beeinflussen, sind alle Änderungen an den angeschlossenen Geräten und den vorgesehenen Betriebsweisen nur in Absprache mit dem Rechenzentrum zulässig.
- 3.3 Der Benutzerin oder dem Benutzer ist es untersagt, ohne Absprache mit dem Rechenzentrum Netzadressen zu ändern oder neue Netzadressen einzuführen.
- 3.4 Der Datenverkehr einer Benutzerin oder eines Benutzers darf den Datenverkehr anderer Benutzer/-innen nicht unangemessen beeinträchtigen, z.B. durch ungezielte und übermäßige Verbreitung von Informationen.
- 3.5 Jedes unbefugte Mitlesen oder Auswerten von Nachrichteninhalten sowie die Weitergabe unbeabsichtigt erhaltener Informationen ist untersagt.
- 3.6 Die Benutzerin oder der Benutzer ist verpflichtet, dem Rechenzentrum unverzüglich einen erkannten Mißbrauch des Hochschulnetzes bzw. Störungen am Netz anzuzeigen.
- 3.7 Im Sinne des Datenschutzgesetzes schutzwürdige Daten dürfen nur in verschlüsselter Form auf das Hochschulnetz geleitet werden, da die Abhörsicherheit des Netzes nicht gewährleistet werden kann.
- 3.8 Vor Übertragung von sehr großen Datenmengen bzw. von schutzwürdigen Daten hat der „Rechnerbetreiber“ Absprachen mit dem Rechenzentrum zu treffen.

4 Aufgaben und Pflichten des Rechnerbetreibers

- 4.1 Der Anschluß eines „Rechners“ an das Hochschulnetz sowie der Ausbau des Leitungsnetzes müssen vom „Rechnerbetreiber“ beim Rechenzentrum beantragt werden. Die Entscheidung über den Antrag liegt beim Rechenzentrum.
- 4.2 Der „Rechnerbetreiber“ ist für die ordnungsgemäße Nutzung des Hochschulnetzes verantwortlich, da nur er den Zugang zu seinen „Rechnern“ und damit auch zum Netz kontrollieren kann. Insbesondere hat er darauf zu achten, daß nur dazu berechtigte Nutzerinnen und Nutzer Zugang zum Netz bekommen und daß über den „Rechner“ kein unautorisierter Netzzugang erschlossen wird.
- 4.3 Der „Rechnerbetreiber“ verpflichtet die Nutzer/-innen seiner Netzanschlüsse auf Einhaltung der Benutzungsordnung. [Anhang ??]
- 4.4 Das Hochschulnetz sowie die Datenverbindungen nach außen dürfen nur für Aufgaben in Lehre und Forschung genutzt werden.
- 4.5 Das Rechenzentrum teilt den „Rechnerbetreibern“ Adressenbereiche für Netzadressen zu, die von diesen z.T. selbst ausgefüllt werden können.
- 4.6 Soweit erforderlich werden zwischen Rechenzentrum und „Rechnerbetreiber“ besondere Vereinbarungen getroffen, wie z.B.:
 - zum Übergabepunkt,
 - zur Nutzung spezieller Netzdienste,
 - zu Kosten (z.B. Einrichtungs-, Wartungskosten, Verkehrsgebühren).

F Richtlinien zum Betrieb von www-Servern und zur Nutzung von www-Diensten an der Technischen Universität Braunschweig

Dieser Text basiert auf einem Entwurf des Arbeitskreises „Internet“ der Hochschule. Die Senatskommission für die elektronische Datenverarbeitung (SEDV) hat den Entwurf in dieser Fassung verabschiedet und wird ihn zur endgültigen Beschlußfassung dem Senat vorlegen.

Stand: 01. 2. 99

1 Grundsätze des Betriebs von www-Servern

- 1.1 Die Technische Universität Braunschweig betreibt einen www-Server. Er steht allen Organisationseinheiten, kooperierenden Institutionen, Mitgliedern und Angehörigen der Universität zur Verfügung. Die Organisationseinheiten der Universität können eigene www-Server betreiben.
- 1.2 Die Abteilung 52 koordiniert im Auftrage der Hochschulleitung und in Absprache mit der Presse- und Öffentlichkeitsarbeit das Informationsangebot des zentralen www-Servers. Das Rechenzentrum übernimmt als Betreiber des www-Servers die technische Realisierung und die Betreuung des Systems.

2 Inhalt und Gestaltung von www-Seiten

- 2.1 Der Inhalt von www-Seiten muß den Anforderungen der DFN-Benutzungsordnung [Anhang ??] und der DV-Nutzungsordnung der Hochschule [Anhang ??] genügen.
- 2.2 Der Inhalt von www-Seiten muß gesetzliche Bestimmungen einhalten, insbesondere das Informations- und Kommunikationsdienste-Gesetz. Zu beachten sind u.a. der Schutz von personenbezogenen Daten, Urheber- und Lizenzrechte, Persönlichkeitsrechte und Strafgesetze. Im Strafbgesetzbuch ist u.a. geregelt, daß die Propaganda für verfassungswidrige Organisationen, die Verbreitung von rassistischem Gedankengut, Pornographie sowie Beleidigungen und Verleumdungen zu unterlassen sind.
- 2.3 Daten über Zugriffe auf www-Seiten dürfen nur gespeichert werden, um eine anonyme Zugriffsstatistik zu erstellen oder um eine Überprüfung der Zugriffsberechtigung seitens der Domain des zugreifenden Systems zu ermöglichen. Daher ist eine Integration von Tools zur Protokollierung von Zugriffen in www-Seiten in der Regel unzulässig und hat zu unterbleiben. — Erhebung und Speicherung entsprechender Daten kann ausnahmsweise zulässig sein, sofern im Sinne des Niedersächsischen Datenschutzgesetzes die Einwilligung der Betroffenen gegeben ist und die Hochschulleitung zugestimmt hat.

2.4 Die Hochschule ist bemüht, ihr Informationsangebot so breit und attraktiv wie möglich zu gestalten und setzt auf die engagierte Mitarbeit aller ihrer Angehörigen. Um diesem Anspruch gerecht zu werden, sind die Hochschule und ihre Organisationseinheiten berechtigt, ohne Rückfrage bei ihren Mitgliedern und Angehörigen die folgende Daten weltweit zur Verfügung zu stellen:

- die offizielle Bezeichnung der Einheit sowie
 - Adresse, Telefon- und Fax-Nummer, E-Mail-Adresse
 - Geschäftsverteilungsplan
 - angebotene Lehrveranstaltungen (Titel, Nummer, Ort und Zeit, Name des Dozenten/der Dozentin)
 - Listen von Gremien und deren Mitglieder
 - bereits in anderen Medien veröffentlichte Artikel und Beiträge in ungekürzter oder in einer von der verantwortlichen Organisationseinheit gekürzten Fassung, soweit kein Copyright verletzt wird
- die folgenden Daten ihrer Mitglieder und Angehörigen:
 - Name, Vorname, Geschlecht
 - Zugehörigkeit zu Organisationseinheiten
 - dienstliche Telefon- und Fax-Nummer, E-Mail-Adresse
 - (gestrichen: ~~private Telefonnummer, soweit die Person der Residenzpflicht unterliegt~~)
 - dienstliche Funktionen und Aufgaben
 - angebotene Lehrveranstaltungen

2.5 www-Datenbereiche dürfen in der Regel nicht Dritten (Personen bzw. Organisationen) zur Nutzung überlassen werden. In Ausnahmefällen kann mit Genehmigung der Hochschulleitung nicht gewinnorientierten öffentlichen Einrichtungen im Rahmen der Amtshilfe eine Mitnutzung des www-Servers gewährt werden.

2.6 www-Seiten dürfen in der Regel nicht kommerziell genutzt werden. Erlaubt ist dagegen den Organisationseinheiten der Hochschule die Nennung von Förderern und Sponsoren samt Firmen- und Produkt-Logos auf je einer eigens dafür eingerichteten Seite. Derartige Seiten sind hochschulweit einheitlich zu gestalten und entsprechend zu kennzeichnen. Entsprechende Vereinbarungen mit Förderern sind der Hochschulleitung bekanntzugeben.

2.7 Die Gestaltung der www-Seiten sollte sich an den allgemein anerkannten Gestaltungsregeln orientieren. Zu diesen zählen insbesondere die diesbezüglichen Gestaltungsempfehlungen der interuniversitären Arbeitsgruppe. Es ist darauf zu achten, daß das Erscheinungsbild der Universität im Internet dem in anderen Medien vergleichbar ist. Für Logos und Signets der Hochschule sind nur die offiziellen Versionen (<http://www.tu-bs.de/pressestelle/icons/index.html>) zu verwenden. Abteilung 52 empfiehlt Gestaltungselemente, die in den www-Seiten der Hochschulverwaltung verwendet werden.

3 Verantwortlichkeiten des Informationsanbietenden

- 3.1 Die für das jeweilige Informationsangebot verantwortliche Institution bzw. Person (Universitätsverwaltung, Rechenzentrum, Fachbereich, Institut, ... oder Einzelperson) ist für den Inhalt der von ihr bereitgestellten www-Seite, ihre Pflege und die Herstellung von Verweisen auf andere www-Seiten verantwortlich. Die Verantwortlichkeit erstreckt sich auch auf die Einhaltung gesetzlicher Vorschriften.
- 3.2 Die Verantwortung für den Inhalt einer www-Seite umfaßt in eingeschränkter Weise auch Hypertext-Referenzen auf andere Dokumente. Letztere sind gelegentlich zu überprüfen, ob sie ihrerseits den gesetzlichen Anforderungen genügen. Ist das erkennbar nicht der Fall, muß eine betreffende Referenz entfernt oder auf die rechtliche Fragwürdigkeit des betreffenden Dokumentes hingewiesen werden.
- 3.3 Ergänzend zum www-Angebot der Universität bzw. ihrer Organisationseinheiten können Mitglieder und Angehörige der Universität, die über eine Nutzungsberechtigung des RZ oder einer anderen Einrichtung der Universität verfügen, im Rahmen der disponiblen Ressourcen persönliche www-Seiten anbieten, auf denen auch private Themen behandelt werden können. — Der Übergang zu den persönlichen www-Seiten ist deutlich zu kennzeichnen.
- 3.4 Auf jeder www-Seite ist die für die Bereitstellung der Information verantwortliche Organisationseinheit einschließlich Bearbeiter bzw. Einzelperson sowie das Datum der Erstellung bzw. Modifikation zu nennen. Es soll ein Link auf eine E-Mail-Adresse zur Verfügung gestellt werden, über die weitere Auskünfte bzw. Informationen zur Seite eingeholt werden können. Bei hierarchisch nachgegliederten Seiten können diese Angaben entfallen, sofern ein eindeutiger Zusammenhang zwischen den Seiten besteht.

4 Verstöße gegen die Regelung des www-Angebotes

- 4.1 www-Seiten, deren Inhalte offensichtlich gegen diese Ordnung, gegen vorrangige Ordnungen und Regeln oder gegen geltendes Recht verstoßen, sind vom Betreiber des jeweiligen www-Servers unverzüglich zu löschen.
- 4.2 www-Seiten, aus denen nicht unmittelbar zu entnehmen ist, wer für sie verantwortlich ist, können gelöscht werden.
- 4.3 Ist fraglich, ob der Inhalt einer www-Seite im Sinne des ersten Absatzes zu beanstanden ist, informiert der Betreiber des www-Servers die jeweilige Anbieterin bzw. den jeweiligen Anbieter über die Beanstandung und bittet um Abhilfe. Kommt sie/er diesem Wunsch nicht nach und kann sie/er auch nicht nachvollziehbar begründen, wieso die beanstandete Seite unverzichtbar ist (z. B. für Zwecke von Forschung und Lehre), kann die Seite vom Server-Betreiber gesperrt oder gelöscht

werden. — In Zweifelsfällen hat die Hochschulleitung gemäß der Rechtslage zu entscheiden.

- 4.4 Der Server-Betreiber ist nicht verpflichtet, eine Routinedurchsicht der www-Seiten auf seinem Server durchzuführen. Erst bei positiver Kenntnis eines Verstoßes gegen diese Ordnung wird der Server-Betreiber tätig und auf eine Abstellung hinwirken.

G Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste

– vom Vorstand beschlossen am 16.05.1994 und geändert am 18.10.1994 –

Stand: 09.07.99

Ziel der Benutzerordnung ist es, die Zusammenarbeit der Anwender untereinander zu regeln. Um dieses Ziel zu erreichen, werden im folgenden eine Reihe von unterstützenden organisatorischen Maßnahmen durch die nutzenden Einrichtungen gefordert und Verhaltensregeln für einen sinnvollen Umgang mit den Netzressourcen und zur Vermeidung mißbräuchlicher Nutzung aufgestellt.

Die Benutzerordnung richtet sich in erster Linie an Personen, die für die Bereitstellung von Kommunikationsdiensten in den Mitgliedseinrichtungen des DFN-Vereins verantwortlich sind. Es wird erwartet, daß jede Einrichtung ihre Endnutzer von dieser Benutzerordnung in Kenntnis setzt. Darüber hinaus wird empfohlen, für die lokal angebotenen Kommunikationsdienste eine eigene Benutzerordnung zu erstellen, die mit den in diesem Dokument aufgestellten Richtlinien in Einklang steht oder auf sie verweist.

Das Einhalten dieser Ordnung liegt im gemeinsamen Interesse aller Beteiligten, da die Verschwendung von Netzressourcen oder deren Mißbrauch zu einer Erhöhung der Nutzungsentgelte und zu Unregelmäßigkeiten bei der Nutzung der Dienste führen könnte.

1 Geltungsbereich

Die Benutzerordnung bezieht sich auf die DFN-Dienste, die auf der Grundlage des Wissenschaftsnetzes (WiN) bereitgestellt werden und dazu dienen, den nutzenden Einrichtungen eine leistungsfähige und störungsfreie Kommunikationsinfrastruktur bereitzustellen.

Zum einen handelt es sich dabei um das WiN mit Übergängen zu anderen Netzen, die für die Kommunikation zur Verfügung gestellt werden, zum anderen um die Infrastruktur für elektronische Post (z. B. Gateways und Relays) und um Informationsdienste.

2 Anforderungen an die nutzenden Einrichtungen

Jede am DFN beteiligte Einrichtung trägt Sorge für die Wahrnehmung der Aufgaben des Netzadministrators, des Postmasters und der Verantwortlichen für Anwendungen sowie für Beratung und Ausbildung. Die Aufgaben müssen nicht notwendigerweise von verschiedenen Personen in der Einrichtung erbracht werden. Je nach Größe der Einrichtung wird eine Person mehr als eine der beschriebenen Aufgaben wahrnehmen. Es ist jedoch erforderlich, daß jede Einrichtung die für die genannten Funktionen verantwortlichen Personen mit den Aufgaben betraut.

Die mit der Wahrnehmung der Funktionen betrauten Personen sollen verpflichtet werden, den im DFN-Verein abgesprochenen Routing-Strategien (z. B. IP-Routing, Mail-Routing) zu folgen.

2.1 Netzadministratorfunktion

Der DFN-Verein empfiehlt, dem örtlichen Netzadministrator folgende Aufgaben zu übertragen: Der Netzadministrator sorgt für

- die Sicherung und Sicherheit des Netzzugangs,
- die Funktionsfähigkeit der Untervermittlung,
- die Netzverwaltung (Routerkonfiguration und -management, IP-Host-Adressvergabe),
- die Domainverwaltung (Betrieb des Nameservers, Verwaltung der Zonendaten und Domain-Namensvergabe),
- die Strukturierung der Datenflüsse,
- die Fehlererkennung, Fehlermeldung und ggf. Fehlerbehebung,
- die Sicherstellung ununterbrochener Betriebsbereitschaft,
- den Kontakt zum DFN-Verein zur Sicherstellung des störungsfreien WiN-Zugangs.

2.2 Postmasterfunktion

Zum reibungslosen Ablauf des Mailedienstes soll ein Postmaster benannt werden, der folgende Aufgaben wahrnimmt:

- Bereitstellen der Mailedienste auf lokaler Ebene,
- Pflege der Adreßtabellen,
- Anlaufstelle bei Mailproblemen für Endnutzer sowie für die Betreiber von Gateway- und Relaydiensten.

2.3 Funktion eines Verantwortlichen für Anwendungen

Ein Verantwortlicher für Anwendungen soll benannt werden für folgende Aufgaben:

- Pflege der angebotenen Services (Mailserver, Newsserver, FTP-Server),
- Pflege weiterer Kommunikationsdienste,
- Fehlermanagement.

2.4 Beratungs- und Schulungsfunktion

Die Ausübung dieser Funktion ist notwendig, um Fehlbedienungen durch die Endnutzer zu vermeiden. Sie setzt sich aus folgenden Aufgaben zusammen:

- Bereitstellen einer telefonischen Beratungsstelle während der Arbeitszeit,
- Bereitstellen von Informations- und Schulungsmaterial,
- Aufklärung über Auswirkungen von Fehlverhalten bei den Endnutzern.

3 Mißbrauch

3.1 Mißbräuchliche Nutzung

Mißbräuchlich ist die Nutzung der DFN-Dienste, wenn das Verhalten der Benutzer gegen einschlägige Schutzvorschriften (u.a. Strafgesetz, Jugendschutzgesetz, Datenschutzrecht) verstößt.

Aufgrund ihrer Fachkunde ist bei den Benutzern der Kommunikationsdienste die jeweilige, insbesondere strafrechtliche Relevanz etwa der Computer-Kriminalität, des Vertriebs pornographischer Bilder und Schriften oder des Diebstahls, der Veränderung oder sonstige Manipulation von bzw. an Daten und Programmen als bekannt vorzusetzen. Diese Fachkenntnis bezieht sich auch auf die Sensibilität der Übertragung von Daten, die geeignet sind, das Persönlichkeitsrecht anderer und/oder deren Privatsphäre zu beeinträchtigen oder bestehende Urheberrechte bzw. auf diesen gründende Lizenzen zu verletzen.

Als mißbräuchlich ist auch eine Nutzung zu bezeichnen, die folgende, nicht abschließend aufgeführte Sachverhaltskonstellationen erfüllt:

- unberechtigter Zugriff zu Daten und Programmen, d.h. mangels Zustimmung unberechtigter Zugriff auf Informationen und Ressourcen anderer verfügbungsbefugter Nutzer
- Vernichtung von Daten und Programmen, d.h. Verfälschung und/oder Vernichtung von Informationen anderer Nutzer – insbesondere auch durch die „Infizierung“ mit Computerviren
- Netzbehinderung, d.h. Behinderungen und/oder Störungen des Netzbetriebes oder anderer netzteilnehmender Nutzer, z. B. durch
 - ungesichertes Experimentieren im Netz, etwa durch Versuche zum „Knacken“ von Paßwörtern,
 - nichtangekündigte und/oder unbegründete massive Belastung des Netzes zum Nachteil anderer Nutzer oder Dritter.

3.2 Empfehlungen an die nutzenden Einrichtungen zur Verhinderung des Mißbrauchs

Beim Mißbrauch der DFN-Dienste kann man grob unterscheiden zwischen Mißbrauch aus Unkenntnis, fahrlässigem und vorsätzlichem Mißbrauch. Je nach Art des Mißbrauchs sind unterschiedliche Aktivitäten zu seiner Verhinderung gefragt. Sie reichen von der Aufklärung der Nutzer, über erhöhte technische Sicherheitsmaßnahmen bis hin zur Androhung von Nutzungsausschluß und Haftung für schuldhaft verursachte Schäden.

Voraussetzung für die Aufklärung von Mißbräuchen ist, daß die Personen, denen Zugang zum DFN gewährt wird, namentlich autorisiert sind. Die Einrichtung, die Netzzugang gewährt, darf daher natürlichen Personen den Zugang nur ermöglichen, wenn die Personen eine Berechtigung zur Nutzung haben.

Durch die Wahrnehmung der geforderten Schulungs- und Beratungsfunktion und durch Aufklärungsarbeit über Auswirkungen von falschem Nutzungsverhalten auf andere Nutzer kann dem Mißbrauch aus Unkenntnis und dem fahrlässigen Mißbrauch entgegengewirkt werden. Dazu gehört insbesondere, die Endnutzer zur vertraulichen Behandlung aller Paßworte, die für den Zugang zu den Kommunikationsdiensten benötigt werden, zu verpflichten und sie dazu anzuhalten, ihre Paßworte so zu wählen, daß sie nicht durch einfache Crackprogramme entschlüsselt werden können.

Darüber hinaus sollten die Betreiber von Kommunikationsdiensten in zumutbarem Umfang Verfahren bereitstellen, die den persönlichen Charakter und die Vertraulichkeit der auf elektronischem Wege ausgetauschten Nachrichten oder sensitiven Daten wahren und schützen. Je nach Sicherheitsrelevanz der Daten wird folgendes empfohlen:

- Einsetzen der vom Hersteller gelieferten Sicherheitsmechanismen (z. B. Paßwortschutz),
- Anwendung topologischer Maßnahmen (Abtrennen sicherheitsrelevanter Systeme durch Router und Bridges),
- Netzüberwachung (z. B. Protokollierung von Zugriffen),
- Einhalten von Sicherheitsklassen (s. „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (ITSEC), Luxemburg 1991).

In den Fällen, wo Nutzern der uneingeschränkte Zugang zu bestimmten Datenbeständen gewährt wird, ist durch geeignete Maßnahmen dafür zu sorgen, daß die Nutzer über diesen Weg nicht den unautorisierten Zugang zu weiteren, nicht-öffentlichen Datenbeständen erhalten können. Die Betreiber sind darüber hinaus gehalten, den DFN-Verein beim Aufspüren und Verhindern unzulässiger Nutzung in zumutbarem Umfang zu unterstützen.

Zusätzlich soll der Endnutzer durch lokale Regelwerke auf den zulässigen Gebrauch der Kommunikationsdienste und die Auswirkungen von Fehlverhalten hingewiesen bzw. vor Mißbrauch gewarnt werden.

4 Konsequenzen bei Verstößen

Die das Deutsche Forschungsnetz nutzenden Einrichtungen sind verpflichtet, ihre Endnutzer mit der Benutzungsordnung und den für sie relevanten Inhalten der Verträge mit dem DFN-Verein vertraut zu machen.

Bei Verstößen gegen die Nutzungsregelungen sind die nutzenden Einrichtungen gehalten, den Mißbrauch unverzüglich abzustellen und sich untereinander zu informieren.

Sollte es zur Wahrung der Interessen aller Einrichtungen, die die Kommunikationsdienste des DFN-Vereins nutzen, erforderlich sein, ist der DFN-Verein frei, aufgrund der unzulässigen Nutzung einzelne Personen oder Einrichtungen von der Nutzung der angebotenen Dienste oder Teilen davon auszuschließen. In besonders schwerwiegenden Fällen, bei denen die unzulässige Nutzung eine Verletzung von geltendem Recht darstellt, können zivil- oder strafrechtliche Schritte eingeleitet werden.

H Glossar

Account die Zugangsberechtigung zu einem Computer oder Computersystem. Zum Account gehören Nutzerkennzeichen - auch login genannt - und Paßwort.

Administrator kurz Admin: Jemand, der sich um die Technik kümmert, Soft- und Hardware einrichtet, Fehler behebt

Archie weltweites Datenbanksystem mit Dateiverzeichnissen von über 1000 ftp-Servern

Authentifizierung Vorgang des Nachweises einer bestimmten Identität. Mit Hilfe eines Geheimnisses (z.B. Paßwort) oder typischen Merkmales (z.B. Stimmabdruck) überzeugt man ein System von der vorgegebenen Identität

Client Programm oder Rechner, welcher den Dienst eines Servers in Anspruch nimmt

DNS Domain Name Service, Umsetzung von IP-Adressen auf Host- und Domainnamen

E-Mail Versenden, Empfangen, Lagern und Katalogisieren von Nachrichten über Netze mittels **Simple Mail Transfer Protocol** unter TCP/IP

Firewall Ein Rechner der zwischen zwei Netzen steht und zwischen diesen die hin- und herlaufenden Daten filtert. Zweck ist, Hackern das Einbrechen in die Rechner „auf der anderen Seite“ nicht zu einfach zu machen, vergleichbar mit einer Feuerschutzwand - daher auch der Name

FTP Kopieren von (großen) Dateien zwischen Rechnern mittels **File Transfer Protocol** auf TCP/IP

Homepage Startseite eines Informationsangebots im World Wide Web

Homeverzeichnis Verzeichnis, in dem der Nutzer seine eigenen Daten ablegt. Auf UNIX mit `~loginname` erreichbar

IRC Internet Relay Chat, weltweites Mehrbenutzer-Kommunikationssystem, Server verwalten viele Kommunikationskanäle, Benutzer unterhalten sich auf den Kanälen in Gruppen oder individuell

MAC-Adresse Abkürzung für **Media Access Control address**, eine weltweit eindeutige Kennzeichnung aller Geräte innerhalb eines Netzwerkes.

NFS Network File System, das von Sun eingeführte Protokoll zur gemeinsamen Nutzung von Dateisystemen im Netzwerk.

Protokoll Vorschrift für die Kommunikationsabfolge mehrerer Teilnehmer. Dient zum Datenaustausch oder zur Steuerungsübergabe. Protokolle sind oft genormt.

Proxy Service, der Objektdaten verschiedener Netzdienste wie HTTP, FTP, GOPHER oder News zwischenspeichert und entsprechende Anfragen aus seinem lokalen Datenbestand schnellstens bedient (caching) oder weiterreicht (proxying). Dadurch werden die Zugriffszeiten auf schon im Cache befindliche Daten enorm verbessert und die Übertragungswege aus dem Internet entlastet.

RfC Request for Comment sind die Dokumente, in denen die Standards des Internet definiert sind.

Server Programm oder Rechner, welcher eine bestimmte Serviceleistung (Dienst) zur Verfügung stellt. (Compute-, File-, WWW-, Mail-Server, etc.)

SMB Server Message Block, das insbesondere von Windows verwendete Protokoll, um Dateisysteme, Drucker etc. gemeinsam im Netzwerk zu nutzen sowie um Listen der verfügbaren Ressourcen zu erstellen und auszutauschen.

Subnetz Eine Menge an Rechnern mit gleichem Netzteil der IP-Adresse

telnet Internet-Protokoll für einen Dialog auf einem anderen (UNIX-)Rechner, Einloggen auf irgendeinem öffentlichen UNIX-Host

UNIX sehr bewährtes Betriebssystem, welches auf Großrechnern und Workstations eingesetzt wird. Entwickelt von AT&T sowie großen amerikanischen Universitäten, 30 Jahre alt

Usenet News weltweite öffentliche Diskussionen („schwarze Bretter“) von Teilnehmern zu beliebigen Themen mittels Network News Transfer Protocol unter TCP/IP, viele tausend Diskussionsgruppen (newsgroups) weltweit, entstanden 1979, lokale Administrationen für spezifische Diskussionsgruppen mit regionaler Bedeutung

WWW World Wide Web („Surfen“ im Internet), das umfassende und führende Informationssystem, www ist multimedial, d.h. es integriert Schrift, Bild, Ton, bewegte Bilder, Video-Clip, Radio/TV Live, wenn entsprechende Multimedia-Tools installiert sind