

Einführung in die Nutzung des **SchunterNet**

3. überarbeitete Auflage – Oktober 2009

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, Windows XP, Windows Vista, Windows 7 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.

Aktualisiert und neugeschrieben von Alexander Riemer und Johannes Starosta

Satz: L^AT_EX

Inhaltsverzeichnis

| | |
|--|-----------|
| 1. Der Verein SchunterNet e.V. | 5 |
| 2. Anmeldung und Netzanschluss | 6 |
| 2.1. Nutzervertrag | 6 |
| 2.2. Netzwerkkarte und MAC-Adresse | 6 |
| 2.3. IP-Adressen und Namen | 9 |
| 2.4. Kosten | 10 |
| 2.5. Minimale Netzkonfiguration | 10 |
| 2.5.1. Windows XP | 11 |
| 2.5.2. Windows Vista | 12 |
| 2.5.3. Windows 7 | 12 |
| 2.5.4. Linux | 12 |
| 2.5.5. Testen des Anschlusses | 12 |
| 2.6. Manuelle Konfiguration der Netzwerkkarte | 13 |
| 2.6.1. Benötigte Daten | 13 |
| 2.6.2. Windows XP | 14 |
| 2.6.3. Linux | 16 |
| 2.6.4. Macintosh | 16 |
| 2.7. Abmeldung | 17 |
| 3. Netzdienste | 18 |
| 3.1. Electronic Mail | 18 |
| 3.2. WWW Server | 19 |
| 3.3. Benutzerserver (jupiter.schunter.etc.tu-bs.de) | 19 |
| 3.3.1. Zugriff auf das Homedirectory | 19 |
| 3.3.2. Private Homepages | 20 |
| 4. Sicherheit | 22 |
| 4.1. Viren, Trojaner, Bugs | 22 |
| 4.1.1. Computerviren | 22 |
| 4.1.2. Trojanische Pferde (Trojan Horses) | 22 |
| 4.1.3. Bugs | 23 |
| 4.2. Paßwörter | 23 |
| A. Satzung des Vereins SchunterNet e.V. | 26 |
| B. Benutzerordnung des SchunterNet e.V. | 29 |
| C. Gebührenordnung des SchunterNet e.V. | 33 |
| D. Nutzungsordnung zur Informationstechnologie der Technischen Universität Braunschweig | 34 |

| | |
|--|-----------|
| E. Ordnung zur IT-Sicherheit der Technischen Universität Braunschweig | 38 |
| F. Informationsdienste-Ordnung der Technischen Universität Braunschweig | 42 |
| G. DFN-Benutzungsordnung | 47 |
| H. Glossar | 51 |

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 Clubhaus 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 Gauss-IT-Zentrum 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.

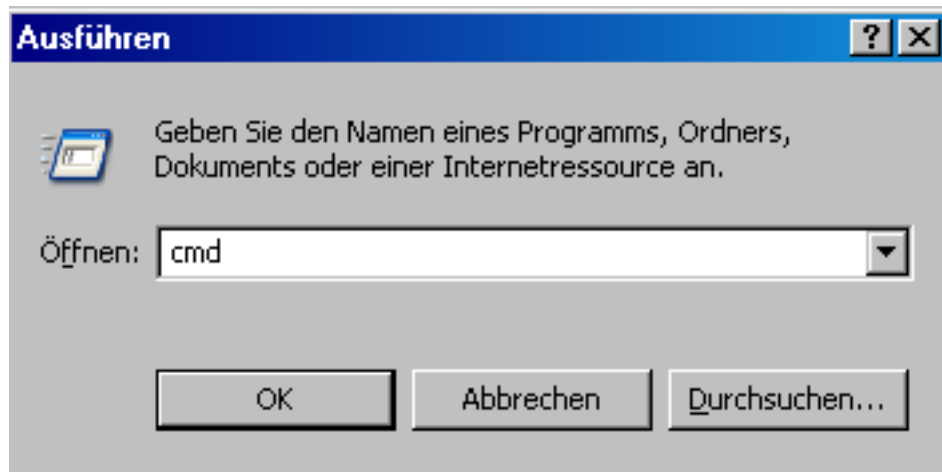
2.2. Netzwerkkarte und MAC-Adresse

In jedem Zimmer befindet sich eine Anschlussdose, in Haus 3 über der Pinwand neben der Kofferklappe. In Haus 1 und Haus 2 findet man die Dose bei den anderen Steckdosen. Zum Anschluss ist ein Netzwerkadapter (Ethernet-Karte) mit RJ45-Buchse und ein Anschlusskabel (Twisted Pair, RJ45, **nicht** crossed over) der benötigten Länge erforderlich. Es kann, falls nicht schon vorhanden, in der ➤ Sprechstunde des SchunterNet erworben werden. Die Bandbreite der Netzkarte bzw. der Netzanbindung kann 10 MBit/s (10BaseT) oder 100 MBit/s (100BaseT) betragen. Macs haben seit 1999 10/100BaseT Ethernet eingebaut, das gilt auch für iMacs/iBooks/PowerBooks.

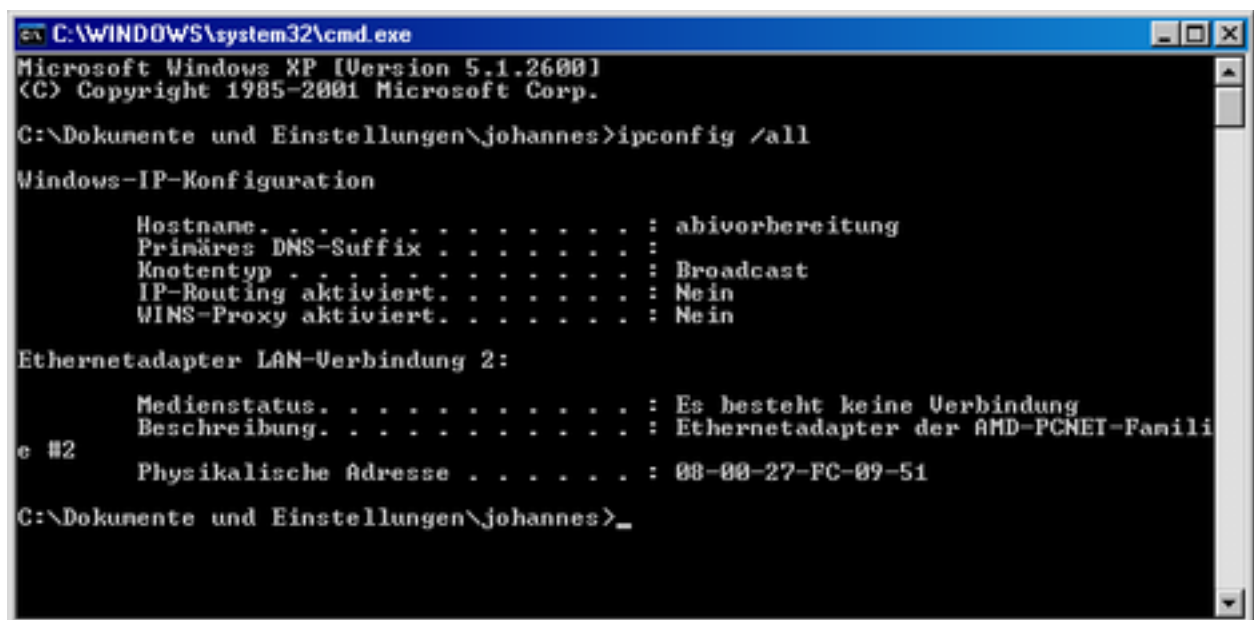
Jede Ethernet-Karte bzw. -Chip hat eine weltweit eindeutige Hardware-(oder ➤ MAC-)Adresse, die fest in der Karte eingestellt ist. Bei älteren Ethernet-Karten ist sie auf einen der Chips aufgeklebt, bei neueren erfährt man sie entweder aus der mitgelieferten Dokumentation, oder durch ein Service-Programm. Die Adresse kann z.B. so aussehen: 00:12:6b:9f:20:cc Je nach Betriebssystem gibt es mehrere Möglichkeiten, die MAC-Adresse herauszufinden.

Windows XP

Unter Windows XP wählt man **Startmenü** ⇒ **Ausführen**. In das sich öffnende Fenster tippt man `cmd` ein und bestätigt dies durch einen Klick auf **Ok**:



In die sich nun öffnende Eingabeaufforderung gibt man den Befehl `ipconfig /all` ein:




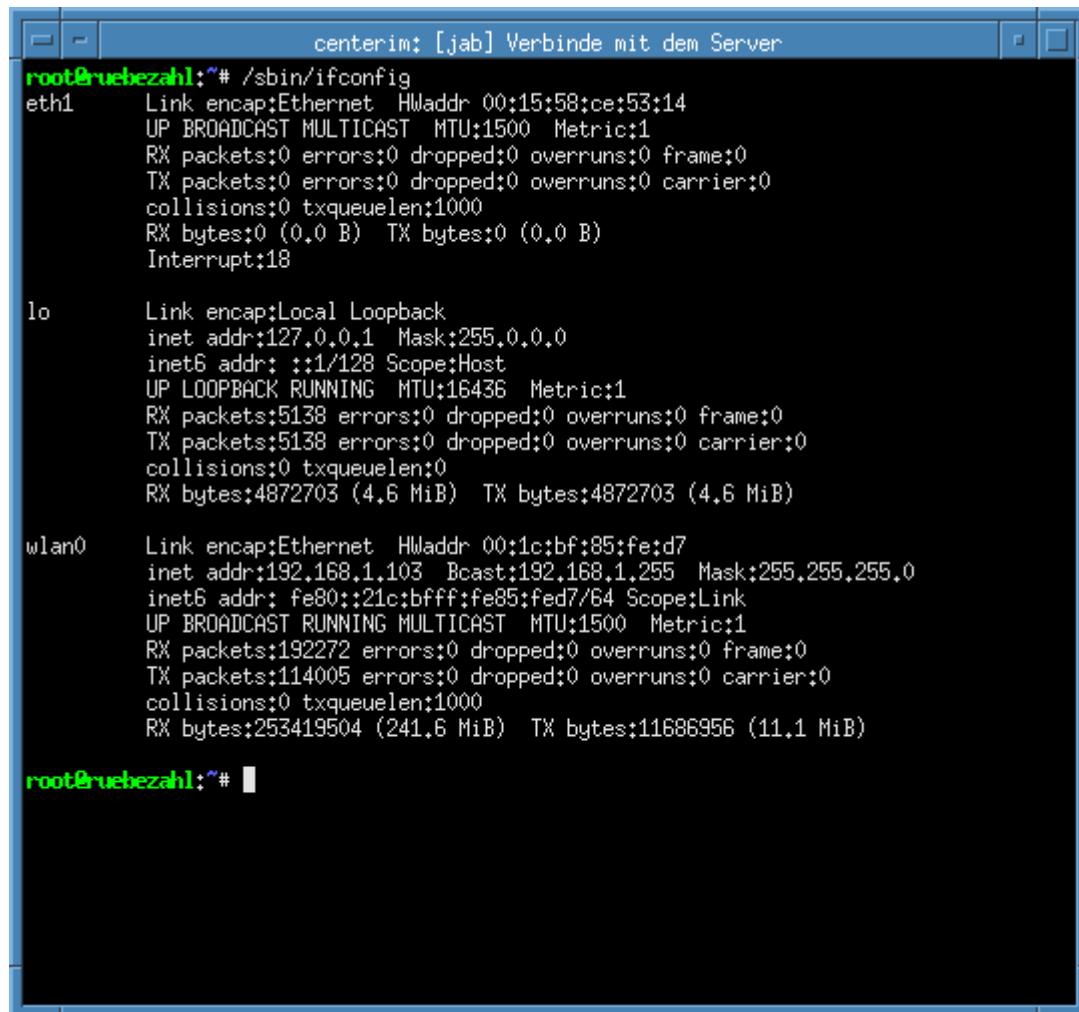
Nun muss man aufpassen, dass man nicht die falsche MAC-Adresse, z.B. der WLAN-Karte erwischt. Gesucht wird die der Ethernetkarte. Im Screenshot wäre dies zum Beispiel der texttt„Ethernetadapter LAN-Verbindung 2“. Die MAC-Adresse selbst verbirgt sich hinter der psysikalischen Adresse, hier also: „0B-00-27-FC-09-51“.

Windows Vista/7**Mac OS**

Unter MacOS X kann die MAC-Adresse mit den „Apple System Profiler“ ermittelt werden: Unter älteren Systemen (Mac OS 9.22 und dessen Vorgänger) 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.

Unix/Linux

Vorbemerkung: Je nach Distribution kann es kleinere Unterschiede geben. Die folgende Anleitung wurde für Debian und Ubuntu getestet und sollte sich leicht an andere Distributionen anpassen lassen. Unter UNIX/Linux öffnet man zunächst ein Terminal. Dort gibt man dann den Befehl `ifconfig` ein. Unter Umständen muss der absolute Pfad `ifconfig` benutzt werden. Die Ausgabe könnte so aussehen:



```
centerim: [jab] Verbinde mit dem Server
root@ruebezahl:~# /sbin/ifconfig
eth1      Link encap:Ethernet  HWaddr 00:15:58:ce:53:14
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:18

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:5138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4872703 (4.6 MiB)  TX bytes:4872703 (4.6 MiB)

wlan0     Link encap:Ethernet  HWaddr 00:1c:bf:85:fe:d7
          inet addr:192.168.1.103 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::21c:bfff:fe85:fed7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:192272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114005 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:253419504 (241.6 MiB)  TX bytes:11686956 (11.1 MiB)

root@ruebezahl:~#
```

Aufpassen muss man nun, dass man nicht die falsche MAC-Adresse notiert, z.B. von der WLAN-Karte. Gesucht ist die MAC-Adresse der Ethernetkarte. Diese fängt zumeist mit „eth“ an, hier also „eth1“. Davon ist nun die MAC-Adresse gesucht, auch „HWAddr“ oder „Hardwareadresse“ genannt, hier also: „ 00:15:58:ce:53:14“.

2.3. 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 134.169.168.xxx und 134.169.169.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.

2.4. Kosten

Das *SchunterNet* wurde mit einem zinsfreien Kredit des Studentenwerks finanziert, welcher im Zeitraum von fünf Jahren in monatlichen Raten zurückzuzahlen war. Diese Kosten wurden auf eine monatliche Nutzungsgebühr nach der Gebührenordnung [Anhang C] umgelegt. Inzwischen sind die laufenden Kosten (Glasfaserleitung zum APM/IT-Zentrum und Systemwartung) in die Nutzungsgebühr enthalten.

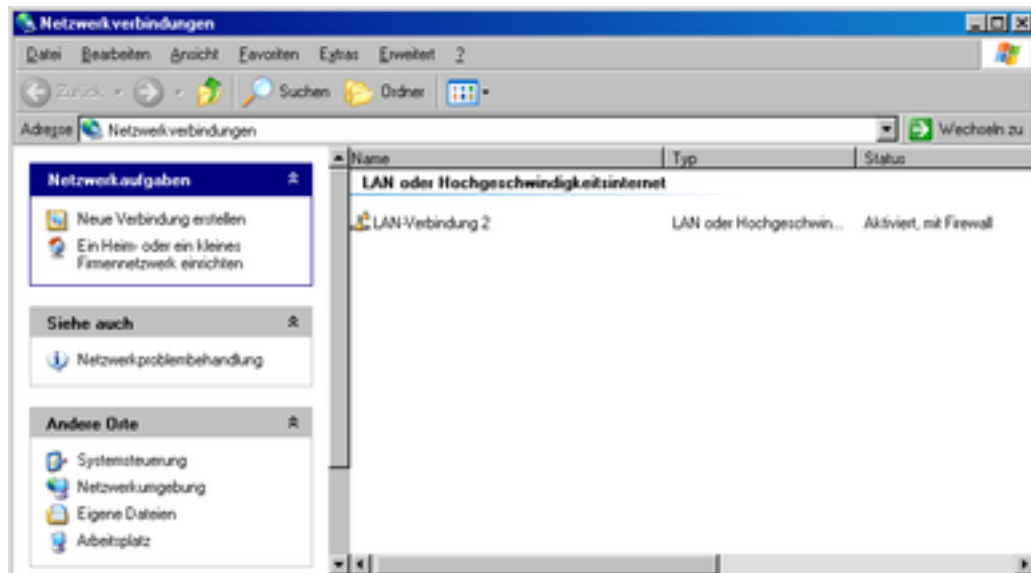
Um den Aufwand für den Kassenwart in Grenzen zu halten, ist die Zahlung durch Einzugsermächtigung der Regelfall, ein Vordruck befindet sich am Netzantrag. Bitte beachtet, daß die Banken bei nicht gedecktem Konto oder aus anderen Gründen nicht ausgeführten Lastschriften Bearbeitungsgebühren erheben, die bis zu 10,-€ betragen können und euch durch den Verein in voller Höhe berechnet werden. In Ausnahmefällen kann die Nutzungsgebühr während der ↗Sprechstunde in bar beglichen werden. [Anhang C]

2.5. Minimale Netzkonfiguration

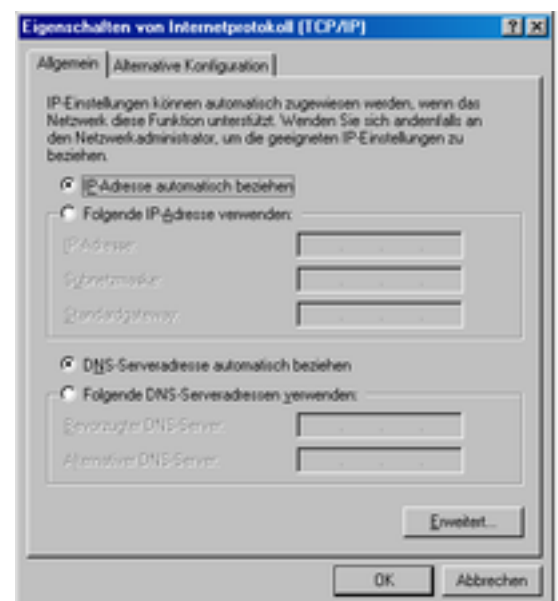
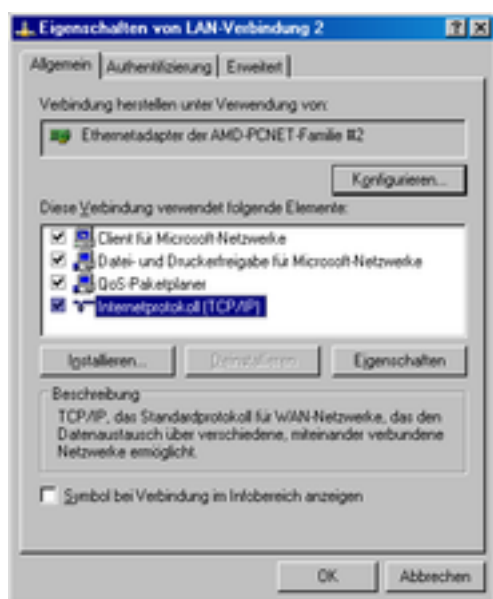
Bei fast allen Betriebssystemen müssen während der Installation ein paar Angaben gemacht werden, die überall gleichartig sind. In den meisten Fällen sollte es dabei reichen, wenn man in den Netzwerkeinstellungen „IP-Adresse automatisch beziehen“, „DHCP verwenden“ oder ähnliches auswählt. Die Einzelheiten werden für die verschiedenen Betriebssysteme im Folgenden beschrieben.

2.5.1. Windows XP

Man klickt sich durch über **Startmenü** ⇒ **Einstellungen** ⇒ **Systemsteuerung** zum Fenster **Netzwerkverbindungen** durch:



Hier ist nun die richtige Netzwerkverbindung auszuwählen. Wie man sie ermittelt, wird im Abschnitt zur MAC-Adresse beschrieben. Zunächst sollte man ihren Status überprüfen: Die Netzwerkverbindung muss aktiviert sein. Andernfalls muss sie mittels **Rechtsklick** ⇒ **Aktivieren** aktiviert werden. Anschließend ruft man mit **Rechtsklick** ⇒ **Eigenschaften** das linke Fenster auf:



Hier ist nun auf `Internetprotokoll (TCP/IP)` und anschließend auf `Eigenschaften` zu klicken. Es sollte sich das rechte Fenster öffnen. Die Einstellungen sollten mit den abgebildeten übereinstimmen. Andersweitig sind sie zu ändern und mit einem beherzten Klick auf `Ok` zu bestätigen. Damit sollte dann in der Tat alles ok sein.

2.5.2. Windows Vista

2.5.3. Windows 7

2.5.4. Linux

Wie schon bei der MAC-Adresse gilt: Je nach Distribution kann es kleinere Unterschiede geben. Die folgende Anleitung wurde für Debian und Ubuntu getestet und sollte sich leicht an andere Distributionen anpassen lassen. Die folgenden Einstellungen müssen als Administrator („root“) vorgenommen werden. Je nach Distribution ist es dazu erforderlich, sich als root anzumelden, oder anderweitig als Administrator auszuweisen. In Ubuntu erfolgt dies beispielsweise mit Hilfe des Programms `sudo`.

Die Einstellungen werden durch Bearbeiten der Datei `/etc/network/interfaces` vorgenommen. Sie sollte danach folgende Einträge erhalten:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto eth1
iface eth1 inet dhcp
```

Dabei muss `eth1` durch das Kürzel der jeweiligen Netzwerkkarte ersetzt werden. Wie man diese Netzwerkkarte herausfindet ist im Abschnitt zur MAC-Adresse beschrieben. Anschließend muss man diese Änderungen noch aktivieren. Dazu gibt man in eine Konsole nacheinander folgende Befehle ein:

```
ifdown eth1
ifup eth1
```

Wieder muss `eth1` durch das entsprechende Kürzel ersetzt werden. Damit ist die Konfiguration erledigt.

2.5.5. Testen des Anschlusses

Sind die Einstellungen erledigt, sollte man die Einstellung testen. In den meisten Fällen sollte alles klappen. Sollte dies nicht der Fall sein, gibt es folgende Möglichkeiten: Die mit Abstand

häufigste Fehlerquelle ist es, bei der Anmeldung eine falsche MAC-Adresse angegeben zu haben. Es empfiehlt sich nun, die Anmeldebestätigung herauszusuchen und die dort angegebene MAC-Adresse mit der tatsächlichen zu vergleichen. Sollte man sie vergessen haben (nicht sooo überraschend bei einer Folge aus hexadezimalen Ziffern), kann man sie ja mit den aus Abschnitt 2.2 genannten Methoden erneut ermitteln. Sollte sie falsch sein, kann man die Richtige den Admins in der Sprechstunde oder über eine Email an admin@schunternet.de mitteilen¹.

Ein anderer häufiger Fehler ist das Benutzen des zweiten Anschlusses. Jedes Zimmer ist mit einer Dose mit zwei Anschlüssen ausgestattet. Die Zweite ist im Normalfall aber nicht freigeschaltet. Dieses Problem sollte sich aber schnell beheben lassen. Stellenweise sind einige Dosen auch falsch angeschlossen worden. In so einen Fall sollte man umgehend einen der Hausmeister und uns informieren, damit entsprechend Abhilfe geschaffen werden kann.

Können alle diese Fehler ausgeschlossen werden, kann man sein Glück mit der manuellen Konfiguration der Netzwerkkarte versuchen. Und natürlich ist die Sprechstunde kein Selbstzweck, sondern durchaus dafür da, Probleme anzusprechen und dann auch zu lösen :)

2.6. Manuelle Konfiguration der Netzwerkkarte

Eine Anmerkung vorweg: Im Normalfall sollten die folgenden Schritte gar nicht nötig sein, da im Netzwerk ein DHCP-Server arbeitet, der alles automatisch erledigt. Allerdings kann es sehr selten dazu kommen, dass dieser seinen Geist aufgibt. Auch zur Fehlersuche können sie hilfreich sein. Aber: **Sie sollten nur getätigt werden, wenn man genau weiss was man tut!!! Ein Fehler kann zur Sperre führen!!!** Der Hintergrund ist, dass zur Vermeidung von Mißbrauch einer unser Server eine Art Abwehrprogramm laufen lässt. Dieses Programm bemerkt eventuelle Angriffe und sperrt dann den entsprechenden Rechner. Aus technischer Sicht ist ein Mißbrauch und ein Fehler aber nicht zu unterscheiden. Daher nochmal der Hinweis: **Folgendes nur tun, wenn man sich seiner Sache ganz sicher ist!!! Ansonsten wird gerne in der Sprechstunde weitergeholfen!**

2.6.1. Benötigte Daten

Die nötigen Daten sind auf der Anmeldebestätigung vermerkt, die man nach der Freischaltung des Anschlusses erhalten hat. Sie werden im folgenden näher erläutert:

TCP/IP-Adresse bzw. Host-Adresse hier muss die sogenannte IP-Adresse des eigenen Rechners eingegeben werden, z.B. 134.169.168.255.

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

¹Wie soll das gehen ohne Internet? Hier ist nun Fantasie gefragt: Vom Fragen des Nachbarn, über die Computerräume der Uni gibt es ein breites Feld an Möglichkeiten :)

innerhalb des Wohnheims (und innerhalb der TU) immer gleich und zwar 134.169. Die dritte Zahl ist im Wohnheim entweder 168 oder 169. 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 134.169.168.255 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 134.169.168.0 und als Broadcastadresse 134.169.169.255 eingetragen werden.

DNS/Name Server, Router, Gateway Hier muss immer die IP-Adresse 134.169.168.1 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 2.3) eingetragen werden.

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

2.6.2. Windows XP

Zunächst öffne man wieder mittels `Startmenü` ⇒ `Einstellungen` ⇒ `Systemsteuerung` das Fenster `Netzwerkverbindungen`. Nach Überprüfung des Status der richtigen Netzwerkverbindung, öffne man mit `Rechtsklick` ⇒ `Einstellungen` folgendes Fenster:

Hier ist nun auf `Internetprotokoll (TCP/IP)` und anschließend auf `Eigenschaften` zu klicken. Es sollte sich nun ein neues Fenster öffnen, in dem man die Daten von der Anmeldebestätigung eintragen kann:



Dabei sind statt der abgebildeten Daten natürlich die auf der Bestätigung abgedruckten einzutragen.

2.6.3. Linux

Auch hier gilt: Je nach Distribution kann es kleinere Unterschiede geben. Die folgende Anleitung wurde für Debian und Ubuntu getestet und sollte sich leicht an andere Distributionen anpassen lassen. Auch bei der manuellen Konfiguration werden Adminrechte benötigt. Mit diesen versehen bearbeitet man dann die Datei `/etc/network/interfaces`, die danach so aussehen sollte:

```
# The loopback network interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
# The primary network interface
auto eth1
iface eth1 inet static
address 134.169.168.255
netmask 255.255.254.0
gateway 134.169.168.1
```

Statt 134.169.168.255 gibt man die auf der Anmeldebestätigung zugeteilte Adresse ein. `eth1` ist wieder durch das Kürzel der entsprechenden Netzwerkkarte zu ersetzen. Abhängig von der vorliegenden Linux-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
134.169.168.255 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 134.169.168.1
# end of /etc/resolv.conf
```

2.6.4. Macintosh

Die Konfiguration des Macintosh erfolgt analog zu der für Windows 95/98 usw. beschriebenen. Die dazu aufzurufenden Kontrollfelder (Apfel-Menü \Rightarrow 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 25. 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. Standardmäßig werden die Emails an die bei der Anmeldung angegebene Emailadresse gesendet. Möchte man diese Adresse ändern, ist die Datei `.forward` auf den Benutzerserver zu bearbeiten. Möchte man den Zugang über das SchunterNet nutzen, ist sie zu entfernen. Mehr Informationen zum Arbeiten auf den Benutzerserver unter 3.3 auf 19.

Zum Senden und Empfangen von E-Mail im SchunterNet sind nach Entfernen der `.forward` noch einige Einstellungen notwendig. Dazu geht man z.B. unter Thunderbird wie folgt vor:

Bearbeiten ⇒ Einstellungen ⇒ Konten ⇒ Konto hinzufügen: ⇒ E-Mail-Konto ⇒
E-Mail-Adresse `Vorname.Nachname@schunternet.de` ⇒ POP|IMAP ⇒ Posteingang-Server
`pop.schunter.etc.tu-bs.de|imap.schunter.etc.tu-bs.de` ⇒ Postausgang-Server (SMTP)

`mail.schunter.etc.tu-bs.de` ⇒ Benutzername `loginname@schunter.etc.tu-bs.de`

Ob man POP oder IMAP wählt, ist im Prinzip egal, der Unterschied ist, dass bei IMAP alle Emails auf den Server bleiben, inklusive der Ordnerstruktur. Auf diese kann dann auch via Webmail unter <https://www.schunter.etc.tu-bs.de/squirrelmail> zugreifen. Nun muss man noch eine Kontobezeichnung wählen und auf „Fertig stellen“ klicken. Danach kann dann das Emailprogramm genutzt werden. Bei anderen Emailprogrammen ist die Einrichtung ähnlich. Zur Sicherheit bei Email sieh auch noch 4.1 und 4.2.

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) Der an der TU vergebene Mailalias der Form `V.Nachname@tu-bs.de` kann direkt auf den Wohnheimserver umgeleitet werden. Dies kann jeder über den Benutzerdatendienst des IT-Zentrums der TU-Braunschweig (<https://www2.tu-bs.de/it/services/benutzer/bdd>) 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 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 Server

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.

3.3. Benutzerserver (`jupiter.schunter.etc.tu-bs.de`)

3.3.1. Zugriff auf das Homedirectory

Wie so oft gibt es auch hier mehrere Möglichkeiten:

... 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-Directorys per anonymous-ftp ist nicht möglich. Außerdem ist ftp nicht gerade das sicherste Verfahren, da alle Passwörter in Klartext übertragen werden. Deswegen empfehlen wir die Verwendung des deutlich sichereren scp/sftp-Protokolls.

... per sftp/scp

Die Vorgehensweise ist hier ähnlich wie unter ftp, aber mit den Vorteil, dass alle Verbindungen verschlüsselt werden. Unter Unix-Systemen inklusive Mac OS X, sind in der Regel sftp und scp für die Konsole schon vorhanden. Die gängigen Desktops (Gnome/Kde) haben meistens schon

einen graphischen Client direkt integriert, womit sich der Zugang über `sftp://login@jupiter.schunter.etc.tu-bs.de/` herstellen lässt. Danach nur noch Passwort eintippen und man ist verbunden. Je nach verwendetem System kann die URL auch `scp://login@jupiter.schunter.etc.tu-bs.de/` oder `ssh://login@jupiter.schunter.etc.tu-bs.de/` lauten. Für Windows empfiehlt sich als Client das kostenlose Programm WinSCP und für Mac OS X gibt es unter anderen Cyberduck.

... durch Einloggen auf dem Server

Mit `ssh` kann man sich direkt auf dem \rightarrow Server (Name: „jupiter.schunter.etc.tu-bs.de“) einloggen und in einer \rightarrow UNIX-Shell-Umgebung (`bash`) arbeiten. Als Texteditoren stehen z.B. `vi` (bzw. `vim`, `elvis`) und `joe` sowie `emacs` zur Verfügung. Allerdings wollen wir aus Sicherheitsgründen diese Funktionalität bald einschränken, dass neue Benutzer zunächst sich nur via `scp/sftp` verbinden können. Auf Anfrage wird man allerdings einen vollwertigen Zugriff erreichen können

3.3.2. 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 \rightarrow WWW-Server als Dokumenten-Verzeichnis für persönliche \rightarrow WWW-Seiten interpretiert. Eine dort liegende Datei mit dem Namen `index.html` wird als \rightarrow Homepage interpretiert (alternativ ist auch `index.htm` möglich). Der URL dieser \rightarrow Homepage besteht aus dem Namen des \rightarrow 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 \rightarrow 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 \rightarrow Authentifizierung
- Kommando: `mkdir ~/public_html` zur Erzeugung des Unterverzeichnisses, in dem die \rightarrow 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 \rightarrow ftp oder `sftp` mit graphischer Oberfläche angelegt werden, z.B. mit `WS_FTP` oder `WinSCP`. 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.

4. Sicherheit

4.1. 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:

4.1.1. 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.

4.1.2. 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>.

4.1.3. 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

4.2. Paßwörter

Wie ändere ich das Paßwort?

Um das Paßwort zu ändern, muss zunächst ein Terminalprogramm gestartet werden, z.B. ➤ ssh. Als Zieladresse wird der Rechner jupiter angegeben (IP-Adresse ist 134.169.168.3, falls der ➤ DNS-Server nicht benutzt werden kann). Man erhält dann folgende (oder ähnliche) Begrüßungsmeldung:

Login:

Password:

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:

```
Linux jupiter.schunter.etc.tu-bs.de 2.6.32-jupiter #1 SMP Sat Dec 12 00:42:27 CET 2009 x86_64
```

```
Willkommen auf dem neuen Jupiter !
```

```
Wichtigste Neuerung : Die Mails werden fortan im Maildir-Format  
abgelegt, siehe Maildir/ Ordner im Homeverzeichnis.
```

```
Last login: Thu Mar 20 15:30:06 on ttyt1 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 `kpasswd` 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.

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 Attacken 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.

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 5.
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 9 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 $\frac{2}{3}$ 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 $\frac{2}{3}$ 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 C]
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 C] verbindlich.
4. Betriebs- und Hardwarekosten werden entsprechend der Gebührenordnung [Anhang C] 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 Newsgruppen 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 C] festgelegten Tarifen zu tragen.
5. Wer über diese Bestimmungen hinaus gegen die Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig [Anhang C], 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: 07. September 2009

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 13,- €(in Worten: dreizehn Euro) nicht überschreiten. Derzeit ist die Gebühr auf 8,- €(in Worten: acht Euro) festgelegt.
3. Zur Absicherung eventueller durch den Nutzer verursachter Forderungen Dritter an den Verein, ist eine Kautions in Höhe der aktuellen monatlichen Nutzungsgebühr zu hinterlegen
4. Alle Folgezahlungen sind bis 15. des Vormonats für den entsprechenden Monat einzuzahlen (jeweils eine Monatsgebühr).
5. Die Zahlung der Nutzungsgebühr erfolgt in erster Linie per Lastschriftinzugsverfahren. Bei Barzahlungen wird eine zusätzliche Gebühr von 2,- €je Zahlung erhoben. Ausnahme stellt die erste Barzahlung dar, bei der keine Barzahlungsgebühr erhoben wird.
6. Schlägt die Abbuchung aus Gründen, die der Nutzer zu vertreten hat, fehl, ist er verpflichtet die anfallenden Bankgebühren sowie die nichteingezogenen Gebühren in Bar zu begleichen. Dabei entfällt die Barzahlungsgebühr in Höhe von 2,- €.
7. Die Nutzungsgebühren werden in erster Linie zur Deckung der laufenden Kosten verwendet. Eventuelle Überschüsse werden für Reparaturen und weitere Investitionen genutzt.
8. Wird ein Zweitanschluss beantragt, so sind die Kosten der Umrüstung in Höhe von 15,- €durch den Antragsteller zu tragen.
9. Durch Benutzer verursachter zusätzlicher Arbeitsaufwand im Sinne §8, Absatz 4, der Benutzerordnung [Anhang B] wird zu einem Stundensatz von 12,00 €in Rechnung gestellt, wobei ein Mindestbetrag von 6,- €erhoben wird.
10. Schäden an vereinseigener Hardware, die durch unsachgemäßen Umgang fahrlässig oder vorsätzlich entstanden sind, gehen in vollem Umfang zu Lasten des Verursachers.
11. Änderungen dieser Gebührenordnung sind in den halbjährlichen Mitgliederversammlungen möglich.

Nutzungsordnung zur Informationstechnologie der Technischen Universität Braunschweig

Inhaltsverzeichnis

Präambel

§ 1 Geltungsbereich

§ 2 Rechte und Pflichten der Benutzer

§ 3 Ordnungsmaßnahmen und Haftung

§ 4 Notfallgruppe

§ 5 Rechenzentrum

§ 6 Sonstige IT-Betreiber

§ 7 Auskunftersuchen

§ 8 Gebühren

§ 9 Inkrafttreten

Präambel

Diese Ordnung regelt die Belange der Informationstechnologie(IT)-basierten Dienste der Technischen Universität Braunschweig (TU BS) sowie Zuständigkeiten, Aufgaben, Rechte und Pflichten der Dienste-Anbieter und -Nutzer.

Nachfolgend genannte Regelungen gelten unter Berücksichtigung der folgenden gesetzlichen Bestimmungen:

- Datenschutzbestimmungen Bundesdatenschutzgesetz (BDSG), Telekommunikations-Datenschutzverordnung (TDSV), Teledienste-Datenschutzgesetz (TDDSG), Niedersächsisches Datenschutzgesetz (ND SG)
- Telekommunikations-Gesetz (TKG)
- Urheberrecht/Lizenzrecht (UrhG)
- Persönlichkeitsrechte (BGB)
- Strafgesetzbuch (StGB), Strafprozessordnung (StPO)

Daneben gelten die Gebühren- und Entgelte-Ordnung der TU BS, die Ordnung zur IT-Sicherheit sowie die Informationsdienste-Ordnung. Darüber hinaus sind auch die vertraglichen Vereinbarungen mit übergeordneten Providern, wie beispielsweise dem DFN, zu beachten.

§ 1 Geltungsbereich

Diese Ordnung findet Anwendung auf alle Mitglieder und Angehörige der TU BS, der Einrichtungen des Studentenwerks Braunschweig sowie auf Angehörige anderer Einrichtungen außerhalb der TU BS, die eine Nutzungsvereinbarung mit der TU BS geschlossen haben. Darüber hinaus gelten die einschlägigen Ordnungen der jeweiligen Einrichtungen.

§ 2 Rechte und Pflichten der Benutzer

(1) Die in § 1 aufgeführten Personen und Einrichtungen können innerhalb ihres Bereiches eigenverantwortlich IT-Geräte betreiben. Hierfür ist ein DV-Koordinator zu benennen, der die IT-Belange nach innen koordiniert und nach außen vertritt; dieser sollte möglichst zum hauptamtlichen Personal der Einrichtung gehören.

(2) Der Anschluss eines IT-Gerätes an das Datennetz sowie Veränderungen daran müssen vom Betreiber mit dem Rechenzentrum koordiniert werden. Ausschließlich das Rechenzentrum teilt dazu den Betreibern Netzadressbereiche zu. Netzbezogene Dienste, die über den unmittelbaren Zuständigkeitsbereich der TU-Einrichtung hinaus gehen, müssen ebenfalls mit dem Rechenzentrum koordiniert werden (beipielsweise E-Mail, News, FTP, Names, etc., vgl. auch Informationsdienste-Ordnung §2(3)).

(3) Die bereitgestellten Ressourcen sind in wirtschaftlicher und dem Nutzungszweck angemessener Weise zu nutzen, ohne dass andere hierdurch beeinträchtigt werden.

(4) Benutzer dürfen Lizenz-Software oder urheberrechtlich geschützte Dokumentationen nicht ohne Genehmigung kopieren, an Dritte weitergeben oder Dritten zugänglich machen. Lizenz-Software darf nicht auf anderen Rechnern als denen verwendet werden, für die die Software lizenziert ist. Die Benutzer sind für die Einhaltung der Lizenzbestimmungen der ihnen zur Verfügung gestellten Software verantwortlich.

Es ist unzulässig, Manipulationen an der Betriebssystem-Software und an Benutzerverzeichnissen vorzunehmen oder Zugriff auf Benutzerbereiche auszuführen, für die keine Berechtigung vorliegt.

(5) Jeder Benutzer ist bei der Verarbeitung und Übertragung von Daten, die schutzwürdig im Sinne der Datenschutzbestimmungen sind, für die Einhaltung der vorgeschriebenen Sicherheitsmaßnahmen selber verantwortlich.

Jedes Mitlesen oder Auswerten von Nachrichteninhalten, die an Dritte adressiert sind, sowie die Weitergabe unbeabsichtigt erhaltener Informationen ist unzulässig.

(6) Die Nutzung der IT-Einrichtungen für kommerzielle Zwecke ist nur mit schriftlicher Zustimmung der Hochschule und nach Festlegung der Gebühren zulässig, soweit es in der Gebühren- und Entgelte-Ordnung vorgesehen ist.

(7) Der Nutzungsberechtigte verpflichtet sich, bei Beendigung des Nutzungsverhältnisses alle ihn betreffenden bzw. von ihm benutzten Ressourcen freizugeben, die ihm von der Hochschule zur Verfügung gestellten Arbeitsmittel zurückzugeben und alle sonstigen Ansprüche, die aus dem Nutzungsverhältnis entstanden sind, zu erfüllen.

(8) Der Benutzer ist verpflichtet, dem Rechenzentrum unverzüglich einen erkannten Missbrauch des Universitätsnetzes bzw. Störungen am Netz anzuzeigen.

§ 3 Ordnungsmaßnahmen und Haftung

(1) Verstößt ein Nutzungsberechtigter gegen diese Benutzungsordnung, insbesondere gegen die sich aus § 2 ergebenden Pflichten, kann ihm die Benutzungserlaubnis eingeschränkt beziehungsweise in schwerwiegenden Fällen die Benutzung untersagt werden. Er ist davon unter Angabe der Gründe in Kenntnis zu setzen. Unabhängig hiervon können strafrechtliche und/oder zivilrechtliche Schritte gegen ihn eingeleitet werden.

(2) Die Benutzer haften für die von ihnen schuldhaft verursachten Schäden sowie für Verluste und Veränderungen der Daten des Rechenzentrums oder Dritter. Sie stellen die Universität von Ansprüchen Dritter frei, sofern etwaige Schäden auf Verstöße gegen diese Benutzungsordnung, insbesondere gegen Lizenzbestimmungen Dritter zurückzuführen sind.

§ 4 Notfallgruppe

- (1) Zur Wiederherstellung des IT-Betriebes im Falle massiver Beeinträchtigungen, Störungen oder Gefährdungen wird eine Notfallgruppe von der Hochschulleitung eingerichtet, die koordinierende und operative Aufgaben im Bereich der Daten-Sicherheit und Qualitätssicherung im IT-Bereich wahrnimmt.
- (2) Die Notfallgruppe informiert Betreiber störungsverursachender Systeme und fordert diese auf, die Störung abzustellen. Wird der Aufforderung zur Störungsbeseitigung nicht umgehend Folge geleistet, ist die Notfallgruppe berechtigt, das störungsverursachende System bis zur Beseitigung der Störung vom Netz zu trennen.
- (3) Handelt es sich bei der Störung um sicherheitsrelevante Vorgänge, ist der IT-Sicherheitsstab umgehend zu informieren (vgl. Ordnung zur IT-Sicherheit).
- (4) Bei bekannt gewordenen erheblichen Verstößen gegen diese Ordnung kann dem Benutzer die Benutzungserlaubnis durch die Notfallgruppe entzogen werden.
- (5) Strafrechtlich relevante Verstöße sind von der Notfallgruppe nach rechtlicher Prüfung bei den zuständigen Behörden anzuzeigen.
- (6) Bei Widerspruch der Verursacher gegen Maßnahmen der Notfallgruppe entscheidet die Leitung der Hochschule über das weitere Vorgehen.

§ 5 Rechenzentrum

- (1) Das Rechenzentrum hat die betriebsfachliche Aufsicht über alle IT-Anlagen der Hochschule und koordiniert die Beschaffung und Ergänzung, soweit nicht Vorgaben der Fachministerien dem entgegen stehen.
- (2) Es stellt IT-Geräte, Software, Zugang zu Informationsdiensten und Dienstleistungen im Zusammenhang mit der IT-Versorgung zur Verfügung und bietet Kurse und Informationsveranstaltungen an.
- (3) Zur Erfüllung der Aufgaben in Lehre und Forschung können Kontingente gemäß eines Verteilungsschlüssels insbesondere für Speicherbereiche, Drucker, Übertragungswege auf Datenleitungen und Rechner-Arbeitsplätze durch die Hochschulleitung vergeben werden.
- (4) Das Rechenzentrum sorgt im allgemein üblichen Rahmen für die Verlust-Sicherung der Daten, die die Benutzer auf elektronischen Datenträgern des Rechenzentrums speichern.
- (5) Es überwacht die Betriebsparameter des Datennetzes kontinuierlich und überprüft stichprobenartig gezielt einzelne Systeme auf Konformität.
- (6) Im Fall von erkannten Rechneinbrüchen (Hacker-Attacken) informiert das Rechenzentrum den IT-Sicherheitsstab (vgl. Ordnung zur IT-Sicherheit) und die Beteiligten und erteilt weitere Hinweise.
- (7) Das Rechenzentrum bewahrt Medien, die mit Daten von Benutzern beschrieben sind, innerhalb einer vom Rechenzentrum festgelegten Frist auf. Die innerhalb dieser Frist nicht abgeholten Medien können vom Rechenzentrum vernichtet werden.
- (8) Das Rechenzentrum haftet für die von seinen 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 ist - soweit rechtlich zulässig - ausgeschlossen. Ansonsten finden die Bestimmungen des §7 der Informationsdienste-Ordnung Anwendung.

(9) Benutzer des Rechenzentrums sind diejenigen Personen, die die Leistungen des Rechenzentrums unmittelbar in Anspruch nehmen. Die Registrierung, mit der auch die Benutzer-Identifikation vergeben wird, wird nach vorheriger schriftlicher Beantragung vom Rechenzentrum erstellt. Sie ist auf die beantragte und bewilligte Nutzungsart beschränkt. Die Registrierung erlischt mit Beendigung des Benutzungsverhältnisses nach Ablauf der erteilten Frist, auf Grund einer entsprechenden Mitteilung des Nutzungsberechtigten oder des DV-Beauftragten oder durch Ausschluß gemäß § 4(4).

§ 6 Sonstige IT-Betreiber

(1) Die Verantwortlichkeit der IT-Betreiber nach §1(1) schließt den fachgerechten Anschluß ihrer Geräte an der Datendose ein.

(2) Die Verantwortung für Installation und Wartung der Leitungen und die Übergabepunkte des Datennetzes liegt bei der Abteilung Betriebstechnik der TU BS. Veränderungen an den Übergabepunkten (Datendosen) und sonstigen Netzkomponenten sind nur in Abstimmung mit dem jeweils Verantwortlichen zulässig.

(3) Die Leiter der jeweiligen TU-Einrichtung, die als IT-Betreiber auftritt, sind für den Betrieb verantwortlich und verpflichten die Nutzer ihrer IT-Geräte auf Einhaltung dieser Nutzungs-Ordnung.

§ 7 Auskunftersuchen

Auskünfte über personenbezogene Daten dürfen nur nach vorheriger Absprache mit dem Rechtsdezernat an Dritte weiter gegeben werden und sind nach Art und Umfang dem Datenschutzbeauftragten der TU BS mitzuteilen.

§ 8 Gebühren

(1) Basisdienste (zum Beispiel E-Mails, Info-Dienste und News) werden im Rahmen des zentralen Angebots allen Nutzern kostenfrei zur Verfügung gestellt, soweit die Gebührenordnung der TU BS nichts anderes vorsieht.

(2) Für Leistungen, die den im Rechenzentrum üblichen Rahmen überschreiten, können zusätzliche Kosten entsprechend der Gebühren- und Entgelte-Ordnung der TU BS erhoben werden.

(3) Die Nutzung von speziellen IT-Diensten sonstiger TU-Einrichtungen ist von den Nutzern mit den Betreibern der jeweiligen TU-Einrichtung direkt zu klären und unterliegt deren Nutzungsordnung. Die Gültigkeit dieser Richtlinien wird damit nicht aufgehoben.

§ 9 Inkrafttreten

Diese Nutzungsordnung tritt am Tage nach ihrer hochschulöffentlichen Bekanntmachung in Kraft, gleichzeitig treten die "Benutzungsordnung für das Rechenzentrum der Technischen Universität Braunschweig" vom Dezember 1994 sowie die "Netzordnung der TU Braunschweig" vom Dezember 1994 außer Kraft.

Ordnung zur IT-Sicherheit der Technischen Universität Braunschweig

Inhaltsverzeichnis

Präambel

- § 1 Gegenstand dieser Ordnung
- § 2 Geltungsbereich
- § 3 Beteiligte am IT-Sicherheitsprozess
- § 4 IT-Sicherheitsbeauftragte
- § 5 Sicherheitsstab
- § 6 Aufgaben der Beteiligten
- § 7 Der IT-Sicherheitsprozess
- § 8 Gefahrenintervention
- § 9 Finanzierung
- § 10 Inkrafttreten

Präambel

Ein leistungsfähiger Universitätsbetrieb erfordert in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf Informationstechnik (IT) und hierbei insbesondere auf vernetzte IT-Systeme stützen. Dafür ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich. Insbesondere die Anbindung der IT-Systeme an das weltweite Datennetz erfordert wirksamen Schutz gegen Fremdeingriffe. Die Thematik der "Sicherheit in der Informationstechnik" ("IT-Sicherheit") bekommt damit für die Technische Universität Braunschweig eine grundsätzliche Bedeutung, die die Entwicklung und Umsetzung eines einheitlichen Sicherheitskonzepts für die Universität erforderlich macht.

§ 1

Gegenstand dieser Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines universitätsweiten IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen unter Berücksichtigung der einschlägigen gesetzlichen Bestimmungen, der Informationsdienste-Ordnung sowie der Nutzungsordnung zur Informationstechnologie.

§ 2

Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Einrichtungen der Technischen Universität (Fachbereiche, wissenschaftliche Einrichtungen, Einrichtungen mit zentraler Funktion, sonstige Einrichtungen) und in technischer Hinsicht auf die gesamte IT-Infrastruktur inkl. der daran betriebenen IT-Systeme der Universität.

§ 3

Beteiligte am IT-Sicherheitsprozess

Im Sinn dieser Ordnung sind am IT-Sicherheitsprozess der Technischen Universität verantwortlich beteiligt:

- Der zentrale IT-Sicherheitsbeauftragte
- Dezentrale IT-Sicherheitsbeauftragte
- Der Sicherheitsstab
- Das Rechenzentrum der TU
- Alle Einrichtungen der Technischen Universität

§ 4

IT-Sicherheitsbeauftragte

(1) Die Hochschulleitung bestellt einen zentralen IT-Sicherheitsbeauftragten und einen Stellvertreter.

(2) Jeder Fachbereich, jede zentrale Einrichtung sowie die Verwaltung hat einen IT-Sicherheitsbeauftragten und Stellvertreter zu benennen (dezentraler Sicherheitsbeauftragter). Mehrere Fachbereiche können einen gemeinsamen Sicherheitsbeauftragten benennen.

Durch diese Benennungen müssen alle IT-Systeme im Geltungsbereich sowie die vor Ort für deren Betrieb verantwortlichen Personen einem IT-Sicherheitsbeauftragten auf Fachbereichs- oder Einrichtungsebene zugeordnet sein.

(3) Bei der Bestellung/Benennung der IT-Sicherheitsbeauftragten sollen der strategische Aspekt und die dafür erforderliche personelle Kontinuität berücksichtigt werden. Die IT-Sicherheitsbeauftragten sollen deshalb möglichst zum hauptamtlichen Personal der Universität gehören. Sie sollen in IT-Sicherheitsfragen besonders geschult werden.

§ 5

Sicherheitsstab

(1) Ständige Mitglieder des Sicherheitsstabs sind:

- der zentrale IT-Sicherheitsbeauftragte (Vorsitz)
- ein Vertreter des Rechenzentrums
- ein Vertreter des Rechtsdezernats
- der Datenschutzbeauftragte der Technischen Universität

(2) Der Gesamtpersonalrat kann ein beratendes Mitglied benennen.

(3) Weitere IT-sachverständige Mitglieder werden von der Hochschulleitung benannt. Die Anzahl der Mitglieder des Sicherheitsstabes soll 10 nicht überschreiten.

§ 6

Aufgaben der Beteiligten

- (1) Der zentrale IT-Sicherheitsbeauftragte ist für Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.
- (2) Das Rechenzentrum ist verantwortlich für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit und gibt in diesem Rahmen Empfehlungen zu technischen Standards zur IT-Sicherheit für die TU vor.
- (3) Der Sicherheitsstab unterstützt den zentralen IT-Sicherheitsbeauftragten, indem er Pläne, Leitlinien und Vorgaben für sämtliche übergreifenden Belange der IT-Sicherheit erarbeitet, Maßnahmen koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.
- (4) Die dezentralen IT-Sicherheitsbeauftragten sind für alle Sicherheitsbelange der IT-Systeme und -Anwendungen in den Bereichen, die ihnen jeweils zugeordnet sind, verantwortlich. Dabei haben sie die Vorgaben des Sicherheitsstabes zu beachten.
- (5) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitungen der Einrichtungen nicht von ihrer Verantwortung zur Umsetzung der IT-Sicherheit in ihrem Bereich.
- (6) Die Einrichtungen der Technischen Universität sind verpflichtet, bei allen Planungen, Verfahren und Entscheidungen mit Bezug zur IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten zu beteiligen. Der dezentrale IT-Sicherheitsbeauftragte hat gegebenenfalls bei Entscheidungen den zentralen IT-Sicherheitsbeauftragten einzubeziehen.

§ 7

Der IT-Sicherheitsprozess

- (1) Der zentrale IT-Sicherheitsbeauftragte initiiert, steuert und kontrolliert unter Beteiligung des Sicherheitsstabs den IT-Sicherheitsprozess, der nach festzulegenden Prioritäten Maßnahmen insbesondere zu schneller Krisenintervention umfassen muss. Zwecks Gewährleistung einer kontinuierlichen Steuerung des IT-Sicherheitsprozesses soll der Sicherheitsstab regelmäßig tagen.
- (2) Die dezentralen IT-Sicherheitsbeauftragten sind verpflichtet, sicherheitsrelevante Informationen jederzeit entgegenzunehmen und das jeweils Erforderliche zu veranlassen. Soweit notwendig, informieren sich dezentrale IT-Sicherheitsbeauftragte zu Ursachen und Maßnahmen durch Kontaktaufnahme zum zentralen IT-Sicherheitsbeauftragten und/oder zum Rechenzentrum.
- (3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Bereich verantwortlich. Sie informieren sich regelmäßig über die Sicherheit der IT-Systeme in ihrem Bereich und veranlassen unverzüglich die notwendigen Maßnahmen zur Gewährleistung der erforderlichen Sicherheit. Sie informieren die Leitung ihrer Einrichtung regelmäßig über den Sicherheitsstandard und auftretende Probleme und schlagen Lösungsmöglichkeiten vor.
- (4) Der zentrale IT-Sicherheitsbeauftragte berichtet der Hochschulleitung und dem Senat aus gegebenem Anlass darüber und macht Vorschläge für die Weiterentwicklung des IT-Sicherheitsprozesses unter Berücksichtigung der Ausgewogenheit, Durchgängigkeit und Angemessenheit der Maßnahmen. Dabei ist die Höhe der voraussichtlichen Kosten der einzelnen Maßnahmen anzugeben.
- (5) Die dezentralen IT-Sicherheitsbeauftragten sind bezüglich ihrer Mitteilungspflichten gegenüber dem zentralen IT-Sicherheitsbeauftragten, der Hochschulleitung und dem Senat unabhängig von Weisungen ihrer Vorgesetzten. Die IT-Sicherheitsbeauftragten geben ihre Berichte auch den Leitungen der betreffenden Einrichtungen zur Kenntnis.

§ 8

Gefahrenintervention

(1) Bei Gefahr in Verzug veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Bereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden - insbesondere für andere Einrichtungen oder für die IT-Infrastruktur der Technischen Universität in Teilen oder insgesamt - nicht anders abzuwenden ist. Unverzüglich sind die Leitung der Einrichtung und das Rechenzentrum zu benachrichtigen, das seinerseits den zentrale/n IT-Sicherheitsbeauftragten benachrichtigt.

(2) Soweit das Rechenzentrum Gefahr in Verzug feststellt, kann es Netzanschlüsse (ggfs. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Technischen Universität in Teilen oder insgesamt nicht anders abzuwenden ist. Die Benachrichtigung des zuständigen dezentralen sowie des zentralen IT-Sicherheitsbeauftragten erfolgt unverzüglich ggfs. nachträglich.

(3) Vor Wiederinbetriebnahme vorübergehend stillgelegter Systeme bzw. gesperrter Netzanschlüsse ist in der Regel die Durchführung hinreichender Sicherheitsmaßnahmen erforderlich. Im Zweifelsfall entscheidet der zentrale IT-Sicherheitsbeauftragte über das weitere Vorgehen.

§ 9

Finanzierung

(1) Die Mittel für spezielle, mit dem zentralen IT-Sicherheitsbeauftragten und dem Rechenzentrum abgestimmte Sicherheitsmaßnahmen in den Einrichtungen der Technischen Universität sowie insbesondere Mittel zur Schulung für die dezentralen IT-Sicherheitsbeauftragten sind von den betreffenden Einrichtungen aufzubringen, die Mittel für diese Zwecke in ihrer Finanzplanung angemessen zu berücksichtigen haben.

(2) Soweit Sicherheitsmaßnahmen aus zentralen Mitteln finanziert werden müssen, ordnet der zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Sicherheitsstab diese nach Dringlichkeit in einer Liste. Mit einer Begründung der Prioritäten schlägt er der Hochschulleitung die Finanzierung vor.

§ 10

Inkrafttreten

Diese Ordnung tritt am Tag nach ihrer hochschulöffentlichen Bekanntmachung in Kraft.

F. Informationsdienste-Ordnung der Technischen Universität Braunschweig

(gültig ab 15.07.2000)

Regelungsinhalte:

- § 1 Definitionen
- § 2 Grundsätze des Betriebs von Informations-Servern
- § 3 Inhalt und Gestaltung von Informationsangeboten
- § 4 Verantwortlichkeiten der Informationsanbietenden
- § 5 Verstöße gegen Vorschriften
- § 6 Haftung der oder des Informationsanbietenden
- § 7 Haftung der Universität
- § 8 In-Kraft-Treten

§ 1 Definitionen

- (1) Diese Ordnung regelt die Bereitstellung von Informationsdiensten und öffentlichen Informationsangeboten durch Organisationseinheiten, Mitglieder und Angehörige der Technischen Universität Braunschweig.
- (2) Informationsdienste sind technische Einrichtungen, mit denen Informationsangebote in elektronischer Form angeboten und abgerufen werden können. Dokumente sind dabei Informationsangebote in jeglicher Form, bestehend aus Texten, Bildern, Grafiken, Programmen, akustischen Darstellungen, Videosequenzen oder anderen multimedialen Gestaltungen.
- (3) Zu den Informationsdiensten gehören z. B.: www (World Wide Web) ftp (Download von Software und Dokumenten) E-Mail (elektronische Post) usenet-News (elektronische Diskussionsforen) irc (Internet Relay Chat) Distributions-Channels (Vertrieb von Informationen in Push-Technik) Directory Services (erweiterte Adressenverwaltung) Streaming-Server (Archive für Video-Dokumente)

§ 2 Grundsätze des Betriebs von Informations-Servern

- (1) Die Technische Universität Braunschweig betreibt zentrale Informationsdienste-Server. Diese stehen allen Organisationseinheiten, Mitgliedern und Angehörigen der Universität - kooperierenden Institutionen, soweit dies vertraglich geregelt ist - zur Verfügung.

- (2) Die Hochschulleitung koordiniert das Informationsangebot der zentralen Informationsdienste-Server. Das Rechenzentrum übernimmt als Betreiber deren technische Realisierung und die Betreuung der Systeme.
- (3) Der Betrieb weiterer, dezentraler Informations-Server bedarf der Zustimmung der Universität. Die Betreiber der dezentralen Informations-Server übernehmen die technische Realisierung, die Betreuung ihrer zugelassenen Systeme sowie die Verantwortung für den Inhalt, soweit Server-Betreibern diese nach den einschlägigen gesetzlichen Bestimmungen obliegt.
- (4) Datenbereiche auf Informations-Servern dürfen in der Regel nicht Dritten (Personen bzw. Organisationen außerhalb der Universität) zur Nutzung überlassen werden. In Ausnahmefällen kann mit Genehmigung der Hochschulleitung nicht gewinnorientierten öffentlichen Einrichtungen im Rahmen der Amtshilfe eine Mitnutzung der Informations-Server gewährt werden.
- (5) Daten über Zugriffe auf Dokumente dürfen nur entsprechend den datenschutzrechtlichen Bestimmungen gespeichert werden, um eine anonyme Zugriffsstatistik zu erstellen. Besteht der Verdacht, dass bei der Nutzung von Informationsdiensten der Hochschule Straftaten begangen wurden oder werden, so ist eine über Satz 1 hinausgehende Aufzeichnung und Speicherung von Daten (und Dateien) zur Beweissicherung zulässig.

§ 3 Inhalt und Gestaltung von Informationsangeboten

- (1) Der Inhalt von Informationsangeboten muss den Anforderungen der DFN-Benutzungsordnung und der DV-Nutzungsordnung der Universität genügen. Die gesetzlichen Bestimmungen, insbesondere das Informations- und Kommunikationsdienstegesetz, der Schutz von personenbezogenen Daten sowie die Urheber-, Lizenz- und Persönlichkeitsrechte sind zu beachten. (Propaganda für verfassungswidrige Organisationen, die Verbreitung von rassistischem Gedankengut, Pornographie sowie Beleidigungen, Verleumdungen, das Ausspähen von Daten, Datenveränderungen, Computersabotage und Computerbetrug stellen in der Regel Straftatbestände dar.)
- (2) Die Universität gestaltet ihr Informationsangebot so breit und attraktiv wie möglich. Sie und ihre Organisationseinheiten sind berechtigt, folgende Daten ihrer Bediensteten zu veröffentlichen (siehe auch Runderlass d. StK, d. MI u.d. übr. Min. v. 28.05.2001 -44.22-30800/5- veröffentlicht in: Nds. Ministerialblatt, 15. Jahrgang, Nummer 25, Seite 571-572): Forschungsergebnisse unter Nennung der Autorinnen und Autoren sowie der Forschungseinrichtung (§ 27 NHG). Ankündigungen und Berichte von Tagungen mit Namen der Referentinnen und Referenten und Kontaktadressen. Namen, Kontaktadressen (einschließlich E-Mail-Adresse, Telefon- und Fax-Nummer) und Forschungsgebiet der unmittelbar in Forschung und Lehre tätigen Bediensteten. Sprechzeiten der lehrenden Bediensteten sowie Bezeichnung, Ort und Zeit der Lehrveranstaltungen. Private Kontaktadressen nur, wenn die vorgenannten Bediensteten sonst dienstlich (z. B. über das Sekretariat) nicht erreichbar sind. Name, Vorname, Telefonnummer, Fax-Nummer, E-Mail-Adresse, Einrichtung / Abteilung von Hochschulmitgliedern. Der Zugriff auf diese Daten ist jedoch beschränkt auf die Domäne tu-bs.de.

- (3) Weitere Angaben dürfen nur mit schriftlich erklärter Einwilligung der Betroffenen veröffentlicht werden. Die betroffenen Bediensteten sind von der Veröffentlichung rechtzeitig in Kenntnis zu setzen. Wenn die Betroffenen wegen überwiegender schutzwürdiger Belange der Veröffentlichung widersprechen, hat sie zu unterbleiben.
- (4) Sofern Daten von Angehörigen (z. B. Lehrbeauftragten, Privatdozentinnen und Privatdozenten, außerplanmäßigen Professorinnen und Professoren) veröffentlicht werden sollen, ist dies besonders zu vereinbaren.
- (5) Name, Kontakt- und E-Mail-Adresse von Studierenden und von Bediensteten, die nicht unter Abs. 2 Ziffer 3 fallen, werden nur nach deren vorheriger Zustimmung veröffentlicht.
- (6) Die Gestaltung der Informationsangebote sollte sich an Gestaltungsrichtlinien orientieren, die die Universitätsleitung zur Verfügung stellt. Als Logo und Signet der Universität ist nur die offizielle Version zu verwenden. Für bestimmte Bereiche (allgemeine TU-Seiten, Fachbereiche) werden Gestaltungselemente angeboten.
- (7) Jedes Informationsangebot soll Angaben über dessen Urheber enthalten (verantwortliche Organisationseinheit, Bearbeiter bzw. Einzelperson, Datum der Erstellung bzw. Modifikation).
- (8) Für die Veröffentlichung von Forschungsarbeiten gelten die gleichen Sorgfaltspflichten, wie für die Veröffentlichung in gedruckter Form.
- (9) Informationsdienste dürfen in der Regel nicht kommerziell genutzt werden. Den Organisationseinheiten der Universität ist die Nennung des Namens von Förderern und Sponsoren samt Firmenlogos gestattet. Entsprechende Vereinbarungen mit Förderern sind der Hochschulleitung bekannt zu geben.

§ 4 Verantwortlichkeiten der Informationsanbietenden

- (1) Die für das jeweilige Informationsangebot Zuständigen - im Folgenden Informationsanbietende genannt - sind unter Beachtung von § 2 Absatz 3 für den Inhalt der von ihnen bereitgestellten Informationsangebote, ihre Pflege und die Herstellung von Verweisen verantwortlich.
- (2) Sofern ergänzend zu den Informationsangeboten der Universität bzw. ihrer Organisationseinheiten, Mitarbeiter und Angehörige der Universität persönliche Dokumente ins Netz stellen, ist der Übergang von den offiziellen Informationsangeboten zu den persönlichen Dokumenten deutlich zu kennzeichnen. Für persönliche Dokumente ist deren Anbieter selbst verantwortlich.
- (3) Die Verantwortlichkeit für den Inhalt eines Informationsangebotes umfasst in eingeschränkter Weise auch Links auf andere Dokumente. Letztere sind gelegentlich zu überprüfen, ob sie ihrerseits den gesetzlichen Anforderungen genügen. Ist das erkennbar nicht der Fall, muss ein betreffender Link entfernt werden. In jedem Fall empfiehlt es sich, bei allen Hyperlinks auf externe Informationsangebote darauf hinzuweisen, dass es sich bei den verlinkten Informationen um fremde Angebote handelt, die außerhalb des Einflussbereichs der Universität liegen.

§ 5 Verstöße gegen Vorschriften

- (1) Informationsangebote, deren Inhalte offensichtlich gegen diese Ordnung, gegen vorrangige Ordnungen und Regeln oder sonstige Rechtsvorschriften verstoßen, sind vom Betreiber des jeweiligen Informations-Servers unverzüglich zu löschen. Die für die beanstandeten Dokumente zuständigen Verantwortlichen sind entsprechend zu informieren.
- (2) Erscheint ein Verstoß nach Absatz 1 Satz 1 zwar nicht offensichtlich, aber möglich, informiert der Betreiber die verantwortliche Person hierüber mit der Bitte, die Rechtmäßigkeit des fraglichen Dokuments zu begründen bzw. das Dokument zu löschen. In Zweifelsfällen ist die Hochschulleitung zu informieren.
- (3) Informationsangebote, aus denen nicht unmittelbar zu entnehmen ist, wer für sie verantwortlich ist, können vom jeweiligen Betreiber gelöscht werden.
- (4) Informationsanbietende können vorübergehend oder dauerhaft in der Benutzung der DV-Ressourcen beschränkt oder hiervon ausgeschlossen werden, wenn sie schuldhaft gegen diese Ordnung, insbesondere gegen die in §§ 2 bis 4 aufgeführten Pflichten verstoßen oder sie die DV-Ressourcen der Universität für strafbare Handlungen missbrauchen oder der Universität durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen.

Diese Maßnahmen werden erst nach vorheriger erfolgloser Abmahnung durch den Server-Betreiber getroffen.

- (5) Über vorübergehende Nutzungseinschränkungen entscheidet der jeweilige Betreiber nach Anhörung der oder des Informationsanbietenden. Die Informationsanbietenden sind über den Zeitpunkt der Einschränkung zu informieren, ihnen ist Gelegenheit zu geben, die vorhandenen Daten zu sichern. Eine vorübergehende Nutzungseinschränkung ist aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint.
- (6) Die Entscheidung über eine dauerhafte Nutzungseinschränkung oder einen vollständigen Ausschluss einer oder eines Informationsanbietenden trifft die Hochschulleitung auf Antrag des Betreibers. Diese Maßnahme kommt nur bei schwerwiegenden oder wiederholten Verstößen nach Absatz 4 in Betracht und setzt voraus, dass auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Absatz 5 gilt entsprechend. Mögliche Ansprüche des jeweiligen Betreibers aus dem Nutzungsverhältnis bleiben hiervon unberührt.
- (7) Der Server-Betreiber ist nicht verpflichtet, eine Routinedurchsicht der Dokumente auf seinem Server durchzuführen. Bei positiver Kenntnis eines Verstoßes gegen diese Ordnung hat der Serverbetreiber gemäß Absatz 1 bis Absatz 6 tätig zu werden.

§ 6 Haftung der oder des Informationsanbietenden

- (1) Die oder der Informationsanbietende (siehe § 4 Abs. 2) haftet für alle Schäden, die der Universität durch schuldhafte Missachtung dieser Ordnung entstehen. Diese Haftung umfasst auch Schäden, die der Universität durch Nutzung ihrer Ressourcen durch unberechtigte Dritte entstanden sind, wenn die oder der Informationsanbietende diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe ihrer oder seiner

Benutzerkennung an Dritte. In diesem Falle kann die Universität von der oder dem Informationsanbietenden nach Maßgabe der Entgeltordnung ein Nutzungsentgelt für die Drittnutzung verlangen.

- (2) Die oder der Informationsanbietende hat die Universität von allen Ansprüchen freizustellen, wenn Dritte die Universität wegen ihrer oder seiner rechtswidrigen Informationsangebote auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die Universität wird gegen die oder den Informationsanbietenden ggf. rechtliche Schritte einleiten, sofern Dritte gegen sie gerichtlich vorgehen.
- (3) Haftungsregelung unberührt. Im Übrigen gelten ergänzend die Bestimmungen der allgemeinen DV-Nutzungsordnung.

§ 7 Haftung der Universität

- (1) Die Universität übernimmt keine Garantie dafür, dass ihre Informations-Server fehlerfrei und jederzeit ohne Unterbrechung laufen. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter sind nicht ausschließbar.
- (2) Die Universität übernimmt keine Verantwortung für die zur Verfügung gestellten Server-Programme. Die Universität haftet auch nicht für den Inhalt, insbesondere insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang vermittelt.
- (3) Die Universität haftet nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiter, es sei denn, dass eine schuldhafte Verletzung wesentlicher Vertragspflichten oder Kardinalpflichten vorliegt. In diesem Fall ist die Haftung der Universität auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden beschränkt. Die Haftungssumme wird - außer bei vorsätzlich herbeigeführten Schäden - auf 1.000 DM begrenzt.
- (4) Mögliche Amtshaftungsansprüche gegen die Universität bleiben von den vorstehenden Regelungen unberührt.

§ 8 In-Kraft-Treten

Diese Ordnung tritt am Tage nach ihrer hochschulöffentlichen Bekanntmachung in Kraft.

G. Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste

– vom Vorstand beschlossen am 16.05.1994 und geändert am 09.08.2001 –

Stand: 30.05.2009

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-Adress- vergabe),
- 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 vorauszusetzen. 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

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, von SFTP abgelöst.

SFTP Kopieren von großen Dateien zwischen Rechnern mittels SSH 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

Linux Eine frei verfügbare, weit verbreitete Version von ↗Unix

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 **R**equest for **C**omment 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 **S**erver **M**essage **B**lock, 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.

Sprechstunde Jeden Montag von 19.00 Uhr bis 19.30 Uhr wird eine Sprechstunde im Clubhaus angeboten. Hier können Probleme beim Netzbetrieb besprochen oder der Netzantrag abgeholt und eingereicht werden.

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, mittlerweile durch ssh abgelöst

ssh nternet-Protokoll für einen Dialog auf einem anderen (UNIX-)Rechner, Einloggen auf irgendeinem öffentlichen UNIX-Host, anders als bei telnet wird hierbei die Verbindung verschlüsselt. Basis für SFTP.

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 **N**etwork **N**ews **T**ransfer **P**rotocol unter TCP/IP, viele tausend Diskussionsgruppen (newsgroups) weltweit, entstanden 1979, lokale Administrationen für spezifische Diskussionsgruppen mit regionaler Bedeutung

WWW **W**orld **W**ide **W**eb („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