connect

Mitteilungsblatt des Rechenzentrums der Universität Augsburg — 1/1997

Erschienen im Februar 1997

Inhalt

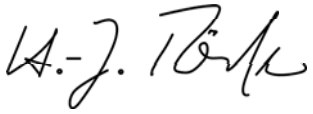
Liebe connect-Leser,

wie Sie der Rubrik „Ansprechpartner im Rechenzentrum“ entnehmen können, steht Herr Jürgen Pitschel dem Rechenzentrum nur noch bis zum 31.01.1997 als Technisch-Organisatorischer Direktor voll zur Verfügung. Er wechselt zum 01.02.1997 in die Zentrale Universitätsverwaltung, um dort die Datenverarbeitungsabteilung zu übernehmen, bzw. aufzubauen. Die Universität Augsburg vollzieht damit — wie andere Universitäten es schon lange getan haben — eine Trennung zwischen der wissenschaftlichen und der administrativen Datenverarbeitung, welche in vieler Hinsicht für beide Seiten vorteilhaft sein kann. Herr Pitschel gehört zu den ersten Mitarbeitern der Universität, der er seit 1972 angehört, und hat das Rechenzentrum als dessen Leiter aufgebaut. Er hat das Angebot des Kanzlers, in die Universitätsverwaltung zu wechseln, gerne angenommen, zumal es immer schwerer wird, in der wissenschaftlichen Datenverarbeitung den wachsenden Bedürfnissen der Kunden mit der beschränkten Personalausstattung des Rechenzentrums gerecht zu werden. Ich akzeptiere seinen Wunsch mit Bedauern, wünsche ihm für seine neue Tätigkeit viel Erfolg und danke ihm für die im Rechenzentrum geleistete Arbeit. Als Mitarbeiter, die zur Zeit schon für die Verwaltung arbeiten, werden demnächst Frau Katzer und die Herren Glöckner und Stöhr mit ihm ziehen. Auch ihnen sei an dieser Stelle für ihre bisherige Arbeit gedankt.

Bis zur Wiederbesetzung der Stelle des Technisch-Organisatorischen Direktors wird uns Herr Pitschel beratend zur Verfügung stehen. Ich bitte unsere Klientel um Verständnis, wenn es dennoch hie und da zu Engpässen kommen sollte.

Auch diese Ausgabe von **connect** widmet dem Internet großen Raum, wobei nach der schönen Einführung von G. Wilhelms über die Bedienung des Netscape Navigators K. Faßnacht mit einem sehr lesenswerten Aufsatz über Sicherheit im Internet zu Worte kommt. Professor Heintschel von Heinegg war so freundlich, aus der Sicht des Juristen einen Beitrag zur Computerkriminalität beizusteuern. Man kann ihm entnehmen, daß es kein Kavaliersdelikt ist, in anderer Leute Rechner einzubrechen, unberechtigt Daten oder Programme zu erschnüffeln oder gar zu verändern. Leider — das lehrt die Erfahrung — ist das Unrechtsbewußtsein auf diesem Gebiet noch sehr unterentwickelt. Der Abgesang auf die teflon von Frau B. Schmidt zeigt, daß es manchmal schwer fällt, ein lieb gewordenes, (fast) eigenes Kind dem Fortschritt zu opfern. Der nachfolgende Artikel von M. Lev informiert über die neuen Wählzugänge zum Hochschulnetz. Einen interessanten Blick über den Zaun der Physik bietet R. Utermann mit seinem Artikel „Netwerkrechner — Rechnernetzwerk“. Was wären wir ohne die aktive Mitwirkung der DV-Nutzer, insbesondere der DV-Betreuer und -Berater!

Ich hoffe, daß auch die übrigen **connect**-Beiträge von Ihnen als hilfreich empfunden werden. Allen, die ihr Interesse an der Arbeit des Rechenzentrums durch Mitwirkung, Anregungen oder Kritik gezeigt haben, sei herzlich gedankt.



1. Mit dem Netscape Navigator ins Internet

Dr. Gerhard Wilhelms, Kontaktstudium

Der Netscape Navigator ist ein WWW-Browser, also ein Zugriffsprogramm für den Internetdienst Word Wide Web, kurz WWW oder W3. Durch die integrierenden Eigenschaften des Dienstes WWW haben Sie über einen Browser praktisch Zugriff auf alle Internet-Dienste. Sie brauchen also nur einmal eine Konfigurierung vorzunehmen und die Bedienung eines Programms zu lernen. Damit liegt Ihnen das gesamte Internet zu Füßen, inklusive Suchdiensten, Dateiübertragung, News, Gopher, u. v. m.

Unter den derzeit verfügbaren Browsern kristallisieren sich momentan zwei als marktbeherrschend heraus, nämlich der Navigator von Netscape und der Internet Explorer von Microsoft. Letzterer wird nur für die Betriebssysteme Windows und MacOS angeboten und ist erst seit kurzem auf dem Markt. Aus diesem Grund habe ich die Besprechung von Netscape Navigator in der Version 3.01 für diesen Artikel vorgezogen. Allerdings sind keine gravierenden Unterschiede in Leistungsfähigkeit und Bedienung festzustellen, so daß auch die Fans des Internet Explorer einige gute Tips aus diesem Artikel herausziehen können.

Bezugsquelle und Lizenz

Die offizielle Bezugsquelle für den Netscape Navigator ist der WWW-Server *home.netscape.com*. Dieser Server ist jedoch in den USA angesiedelt, was schlechte Übertragungsraten bedeutet. Da das Programmpaket minimal ca. 2.5 MByte umfaßt, mit Zusatzkomponenten sogar leicht 5 MByte, ist die Übertragung von einem näher liegenden FTP-Server vorzuziehen. Einer dieser Server ist z. B. *ftp.Uni-Augsburg.DE*.

Die Universität Augsburg hat als Bildungseinrichtung das Angebot von Netscape angenommen, Netscape-Software auf einem lokalen Rechner zu speichern und zur weiteren Verteilung zur Verfügung zu stellen. Die Vorteile für beide Seiten liegen auf der Hand: Die Universität Augsburg hat einen der populärsten Browser immer in der jeweils aktuellsten Fassung zum schnellen Zugriff vorliegen, und Netscape kann für europäische Kunden einen schnellen Netzzugriff bieten.

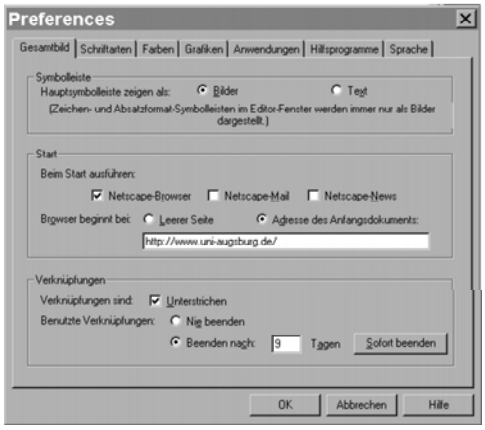
Der Navigator liegt im Verzeichnis */pub/packages/netscape/navigator* und darf von Angehörigen von Bildungseinrichtungen uneingeschränkt und kostenfrei benutzt werden.

Die Software liegt für die gängigen Rechner- und Betriebssystemtypen jeweils als gepacktes Archiv vor, das Sie entpacken und entarchivieren müssen. Unter Windows haben Sie es am einfachsten, denn hier liegt das Archiv in einer selbstentpackenden Form als *.EXE*-Datei vor, die Sie einfach wie ein Programm starten. Für den Macintosh sollten Sie sich z. B. von *MacFTP.RZ.Uni-Augsburg.DE* den Stuffit-Expander besorgen, für UNIX benötigen Sie *tar* und *gzip*. Die jeweiligen Installationsanweisungen stehen in den *README*-Dateien und sind leicht nachzuvollziehen.

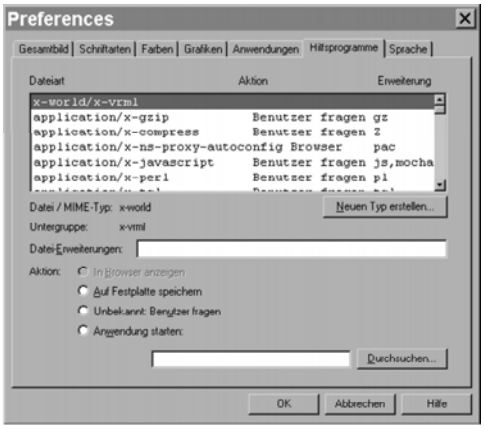
Konfigurierung

Nachdem der Navigator installiert ist, sind zum Zugriff auf das Internet noch einige Einstellungen notwendig. Ich gehe für die folgenden Abschnitte davon aus, daß Sie Ihren Rechner entweder direkt am Universitätsnetz angeschlossen haben, oder über den Rechner *rzibm01.RZ.Uni-Augsburg.DE* per Modem eine Netzverbindung herstellen. In beiden Fällen ist ordnungsgemäß installierte und konfigurierte TCP/IP-Software notwendig. Für die Modem-Variante lesen Sie bitte den Artikel „Wählzugang zum Hochschulnetz“ von M. Lev. In der Universität hilft Ihnen sicher gerne Ihr EDV-Berater.

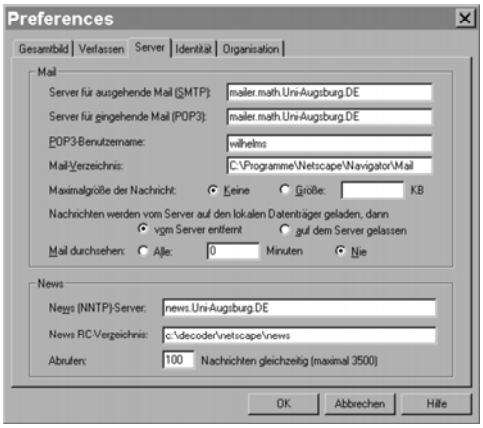
Starten Sie jetzt den Navigator. Gegebenenfalls versucht das Programm, sofort eine Netzwerkverbindung aufzubauen, was auch ohne die persönlichen Einstellungen gelingen sollte. Sie können aber auch den Verbindungsversuch (erkennbar am animierten Netscape-Logo am rechten oberen Fensterrand) durch Anklicken des Icons mit dem roten Punkt abbrechen, weil üblicherweise eine Verbindung zum stark überlaufenen Netscape-Rechner hergestellt wird, die sehr lange Übertragungszeiten erfordert. Jetzt können Sie die Einstellungen unter dem Menüpunkt OPTIONEN vornehmen. Wählen Sie zunächst die allgemeinen Einstellungen. Daraufhin wird dieses Formular eingeblendet.



Über die Register am oberen Rand können Sie Untergruppen der allgemeinen Einstellungen auswählen. Momentan ist nur wichtig, unter GESAMTBILD die Startseite im Internet anzugeben, die beim Start des Navigators automatisch geladen und angezeigt werden soll. Für die Universität Augsburg könnte dies z. B. *http://www.Uni-Augsburg.DE/* sein. Später können sich die beiden Register ANWENDUNGEN und HILFSPROGRAMME als interessant erweisen. Hier können Sie bestimmte externe Programme eintragen, die bei anderen Protokollen als *http* angewendet werden (z. B. *telnet*) bzw. bei bestimmten Dateiarten zum Einsatz kommen (z. B. GhostScript bei PostScript-Dateien oder Winzip bei *.ZIP*-Archiven). Normalerweise werden unbekannte Dateiformate entweder im Browserfenster angezeigt oder per Dateiauswahlbox zur Speicherung auf der lokalen Festplatte vorgeschlagen. Geeignete Einträge unter Hilfsprogramme befähigen den Navigator, externe Programme zum sofortigen Bearbeiten bestimmter Dateien aufzurufen. Die Abbildung zeigt das Formular zur Zuordnung von Dateitypen und externen Hilfsprogrammen.



Wesentlich wichtiger für den Einsatz des Navigators mit dem Internet sind die Mail- und News-Einstellungen. Auch diese Optionen sind über Register in Untergruppen eingeteilt. Beginnen wir mit den Einstellungen der SERVER-Gruppe, die Sie in der Abbildung sehen.



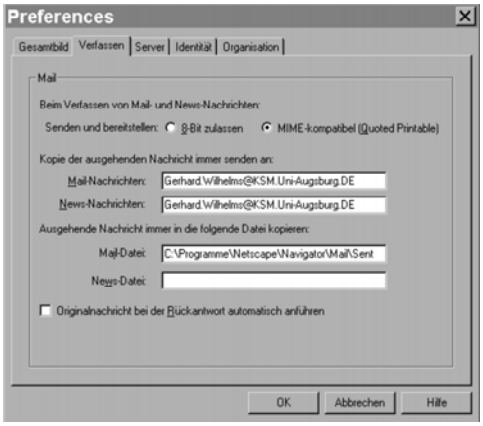
Die Einstellung für den News-Server im unteren Formularteil ist für alle Angehörigen der Universität gleich: *news.Uni-Augsburg.DE*. Das News-RC-Verzeichnis ist frei wählbar und dient zur Speicherung Ihrer ausgewählten Newsgruppen bzw. zum Markieren der gelesenen Artikel.

Für eMail müssen Sie die entsprechenden Angaben in den ersten drei Zeilen machen. Die beiden Einträge für ausgehende Mail (SMTP) und eingehende Mail (POP3) sind üblicherweise gleich und bezeichnen den Mail-Server Ihrer Dienststelle bzw. den Rechner *rzibm01.RZ.Uni-Augsburg.DE* für Studentinnen und Studenten. Der POP3-Benutzername ist Ihr Account auf dem Mail-Server. Achten sie beim Eingeben auf Klein- und Großschreibung!

Das Mail-Verzeichnis dient zum Speichern von eMails. Üblicherweise werden separate Unterverzeichnisse *Inbox*, *Outbox* und *Trash* für eingegangene, geschickte und gelöschte eMails angelegt.

Damit haben Sie die notwendigen Einstellungen zum Benutzen von eMail und News schon erledigt. Allerdings machen einige weitere Einstellungen die Arbeit wesentlich angenehmer, besonders für Ihre Partner im Internet.

Das Register VERFASSEN bietet die Möglichkeit, automatisch Kopien Ihrer eMail- und News-Artikel an bestimmte eMail-Adressen zu schicken. Sehr angenehm ist auch die Option, die Originalnachricht bei der Rückantwort automatisch anzuführen, denn dann können Sie gezielt zitieren und antworten. In der Abbildung ist diese Option noch nicht aktiviert.

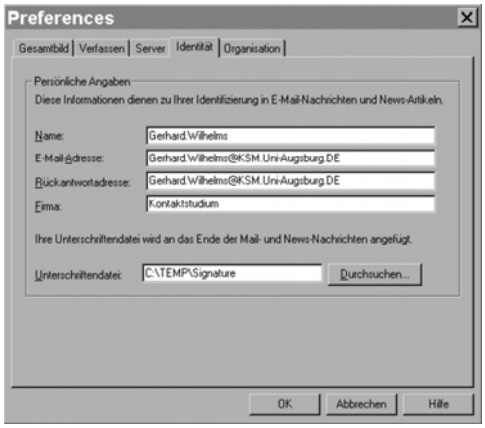


Zum Senden sollten Sie die Option MIME (Multipurpose Internet Mail Extensions) aktivieren, da mit dieser Einstellung Umlaute und scharfes S auch zwischen verschiedenartigen Rechnern meistens ordnungsgemäß übertragen werden. Allerdings benötigt Ihr Partner zum Empfang ebenfalls ein MIME-fähiges eMail-Programm.

Das Register IDENTITÄT bestimmt Ihr persönliches Auftreten, weil Sie hier die Absendereinträge vornehmen. Insbesondere ersetzen Sie hier Ihren Account durch Ihren richtigen Namen bzw. die echte eMail-Adresse mit Rechnerangabe durch die vom Systemverwalter vergebene und üblicherweise aussagekräftigere symbolische eMail-Adresse. Die Unterschriftendatei ist eine gewöhnliche Textdatei, die automatisch an jede eMail bzw. jeden News-Artikel angehängt wird. Sie dient somit als Briefkopf. Meine Unterschriftendatei sieht wie folgt aus:

```
Gerhard Wilhelms
-----------------------------------------------------------------
Universitaet Augsburg
Kontaktstudium - Programmleiter EDV und Neue Medien
Universitaetsstrasse 16                Tel : +49 +821/598-4025
D-86135 Augsburg                       Fax :          598-4213
eMail: Gerhard.Wilhelms@KSM.Uni-Augsburg.DE
WWW: http://www.KSM.Uni-Augsburg.DE/~wilhelms/
```

Das komplett ausgefüllte Register sehen Sie hier.



Unter dem Register ORGANISATION können Sie Ihr Kennwort für den eMail-Rechner automatisch speichern lassen. In diesem Fall kann allerdings jede Person, die sich Zugang zu Ihrem Rechner verschafft, Ihre eMail lesen.

Da wir gerade beim Thema Sicherheit sind: Unter den Netzwerkeinstellungen finden Sie unter dem Register SPRACHE die Möglichkeit, Java und Java-Script zu deaktivieren. Allerdings schränkt der Navigator von vorneherein die Zugriffsmöglichkeiten über Java-Applets schon so weit ein, daß kein Schaden für Ihre Daten zu befürchten ist. Z. B. dürfen Applets auf Ihrem Rechner keine Dateien lesen bzw. schreiben. Netzwerkverbindungen sind nur zu dem Rechner zulässig, vom dem das Applet geladen wurde. Damit können auch über böswillige Applets nur Informationen zum Betriebssystem Ihres Rechners abgefragt werden, jedoch keine Paßwörter und andere sicherheitsrelevante Informationen. Weitere Einstellungen zum Thema Sicherheit finden Sie unter dem eigenen Menüpunkt.

Grundlegende Bedienung und Tips

WWW ist ein hypertextbasiertes Informationssystem, standardmäßig mit formatiertem Text, Grafiken, interaktiven Grafiken, Formularen, ausführbaren Scripten und externen Programmen. Es ist erweiterbar durch Tabellen, Formeln und eingebettete Grafiken.

Bedingt durch die integrierenden Eigenschaften des Dienstes (kann alle anderen Dienste ebenfalls leisten) und die grafischen und interaktiven Möglichkeiten ist WWW der populärste Internetdienst geworden.

Unter Hypertext versteht man Textdokumente mit interaktiven Querverweisen. Die Auswahl eines sogenannten Hyperlinks bewirkt das Laden und Anzeigen des Dokuments, auf das der Link zeigt. Die Querverweise/Links sind entweder durch markierbare Grafiken oder durch farbig anders dargestellten, meistens unterstrichenen Text realisiert. Voreinstellung bei Netscape sind blaue Farbe und Unterstreichung. Das sich Bewegen zwischen Hypertextdokumenten nennt man browsen oder navigieren, daher die Namen der entsprechenden Client-Programme zum Zugriff auf das WWW.

Internet-Adressen

Die größte Anfangsschwierigkeit bei der Arbeit mit dem WWW ist die Eingabe der korrekten Adressen, die die Lage der Dokumente bzw. Adressen der Kommunikationspartner beschreiben.

Internet-Rechner besitzen eindeutige Adressen. Zunächst gibt es die sog. Hardwareadresse, die vom Hersteller der Netzwerkkarte vergeben wird. Bei Rechnern mit Modem gibt es diese Adresse nicht. Vom jeweiligen *NIC* (Network Information Center) wird dem Rechner eine eindeutige weitere Adresse zugeteilt, die aus vier Oktetten bestehende *IP*-Adresse, die einen Subnetz- und einen Rechneradreßteil enthält. Auf der Basis dieser Adressen werden Datenpakete auf dem Internet weitervermittelt. Jede Station auf dem Weg von Quell- zu Zielrechner liest diese Adresse und leitet das Paket entsprechend weiter. Zum leichteren Umgang für die beteiligten Menschen wurde der *DNS* geschaffen, die eine Zuordnung von symbolischen Namen zu den *IP*-Adressen vornimmt. Diese Domainnamen bestehen aus

einzelnen Subdomainnamen und Rechnernamen, die ebenfalls weltweit eindeutig sind. Ausgehend vom Rechnernamen wird ein Domainname dadurch gebildet, daß dem Pfad durch den *DNS*-Raum bis zur Wurzel gefolgt wird, wobei an den Knoten jeweils ein Punkt eingefügt wird.

Weitere Regeln sind:

- bis zu 127 Level
- Knotenbeschriftung bis zu 63 Zeichen

Beispiele für DNS-Namen haben Sie schon gesehen, z. B. *www.Uni-Augsburg.DE* oder *kora.KSM.Uni-Augsburg.DE*.

eMail-Adressen bestehen normalerweise nur aus einem Benutzernamen, gefolgt vom `@`-Zeichen (Gesprochen: at oder Klammeraffe), wiederum gefolgt von einem *DNS*-Rechner oder -domainnamen. Falls der Benutzername ein Accountname und der folgende Teil ein Rechnername ist, liegt eine eindeutige Adressierung vor. Wenn lediglich eine Domainadresse bzw. im vorderen Adreßteil ein symbolischer Name vergeben sind, muß der hinter eMail stehende *sendmail*-Dæmon eine Adreßkonvertierung vornehmen. Die Konfiguration dieser Konvertierung ist so flexibel und kompliziert, daß ein eigener Artikel geschrieben werden könnte. Ich verweise hierzu auf die hervorragende Literatur (Bryan Costales, *sendmail*).

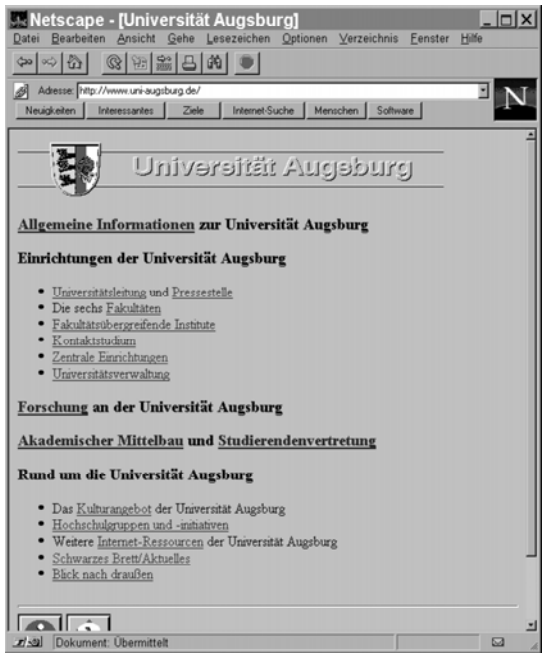
Für das WWW werden für die einzelnen Seiten sog. URLs (Uniform Resource Locator) benutzt, die im Prinzip die Adresse eines Objekts im Internet darstellen. Eine URL hat folgendes Aussehen:

```
<protocol>://<Rechnername><Dateibezeichner>[#Pos]
```

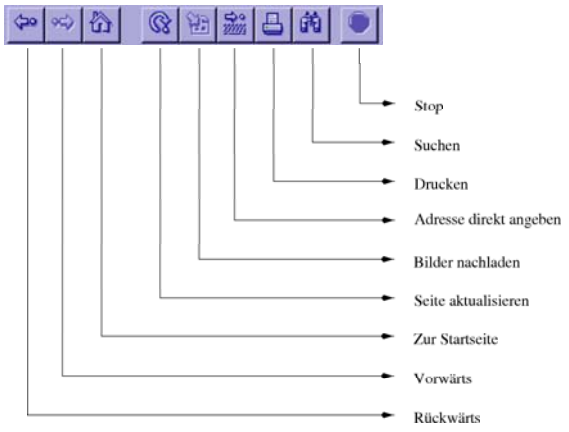
Das Protokoll gibt den zugrundeliegenden Dienst an. Möglich sind zur Zeit *file* (Datei auf dem lokalen Rechner), *http* (Hypertext, WWW), *news* (Newsartikel, -gruppe), *telnet* (Terminalverbindung), *gopher* (Gopher-Rechner) und *ftp* (*FTP*-Rechner, -datei). Der Rechnername kann ein Domainname oder eine IP-Adresse sein. Der Dateibezeichner ist ein gültiger Dateiname auf dem entfernten Rechner und ist systembedingt sensitiv auf Klein-/Großschreibung. Das oft verwendete Zeichen ~ bezeichnet ein *UNIX*-Benutzerverzeichnis. Der optionale Parameter *Pos* dient zur direkten Anzeige einer späteren Textstelle eines Hypertext-Dokuments.

Navigator

Nach dieser grauen Theorie wenden wir uns wieder dem Navigator zu. Im Prinzip wissen wir also, daß der Navigator mit einer korrekten URL irgendetwas sinnvolles anfängt, abhängig vom Protokoll. Geben Sie in der Zeile Adresse/Location die URL *http://www.Uni-Augsburg.DE/* ein, falls diese Seite noch nicht angezeigt wird. Sie erhalten daraufhin eine Anzeige der Startseite des Universitätsservers.



Auf dieser Seite finden Sie eine Reihe von Hyperlinks, die im Prinzip nichts anderes sind, als andere URLs, die beim Anklicken automatisch geladen und angezeigt werden. Noch unbekannte Querverweise werden dabei blau angezeigt, schon vorher besuchte in roter Farbe (im Beispiel der Punkt „Zentrale Einrichtungen“). Falls das ausgewählte Dokument nicht auf die Bildschirmseite paßt, werden Rollbalken zum Scrollen eingeblendet (im obigen Beispiel rechts). Zur Orientierung sehen Sie die URL der eingeblendeten Seite in der Zeile Adresse/Location. Bewegen Sie jetzt den Mauszeiger über die Seite. Sobald Sie einen Querverweis erreichen, wird in der Statuszeile am unteren Fensterrand die zugehörige URL eingeblendet. Klicken Sie jetzt mit der linken Maustaste einen Querverweis an. Die neue Seite wird geladen, erkennbar am animierten Netscape-Logo am oberen rechten Fensterrand bzw. am jetzt rot dargestellten, äußersten rechten Icon in der Iconleiste, die Sie unten erläutert bekommen.



Sie haben jetzt eine weitere Seite geladen und damit den ersten Navigationsschritt unternommen. Im Prinzip können Sie sich über Querverweise durch das gesamte Internet „hangeln“. Manchmal möchte man allerdings wieder zurück zur Ausgangsseite, aber ein Querverweis fehlt. Was tun? Hier kommt die Iconleiste ins Spiel. Die beiden Icons links außen dienen zum Rückwärts- bzw. Vorwärtsblättern in den besuchten Seiten. Allerdings sind die Icons nur aktiv, wenn wirklich geblättert werden kann. Beim ersten Aufruf des Browsers gibt es keine Seite zum Blättern. Jetzt können Sie allerdings zur Startseite zurückblättern, danach zur gerade angezeigten Seite vorwärtsblättern. Haben Sie sich im Internet-Dschungel verlaufen, können Sie mit dem dritten Icon zur Startseite zurückkehren.

Das vierte Icon dient zur Aktualisierung der angezeigten Seite. Haben Sie z. B. mit dem rechten Stop-Icon eine Übertragung unterbrochen, können Sie über dieses Icon eine Übertragung von vorne starten.

Das fünfte Icon dient zum Nachladen der Bilder eines Dokuments, falls Sie diese Option deaktiviert haben. (Empfiehlt sich wegen der kürzeren Ladezeiten. Unter Menüpunkt Optionen finden Sie den Schalter!)

Das nächste Icon öffnet eine Eingabemaske für eine URL. Im Prinzip können Sie aber die Zeile Adresse/Location gleichwertig verwenden. Haben Sie in einer Zeitschrift oder auf sonstigem nichtelektronischen Weg eine interessante URL gefunden, können Sie diese direkt eingeben.

Das sechste Icon dient zum Drucken des gesamten Dokuments, allerdings ohne die Dokumente, die hinter Querverweisen stehen.

Das siebte Icon hilft Ihnen beim Suchen in der angezeigten Seite. Sie können einen Suchbegriff eingeben. Der Browser scrollt dann das Dokument zur Fundstelle und markiert den gefundenen Begriff.

Das letzte Icon kennen Sie schon; es dient zum Abbrechen laufender Übertragungen. Dauert Ihnen das Laden einer Seite zu lange, bzw. haben Sie schon einen interessanten Querverweis weiter oben auf der Seite entdeckt, können Sie die weitere Übertragung hier abbrechen. Bereits sichtbare Dokumententeile bleiben erhalten.

Weitere Tips

Dauert Ihnen die Übertragung eines Dokuments zu lange, können Sie über Menüpunkt DATEI—NEUER WEB-BROWSER ein weiteres Fenster einblenden und parallel arbeiten.

Falls Sie interessiert, wie die Dokumente des WWW programmiert werden, können Sie unter ANSICHT—DOKUMENTQUELLTEXT den zugehörigen *HTML*-Code der angezeigten Seite anzeigen lassen. Dies ist der beste Weg, um diese Sprache zu lernen.

Falls Sie eine interessante Seite auf Ihrem Rechner lokal speichern wollen, können Sie das mit Menüpunkt DATEI—SPEICHERN tun. Allerdings wird dabei nur der HTML-Text des Dokuments *ohne Bilder* gespeichert. Die Bilder können Sie aber mit der rechten Maustaste (Macintosh: Maustaste lange gedrückt halten) anklicken und eigens übertragen und speichern. Bei aktiviertem Festplatten-Cache können Sie über Menüpunkt ANSICHT—DOKUMENTINFORMATION herausfinden, wo in den Tiefen des Dateisystems die Bilder/Dokumente zwischengespeichert sind und diese lokalen Daten kopieren.

Nicht ganz so mühevoll gestaltet sich die Verwendung von Lesezeichen/Bookmarks, wenn Sie später ein Dokument nochmals lesen wollen. Mit Menüpunkt LESEZEICHEN—HINZUFÜGEN oder dem Hyperlink-Popup-Menü (rechte Maustaste auf Querverweis klicken, Macintosh Maustaste lange drücken) können Sie die URL der angezeigten Seite als Lesezeichen markieren und später über das Lesezeichen/Bookmark-Menü direkt anspringen. Unter Menüpunkt FENSTER—LESEZEICHEN können Sie Ihre Lesezeichen ordnen und strukturieren, ähnlich wie ein Dateisystem.

Haben Sie eine Seite mit mehreren interessanten Querverweisen entdeckt (z. B. die Ergebnisliste einer Suchmaschine), können Sie entweder nacheinander durch Anklicken des Rückwärts-Icon die Querverweise durcharbeiten, oder mit dem Hyperlink-Popup-Menü für jeden Querverweis ein neues Fenster öffnen, was wesentlich schneller zum Ziel führt.

Andere Netzwerkdienste

Der Navigator integriert die anderen Netzwerkdienste unter einer einheitlichen Benutzerschnittstelle. Die Anzeigen der Dienste Gopher und *FTP* werden dabei direkt im Browser-Fenster dargestellt, so daß fast kein Unterschied zu *WWW-Texten* feststellbar ist.

Bei *FTP* erhält man eine Anzeige des Platteninhalts, ähnlich wie vom Dateimanager oder Explorer. Anklicken von Verzeichnissen wechselt in das Verzeichnis (zurück mit Icon oder dem obersten Eintrag), Anklicken von Dateien bringt diese entweder zur Anzeige im Browserfenster bzw. ermöglicht den Download (rechte Maustaste).

Für die Dienste eMail und News bietet der Navigator eigene Fenster, die Sie durch Menüpunkt FENSTER—NETSCAPE-MAIL bzw. FENSTER—NETSCAPE-NEWS aufrufen. Zur Erklärung der Bedienung benötige ich allerdings einen eigenen Artikel, den Sie in der nächsten **connect** finden werden.

Der schnelle Anfang

Naturgemäß bereiten die ersten Schritte im Internet die größten Schwierigkeiten, weil durch das Fehlen zentraler Organisationsstrukturen keine Gesamtverzeichnisse für Informationen vorhanden sind, seien es eMail-Adressen oder Fachinformationen. Damit Ihnen die ersten Schritte etwas leichter fallen, habe ich meine Lesezeichen/Bookmarks öffentlich zugänglich gemacht. Unter dem ersten Eintrag *Information and Navigation* finden Sie eine Vielzahl von Querverweisen, die Ihnen beim Auffinden von Informationen behilflich sein können. Die Adresse: *http://www.KSM.Uni-Augsburg.DE/~wilhelms/bookmarks.html*

2. Sicherheit im Internet

Konrad Faßnacht, Institut für Mathematik

Das Internet hat in den letzten beiden Jahren durch seine revolutionäre Art der Informationsbeschaffung und Informationsbereitstellung eine nicht mehr wegzudenkende wirtschaftliche, gesellschaftliche und auch politische Bedeutung erlangt. Gleichzeitig werden die Nutzer des Internets mit Gefahren des Datendiebstahls und der Datenmanipulation konfrontiert, welche ebenfalls revolutionär zu nennen sind. Der Aufsatz gibt einen Überblick über die vom Internet ausgehenden Gefährdungen für die Rechnernetze und Computersysteme der Internetanwender. Er zeigt die Gegenstände von Internetangriffen auf und stellt die Methoden vor, mit denen Angreifer aus dem Internet versuchen, ihre Ziele zu erreichen. Um Abwehrmechanismen entwickeln zu können, wird geklärt, um welche Personenkreise es sich bei den Angreifern handelt und welche Schwachstellen sie für ihre Aktionen ausnützen. Schließlich wird kurz skizziert, wie der einzelne Anwender durch „harte" Paßwörter Angriffe erschweren kann und wie die Netz- und Systemverantwortlichen durch den Aufbau von Firewalls ihre Netze und Systeme sicherer machen können.

Einleitung

Das bereits in den 60er Jahren entwickelte Internet führte aufgrund der komplizierten und nur für Spezialisten verständlichen Bedienung lange Jahre ein Schattendasein neben der zur damaligen Zeit dominierenden Großrechnerkommunikation. Im Laufe der 80er und 90er Jahre wandelte sich das Bild jedoch grundlegend. Anstelle der Mainframes traten offen konzipierte Systeme wie Workstations und PCs, die Client/Server-Architektur setzte sich in weiten Bereichen durch, die Kommunikation verlagerte sich auf moderne Rechnernetze; die TCP/IP-Protokolle des Internets entwickelten sich zu den am häufigsten eingesetzten Kommunikationsprotokollen. Anfang der 90er Jahre schaffte das Internet den endgültigen Durchbruch, als mit dem World Wide Web (WWW) eine graphisch orientierte und somit leicht zu bedienende Internetanwendung entwickelt worden war. Geschickte Marketingstrategien vor allem von Netscape führten zu einer raschen Verbreitung der sogenannten WWW-Browser, die auch Laien einen problemlosen Zugriff auf alle Informationen des Internets ermöglichen. Gleichzeitig ist es sehr einfach, eigene Informationen im Internet bereitzustellen. Mit dem Internet steht somit eine revolutionäre Technik zur Beschaffung und Bereitstellung von Informationen zur Verfügung.

Andererseits muß bedacht werden, daß man mit dem Zugang zum Internet Teil eines weltweiten und Millionen von Computern und Anwendern umfassenden Netzwerks wird. Jedes lokale Rechnernetz, jeder Server und jeder PC, der permanent oder zeitweise an das Internet angeschlossen ist, setzt sich somit auch der Gefahr aus, daß er über das Internet in irgendeiner Art und Weise angegriffen wird. Das Internet ist in diesem Sinne auch eine revolutionäre Technologie, um Daten zu stehlen, zu verändern oder zu zerstören. Der Artikel gibt einen Überblick über die vom Internet ausgehenden Gefahren und zeigt verschiedene Möglichkeiten des Schutzes vor diesen Gefahren auf.

Sicherheitsstudien und ein Beispiel

Die Problematik der Sicherheit in Computersystemen und Rechnernetzen ist im Prinzip nicht neu, erfährt aber durch die rasch wachsende Verbreitung des Internets eine neue Dimension. Um die Bedeutung dieser Bedrohung beurteilen zu können, wurden in den letzten Jahren eine ganze Reihe von Sicherheitsstudien durchgeführt, die sich nicht ausschließlich

auf das Internet beschränken. Einige Ergebnisse werden im folgenden vorgestellt.

- In einer von Ernst & Young 1994 in den USA durchgeführten Studie wurden 1 271 Unternehmen befragt, ob sie in den letzten beiden Jahren finanzielle Verluste durch Probleme mit der Informationssicherheit hatten. Ca. 50% der betrachteten Unternehmen bejahten diese Frage. Dabei zeigte sich, daß 2/3 dieser Fälle auf das Fehlverhalten der eigenen Mitarbeiter zurückzuführen ist, wovon wiederum die Hälfte ohne Absicht geschah.
- Eine 1995 in Deutschland durchgeführte Studie der Gartner Group besagt, daß 87% der deutschen Unternehmen mit Internetanschluß bereits Opfer von Eindringlingen waren.
- Dem 1988 gegründeten Computer Emergency Response Team (CERT) wurden 1989 132 Sicherheitsvorfälle gemeldet. 1994 waren es bereits 2 241 Sicherheitsvorfälle, wovon insgesamt ca. 40 000 (!) Netzwerke betroffen waren.
- Das National Center for Computer Crime veröffentlichte eine Untersuchung, nach der die Dunkelziffer von Computerdelikten sehr hoch ist. Danach werden nur ca. 1% aller Computerdelikte entdeckt und hiervon wiederum nur ca. 14% angezeigt.
- Ein Großversuch der Abteilung „Information Services“ des US Verteidigungsministeriums bestätigt diese Dunkelziffer. So wurden in deren Auftrag Einbruchsversuche auf 8 932 eigene Server und Mainframes unternommen, von denen 7 860 Versuche erfolgreich waren. Von den erfolgreichen Einbrüchen wurden lediglich 390 entdeckt und nur 19 angezeigt.

Ein Beispiel soll zeigen, welche Auswirkungen Sicherheitslücken in Rechnernetzen haben können. So stellte das Rechenzentrum der Texas A&M University im Jahre 1992 fest, daß aus ihrem Rechnernetz heraus über das Internet Angriffe auf die Netze anderer Organisationen stattfanden. Eine Überprüfung der Systeme ergab, daß Hacker von außerhalb der Universität eingedrungen waren und bestimmte Rechner als Sprungbrett für weitere Angriffe nutzten. Die Mitarbeiter des Rechenzentrums nahmen die betroffenen Systeme vom Netz, installierten Betriebssystem und Applikationen neu, aktivierten weitere Sicherheitsmechanismen und nahmen die vermeintlich sicheren Systeme wieder in Betrieb. Nach einer Woche mußten erneut Angriffsversuche aus der Universität heraus festgestellt werden. Eine daraufhin eingeleitete, sehr detaillierte und weitreichende Analyse des gesamten Universitätsnetzes ergab, daß ein Team von Hackern das komplette Rechnernetz mit 12 000 angeschlossenen Systemen unter seine Kontrolle gebracht hatte. So wurden Password-Cracking-Programme, modifizierte Login-Software, Sniffer-Programme zur Aufzeichnung des Datenverkehrs und vieles mehr entdeckt. Es stellte sich heraus, daß die Angriffe auf Netze und Systeme in zwei Wellen erfolgten: Eine erste Welle von exzellenten Systemspezialisten überwand die Sicherheitsmechanismen und stellte die gewonnenen Informationen bezüglich Sicherheitslücken oder Paßwörter anderen Hackern zur Verfügung, indem sie einige Unix-Rechner als Bulletin-Boards mißbrauchten. Eine zweite Welle von Hackern mit nur wenigen Systemkenntnissen nutzte diese Angaben, um auf den Systemen nach verwertbaren Informationen zu suchen.

Gegenstand eines Internetangriffes

Der Aufbau einer leistungsfähigen Sicherheitsarchitektur zum Schutz vor Angriffen

aus dem Internet erfordert es, daß man sich zunächst Gedanken darüber macht, welche Objekte Ziel eines Angriffes werden könnten. Die Angriffsziele lassen sich in drei Klassen einteilen.

(1) Angriffe auf *Daten und Informationen* verfolgen die Absicht, deren Vertraulichkeit, Integrität oder Verfügbarkeit zu unterlaufen. Eine Verletzung der *Vertraulichkeit* liegt vor, wenn sich ein Angreifer unberechtigt Zugang zu Daten und Informationen beschafft. Wenn die Daten und Informationen außerdem verändert oder manipuliert werden oder wenn unbefugt Daten hinzugefügt werden, so handelt es sich um Angriffe auf die *Integrität*. Schließlich kann ein Angreifer den Zugang eines Anwenders auf seine Daten verhindern, indem er zum Beispiel die Daten löscht, den Zugang durch eigene Paßwörter blockiert oder den Systemzugang lahmlegt. Die *Verfügbarkeit* der Daten wird somit vorübergehend oder dauerhaft behindert.

Jeder Anwender sollte sich also folgende Fragen über die Sicherheit seiner Daten stellen:

- Sind meine Daten vertraulich in dem Sinne daß nicht jeder auf sie zugreifen können soll?
- Spielt es eine Rolle, wenn jemand meine Daten unberechtigt manipuliert?
- Sollen mir meine Daten zu jeder Zeit zur Verfügung stehen?

Falls mindestens eine Frage mit einem Ja beantwortet wird, so sollte sich der Anwender Gedanken über den Schutz seiner Daten machen. Werden hingegen alle Fragen mit Nein beantwortet, so sollte man sich Gedanken darüber machen, ob es diese Daten überhaupt Wert sind, daß man Speicherplatz dafür verschwendet.

(2) Angreifer auf die *Ressourcen* eines Rechner- oder Kommunikationssystems verfolgen die Absicht, Rechnerleistung, Speicherplatz, Kommunikationsdienste und vieles mehr unbefugt zu Nutzen. Das Unrechtsempfinden der Angreifer ist hier sehr niedrig. Viele Hacker argumentieren, daß „es doch überhaupt keine Rolle spielt, wenn ein unbenutztes oder wenig benutztes System vorübergehend für meine Zwecke verwendet wird“. Aber was ist, wenn ein Anwender sein System für eine ressourcenintensive Berechnung zu einer Zeit benötigt, zu welcher unberechtigter Weise der Prozeß eines Angreifers auf seiner Maschine läuft? Oder wie würde ein Autofahrer reagieren, wenn ein Fremder sich während dessen Arbeitszeit dessen Wagen leiht und dies hinterher damit entschuldigt, daß das Kraftfahrzeug ja doch nur ungenutzt auf dem Parkplatz herumgestanden habe und er es ja abends wieder zurückgebracht hätte?

(3) Angriffe auf das *Ansehen* von Personen oder Unternehmen haben einen Ansehensverlust zur Folge. Dabei unterscheidet man den Ansehensverlust, der bewußt durch Identitätsfälschungen z. B. bei eMail herbeigeführt wird, und den Ansehensverlust von Unternehmen aufgrund von Einbrüchen in deren Netze und Systeme. So mußten die Telekom (damals noch Deutsche Bundespost) und die Hamburger Sparkasse einen starken Verlust ihres Ansehens hinnehmen, als es 1984 Mitgliedern des Chaos Computer Clubs Hamburg gelang, die Bank durch Ausnutzen eines Fehlers im BTX-System der Telekom in wenigen Stunden um mehr als 100 000.– DM zu erleichtern.

Angriffsmethoden

Im letzten Abschnitt wurden die Angriffsobjekte beschrieben. Nun soll dargestellt werden, mit welchen Methoden es Angreifern gelingt, ihre Ziele zu erreichen. Es sei an dieser Stelle erwähnt, daß die Angriffspraktiken sehr vielfältig sind. Eine detaillierte Behandlung

würde ein eigenes Buch füllen. Daher sollen hier nur einige Methoden exemplarisch vorgestellt werden.

Eine sehr einfache Methode des Informationsdiebstahls ist das *Monitoring* der Netzwerkaktivitäten. Hierzu wird mit sogenannten Sniffer-Programmen der Datenverkehr eines Shared-Medium-Netzes teilweise oder vollständig aufgezeichnet. Sniffer-Programme können lokal auf einem PC oder einer Workstation eingesetzt werden, sie lassen sich aber auch unbemerkt auf einem entfernten Unix-System installieren. Während ein Netzwerkcontroller normalerweise im Non-Promiscous-Mode arbeitet und somit nur Datenpakete entgegennimmt, welche an den zugehörigen Rechner adressiert sind, versetzen Sniffer-Programme den Netzwerkcontroller in den Promiscous-Mode. In diesem Modus können alle Datenpakete auf dem Netz mitgelesen werden. Sniffer-Programme werden vorzugsweise eingesetzt, um Kennungen und Paßwörter aus dem Datenverkehr herauszufiltern. Da Internetdienste wie FTP, Telnet oder rlogin diese Authentifizierungsinformationen im Klartext übertragen, ist die Beschaffung dieser Informationen kein Problem. Sniffer-Angriffe werden somit häufig zur Vorbereitung eines Angriffs auf Rechnersysteme durchgeführt.

Umfangreichere Angriffe auf Daten und Informationen erreicht man durch das *Eindringen in Rechnernetze und Systeme*. Ein Angreifer beschafft sich die hierfür notwendigen Informationen durch

- einfaches Erraten von Paßwörtern;
- Entschlüsseln von gestohlenen Paßwortdateien (z. B. der Unix-Datei passwd);
- dem oben angesprochenen Monitoring von Netzwerkaktivitäten;
- durch Social-Engineering-Angriffe, bei denen durch geschickte telephonische Manipulation von Anwendern oder Rechenzentrumsmitarbeitern Authentifizierungsinformationen beschafft werden;
- durch viele andere Methoden.

Mit diesen Informationen kann der Angreifer nun direkt Angriffe auf Daten und Informationen vornehmen. Ist er zudem im Besitz von Administratorrechten (z. B. des Root-Paßworts bei Unix-Systemen), so kann er das komplette System kontrollieren und meist von diesem System aus relativ einfach weitere Angriffe unternehmen.

Auch die Methoden für die Blockade von Ressourcen sind vielfältig. So ist es ein leichtes für jeden Angreifer, *Login-Sperren* zu aktivieren. Login-Sperren werden benutzt, um einem Angreifer das Erraten von Paßwörtern praktisch unmöglich zu machen. Nach der in der Regel dritten Falscheingabe des Paßworts wird hier die Kennung gesperrt und kann nur vom Systemverwalter wieder freigegeben werden. Ein Angreifer kann dies ausnutzen, um den Zugang eines Anwenders zu seinen Daten zu erschweren.

Etwas subtiler ist die *Überflutung von Netzen und Systemen* mit unsinnigen Datenpaketen. Hierdurch kann die Leistungsfähigkeit eines Netzes stark eingeschränkt werden, Systeme können in undefinierte Zustände oder sogar zum Absturz gebracht werden.

Sehr gefährlich ist die *Umleitung von Diensten*. So kann es zum Beispiel durch eine Umleitung von FTP dazu kommen, daß ein Anwender auf die gewünschten Daten eines FTP-Servers nicht mehr zugreifen kann. Es kann aber auch geschehen, daß der Anwender Daten per FTP auf einem falschen Server ablegt. Wenn es sich dabei zudem noch um vertrauliche Daten handelt, so ist der Schaden oft sehr groß.

Verschiedene organisatorische Maßnahmen haben die *Verbreitung von Viren* in den letzten Jahren deutlich reduziert. Man denke dabei nur an das Verbot der Verwendung privater Disketten oder den Einsatz diskloser Rechner. Die Nutzung des Internets hat die Gefahr der Virenverseuchung wieder stark erhöht. Dem Anwender muß klar sein, daß jedes Programm, welches er sich aus dem Internet holt, von Viren befallen sein kann. Da hier Verbote kaum helfen, ist es sehr wichtig, alle Anwender hinsichtlich dieser Gefahr zu sensibilisieren. So sollte unbedingt jedes Programm aus dem Internet vor der Nutzung durch ein Virenprüfprogramm getestet werden. Eine besondere Gefahr stellen *Trojanische Pferde dar*. Hierbei handelt es sich um eine Virenform, die nicht die Aufgabe hat, sich zu vervielfältigen und andere Systeme zu befallen. Trojanische Pferde haben ganz spezifische Funktionen. So gibt es *Trojanische Pferde*, welche den Auftrag haben, Authentifizierungsinformationen zu sammeln, diese dann per eMail an den Angreifer zu senden und sich selbst wieder aus dem befallenen System zu entfernen. Der Angreifer hat dann alle Informationen, um in das ausspionierte System einzubrechen.

Schließlich ist eine häufige Angriffsmethode das *Vortäuschen einer falschen Identität*. Die Absichten, die sich dahinter verbergen, sind wiederum sehr vielfältig. So kann ein Angreifer den Zweck verfolgen, kompromitierende eMail unter dem Namen einer anderen Person zu verbreiten, um dessen Ansehen zu schädigen. Auch Angriffe auf Daten und Informationen sind möglich, indem der Angreifer seine Maschine als einen vertrauenswürdigen Rechner tarnt, welcher bestimmte Informationen von einem Server abrufen darf.

Angreifertypen

Die erfolgreiche Abwehr von Angriffen erfordert nicht nur Kenntnisse über die Angriffsobjekte und über die Angriffsmethoden, sondern auch über den Gegner selbst. Die folgende Klassifikation verschafft einen Überblick über die potentiellen Angreifer.

(1) *Funktionelle „Angreifer“*; hierbei handelt es sich nicht um Angreifer im strengen Wortsinn, sondern um Gefährdungen, die in ihren Folgen einem Angriff gleichkommen. Hierzu gehören:

- Dummheit und Unachtsamkeit;
- unzureichende Ausbildung;
- technische Pannen.

(2) *Personelle Angreifer herkömmlicher Art*; darunter versteht man Personenkreise, die bereits sehr frühzeitig die Schwachstellen des Internets für Angriffe ausgenutzt haben. Hierzu gehören:

- *aktive oder ehemalige Mitarbeiter* des eigenen Unternehmens, die entlassen worden sind, sich ungerecht behandelt fühlen, unzufrieden mit ihrer Situation oder aus anderen Gründen frustriert sind;
- *Studenten und Schüler*, die neugierig sind, häufig ein gutes Expertenwissen aufweisen, Zugang zu den erforderlichen Geräten besitzen und viel Zeit haben;
- *Joyrider*, die aus Langeweile versuchen, Netze und Systeme zu „knacken“;
- *Rekordjäger*, die in möglichst viele Netze und Systeme einbrechen wollen und jedes noch so kleine System „mitnehmen“;
- *Vandalen*, die auf Zerstörung aus sind und sich in den meisten Fällen ganz bestimmte Gegner wie z. B. die Telekommunikationsunternehmen ausgesucht haben, welche sie bewußt schädigen wollen;

- Hacker und Cracker aus der Computer-Untergrundszene, die über hochkarätiges Expertenwissen verfügen und Sicherheitslücken rigoros ausnützen.

(3) *Personelle Angreifer moderner Art*; dieser Personenkreis hat sich in den letzten Jahren gebildet, als kriminelle Elemente den Vorzug des Internets als Kommunikationsmittel zu schätzen lernten. Oftmals handelt es sich hierbei um exzellente Hacker, die für Spionagezwecke oder zu kriminellen Aktionen angeworben sind. Von Angreifern dieser Gruppe geht eine nicht zu unterschätzende Gefahr für Staat, Wirtschaft und Gesellschaft aus. Zu dieser Klasse gehören:

- *Industriespione* aus dem Umfeld der Wettbewerber;
- *politische Spione* im Auftrag von Geheimdiensten;
- *Kriminelle* aus dem Bereich der organisierten Kriminalität.

Organisatorische und technische Schwachstellen

Es war bereits davon die Rede, daß Angreifer gezielt nach Schwachstellen in Netzen und System suchen und diese dann für ihre Zwecke ausnutzen. Aufgabe einer Sicherheitsstrategie ist es, diese Schwachstellen zu erkennen und zu beseitigen bzw. dort, wo eine Beseitigung nicht möglich ist, Vorkehrung gegen die Verwertung der Schwachstellen durch Angreifer zu treffen.

In vielen Unternehmen findet man derzeit noch immer die Situation vor, daß überhaupt keine Sicherheitsmaßnahmen ergriffen werden. Dies geschieht teils aus Unkenntnis, teils aus Ignoranz. Unternehmen ohne Sicherheitsvorkehrungen, aber mit Internetanschluß sind in der Regel bereits Opfer von Eindringlingen — sie wissen es nur noch nicht!

Entscheidet sich ein Unternehmen zum Einsatz von Sicherheitsvorkehrungen, so ist es von größter Bedeutung, daß die Systeme sehr sorgfältig konfiguriert und administriert werden. Hierzu sind gut ausgebildete und engagierte Systembetreuer notwendig. Mangelhaft konfigurierte und administrierte Systeme, aber auch schlecht aus- bzw. weitergebildete Systemadministratoren stellen ein sehr hohes Sicherheitsrisiko dar.

Beim Aufbau einer Sicherheitsarchitektur ist zu bedenken, daß alle Betriebsysteme, aber auch die TCP/IP-Kommunikationsprotokolle und die Internet-Dienstprogramme wie WWW, FTP oder Telnet prinzipielle Sicherheitslücken aufweisen. Diese lassen sich auch durch eine perfekte Konfiguration nicht beseitigen. Vielmehr sind andere Maßnahmen wie der Aufbau eines Firewalls erforderlich, welcher dann aber wieder sehr kompetent gepflegt werden muß.

Jeder Systemadministrator, aber auch jeder Anwender, sollte sich stets bewußt sein, daß kein Programm fehlerfrei ist. So sind auch die bei der Internetnutzung eingesetzten Dienstprogramme mehr oder weniger fehlerhaft. Angreifer nutzen diese Fehler aus, um Sicherheitslücken zu identifizieren und diese als Angriffspunkte auszunutzen.

In vielen Unternehmen fehlt ein engagierter Sicherheitsbeauftragter. Entweder wird diese Position überhaupt nicht ausgewiesen bzw. besetzt, oder es wird eine Alibifunktion für einen Mitarbeiter geschaffen, der dann das Sicherheitsthema als Nebentätigkeit sporadisch behandelt. Entsprechend fehlen in derartigen Unternehmen Sicherheitsrichtlinien.

Systemsicherheit durch Paßwörter

Es gibt eine Vielzahl von Möglichkeiten, um Systeme sicherer zu machen. Hierfür benötigt man in der Regel aber gute Systemkenntnisse.

Was kann aber der einzelne Anwender mit sehr geringen Systemkenntnissen für seine Sicherheit tun? Das einfachste Mittel ist der Schutz von Zugangsberechtigungen durch Paßwörter. Leider wird dieser Schutzmechanismus oft nur sehr unzureichend oder auch gar nicht genutzt, so daß es für Angreifer ein leichtes ist, diese Sicherheitsschranke zu überwinden. Die folgenden Ausführungen sollen den Anwender motivieren, sich Gedanken über die Verwendung von Paßworten zu machen.

Paßwörter sind meist nicht so sicher, wie es der Anwender glaubt. Es ist für einen Angreifer meist ein leichtes, in den Besitz von Paßwörtern zu kommen. Hierfür gibt es verschiedene Angriffsstrategien.

Ein sehr probates Mittel ist das Erraten von Login-/Paßwortkombinationen. Viele Anwender benützen den eigenen Vornamen als Paßwort oder den Vornamen von Familienmitgliedern, den letzten Urlaubsort, die eigene Telefonnummer, die Login-Kennung oder triviale Worte, die einem bei der Paßwortwahl spontan in den Sinn kommen. Es ist kein Witz, daß in Bayern ein sehr beliebtes Paßwort das Wort „Bier“ ist!

Systematischer lassen sich Paßworte mit Hilfe geeigneter Programme erraten. Diese Programme greifen auf elektronische Wörterbücher zurück und probieren die enthaltenen Worte der Reihe nach durch. Auf diese Art und Weise lassen sich sogar verschlüsselte Paßwörter aus der Unixdatei passwd erraten.

Da Internetdienste wie FTP, Telnet oder Rlogin Login-/Paßwortinformationen im Klartext übertragen, ist es durch den geeigneten Einsatz von Sniffer-Programmen oder Trojanischen Pferden kein Problem, in kurzer Zeit eine Vielzahl an Authentifizierungsinformationen zu sammeln und mit diesen einen Angriff auf die entsprechenden Computersysteme zu starten.

Schließlich verspricht auch das sogenannte „Social Hacking“ großen Erfolg beim Angriff auf Paßwörter. Unter Social Hacking versteht man das Ausnutzen gesellschaftlicher Spielregeln, um an gewünschte vertrauliche Informationen zu gelangen. Ein Beispiel soll dies verdeutlichen. Ein Angreifer entnimmt der Web-Page des Unternehmens XYZ, daß der Abteilungsleiter des Vertriebs Huber heißt. Er ruft im Rechenzentrum der Firma XYZ an und gibt sich als eben jener Huber aus. Lautstark schimpft er, daß er sich nicht in seinem Rechner einloggen könne und immer mit der Meldung „Authentication Failure“ abgewiesen werde. Unter Androhung von Sanktionen bei Nichtbefolgung fordert er den Mitarbeiter des Rechenzentrums auf, sofort das Paßwort seiner Kennung „Huber“ zu löschen. Er würde dann gleich ein neues Paßwort vergeben. Wenn der Mitarbeiter dies ohne Rückruf oder ähnliche Absicherung macht, so hat er das Spiel verloren. In wenigen Minuten werden dem Angreifer sämtliche Vertriebsdaten und vielleicht noch viel mehr Informationen offen stehen.

Es gibt verschiedene Möglichkeiten, um sich vor Paßwortangriffen zu schützen. Die einfachste und preiswerteste Art, die man immer anwenden sollte, ist die Wahl von „harten“ Paßwörtern und der regelmäßige Paßwortwechsel. Harte Paßworte sind selbst mit umfangreichen Wortbibliotheken nicht zu erraten, sollten aber trotzdem leicht zu merken sein. Folgendes Paßwort ist zum Beispiel nicht zu erraten: IldM;iws4md. Dieses Paßwort ist leicht zu merken, wenn man den folgenden Satz im Gedächtnis hat: „Ich liebe das Mittelmeer; ich war schon 4 mal dort“. Das Paßwort besteht aus den Anfangsbuchstaben der einzelnen Worte inklusive den Sonderzeichen und Ziffern.

Gegen Sniffer-Programme und Trojanische Pferde bieten jedoch auch die härtesten Paßwörter keinen Schutz. Dennoch gibt es mehrere Schutzmaßnahmen, die je nach Si-

cherheitsbedürfnis einzeln oder in Kombination angewendet werden sollten, so z. B.

- die Einrichtung eines Firewalls durch den Netzverantwortlichen zur Kontolle des Zugangs auf das zu schützende Netz;
- die Verschlüsselung der Daten, speziell dann, wenn sie über unsichere Netze wie das Internet übertragen werden sollen;
- die Verwendung von Einmalpaßwörtern oder die Verwendung personenbezogener Identifikationsmerkmale (Fingerabdruck, Stimme);
- nicht zuletzt das Bewußtsein der Anwender bezüglich der vom Internet ausgehenden Gefahren.

Netzsicherheit durch Firewallsysteme

Es ist speziell in größeren Netzen unmöglich, alle Systeme einzeln gegen potentielle Gefahren aus dem Internet abzusichern. Der Verwaltungsaufwand und die Fehleranfälligkeit einer derartigen Sicherheitsstrategie wären viel zu groß. Wesentlich effizienter ist es, den Zugang zum privaten Netz, also die Schnittstelle zwischen internem LAN und Internet, durch den Aufbau eines Firewalls abzusichern. Unter einem Firewall versteht man Netzwerk-Komponenten (Hardware und Software), welche den Zugriff zwischen einem privaten, internen Netz und einem öffentlichen Netz wie dem Internet regeln bzw. beschränken.

Die Aufgabe von Firewallsystemen ist es somit,

- gesicherte und ungesicherte Netze zu verbinden;
- das gesicherte Netz zu schützen und den Zugriff auf das ungesicherte Netz zu regeln;
- den einzigen Zugang vom gesicherten zum ungesicherten Netz zur Verfügung zu stellen.

Ein Firewall dient somit dazu, die Sicherheitsregeln eines Unternehmens oder einer Organisation an einem bestimmten Zugangspunkt zum internen Netz zu realisieren. An diesem Zugangspunkt konzentrieren sich alle Sicherheitsmechanismen zur Regelung des Zugriffs auf ein internes Netz. Der Firewall legt fest,

- auf welche internen Dienste vom Internet aus zugegriffen werden darf;
- wer auf diese internen Dienste zugreifen darf;
- auf welche externen Dienste interne Anwender zugreifen dürfen.

Wichtig ist, daß der Firewall auch tatsächlich der einzige Zugang zum internen Netz ist. Dann kann auch der gesamte Verkehr zwischen dem gesicherten Netz und dem Internet durch den Firewall überwacht, kontrolliert und zum Teil aufgezeichnet werden. Hierdurch lassen sich Angriffsversuche oder erfolgreiche Angriffe dokumentieren.

Ein Firewall bietet natürlich keinen Schutz vor bösartigen Insidern. Er ist auch nicht in der Lage, Viren, Trojanische Pferde, eMail-Angriffe oder ähnliche Angriffe abzuwehren. Und er bietet keinen Schutz vor dem Fehlerverhalten von Mitarbeitern.

Der Aufbau eines Firewalls ist in Abhängigkeit von den Sicherheitsbedürfnissen des Unternehmens oder der Organisation eine sehr komplexe Tätigkeit. Die Architektur eines Firewalls reicht dabei von einem einfachen Screening Router zwischen geschütztem und ungeschütztem Netz bis hin zu komplizierten, mehrstufig aufgebauten Sicherheitszonen. Allerdings sollte keine Organisation, die an das Internet angeschlossen ist, auf die Installation

eines Firewalls basierend auf der organisationsspezifischen Sicherheitsarchitektur verzichten. Ein Angriff mit großen Schäden für die Organisation ist sonst nur eine Frage der Zeit.

Ausblick

Das Thema Sicherheit in Rechnernetzen ist in den letzten beiden Jahren verstärkt in das Bewußtsein der Unternehmensleitungen gedrungen. Entsprechend wird zur Zeit vielerorts eine Sicherheitsarchitektur zum Schutz von Rechnernetzen und Computersystemen aufgebaut. Dies ist um so wichtiger, da zu erwarten ist, daß in den nächsten Jahren mit der weiteren Verbreitung des Internets und dem Entstehen neuer Internetanwendungen auch neue und gefährliche Bedrohungen entstehen werden. Eine wichtige Rolle bei der Abwehr von Angriffen auf Daten und Informationen werden hierbei Verschlüsselungstechnologien spielen.

An den amerikanischen Universitäten wurden in der letzten Zeit verstärkt Sicherheitsarchitekturen installiert, da eine Vielzahl von erfolgreichen Einbrüchen mit teilweise großen Schäden die Problematik drastisch bewußt gemacht hat. So sind viele US-Universitäten inzwischen durch mehr oder weniger gute Firewallsysteme geschützt. Die meisten deutschen Universitäten schieben das Thema derzeit noch vor sich her. Aber auch hier kann man absehen, wann Einbrüche in großem Stil mit empfindlichen Datenverlusten eine aktivere Sicherheitspolitk erforderlich machen werden.

Literaturverzeichnis

[1] Chapman, D.B., Zwicky, E. (1996). *Einrichten von Internet Firewalls* O'Reilly / Thomson Publ.

[2] Cheswick, W. (1996). *Firewalls und Sicherheit im Internet* Addison-Wesley.

[3] Garfinkel, S., Spafford, G. (1996). *Practical UNIX Security.* O'Reilly.

[4] Kyas, O. (1996). *Sicherheit im Internet* Datacom, Bergheim.

[5] Ruland, C. *Informationssicherheit in Datennetzen* Datacom, Bergheim.

3. Computerkriminalität

Professor Dr. Heintschel von Heinegg, Professor für Öffentliches Recht

Bis zum Jahre 1986 waren die Möglichkeiten, der Computerkriminalität mit den Mitteln des Strafrechts zu begegnen, recht beschränkt. Die bestehenden Straftatbestände des Strafgesetzbuches (StGB) wie auch anderer Gesetze waren auf diese Handlungen verständlicherweise nicht zugeschnitten. Insbesondere die neuen Erscheinungsformen der Wirtschaftskriminalität, die durch den zunehmenden Einsatz von Datenverarbeitungsanlagen in Wirtschaft und Verwaltung auftraten, konnten entweder nur mit Mühe unter die alten Gesetzesbestimmungen subsumiert oder aber gar nicht geahndet werden. Durch das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität vom 15. Mai 1986 und weitere gesetzgeberische Maßnahmen wurde dieser wegen des durch die Computerkriminalität verursachten erheblichen Schadens gemeinhin als unbefriedigend empfundene Zustand weitgehend beseitigt.

Es sei aber bereits an dieser Stelle hervorgehoben, daß die Gesetzesänderungen nicht zu einer Strafbarkeit der unbefugten Nutzung von Datenverarbeitungsanlagen und des unerlaubten Zugangs zu EDV-Systemen geführt haben. Insoweit überwog die Furcht des Gesetzgebers vor einer „Überkriminalisierung". Dies bedeutet indes nicht, daß es hinsicht-

lich der unbefugten Nutzung und des unbefugten Zugangs keine rechtliche Handhabe gäbe. Insoweit kommen — abgesehen von der Computer- und Datenspionage, auf die noch einzugehen sein wird — selbstverständlich zivilrechtliche Mittel wie Schadenersatz und Kündigung in Betracht. Überdies können nach Maßgabe der Benutzungsordnungen etwa universitärer Einrichtungen weitere Rechtsfolgen an den unberechtigten Zugang z. B. zu Datennetzen geknüpft werden. So ist es üblich, daß der ohne Genehmigung bzw. gültiges Paßwort oder mit fremdem Paßwort erfolgte Zugang zu einem Datennetz den (zeitweisen) Ausschluß von der Benutzung zur Folge hat. Gleiches gilt für den Fall, daß der Nutzer in sonstiger Weise das Datennetz mißbraucht, indem er beispielsweise auf Kosten der Universität kommerzielle Anbieter anwählt, rechts- bzw. linksradikale politische Erklärungen oder Pornographie über das Netz verbreitet. In diesen Fällen kann auch ein nicht unmittelbar mit der Computerkriminalität zusammenhängender Straftatbestand verwirklicht werden.

Freilich umfaßt der Begriff der Computerkriminalität nicht — wie es die entsprechende Definition der OECD aus dem Jahre 1986 vorsah — „any illegal, unethical, or unauthorized behaviour relating to the automatic processing and the transmission of data“. Eine derart weitreichende Begriffsbestimmung ist für die Zwecke des Strafrechts ungeeignet. Vielmehr rechnet man in Deutschland zur Computerkriminalität Taten, die bei ihrer Ausführung die Kenntnis oder den Einsatz von Computer- oder Kommunikations- und Informationstechnologie voraussetzen und die das Verfügungsrecht an immateriellen Gütern verletzen oder die Funktionsfähigkeit dieser Technologien beeinträchtigen. Strafbar sind demgemäß Computerbetrug, Fälschung beweiserheblicher Daten, Datenveränderung und Computersabotage, Computer- und Datenspionage, sog. Programm- und Chip-Piraterie sowie sonstige Datenschutzdelikte.

Computerbetrug

Nach § 263a StGB macht sich wegen sog. Computerbetrugs strafbar (Geldstrafe, Freiheitsstrafe bis zu fünf, in besonders schweren Fällen bis zu zehn Jahren), wer in Bereicherungsabsicht vorsätzlich das Ergebnis eines Datenverarbeitungsvorgangs so beeinflußt, daß das Vermögen eines anderen beschädigt wird. Es geht mithin um Manipulationen der technischen Vorgänge, bei denen durch Aufnahme von Daten und ihre Verknüpfung nach Programmen bestimmte Arbeitsergebnisse erzielt werden. Erfaßt werden zum einen sog. Inputmanipulationen, d. h. die unmittelbare oder mittelbare Eingabe falscher oder unvollständiger Daten sowie die unbefugte Eingabe von Daten durch einen Nichtberechtigten. Einen besonderen Fall bildet die Programmanipulation, mithin die unrichtige Gestaltung des Programms, also der in Form von Daten fixierten Arbeitsanweisung an den Computer. Sie umfaßt neben dem Neuschreiben ganzer Programme oder Programmteile u. a. das Hinzufügen, die Veränderung oder das Löschen einzelner Programmablaufschritte sowie die Herstellung von Umgehungen der Systemkontrollen. Schließlich erfüllen auch Veränderungen des Ablaufs der Datenverarbeitung, die sich auf das Ergebnis der Datenverarbeitung auswirken (sog. Outputmanipulationen) den Tatbestand.

Von § 263a StGB erfaßt wird insbesondere der Betrug mittels rechtswidrig erlangter oder gefälschter Codekarten für Geldausgabe- bzw. Kassenautomaten. Da indes auch die „unbefugte Verwendung von Daten“ geregelt ist, findet diese Vorschrift ebenfalls Anwendung auf den berechtigten Inhaber, der mit der Karte Geld abhebt, obwohl das Konto keine Deckung mehr aufweist. Als Computerbetrug einzuordnen ist zudem der Fall, daß unter Einsatz eines rechtswidrig erlangten Computerprogramms

auf den Ablauf des Datenverarbeitungsvorgangs eines Geld- oder Glücksspielautomaten eingewirkt wird. Ein Blick in die Polizeiliche Kriminalstatistik des Jahres 1995 verdeutlicht, daß der Betrug mittels rechtswidrig erlangter Karten für Geldausgabe- bzw. Kassenautomaten mit insgesamt 23315 Fällen die des sonstigen Computerbetrugs (3575 Fälle) bei weitem überwiegt. Freilich darf nicht unberücksichtigt bleiben, daß in der Statistik nur die der Polizei bekanntgewordenen Straftaten erfaßt werden.

Fälschung beweiserheblicher Daten

Bei der Fälschung beweiserheblicher Daten im Sinne der §§ 269, 270 StGB geht es um den Schutz der Sicherheit und Zuverlässigkeit des Rechts- und Beweisverkehrs. Dieser soll vor Beeinträchtigungen geschützt werden, die durch unberechtigt vorgenommene Datenspeicherungen oder Veränderungen an solchen Daten in Datenbanken entstehen, die als „elektronische Urkunden“ den normalen Urkunden gleichstehen. Strafbar macht sich, wer zur Täuschung im Rechtsverkehr vorsätzlich beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde. Umfaßt von § 269 StGB ist selbstverständlich auch der Gebrauch derart gespeicherter oder veränderter Daten. Insoweit stellt § 270 StGB klar, daß auch der Dialog zwischen Computern, mithin die Fälle einbezogen sind, in denen nicht die unmittelbare Täuschung eines Menschen, sondern die fälschliche Beeinflussung einer Datenverarbeitung bezweckt wird. Zu beachten ist in diesem Zusammenhang, daß die bloße Eingabe falscher Daten durch den Eingabeberechtigten nach den §§ 269, 270 StGB nicht strafbar ist. Anders als im Falle des Computerbetrugs nimmt sich die Fälschung beweiserheblicher Daten mit lediglich 227 Fällen in der Polizeilichen Kriminalstatistik für das Jahr 1995 recht bescheiden aus. Doch stellt dies im Vergleich zu 1994 mit 179 Fällen eine Steigerung von 26,8 v. H. dar.

Der strafrechtliche Schutz umfaßt bei öffentlichen Urkunden auch deren inhaltliche Richtigkeit. Zudem hat der Gesetzgeber den Schutzbereich der §§ 271 ff., 348 StGB auf falsche Speicherungen in öffentlichen Dateien erstreckt. Strafbar ist schließlich auch der Fall, daß der Täter beweiserhebliche Daten, über die er nicht oder nicht ausschließlich zu verfügen berechtigt ist, löscht, unterdrückt, unbrauchbar macht oder verändert, um einem anderen Nachteil zuzufügen.

Datenveränderung und Computersabotage

Wenngleich das Löschen von Daten, an deren Verfügbarkeit und Unversehrtheit ein anderer ein unmittelbares Interesse hat, gemeinhin als Sachbeschädigung (§ 303 StGB) eingeordnet wird, werden die Vernichtung und die Veränderung von Daten während der Übermittlungsphase nicht mehr von § 303 StGB erfaßt. Nach § 303a StGB macht sich nunmehr aber strafbar (Geldstrafe, Freiheitsstrafe bis zu zwei Jahren), wer vorsätzlich und rechtswidrig unmittelbar nicht wahrnehmbare gespeicherte oder übermittelte Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Es werden mithin alle Beeinträchtigungen der Verwendbarkeit erfaßt. Dazu zählt in besonderem Maße das Einpflanzen von Computerviren oder das Einladen von crash-Programmen.

Nicht ausreichend abgedeckt von § 303a StGB wird die mit einem erheblichen wirtschaftlichen Schaden verbundenen Computersabotage. Es geht hier nicht nur um Fälle, in denen es durch Datenveränderung (crash-Programme) zu einer Störung der Datenverarbeitung kommt. Umfaßt sind vielmehr auch die Fälle, in denen (etwa durch verärgerte Mitarbeiter) EDV-Anlagen beschädigt oder gestört werden, indem z. B. Büroklammern

eingeführt oder Stecker vertauscht werden. Nach § 303b StGB macht sich strafbar (Geldstrafe, Freiheitsstrafe bis zu fünf Jahren), wer eine für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde wesentliche Datenverarbeitung durch Sabotagehandlungen der soeben beschriebenen Art stört. Erfaßt von § 303b StGB wird auch der Angriff auf eigene Anlagen oder Datenträger, wenn dies zu einer Störung der für die genannten Einrichtungen vorgenommenen Datenverarbeitung führt.

Die Schwierigkeiten der Ermittlung dieser Straftaten wird durch einen Blick wiederum in die Polizeiliche Kriminalstatistik vor Augen geführt. Während im Jahr 1994 188 Fälle erfaßt wurden, steigerte sich die Zahl der der Polizei im Jahre 1995 bekanntgewordenen Delikte auf lediglich 192, was einer Steigerung von 2,1 v. H. entspricht. Die Dunkelziffer dürfte um ein Vielfaches höher liegen.

Computer- und Datenspionage

Wenngleich die unbefugte Nutzung von und der unbefugte Zugang zu EDV-Anlagen nicht strafbar ist, verhält sich dies anders im Fall der Computer- und Datenspionage. § 202a StGB stellt nämlich das unbefugte Verschaffen von besonders gesicherten, nicht für den Täter bestimmten Daten unter Strafe (Geldstrafe bzw. Freiheitsstrafe bis zu zwei Jahren). Geschützt wird durch diese Bestimmung das Geheimhaltungsinteresse des Verfügungsberechtigten. Dieses Interesse an der Geheimhaltung muß allerdings durch entsprechende Sicherungsmaßnahmen dokumentiert sein. Diese umfassen neben mechanischen (z. B. Behältnisse, Schlösser) auch Sicherungen der Hard- und Software, also Paßworte, Magnetkarten, Sperrvermerke und Datenverschlüsselungen. Personenbezogene organisatorische Maßnahmen sind allerdings nicht ausreichend. Ein „Verschaffen“ ist gegeben, wenn der Täter Datenträger mit Daten entwendet, Daten auf einen Datenträger überträgt, eine Kopie erstellt oder auf sonstige Weise den Inhalt der Daten wahrnimmt.

Eine zusätzliche Strafbarkeit begründet § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) in bezug auf gespeicherte Betriebs- und Geschäftsgeheimnisse. Danach ist das unbefugte Verschaffen (zum Begriff des Verschaffens s. o.) dieser gespeicherten Geheimnisse strafbar, wenn der Täter zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der bloßen Absicht handelt, dem Geschäftsinhaber Schaden zuzufügen. Hervorgehoben sei, daß es anders als im Fall des § 202a StGB gemäß § 17 UWG auf eine besondere Datensicherung nicht ankommt. Die Tat kann nicht nur durch Betriebsfremde, sondern auch durch Betriebsangehörige begangen werden. Schließlich ist auch derjenige, der sich der Geheimnishehlerei schuldig macht, strafbar, mithin der, der unbefugt verschaffte Betriebs- und Geschäftsgeheimnisse unbefugt verwertet oder anderen mitteilt.

Programm- und Chip-Piraterie

Programme für die Datenverarbeitung sind urheberrechtlich geschützt, wenn sie eine „persönliche geistige Schöpfung“ darstellen. Wer vorsätzlich ein solches Werk ohne Einwilligung des Berechtigten vervielfältigt, verbreitet oder öffentlich weitergibt, macht sich nach den §§ 106, 69a UrhG strafbar (Geldstrafe bzw. Freiheitsstrafe bis zu drei Jahren). Gleiches gilt hinsichtlich des Kopierens ohne Einwilligung. Vervielfältigt oder verbreitet der Täter das derart geschützte Programm gewerbsmäßig (§ 108a UrhG), beträgt die Höchststrafe fünf Jahre. Das ist der Fall, wenn es dem Täter darauf ankommt, sich aus wiederholter Begehung eine fortlaufende Haupt- oder auch nur Nebeneinnahmequelle von einiger Dauer und einigem Umfang zu verschaffen. Erfaßt ist also vor allem das

professionelle Raubkopierertum. Im Vergleich zu 363 Fällen der privaten Software-Piraterie wurden in der Polizeilichen Kriminalstatistik des Jahres 1995 lediglich 120 Fälle der gewerblichen Software-Piraterie erfaßt. Hervorzuheben ist indes, daß dies gegenüber den für das Jahr 1994 erfaßten Fällen insgesamt eine Steigerung von 35,7 v. H. bedeutet.

Strafvorschriften enthält zudem das Gesetz über den Schutz von Topographien von mikroelektrischen Halbleitererzeugnissen vom 22. Oktober 1987, das eine europäische Richtlinie umsetzt. Gemäß § 10 macht sich strafbar, wer Mikrochips bzw. Topographien ohne Zustimmung des Berechtigten nachbildet, anbietet, in Verkehr bringt, verbreitet oder zu diesen Zwecken einführt. Nicht umfaßt ist allerdings das Kopieren zum Zwecke der Bewertung und deren geschäftlicher Verwertung.

Datenschutzdelikte

Bereits seit dem 1. 1. 1975 ist die unbefugte Offenbarung und Verwertung von Einzelangaben über persönliche und sachliche Verhältnisse eines anderen, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind, mit Strafe bedroht. Darunter fallen grundsätzlich nicht Mitteilungen im Behördenverkehr, es sei denn, auch diese sind gesetzlich untersagt. Gemäß § 43 Abs. 1 Bundesdatenschutzgesetz (BDSG) macht sich strafbar (Geldstrafe bzw. Freiheitsstrafe bis zu einem Jahr), wer vorsätzlich nicht offenkundige personenbezogene Daten (1) speichert, verändert oder übermittelt, (2) zum Abruf mittels automatisierten Verfahrens bereithält oder (3) abruft oder sich oder einem anderen aus Dateien verschafft. Ebenso strafbar ist gemäß Absatz 2, wer (1) die Übermittlung derart geschützter Daten durch unrichtige Angaben erschleicht, (2) entgegen den Bestimmungen des BDSG die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder (3) bestimmte Merkmale mit den Einzelangaben zusammenführt. Handelt der Täter gegen Entgelt bzw. mit Bereicherungs- oder Schädigungsabsicht beträgt die Höchststrafe zwei Jahre. Vergleichbare Vorschriften finden sich in den Datenschutzgesetzen der Länder. Auch die Datenschutzdelikte nehmen sich in der Polizeilichen Kriminalstatistik für 1995 mit insgesamt 232 Fällen bescheiden aus. Doch auch hier ist im Vergleich zum Vorjahr (194 Fälle) eine Steigerung von 19,6 v. H. zu verzeichnen.

4. Eine kurze Geschichte der Zeit

Bettina Schmidt, Rechenzentrum

Neulich erst war es, als ich — warum nur habe ich sie nicht gleich bemerkt — über eine Anzeige stolperte. „Oh, Entschuldigung“, sagte die Anzeige höflich, „ich wollte niemand im Wege sein.“ So betrachtete ich sie genauer.

Es war eine traurige Anzeige. Eine Todesanzeige.

Nach harter Arbeit, Schmähungen und Systemangriffen wurde ihr der Strom entzogen
teflon.RZ.Uni-Augsburg.DE
⋆ 1992 †1996

Die letzten TCP/IP-Pakete werden im Laufe des Wintersemesters versandt.

Es wird gebeten, von Beileids-eMails abzusehen.
Es trauern:
root, stellvertretend für eine große Benutzergemeinde
dæmon, stellvertretend für alle diensttuenden Geister
ZyXEL Elite 2864ID, stellvertretend für alle Modems

Aber ich wurde aus dem Text nicht ganz schlau. Wer war da gestorben? Ein ganzes Post-Unternehmen mit all seinen Angestellten? So fragte ich die Anzeige.

„Ja“, antwortete diese betrübt, „so könnte man das auch nennen. Die teflon ist ein Computer, genauer gesagt, der erste Modemzugang des Rechenzentrums für die Allgemeinheit. Sie wurde jetzt durch eine große und professionelle Lösung ersetzt. Tja, so ist das nunmal. Wie ein kleiner Familienbetrieb gegenüber einem Großmarkt.“ Die Anzeige warf mir einen prüfenden Blick zu, ob ich wohl den persönlichen Service der Anonymität vorzöge. Ich hatte den Eindruck, daß hier jemand nicht mit der modernen Entwicklung Schritt halten konnte und deshalb in Selbstmitleid versank. So wollte ich das klären: „Aber ein großes Geschäft bietet doch Vorteile, es gibt ein größeres Angebot, die Preise sind günstiger — natürlich ist das Gros des Personals nicht vom Fach — aber was hat das alles mit Computern zu tun, und was spricht gegen eine professionelle Erneuerung?“

Meine Gesprächspartnerin knickte ein wenig pikiert mit ihren Ecken. „Ein solcher Computer ist wie ein Service-Unternehmen“, belehrte sie mich, „es werden gewisse Dienstleistungen angeboten. Bei beiden Servern, dem alten und dem neuen, sind das POP, SMTP, HTTP, und FTP. Die teflon hatte zudem noch Telnet, Finger und Talk zu bieten. So gesehen ist das Angebot kleiner geworden. Dadurch ist der neue Server natürlich wartungsfreundlicher und die Benutzerbetreuung einfacher geworden, hat insgesamt gesehen weniger rechenintensives zu tun und kann daher eine größere Menge Benutzer gleichzeitig bedienen. Und dieser Server ist ja nur ein Teil der neuen Lösung, er stellt die Protokolle zur Verfügung. Das Pendant dazu ist eine Maschine, die zwei Einwahlkaskaden von je 30 Anschlüssen verwaltet. So ist die ganze Last auf zwei Rechner verteilt.

Im Gegensatz dazu war die teflon ursprünglich aus Ersatzteilen zusammengebaut und stellte nur sieben analoge und einen ISDN-Zugang zur Verfügung. Vor dem automatischen Verfahren, im WWW über die Benutzernummer ein Login zu beantragen, wurden alle Benutzer per Hand eingetragen, dadurch wurde schon immer persönlicher Kontakt gefördert. Studenten und Beschäftigte bekamen immer individuelle Beratung, Hilfe bei speziellen Problemen, ob das jetzt eMail oder Shell-Programmierung anbelangte. Es wurden auch Benutzerwünsche nach eigener Software

erfüllt.“

Die Anzeige schien ob dieser langen Rede etwas erschöpft. Soweit ich verstanden hatte, wich ein Server mit reichhaltigem Angebot und individueller Betreuung aber wenig Zugängen einem stabilen Server-Gespann mit nun wirklich erheblich mehr Zugängen, dafür aber pflegeleichterem Angebot. Stabilität und vergrößerte Zugangskapazität waren doch Vorteile, die nicht von der Hand zu weisen waren.

Warum schien meine Gesprächspartnerin also so betrübt? Vielleicht weil es in der Natur einer Todesanzeige lag? „Oh, nein“, erwiderte diese, „an den Tod habe ich mich schon gewöhnt. Ab und zu arbeite ich ja auch als Glückwunsch-Telegramm. Bedauerlich ist, daß die teflon immer als Stiefkind behandelt wurde, daß die Nutznießer laut schrien, wenn's um Kritik ging, aber leise blieben, wenn's der Würdigung bedurft hätte. Und letztendlich haben diverse Hack-Versuche und unfaires Verhalten einiger weniger nun den Nutzern des neuen Systems Dienste wie Telnet unmöglich gemacht. Vertrauen ist gut, besser ist es, Querulanten möglichst wenig Angriffspunkte zu bieten!“

Sprach's und verschwand raschelnd in der Bedeutungslosigkeit.

Ich blieb zurück, gerührt vom Leben und Sterben in der Daten-Welt, und war froh, daß ich, das Flugblatt, meiner Kollegin nicht die bedruckte Seite zugewandt hatte, auf der in großen Lettern stand:

JETZT GANZ NEU!!! PROBLEMLOSER PPP-ZUGANG!!! 60 ANSCHLÜSSE!!!

---

5. Wählzugang zum Hochschulnetz

Dr. Milos Lev, Rechenzentrum

Im November 1997 wurde der bisherige Modemzugang mit acht Leitungen (Teflon) durch einen modernen Modemserver ersetzt, welcher insgesamt 60 Wählzugänge zum Universitätsnetz bietet. Das alte System war durch die Vielzahl der Nutzer und die äußerst geringe Anzahl von Modemverbindungen ständig überlastet. Die Anschaffungskosten des Servers vom Typ Ascend MAX4000, mit 2 S_{2M}-Schnittstellen betrugen rund 70 000.– DM. Jede dieser S_{2M}-Schnittstellen bedient 30 ISDN-Zugänge. Von diesen 60 Leitungen können bis zu 30 Anschlüsse wahlweise auch analog betrieben werden. Die 60 Zugangsleitungen sind gleichmäßig auf zwei Telefonnummern verteilt: *(0821) 257750* oder *257760*.

Als Zugangsrechner dient eine IBM RS/6000-Workstation *(rzibm01.RZ.Uni-Augsburg.DE)* mit AIX Betriebssystem.

Um ins Hochschulnetz zu gelangen, ist eine Zugangsberechtigung, d. h. eine Nutzerkennung (Login) und ein Paßwort, für diesen Rechner notwendig. Der Modemserver überprüft beim Einwählvorgang unter Zuhilfenahme des Zugangsrechners die Benutzerkennung und das Paßwort. Bis jetzt haben bereits über 3 000 Studenten eine Zugangsberechtigung erhalten.

Kennung und Paßwort werden auf Antrag vom Rechenzentrum ausgegeben. Dafür gelten zur Zeit folgende Regelungen:

- Studierende können über die WWW-Seite *http://www.Student.Uni-Augsburg.DE/* das Antragsformular selbständig ausfüllen und ausdrucken. Im Antragsformular dient die Bibliotheksnummer des Studentenausweises als Berechtigungsnummer. Nach Abgabe des *unterschriebenen* Formulars im Rechenzentrum wird die Benutzerkennung freigegeben. Eine explizite Verlängerung zu Beginn jedes neuen Semesters ist nicht mehr notwendig. Das System überprüft, ob eine Nutzungsberechtigung (aufgrund erfolgter Immatrikulation) weiterhin vorliegt und verlängert in diesem Fall die Benutzerkennung automatisch.
- Für Mitarbeiter der Universität sind die Anträge bei den DV-Betreuern der einzelnen Fakultäten oder Einrichtungen erhältlich. Es wird angestrebt, daß die DV-Betreuer selbst die Logins über WWW-Seiten vergeben können.

Für Studenten wird mit einer Benutzerkennung auf dem Rechner *rzibm01.RZ.Uni-Augsburg.DE* auch die eMail-Adresse eingerichtet. Sie lautet: *Vorname.Nachname@Student.Uni-Augsburg.DE*. Für Mitarbeiter der Universität werden die eMail-Adressen nach wie vor von den DV-Betreuern eingerichtet.

Als Kommunikationsprotokoll für den Zugang zum Hochschulnetz wird das Point-to-Point-Protokoll (PPP) verwendet. Damit ist der Rechner in das Hochschulnetz integriert und alle Netzdienste können über das IP-Protokoll in Anspruch genommen werden (siehe Abbildung 5.1). Andere Kommunikationsprotokolle werden momentan nicht unterstützt. Die Zugangsberechtigung wird beim Anmelden über das *Password Authentication Protocol (PAP)* überprüft, die Anmeldung über einen Dialog ist nicht möglich.

Für Fragen und Hilfestellungen ist die Modemberatung, Herr Matthias Meier, zu seinen Sprechzeiten (montags und dienstags jeweils von 9:00 bis 11:00 Uhr) für Sie da.

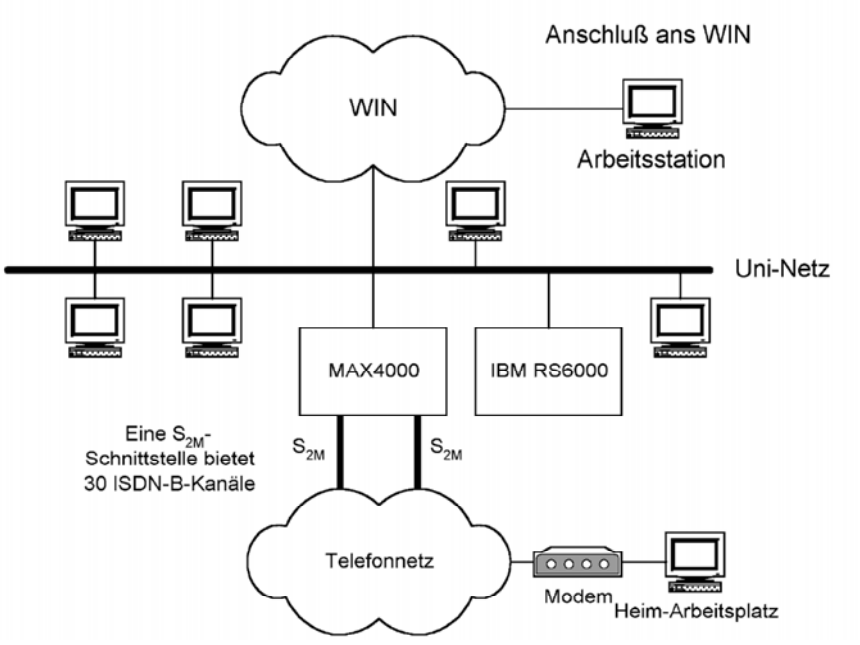


Abb. 5.1: Zugang zum Uni-Netz von außerhalb

Die nachfolgenden Abschnitte sollen Ihnen Konfigurationstips zum PPP-Protokoll für Ihr heimisches Rechnersystem bieten.

PPP unter Windows 95

Von Matthias Meier

Um unter Windows 95 eine PPP-Verbindung zur Universität aufzubauen sind zwei Schritte nötig:

Als erstes muß man im Netzwerk-Setup den Client für Microsoft-Netzwerke, den DFÜ-Adapter (Windows 95 emuliert hierbei eine Netzwerkkarte über das Modem) und natürlich das TCP/IP-Protokoll hinzufügen. Hierbei ist eingentlich nur zu beachten, daß der DNS (Domain Name Server, 137.250.1.254) richtig angegeben wird und die IP-Adresse automatisch bezogen wird. Die restlichen Angaben, wie Gateway, Host und Domäne werden von der *rzibm01.RZ.Uni-Augsburg.DE* fest vorgegeben.

Der zweite Schritt besteht darin, eine neue Verbindung im DFÜ-Netzwerk zu erstellen und zu konfigurieren. Außer den richtigen Telefonnummern ist eigentlich nur zu beachten, daß im Menü *Eigenschaften* im Unterpunkt *Konfigurieren-Optionen-Verbindungsoptionen* das Terminalfenster nach dem Wählen deaktiviert ist, da der neue Modemserver die Benutzer über das Password Authentication Protokol (PAP) identifiziert und Windows 95 sonst auf ein Terminalfenster wartet, das nicht mehr unterstützt wird. Sollten Sie eine ISDN-Karte verwenden, so installieren Sie, sofern vorhanden, einen sogenannten CAPI-Port Treiber (dieser stellt Ihnen die ISDN-Karte wie ein normales, analoges Modem zur Verfügung) und verwenden statt des analogen Modems Ihr ISDN-Modem im DFÜ-Netzwerk. Auch sollte man nicht vergessen, daß bei Unix Groß- und Kleinbuchstaben unterschieden werden (z. B. beim Login und dem Paßwort!). Weitere Informationen findet man in der Windows Hilfe unter dem Stichpunkt: *DFÜ-Netzwerk* und dem Thema „So verbinden Sie sich per DFÜ-Netzwerk mit dem Internet“

PPP unter Windows 3.1x

Von Matthias Meier

Die einfachste Möglichkeit unter Windows 3.1x eine PPP-Verbindung zur Universität aufzubauen, ist das Verwenden des Sharewareprogramms *Trumpet Winsock*. Dies läuft ebenfalls in zwei Schritten ab:

Zuerst muß das Programm konfiguriert werden. Hierbei sind die beiden Menüpunkte „Setup“ und „PPP options“ im Menü *File* wichtig. Im ersten werden die allgemeinen Konfigurationseinstellungen zur Universität Augsburg eingestellt. Als IP-Adresse sollte man die 0.0.0.0 (entspricht dynamischer IP), als Name-Server die 137.250.1.254 und als Domain suffix RZ.Uni-Augsburg.DE eintragen. Desweiteren: MTU 1500, TCP RWIN 4096, TCP MSS 1460, TCP RTO MAX 60 und Internal PPP aktivieren. Im zweiten Menüpunkt werden die benutzerspezifischen Informationen, wie Login und Paßwort eingetragen, wobei man nicht vergessen darf, PAP zu aktivieren.

Der zweite Schritt ist dann die Anwahl des Modemservers an der Uni. Hierzu sollte man den Eintrag „Manual login“ im Menü „Dialer“ aufrufen. Als Initialisierungs-String sollte i. a. „ATZ“ genügen und die Anwahl erfolgt über „ATDT 257750“. Sobald man nun eine Meldung des Modems sieht, die „CONNECT“ oder ähnlich lautet, müssen Sie sofort die Escape-Taste drücken noch bevor eine Login-Eingabeaufforderung erscheint. Erscheint diese doch, so müssen Sie die Anwahl wiederholen.

Eine ausführliche Anleitung sowie weitere Informationen finden Sie im Internet unter: *http://www.student.Uni-Augsburg.DE/~matthias/*

PPP unter Linux

Von Matthias Wagner

Der Aufbau eines PPP-Links zum Modemserver des Rechenzentrums unter Linux erfolgt in zwei Schritten: Zunächst wird eine Verbindung zwischen beiden Modems aufgebaut. Dies kann mit Hilfe des Programms *chat* erfolgen. Ist die Verbindung vorhanden, wird die Kontrolle dem lokalen PPP Dæmon übergeben, der den Austausch von Benutzerkennung und Passwort nach dem Protokoll PAP vornimmt, Parameter der Übertragung festlegt sowie die Verbindung initialisiert.

In den folgenden Abschnitten werden die benötigten Konfigurationsdateien schrittweise vorgestellt. Hierbei ist ein System mit Kernel 2.0.18, ppp 2.2.0 und einem Benutzer *obelix* vorausgesetzt, der sich unter Verwendung des Passworts *idefix* von seinem Rechner mit Namen *majestix* am Rechenzentrum der Universität Augsburg einwählt.

TCP/IP

Der Systemkern muß TCP/IP und natürlich PPP unterstützen. Für die Konfiguration bzw. die Re-Kompilierung des Linuxsytems siehe z. B. [1].

Um *majestix* vernünftig im Netz der Universität Augsburg betreiben zu können, ist DNS zu konfigurieren, d. h. die Datei */etc/resolv.conf* sollte folgende Einträge haben:

```
search informatik.uni-augsburg.de
rz.uni-augsburg.de
nameserver 137.250.71.254
nameserver 137.250.1.254
```

PAP

Der Modemserver des Rechenzentrums identifiziert seine Benutzer über das Password Authentication Protocol (PAP). Auf der Seite von *majestix* wird diese Information in der Datei */etc/ppp/pap-secrets* gespeichert:

```
*       *       idefix
```

CHAT

Das Programm *chat* wird im Fall von *majestix* das Skript */etc/ppp/scripts/ibm.chat* zum Verbindungsaufbau verwenden:

```
TIMEOUT 3
ABORT   BUSY
ABORT   'NO ANSWER'
ABORT   'NO DIALTONE'
ABORT   'RINGING'
''      ATZ
OK      AT&H1&B1&R1
TIMEOUT 30
OK      ATDT257750
Login
```

Im wesentlichen stehen in einem CHAT-Skript Paare von Zeichenketten, die vom Modem und der Gegenstelle erwartet werden bzw. als Antwort geschickt werden. Oben ist der Befehl *AT&H1&B1&R1* Modem-spezifisch[1]. Er bewirkt, daß die Hardwareflußkontrolle eingeschaltet und die Geschwindigkeit der seriellen Schnittstelle konstant festgelegt ist.

pppd

Existiert eine Verbindung, bleibt nur noch der Start des PPP-Dæmon *pppd*. Besonders einfach ist es, sämtliche Optionen von *pppd* in die dafür vorgesehene Datei */etc/ppp/options* zu schreiben. Auf *majestix* sieht diese Datei folgendermaßen aus:

[1] Verwendet wird das Modem US Robotics Sportster 28800

```
connect "/usr/sbin/chat -v -f
/etc/ppp/scripts/ibm.chat"
modem
lock
noipdefault
user obelix
/dev/cua1
-detach
debug
crtscts
defaultroute
```

In der Option *connect* ist hier der Aufruf des CHAT-Skripts aus Abschnitt 5 untergebracht. Sind alle Konfigurationsdateien korrekt genügt somit der Aufruf *pppd* zum Gesamtaufbau des PPP-Links.

Probleme

In unserem Beispiel werden *pppd* und *chat* mit den Optionen *debug* bzw. *–v* gestartet. Auf einem System-V initialisierten Linux-System[2] werden so möglichst viele Meldungen über den Verlauf des Verbindungsaufbaus in die Datei */var/log/messages* geschrieben. Bei Problemen mit PPP unter Linux helfen also ein *tail –f /var/log/messages* ebenso wie [2], [3] oder die Manual-Pages zu *pppd* und *chat*.

Literaturverzeichnis

[1] M. Beck, H. Böhme, M. Dziadzka, U. Kunitz, R. Magnus, und D. Verworner. *Linux Kernel Programmierung.* Addison-Wesley, 1994. ISBN 3-89319-712-5

[2] R. Hart. Linux PPP-HOWTO. *http://www.fokus.gmd.de/linux/HOWTO/PPP-HOWTO.html*, 1996

[3] O. Kirch. *Linux network administrator's guide.* O'Reilly & Associates, 1995. ISBN 1-56592-087-2

[2] z. B. S.u.S.E Linux 2.3

PPP mit dem Macintosh

Von Werner Bauer

Um vom Mac aus über die *rzibm01.RZ.Uni-Augsburg.DE* ins Internet zu gelangen, benötigt man die Macintosh Netzwerksoftware und eine Erweiterung für das PPP-Protokoll.

Je nach Macintosh gibt es verschiedene Konfigurationen. Bei älteren Macs ist im System das Kontrollfeld „MacTCP“ integriert, bei neueren Systemen oder bei Installation von *Open Transport* gibt es das Kontrollfeld „TCP/IP“. Es muß eine PPP-Verbindung konfiguriert werden. Dazu benötigt man einen der vielen Public Domain PPP-Installer. Empfehlenswert sind für ältere Macs das „FreePPP 2.5v2“ und für neuere Macs (vor allem unter Open Transport) „OT/PPP“. Diese Software liegt z. B. auf dem Macintosh FTP Server der Universität unter *ftp://macftp.RZ.Uni-Augsburg.DE/pub/comm/ppp/Free-PPP2.5v2.sit* bzw. *ftp://macftp.RZ.Uni-Augsburg.DE/pub/apple/networking/OT_PPP_1.0-Net_Install.sea.* Dazu einfach den Installer zu FreePPP oder OT/PPP starten und installieren lassen. Danach muß der Rechner einmal neu gestartet werden.

Jetzt kann das PPP konfiguriert werden. Bei FreePPP geschieht dies im Programm „FreePPP Setup“ und bei OT/PPP im Kontrollfeld „PPP“. Hierbei erfolgt die Angabe des verwendeten Modems, bzw. des zu verwendenden Initialisierungsstrings für das Modem sowie der Benutzerkennung und des Paßworts. Ganz wichtig sind die folgenden Einstellungen: Im Kontrollfeld „MacTCP“ bzw. „TCP/IP“ den Verbindungstyp auf „FreePPP“ bzw. „PPP“ und den Konfigurationstyp auf „PPP Server“ stellen. Im Unterschied zum Teflon-Modemzugang gibt es auf der *rzibm01.RZ.Uni-Augsburg.DE* kein Verbindungsskript mehr, sondern nur direkt PPP. Das heißt, unter dem Verbindungstyp im

FreePPP Setup bzw. PPP Kontrollfeld darf kein Connect Script mehr aktiviert sein, die Verbindung muß auf PPP direkt eingestellt sein. Ein Installer für den Modemzugang, der alle nötigen Systemkomponenten und Einstellungen vornimmt, ist in Arbeit.

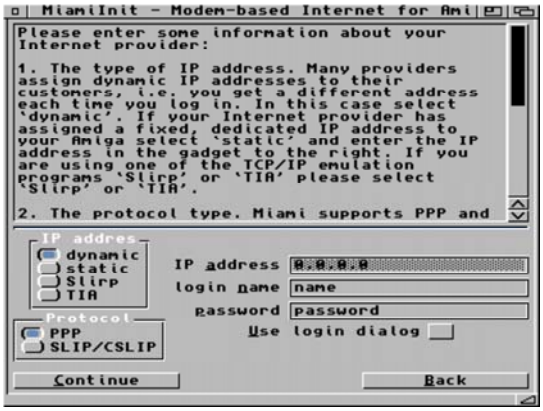
Bei Fragen und Problemen können Sie sich an Herrn Bauer im Rechenzentrum wenden (eMail: Werner.Bauer@RZ.Uni-Augsburg.DE).

PPP mit dem Amiga

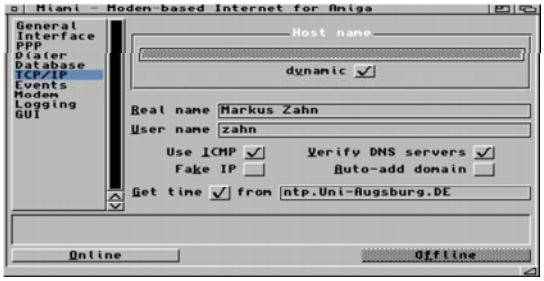
Von Markus Zahn

Um mit dem Amiga eine PPP-Verbindung zum Modemserver des Rechenzentrums aufzubauen, bedient man sich am besten des TCP/IP-Softwarepakets *Miami (Modem-based Internet for Amiga)*. Die minimale Betriebssystemversion für die Nutzung von Miami ist AMIGA OS 2.04, zusätzlich wird noch *MUI (Magic User Interface)* für die ansprechende Benutzerschnittstelle benötigt.

Mit dem Konfigurationsprogramm *MiamiInit* ist Miami über eine graphische Benutzeroberfläche kinderleicht auf die eigenen Bedürfnisse (z. B. den Modemtyp) anzupassen. Die meisten systemabhängigen Konfigurationsparameter werden von MiamiInit bei einer ersten Online-Verbindung automatisch ermittelt. Da der Modemserver User und Paßwort per *Password Authentication Protocol (PAP)* ermittelt, sollte man hinter „Use login dialog“ — wie in der nachfolgenden Abbildung bereits geschehen — das Häkchen entfernen. Natürlich sind „name“ und „password“ durch eigene Angaben zu ersetzen.



Ist die Konfiguration abgeschlossen, so kann von Miami die erzeugte Konfigurationsdatei importiert und anschließend als Standard-Konfiguration für Miami abgespeichert werden, – fertig! Nun kann man sich mit dem Online-Button automatisch mit dem universitären Modemserver verbinden lassen. Um während einer Verbindung zur Universität noch die funkgesteuerte Uhr des Rechenzentrums zur Synchronisation der heimischen Rechneruhr heranzuziehen, kann im TCP/IP-Menü von Miami der Timeserver *ntp.Uni-Augsburg.DE* eingetragen werden:



Bemerkung: Sowohl Miami als auch MUI sind Sharewarepakete, die Ihren vollen Funktionsumfang erst nach erfolgter Registrierung

entfalten. Die über unseren FTP-Server abrufbaren Demo-Versionen der beiden Systeme können jedoch ohne zeitliche Einschränkungen genutzt werden. Die Anleitungen geben hierzu die entsprechenden Hinweise. Die für die verschiedenen Netzdienste (WWW, FTP, News etc.) benötigten Clientprogramme finden sich ebenfalls auf unserem FTP-Server *ftp.Uni-Augsburg.DE.*

6. Rechnernetzwerk — Netzwerkrechner

Ralf Utermann, Institut für Physik

Das Loadleveler-System am Institut für Physik — Ein Bericht aus einer ökologischen Nische.

Es ist noch nicht allzulange her, daß die Rechnerausstattung an Universitäten oder anderen größeren Einrichtungen aus wenigen, teuren Großrechnern (Mainframes) bestand, auf die mit einfachen Terminals zugegriffen wurde. Mittlerweile aber stehen auf und unter den Schreibtischen Geräte mit immer höherer Rechenleistung für immer anspruchsvollere Anwendungen. Selbst wenn Sie den ganzen Tag Texte schreiben, Programme übersetzen und das WWW benutzen: der Prozessor Ihres Rechners verwendet nur einen Bruchteil seiner Kapazität darauf und läuft die meiste Zeit im „Leerlauf". Nachts werden PCs ohnehin oft ausgeschaltet und auch auf einem typischen Unix-System beschäftigen zur Geisterstunde nur wenige Dämonen die Hardware: ein enormes Potential an ungenutzter Rechenleistung. Im folgenden wird ein System vorgestellt, mit dem dieses Potential seit zwei Jahren am Institut für Physik effizient genutzt wird.

Voraussetzungen

Angenommen, Sie haben bisher ihre numerischen (oder andere) Aktivitäten auf ihrem eigenen Rechner abgewickelt. Nun kommen Sie in Parameterbereiche, für die Ihr System nicht mehr ausreicht oder Sie brauchen einfach mehr Programmläufe. Werden die Anforderungen richtig groß, müssen Sie eventuell einen Zugang zu einer der großen Anlagen am Leibniz-Rechenzentrum beantragen (Kontakt: Herr Umpfenbach/RZ). Vermutlich schauen Sie aber erst zu Ihrem Kollegen eine Tür weiter, und fragen ihn, ob denn nicht die Möglichkeit bestünde, auf seinem Rechner ein paar Jobs laufen zu lassen. Im Prinzip wird Ihr Kollege nichts dagegen haben, falls es ihn bei seiner täglichen Arbeit nicht behindert. Dazu sind ein paar Grundvoraussetzungen zu erfüllen:

- Es müssen mehrere Prozesse unabhängig voneinander auf dem Rechner laufen können. Ihr Kollege will ja seine üblichen Aufgaben weiter erledigen können.
- Es muß mehrere Benutzer geben können, die über getrennte Bereiche verfügen: Ihr Kollege wollte nur Rechenzeit anbieten — nicht Einblick in seinen Briefverkehr.
- Die Zeit, die das System durchgehend ohne Neustart wegen Absturz oder Wartung läuft (*uptime*), sollte im Mittel deutlich höher liegen als die typische Programmlaufdauer.

Man benötigt also ein stabiles Multiuser/Multitasking-Betriebssytem; nun noch ein Netzzugang der beteiligten Rechner und Sie können loslegen.

Spätestens nachdem Sie noch einen weiteren Kollegen gefragt haben, erweitert sich obige Liste. Für längerfristiges, komfortableres Arbeiten sollten die Maschinen mit einer

gemeinsamen Namens- und Verzeichnisstruktur verbunden sein (im Unix-Umfeld etwa NFS/NIS oder DCE); ansonsten schlägt man sich mit mehreren Paßwörtern, dem Hin- und Herkopieren von Programmen und Daten, und anderen Annehmlichkeiten herum. Solch eine Umgebung ist an den meisten Instituten im naturwissenschaftlichen Bereich vorhanden.

Batchjob-Verwaltung lokal ...

Leider sind Sie nicht der Einzige geblieben, der auf den schönen neuen Rechner des Kollegen aufmerksam geworden ist. Nun müssen Sie sich mit einem weiteren Mitbenutzer absprechen, wer denn nun wann und wie lange seine Programme rechnen lassen darf. Irgendwann führt dies mit ziemlicher Sicherheit dazu, daß der Rechner überfordert wird und möglicherweise rattert dann stundenlang die Festplatte, weil der Rechner am swapen ist. Der eigentliche Besitzer will zu diesem Zeitpunkt sicher einen dringenden Artikel fertigschreiben, kann nur leider kein einziges Zeichen mehr eintippen. Die Folge: Sie und der konkurrierende Nutzer sind Ihre Rechenerlaubnis los.

Solche Probleme lassen sich mit einem Batchjob-Verwaltungssystem lösen, wie man es von klassischen Großrechnern her kennt. Man definiert Jobklassen, die sich nach Speicherbedarf und Programmlaufdauer oder weiteren Kriterien richten und so eine optimale Nutzung der Maschine ermöglichen.

... und im Netzwerk

In unserem Fall gibt es zusätzliche Probleme, die allein durch Installation einer solchen Software auf allen Rechnern nicht sinnvoll gelöst werden kann. Vor dem Abschicken eines Rechenauftrags müssen Sie immer nachschauen: Wie ist die Situation auf diesem oder jenem Rechner? Wo ist am wenigsten los? Wo ist welche Software installiert? Welcher Rechner ist denn jetzt der schnellste? Mit wieviel Speicher? Und natürlich kommt ab und zu ein neuer Rechner irgendwo im Institut dazu, oder jener bekommt zusätzlichen Speicher installiert, dieser neue Festplatten. Eine sinnvolle Nutzung ist in diesem Fall durch den Einsatz eines Netzwerk-basierten Batchjob-Verwaltungssystems möglich, das alle Rechner in einem Pool zusammenfaßt. Solche Systeme gibt es sowohl im public-domain Bereich (z. B. NQS), wie auch als kommerzielle Software. Gemeinsam ist allen, daß ein einheitlicher und vor allem nur ein Zugang zum Rechner-Pool geschaffen wird. Der Nutzer kommuniziert darüber mit dem ganzen Pool als hätte er nur einen einzigen Rechner vor sich.

LoadLeveler-Pool Physik

Am Institut für Physik ist seit etwa zwei Jahren ein Pool auf der Basis des LoadLeveler (LL) von IBM in Betrieb. Eingegliedert sind im wesentlichen alle IBM RS/6000 Rechner der Physik. Des weiteren können einige Server des Rechenzentrums mitgenutzt werden. Neue Rechner aktueller Leistungsfähigkeit werden laufend eingegliedert, während am unteren Ende veraltete Modelle herausgenommen werden. Im Jahr 1996 hat die Leistungsfähigkeit des gesamten Pools erheblich zugenommen: am oberen Ende ersetzten am Anfang des Jahres drei RS/6000-3CT (POWER2-Prozessor, je 256MB Hauptspeicher) die beiden 550er (siehe **connect** 1/1996), weitere drei 3CT wurden im Laufe des Jahres durch die Lehrstühle Theoretische Physik III (256MB und 128MB) und Theoretische Physik II (64MB, in Kürze 128MB) beschafft. Vor allem bei der neu hinzugekommenen TPIII wurden eine ganze Reihe Arbeitsplätze mit den Modellen 43P (PowerPC-604, meist 64MB RAM) installiert, so daß der LoadLeveler-Pool nun über 25 Rechner umfaßt. Ältere Modelle sind zum Teil als *submit-only* Maschinen integriert: Aufträge können daher von praktisch jedem AIX-Rechner der Physik abgeschickt werden, gerechnet werden sie allerdings nur von den leistungsfähigeren Systemen.

Tabelle 6.1.: Jobklassen im LoadLeveler-Pool Physik. N ist die Anzahl der Maschinen, auf denen diese Klasse zugelassen ist.

	tiny	small	medium	large	very_large	disk	pwr2	pwr2-8h
RAM [MB]	2.5	10	35	100	230	I/O	230	230
N	22	22	17	2	1	5	5	6

Jobklassen

Das Hauptmerkmal unseres Pools ist die unterschiedliche Hauptspeicherausstattung (es gibt Maschinen mit 32, 64, 80, 96, 128 und 256 MB). Auf manchen Maschinen können größere Jobs nicht gerechnet werden während auf der anderen Seite auf manchen sogar mehrere kleine gleichzeitig laufen könnten. Die Jobklassen richten sich deswegen in erster Linie danach, wieviel Hauptspeicher ein Programm maximal nutzen kann (siehe Tabelle 6.1).

Eine Begrenzung der Rechenzeit wurde in diesen Klassen bisher nicht eingeführt (ein Job kann also unter Umständen mehrere Tage oder sogar Wochen laufen), da für diese Jobklassen meistens ein freier Prozessor zur Verfügung steht. Dennoch könnte ein einzelner Benutzer durch entsprechend rücksichtsloses Verhalten den kompletten Pool für andere blockieren: ein Problem, dem mit einer Vielzahl von Konfigurationsparametern begegnet wird.

Für die Rechner auf Basis des POWER2-Prozessors wurden eigene Jobklassen eingerichtet; zwar ist dieses Modell binärkompatibel zu den anderen RS/6000 Rechnern, um aber seine höhere Leistungsfähigkeit voll zu nutzen, müssen die Programme mit speziellen Optionen neu kompiliert werden[1]. Hier stehen nicht so viele Rechner zur Verfügung, so daß eine zusätzliche Klasse (`pwr2-8h`) eingerichtet wurde, in der die CPU-Zeit auf acht Stunden begrenzt ist.

Maschinen

Alle Informationen über die Ausstattung und Performance der Maschinen im Pool wird auf einer Maschine, dem *central manager* gesammelt. Er organisiert auch die Verteilung der Rechenaufträge. Bei einem kommerziellen Produkt wie dem LoadLeveler ist diese zentrale Aufgabe redundant ausgelegt — fällt der *central manager* aus, springt ein Ersatz für ihn ein. Jede Maschine im Pool kann man individuell konfigurieren: ob sie nun einen oder mehrere Jobs aus einer oder mehreren Klassen gleichzeitig laufen läßt, ob vielleicht ein Besitzer seine Maschine nur nachts und am Wochenende zur Verfügung stellen will, welchen Performancewert man ihr zuordnet und wieviel lokalen Plattenplatz man temporär zur Verfügung hat, um nur einige der Möglichkeiten zu erwähnen. Der LoadLeveler startet einen wartenden Job auf der schnellsten Maschine, die gerade frei ist. Eine schöne Eigenschaft des LoadLeveler ist die Möglichkeit, auf die interaktive Nutzung der Maschine zu reagieren: fängt bei einem Desktop-Rechner jemand an zu tippen oder die Maus zu bewegen, hält der LoadLeveler den Job vollständig an und läßt ihn erst wieder loslaufen, wenn sich eine Weile nichts mehr auf der Maschine getan hat. Oder man stoppt die Jobs, wenn der *load average* eine bestimmte Grenze überschreitet. Auf einem reinen Computeserver ist diese Möglichkeit natürlich nicht aktiviert. Für Maschinen, die grundsätzlich interaktiv genutzt werden, ist diese Möglichkeit äußerst wertvoll, denn mit der Zeit empfindet der

[1] `-qarch=pwr2 -qtune=pwr2`

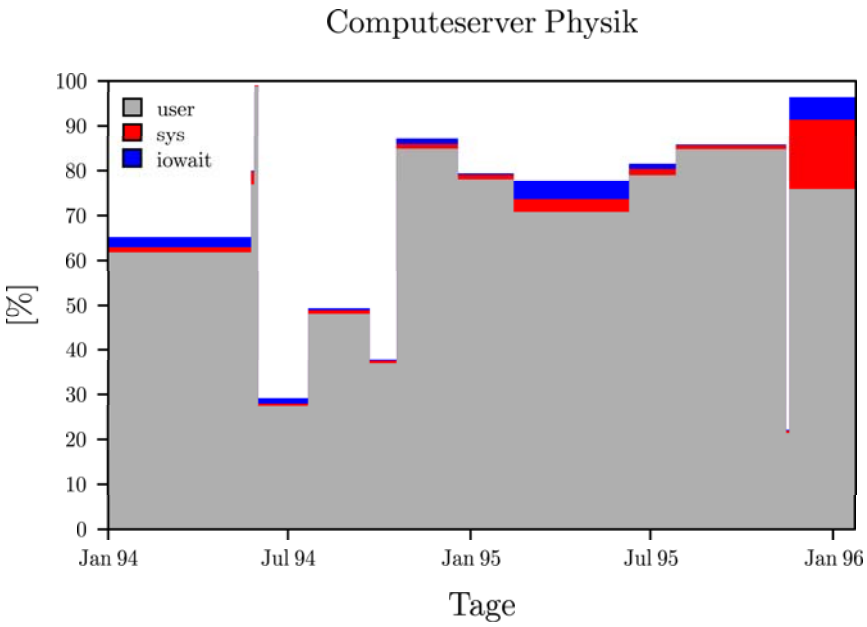


Abbildung 6.1.: Auslastung des Computeservers leopold (RS/6000-580, 256MB) basierend auf `iostat` Daten.

interaktive Benutzer jeden Hintergrundjob, und sei er noch so *nice*, als ziemlich lästig. Aktiviert man diese Einstellung, merkt er bei kleineren Jobs überhaupt nicht, daß von Zeit zu Zeit im Hintergrund gerechnet wird.

Prioritäten

Schickt ein Benutzer einen Job ab, wird ihm eine Priorität zugeordnet, welche die Startreihenfolge festlegt. Die Priorität wird im Augenblick durch den Ausdruck

```
SYSPRIO = (ClassSysprio * 1000)
+ (UserSysprio * 10) - QDate
- (UserRunningJobs * 20000) -
(GroupRunningJobs * 1000)
```

gesetzt. `-QDate` alleine würde eine FIFO-Queue erzeugen: die Jobs würden der Reihe nach abgearbeitet. Diese Reihenfolge wird aber modifiziert. Zum einen haben natürlich Jobklassen, die auf praktisch allen Rechnern laufen können, eine niedrigere Priorität als solche, die auf nur wenige Maschinen angewiesen sind (`ClassSysprio`). Innerhalb seiner Jobs kann der Benutzer noch eine eigene Reihenfolge festlegen (`UserSysprio`). Das Hauptkriterium ist aber, wieviele Aufträge eines Benutzers derzeit schon laufen (`UserRunningJobs`). Jeder laufende Job „kostet“ ihn 20 000 Sekunden. Hat man fünf Aufträge in Bearbeitung, kann ein anderer Benutzer mehr als einen Tag später seinen Auftrag abschicken und kommt trotzdem eher dran.

Zusätzlich ist die Anzahl von Jobs, die ein Benutzer in Bearbeitung haben kann, auf 15 begrenzt. Denn was hilft eine hohe Priorität, wenn keine Maschine frei ist? Damit vermindert man eventuell die Auslastung des gesamten Pools. Die Konfiguration des Systems optimal einzustellen ist ein schwieriger Prozeß.

Benutzerschnittstelle

Der Benutzer kann das System entweder über Kommandoeingaben (`llsubmit, llq, llclass, ...`) oder am Anfang über die graphische Schnittstelle `xloadl` ansprechen. Per `xloadl` kann man sich eine erste Steuerungsdatei (`<name>.cmd`) erstellen und einen guten Überblick über den Pool und seine aktuelle Konfiguration gewinnen. Für weitere Informationen kann der Benutzer im Online Hilfe-System InfoExplorer nachschlagen (`info -l LoadL`).

Auslastung

Mit Hilfe des LoadLeveler ist es in der Physik in den letzten Jahren gelungen, die lokal vorhandenen Workstations weit über das übliche Maß hinaus zu nutzen. Zum einen konnte die Auslastung der zentralen Computeserver nach dem Start im Produktionsbetrieb im April 1995 erheblich gesteigert werden (Beispiel: Abb. 6.1). Zum anderen wurde durch die Einbindung der Arbeitsplatzrechner eine Menge an Rechenzeit genutzt, die weit über die Möglichkeiten unserer Server hinausgehen. Die gesamte Rechenzeit, die über das LoadLeveler System abgewickelt wurde, erhöhte sich von 20 755 CPU-Stunden in 1995 auf 48 625 CPU-Stunden in 1996 (Abb. 6.2), wobei gleichzeitig die durchschnittliche Performance der Maschinen erheblich stieg: eine CPU-Stunde im Pool von 1996 ist erheblich mehr wert als noch 1995. Nach der Besetzung des Lehrstuhls Theoretische Pysik III im Sommer 1996 nahm sowohl die verfügbare Rechenleistung als auch der Bedarf erheblich zu und liegt aktuell bei etwa 2 000 Stunden/Woche.

Ausblick

Der Einsatz des Batchjob-Systems LoadLeveler hat sich als optimales Mittel erwiesen, die vorhandenen Ressourcen zu nutzen. Allerdings kommt es immer wieder zu „Staus“ in der Warteschlange für umfangreichere Jobs: die Programmlaufdauern liegen zu oft bei mehreren Tagen und so sind die wenigen POWER2-Modelle häufig blockiert. Natürlich muß man für aufwendigere Probleme nach München ans Leibniz-Rechenzentrum ausweichen, aber unsere Kontingente dort sind ohnehin „am Anschlag“. Eine Entlastung in diesem Bereich erhoffen wir uns von der baldigen Genehmigung eines größeren Computeservers für unsere Universität.

Für kürzere Jobs wird das vorgestellte System weiterhin die Grundlage bleiben. Und es stellt zusammen mit der floating-point orientierten Hardware, guten f77/f90/C/C++ Compilern, hardware-angepaßten und portablen Numerikbibliotheken, und einem stabilen Betriebssystem einen wesentlichen Grund dar, warum es Nischen gibt, die noch nicht von einer bestimmten Kombination von Mikroprozessor und Betriebssystem überrollt sind ... Aber jetzt höre ich wohl lieber auf.

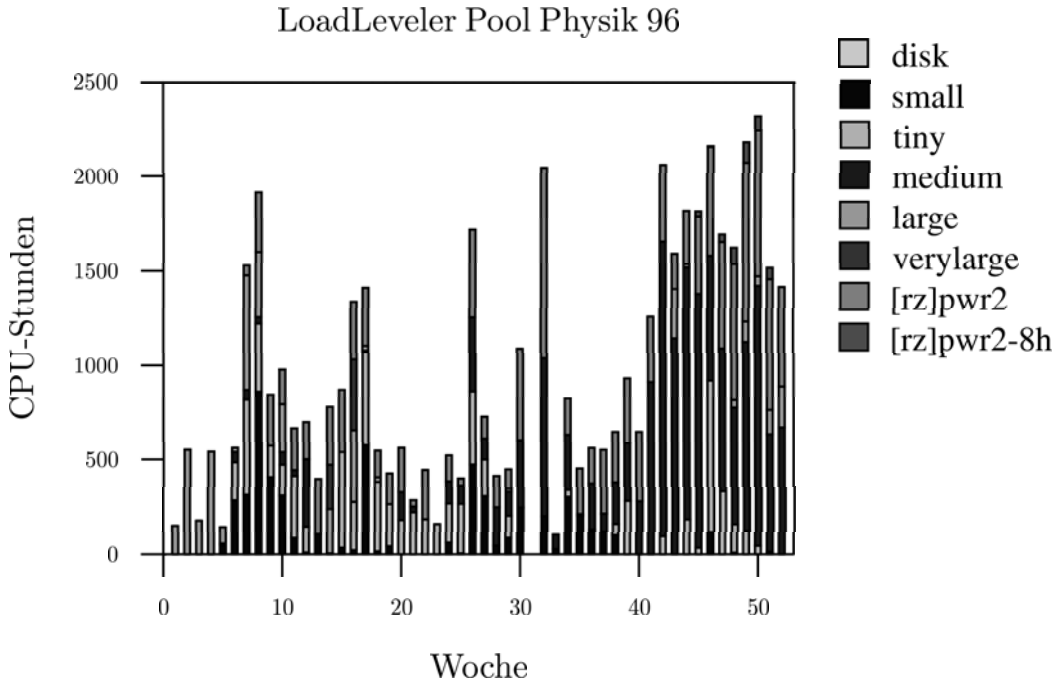


Abbildung 6.2.: LoadLeveler Nutzung pro Woche 1996. Da viele Jobs mehrere Tage und damit oft über die „Abrechnungsgrenze“ laufen, ist die CPU-Zeit der Jobs aufgetragen, die in der jeweiligen Woche fertig wurden: mit ein Grund für die Schwankungen in der Grafik.

7. Für Sie unter die Lupe genommen ...

Markus Zahn, Lehrstuhl für Praktische Informatik I

Ein wichtiges Thema in den bisherigen Ausgaben der ***connect*** *war stets die Nutzung des World Wide Web, denn kaum ein Netzdienst hat wohl mehr zur Popularität des Internets beigetragen. Über das WWW können beliebige Informationen für den weltweiten Zugriff zur Verfügung gestellt und miteinander verbunden werden.*

Die beiden in dieser Ausgabe besprochenen Bücher befassen sich ebenfalls mit dem Thema WWW, insbesondere mit der „WWW-Sprache" HTML (Hypertext Markup Language), die zur Gestaltung von ansprechenden Informationsseiten im Web verwendet wird.

An dieser Stelle möchten wir dem Carl Hanser Verlag danken, der uns diese beiden Bücher kostenlos für eine Besprechung zur Verfügung gestellt hat.

<HTML>-Ratgeber
gelesen von Markus Zahn

Autor Hinrich E. G. Bonin will mit dem <HTML>-Ratgeber „ein komplettes, preiswertes Arbeitsbuch zum Selbststudium und für Lehrveranstaltungen" zur Verfügung stellen. Mit diesem Buch soll eine „Bedarfslücke" bei den vielfach vorhandenen (Online-) Einführungen in HTML geschlossen werden, zumindest was den Einsatz in Bildungseinrichtungen betrifft.

Der Ratgeber verschreibt sich demzufolge der korrekten und planmäßigen Konstruktion von WWW-Publikationen. Neben einer Einführung werden im ersten Teil vor allem die zahlreichen Konstrukte der Hypertext Markup Language erläutert. Für die gebräuchlichen Bausteine der HTML-Sprache (die sogenannten *HTML-Tags*) wird jeweils eine Kurzbeschreibung der Funktionalität, die möglichen Attribute des Konstrukts sowie dessen Zulässigkeitsbereich geliefert. Der zweite Teil des Buchs befaßt sich mit fortgeschrittenen Techniken wie Interaktionen mit Formularen und Erzeugung von dynamischen Dokumenten durch *CGI-Scripts.* Desweiteren werden Themen wie der Aufbau eines WWW-Servers oder Sicherheitsaspekte im Zusammenhang mit dem WWW aufgegriffen. Im dritten Teil werden dem Leser etliche konzeptionelle Empfehlungen für den Aufbau gelungener und leicht zu wartender Publikationen im World Wide Web an die Hand gegeben. Am Ende jedes Abschnitts wird der vermittelte Stoff nochmals knapp zusammengefaßt.

Trotz dieses umfassenden Themenspektrums kann das Buch leider aus mehreren Gründen nicht überzeugen. Beispielsweise werden fein säuberlich die gebräuchlichen HTML-Bausteine aufgeführt, einen Hinweis, in welchen oder ab welchem der inzwischen recht vielfältigen HTML-Dialekte[1] ein beschriebenes Element vorkommt, sucht man jedoch vergebens. Gerade diese Kenntnis kann aber beim Erstellen von Online-Dokumenten von großem Nutzen sein.

Will der Leser einen Eindruck von der Mächtigkeit dynamischer Dokumente gewinnen, so wird ihm im selben Aufwasch noch die Programmiersprache *LISP* nähergebracht ... ein einfaches Beispiel inklusive einer Beschreibung der sich bietenden Möglichkeiten wäre sicher aufschlußreicher! Der zu vermittelnde Sachverhalt bleibt für Laien weitgehend unverständlich, ein Überblick über geeignete Sprachen zur Programmierung von CGI-Scripts fehlt gänzlich. Besser gelungen ist da

[1] Der ursprüngliche HTML-Standard wurde inzwischen mehrmals überarbeitet und erweitert. Standard ist momentan HTML-2.0, wenngleich viele Browser schon Teile der Diskussionsgrundlagen zu HTML-3.0 oder HTML-3.2 (einer abgespeckten Version von HTML-3.0) unterstützen. Außerdem werden von den bekannten Browser-Herstellern neue, nicht standardisierte Sprach-Elemente eingeführt.

schon der Abschnitt über die verschiedenen Gestaltungsmöglichkeiten von Formularen und deren Auswertung auf Serverseite.

Ein weiterer Kritikpunkt: Der Aufbau und die (sichere) Konfiguration eines WWW-Servers wird — wenn auch nur exemplarisch — am Beispiel des *CERN httpd,* Version 3.0 Prerelease 6 erläutert. Die endgültige Version 3.0 des Servers wurde Ende 1994 veröffentlicht und die Weiterentwicklung der Software wurde eingestellt, der <HTML>-Ratgeber erschien Mitte 1996 ...

Als Fazit muß man leider feststellen, daß das Buch nicht zum Kauf empfohlen werden kann. Zur Erstellung statischer Dokumente ist man mit den (allerdings oftmals in Englisch abgefaßten) Online-Dokumentationen besser beraten. Für die Programmierung von CGI-Scripts zur Erstellung dynamischer Dokumente für die Behandlung von Formularen ist man ohnehin auf spezielle Literatur angewiesen.

Bonin, Hinrich F. G.:
<HTML>-Ratgeber: Multimediadokumente im World Wide Web programmieren
Hanser Verlag, 1996
ISBN 3-446-18500-3
Preis 38.- DM, 221 Seiten

WWW — Anbieten und Nutzen

gelesen von Thomas Konert

Das Ziel des Buches *WWW — Anbieten und Nutzen* von Uwe Bergmann ist es, einen detailierten Einblick in die Nutzung der Möglichkeiten des WWW zu geben. Dabei gibt der Autor sowohl eine Einführung in die Bedienung verschiedener Browser, als auch eine sehr genaue Beschreibung zur Konfiguration eines Web-Servers für eigene Präsentationen im Internet. Das Buch beginnt mit einer kurzen Darstellung der Entwicklung des WWW und vermittelt dem Leser danach die benötigten Grundkenntnisse zum Verständnis der nachfolgenden Kapitel. Dazu wird insbesondere die Benutzung eines Browsers anhand zahlreicher Abbildungen erläutert.

In Kapitel zwei geht es dann schon richtig zur Sache: Die Einrichtung eines eigenen WWW-Servers wird besprochen. Die Beschreibung ist dabei sehr detailiert und sollte jeden Leser mit Unix-Kenntnissen zur korrekten Installation eines Servers befähigen. Außer der normalen Inbetriebnahme und Konfiguration des Servers wird noch die Nutzung als Proxy/WWW-Cache dargestellt. Während bis hier alle Erläuterungen sehr ausführlich waren, ist die anschließende Behandlung von CGI-Scripten zur Implementation von Interaktivität etwas kurz geraten. Auch sollte der Leser zum vollen Verständnis über Kenntnisse in der Shell-Programmierung (sh, awk, perl) verfügen. Als Überblick über die sich eröffnenden Möglichkeiten ist die Darstellung aber ausreichend, zumal man vor umfangreicher CGI-Programmierung ohnehin weiterführende Literatur konsultieren sollte. Zum Abschluß des zweiten Kapitels geht der Autor dann noch auf Sicherheitsaspekte ein. Diese gerade mal 14 Seiten Text hinterlassen bei mir aber nicht unbedingt ein wohlig sicheres Gefühl, so daß auch hier die Lektüre spezieller Literatur angeraten ist, insbesondere wenn man einen Firmenserver im Internet verfügbar machen möchte.

In den Kapiteln drei und vier wird die Sprache HTML beschrieben. Der Aufbau ist strukturiert und zu fast allen beschriebenen Sprachelementen sind erläuternde Abbildungen vorhanden. Somit hat man bereits beim Durcharbeiten der Gestaltungsmöglichkeiten eine konkrete Vorstellung vom fertigen Dokument. Der Autor erläutert sowohl den HTML-2.0-Standard als auch die bis jetzt nur teilweise umgesetzte Definition von HTML-3.0.

Das letzte Kapitel vermittelt durch die teilweise Beschreibung des *Hypertext Transfer*

Protocols (HTTP) einen guten Einblick in die Vorgänge beim „Surfen“.

Abgeschlossen wird das Buch durch einen sehr nützlichen Anhang, der insbesondere eine übersichtliche HTML-Befehlsreferenz enthält. Der Abdruck der HTML-2.0 Definition wird hingegen nur für wenige Leser von Interesse sein. Wer das Buch als Nachschlagewerk verwenden will, wird sich über den ausführlichen Index freuen.

Insgesamt macht das Buch einen gemischten Eindruck. Gut geeignet ist es für denjenigen, der sich schnell einen Überblick über die Möglichkeiten des WWW verschaffen möchte. Für die konkrete Umsetzung, also z. B. für den Aufbau eines eigenen WWW-Servers, ist die Lektüre zusätzlicher Bücher unabdingbar.

Bergmann, Uwe:
WWW — Anbieten und Nutzen.
Hanser Verlag, 1996
ISBN 3-446-18458-9
Preis 64.– DM, 349 Seiten

8. Notiert!

Siegfried Stindl, Planung Kommunikationssysteme

Novell im Wissenschaftsnetz

Beim DFN-Verein wurde ein weiteres Forum installiert. Es beschäftigt sich mit „Novell im WiN“. Im Augenblick beteiligen sich ca. 30 Institutionen in diesem Forum. Hier werden Probleme wie eindeutige Adressierung, deutschlandweiter NDS-Server, Preispolitik etc. mit kompetenten Vertretern von Novell diskutiert. Interessenten wenden sich bitte an den Sprecher des Forums, Siegfried Stindl, eMail: stindl@Uni-Augsburg.de oder an den Vertreter des DFN-Vereins in diesem Forum, Herrn Pattloch, eMail: pat@dfn.de.

least cost routing im DFN

Der DFN-Verein hat für Anfang Januar 1997 angekündigt, ein Corporate Network für seine Mitglieder einzurichten. Es wird dann nicht mehr lange dauern, daß von Augsburg nach München oder Hamburg zum Citytarif telefoniert werden kann. Für die Universität Augsburg bedeutet dies eine Einsparung von Telefonkosten in Höhe von ca. 100 000.– DM pro Jahr. Dieses Corporate Network wird dann im Laufe der Zeit auf das B-WiN physikalisch übertragen. Dazu findet Ende Januar beim DFN-Verein ein Symposium für fortgeschrittene Kommunikationstechnik statt. Unter anderem wird auch über die Themen „Telefonie im B-WiN und ATM“ diskutiert werden.

Kostenvorteile bei der Telekom durch die neuen Tarife CityPlus und CityWeekend

Für Universitätsangehörige, die sich ins Universitätsnetz, sei es zum telefonieren, oder zur Datenkommunikation, einwählen wollen, können dies bei den ersten 400 Einheiten jetzt zum halben Preis tun. Einzige Voraussetzung ist, daß Sie zu Hause einen ISDN-Anschluß bzw. ein analoges Telefon, das an einem digitalen Amt hängt, haben. Sie können in dieses Angebot bis zu fünf besonders häufig angerufene Telefonnummern im Citybereich einbeziehen. Für all diese Verbindungen werden dann 0,06 DM pro Einheit berechnet.

Für Leute, die auch am Wochenende sehr viel arbeiten, gibt es noch den CityWeekendtarif. Mit 5.– DM sind Sie dabei. Sie können dann an allen Samstagen, Sonntagen, bundeseinheitlichen Feiertagen, Heilig Abend und an Sylvester ganztägig zum Mondscheintarif telefonieren.

9. Die Leser-Ecke

Liebe **connect**-Redaktion,
sehr geehrter Herr Professor Töpfer,

als **connect**-Leser, der Ihrer Zeitschrift gegenüber positiv eingestellt ist und ihr immer wieder wertvolle Informationen entnimmt, hätte ich eine Bitte, die ich — vor allem angesichts der Kürze des Lebens generell und (Spaß beiseite) angesichts des Umfangs und des Schwierigkeitsgrades von **connect** — an Sie richten möchte:

Wäre es möglich, die Artikel in **connect** den zahlreichen interessierten, aber leider oft nur teil-informierten „EDV-Laien“ etwas zugänglicher zu machen? (Die Klage, das sei alles Fachchinesisch, höre ich recht oft). Könnte man z. B. den einzelnen Artikeln kurze „Summaries“ von ein paar Zeilen voranstellen, damit Leser wissen, was sie erwartet? Oder könnte man — ähnlich wie in der Computer-Beilage der SZ — gelegentlich wichtige oder neue Begriffe am Rande glossieren? Dies würde z. B. einem Anglisten und Literaturwissenschaftler wie mir sehr helfen, wenn ich schnell feststellen muß, ob „Neue Versionen von Maple und SPSS“ ein Artikel ist, den ich studieren müsste oder den ich einfach überschlagen kann. Über eine positive Reaktion würde ich mich sehr freuen. Mit den besten Wünschen für die Zukunft

Rudolf Beck (Lehrstuhl für Englische Literaturwissenschaft)

Sehr geehrter Herr Professor Beck,

vielen Dank für Ihre konstruktive Kritik. Wie Sie sehen, haben wir Ihre Vorschläge, zumindest teilweise, gleich in dieser Ausgabe umsetzen können. Schließlich liegt es auch uns am Herzen, daß die **connect**-Leser zufrieden sind. Über weitere Anregungen würden wir uns sehr freuen,

die *Redaktion.*

10. Ausstattung aller CIP-Pools

Wirtschaftswissenschaftliche Fakultät

CIP-Grundausbildung I

Gebäude/Raum: WiSo, Raum 1114

Fakultät: WiSo

Ansprechpartner: Herr Carl-Martin Preuß

Ausstattung: 30 Arbeitsplätze, 486 PCs, 17“ Monitore

Peripherie: Laserdrucker, Beamer am Dozentenarbeitsplatz

Vernetzung: Lokal und Internet

Software: Windows 3.11, MS Office Prof. 4.3, SPSS, C++, dBASE, diverse Spezialsoftware, WWW, FTP, Ewan, Eudora, News-Reader, Gopher

Nutzung: Vorrangig für Studierende der WiSo

CIP-Grundausbildung II

Gebäude/Raum: WiSo, Raum 2113

Fakultät: WiSo

Ansprechpartner: Herr Carl-Martin Preuß

Ausstattung: 30 Arbeitsplätze, Pentium-PCs, 17“ Monitore

Peripherie: Laserdrucker, Scanner, Beamer am Dozentenarbeitsplatz

Vernetzung: Lokal und Internet

Software: MS Office Prof. 7.0, SPSS, C++, Corel Draw, WWW, FTP, Ewan, Eudora, News-Reader, Gopher

Nutzung: Vorrangig für Studierende der WiSo

Juristische Fakultät

Jura01

Gebäude/Raum: F2, Alte Universität

Fakultät: Jura

Ansprechpartner: Herr Martin Popp

Ausstattung: 19 PCs 486 mit je 16 MB Arbeitsspeicher

Peripherie: HP Drucker 4P

Vernetzung: Lokales Netware 3.12-Netz über Ethernet-Bus

Software: Windows 3.11, Netscape, Eudora, CD-ROM Recherche, MS-Office Paket

Nutzung: Für Studenten und Lehrstuhlmitarbeiter gemäß Betriebs- und Benutzungsordnung der Juristischen Fakultät

Philosophische Fakultät

CIP-Pool Phil

Gebäude/Raum: N1, Raum 1009/Bibliothek

Fachbereich: Phil I/II, Katholische Theologie

Ansprechpartner: Dr. Markus Ohlenroth

Ausstattung: 14 PCs 486 in 1009, 10 PCs 486 in Bibliothek

Peripherie: 1 Scanner, 2 Laserdrucker

Vernetzung: Novell 3.11, 5 PCs in N1 mit Anbindung via IP ans Hochschulnetz

Software: Windows 3.x MS-Word, Paradox, dBASE, Word Perfect für Windows und DOS, Konkordanzprogramm, Scanner- und Bildbearbeitungssoftware

Nutzung: Für Studenten von Phil I/II, Katholische Theologie

CIP-Pool Schillstraße

Gebäude/Raum: Schillstraße

Fachbereich: Phil I

Ansprechpartner: Dr. Markus Ohlenroth

Ausstattung: 8 Macintosh IIs

Peripherie: 1 Laserdrucker, 5 Keyboards

Vernetzung: Apple Talk, 1 Gerät mit IP-Anbindung ans Hochschulnetz

Software: MS-Word, Bildbearbeitungsprogramme und Musikprogramme zum Sampeln, Komponieren und Verfassen von Partituren

Nutzung: Für Studenten der Musikwissenschaften und Kunsterziehung

Mathematisch-Naturwissenschaftliche Fakultät

Macintosh-CIP-Pool

Gebäude/Raum: MNF, Raum 1012/1013

Fachbereich: Rechenzentrum

Ansprechpartner: Herr Rolf Leye

Ausstattung: Ein Server, 14 Arbeitsplätze, Macintosh Power PCs, 24 MB Hauptspeicher, 350 MB Festplatte, System 7.5, Ethernet-Schnittstelle

Peripherie: Apple Postscript Laserdrucker, Farbscanner

Vernetzung: Ethernetvernetzung, Protokolle AppleTalk und TCP/IP

Software: Clarisworks, Canvas, DataDesk, Scanner-Software, JMP, Manet, Maple V R4, Microsoft Excel, Minitab, Netscape, Telnet, Omnipage, Adobe Photoshop, Regard, Statistica, Word Perfect 3.0, Metrowerks Code Warrior

Nutzung: Für Studenten der MNF, sowie Studenten des Fachs Sport

PC-Pool der MNF

Gebäude/Raum: MNF, Raum 2040

Fakultät: MNF

Ansprechpartner: Herr Wolfgang Kolbe

Ausstattung: 18 PCs 486 DX/2-66, 8 MB RAM, 120 MB HD, 3,5“ und 5,25“ FD, 17“ Monitor, Maus

Peripherie: 4 Laserdrucker OKI OL-400e, 1 Netz-Laserdrucker HP LaserJet 4, 1 Netz-Laserdrucker OKI OL-800

Vernetzung: Ethernet mit IPS/SPX und TCP/IP, 10 Mb/s

Software: Windows for Workgroups 3.11, Borland Pascal, Microsoft Visual C++, SPSS/PC für Windows, TEX, Maple V R3

Nutzung: Für Studenten zur Grundausbildung der MNF

Datenbank CIP-Pool

Gebäude/Raum: MNF1, Raum 2035

Fakultät: MNF

Ansprechpartner: Dr. Gerhard Köstler

Ausstattung: 6 Workstations HP 9000/712 mit HP-UX 9.x/10.x, 3 Pentium PC mit Windows 3.11 und 95, 4 X-Terminals HP 700/X

Peripherie: 1 Postscript-Drucker HP Laserjet 4M, 1 Farbscanner HP Scanjet

Vernetzung: Alle Rechner sind an das lokale Netz angeschlossen.

Software: Entwicklungssysteme: C, C++, DB-Systeme: TransBase 4.2.2, DB2 2.1, O2 4.6, Versant 3.0.10, Coral 1.5, Bilddatenbanksystem Ultimedia Manager, Entity-Relationship Designtool S-Designer

Nutzung: Für Studenten zur Fortgeschrittenenausbildung in Informatik

AIX-Pool

Gebäude/Raum: MNF, Raum 1015

Fakultät: MNF

Ansprechpartner: Herr Wolfgang Kolbe

Ausstattung: 19 IBM Power PCs, AIX 4.1.4

Peripherie: Laserdrucker, IBM 7207-001 Streamer (150 MB)

Vernetzung: Über Ethernet (BNC) an das Universitätsnetz

Software: C, C++, Maple, diverse PD-Software

Nutzung: Für Studenten zur Fortgeschrittenenausbildung in Mathematik/Informatik

RZ-Pool Physik

Gebäude/Raum: A1, Raum 009A

Zentrale Einrichtung: Rechenzentrum

Ansprechpartner: Herr Ralf Utermann

Ausstattung: 1 Server IBM-320H mit 32 MB, 7 Clients IBM-320H mit 16 MB ($1x32$ MB), 400 MB, 19“-Monitor (Mono)

Peripherie: CD-ROM, 1 GB, QIC-Tape, Laser-Drucker (QMS-410 PS)

Vernetzung: Ethernet, NIS/NFS Pool

Software: AIX 3.2.4/3.2.5, übliche PD-Software

Nutzung: Vorrangig für Studenten der Physik

A. Ansprechpartner im Rechenzentrum

Nachstehend finden Sie eine Liste der Aufgabenbereiche mit den verantwortlichen Kontaktpersonen. Die Vorwahl für alle Telefon-Nebenstellen ist (0821) 598. Zudem können alle Mitarbeiter über den Nebenstellen-Anschluß 20 28 per Fax, oder nach dem Schema *Vorname.Nachname@RZ.Uni-Augsburg.DE* per eMail erreicht werden.

Wissenschaftliche Leitung:

Professor Dr. Hans-Joachim Töpfer
Lehrstuhl für Praktische Informatik I

Sekretariat: Frau Gabi Hollmann
Raum 2030, ☎ –21 74

Technische Leitung:

bis 31.01.97:
Jürgen Pitschel
Rechenzentrum

Sekretariat: Frau Heidi Wieninger
Raum 2046, ☎ –20 00

ab 01.02.97: N.N.

Planung Kommunikationssysteme:

Siegfried Stindl
Rechenzentrum
Raum 1020, ☎ –20 06

Allg. Dienste, Anwendersoftware:

bis 31.01.97:
Jürgen Pitschel
Rechenzentrum

Sekretariat: Frau Heidi Wieninger
Raum 2046, ☎ –20 00

ab 01.02.97: N.N.

Netzbetrieb/Netzdienste:

Dr. Milos Lev
Rechenzentrum
Raum 2044, ☎ –20 08

Betriebssysteme und Server:

Dr. Leopold Eichner
Rechenzentrum
Raum 2045, ☎ –20 04

Verwaltungs-DV:

Gunter Abraham
Rechenzentrum
Raum 2054, ☎ –20 38

Die Räume der Mitarbeiter liegen sämtlich im Gebäude der Mathematisch-Naturwissenschaftlichen Fakultät und des Rechenzentrums, Universitätsstraße 8.

B. Im Rechenzentrum erhältliche Campus- und Sammellizenzen

Gunter Abraham, Rechenzentrum

Zur Zeit können mehrere Software-Produkte für Zwecke der Lehre und Forschung zu günstigen Bedingungen über das Rechenzentrum bezogen werden. Dieser Anhang enthält eine Kurzbeschreibung dieser Programme und eine Übersichtstabelle, die deren Verfügbarkeit auf verschiedenen Plattformen zusammenfaßt.

Produkt		**Plattform**	
		Personal-computer	Unix-Systeme
AIT	Cray-Workstation-Verbindungs-werkzeuge		SunOS 4.1 IRIX 3.3+ ULTRIX 4.1
Autodesk	CAD-Programm	DOS Windows 3.1 Windows 95 Windows NT	X
AVS	Visualisierungssystem	Windows 95 Windows NT	X
AXIOM	Computer-Algebra-System		IBM AIX
CAP	Verschiedene Softwarepakete der Firma WordPerfect (heute: Corel)	DOS Windows Macintosh	X
Claris	Verschiedene Softwarepakete der Firma Claris	Windows Macintosh	
FuLP	Verschiedene Softwareprodukte der Firma Borland	Windows DOS	
IBM-Software	Compiler und weitere Software der Firma IBM		IBM AIX
IDL	Graphik- und Bildverarbeitung		IBM AIX
KHOROS	Visualisierungssystem		X
Maple	Computer-Algebra-System	X	X
Micrografx		Windows	
MLA	Netware und weitere Produkte der Firma Novell	DOS	
NAG	Fortran-Unterprogrammbibliothek		X
OnNet 2.1	TCP/IP für PCs	Windows 95 Windows NT	
PC/TCP	TCP/IP für PCs	DOS Windows	
Select	Microsoft-Software aus den Bereichen Anwender-, System- und Server-Software	DOS Windows Macintosh	
Dr. Solomons Anti-Virus-Toolkit	Software für Schutz gegen Computerviren	DOS Windows 3.x Windows 95 Windows NT OS/2 Novell Netware 3.x/4.x	

X = auf allen gängigen Plattformen der jeweiligen Rubrik verfügbar
\+ = diese Systemversion oder höher

Produkt		Plattform	
		Personal-computer	Unix-Systeme
SPSS	Statistikprogrammsystem	DOS Windows 95 Windows NT	
TUSTEP	System von Textverarbeitungs-programmen	DOS	
Visio	Software-Produkte der Firma Visio International Ltd.	Windows 3.x Windows 95 Windows NT	

X = auf allen gängigen Plattformen der jeweiligen Rubrik verfügbar
+ = diese Systemversion oder höher

Nähere Informationen zu den aufgeführten Software-Produkten erhalten Sie unter der Telefonnummer 598–20 42 (Frau Kötterle), –20 38 (Herr Abraham) oder –20 18 (Herr Umpfenbach).

C. Lehrveranstaltungen im Sommersemester

Einführung in das Betriebssystem Windows 95	
Anmeldung notwendig!	Kompaktwoche Tutschke
	Termin: 14. 4.–18. 4. 1997 Gebäude: RZ Raum 2040 (DOS-CIP-Raum) Zeit: 9.30–11.30 Uhr

Kommunikationssoftware auf Macintosh	
Anmeldung notwendig!	Kompaktwoche Leye/Bernert
	Termin: 21. 4.–25. 4. 1997 Gebäude: RZ Raum 1013 (PowerMac-CIP-Raum) Zeit: 8.30–11.30 Uhr

Einführung in UNIX	
Anmeldung notwendig!	Kompaktwoche Lev
	Termin: 21. 4.–25. 4. 1997 Gebäude: RZ Raum 1015 (AIX-CIP-Raum) Zeit: 8.30–10.00 Uhr

Einführung in die Statistiksoftware SPSS	
Anmeldung notwendig!	Kompaktwoche Umpfenbach
	Termin: 21. 4.–24. 4. 1997 Gebäude: RZ Raum 2040 (DOS-CIP-Raum) Zeit: 10.30–12.00 Uhr und 13.30–15.00 Uhr

Anmeldung für alle Veranstaltungen bitte im Sekretariat des Rechenzentrums, Telefon-Nummer 598–20 00.

Außerdem wird auf die Vorlesung „Paralleles und verteiltes Rechnen“ von Professor Töpfer im Rahmen der Vorlesungen des Instituts für Informatik hingewiesen.

D. Spezialgeräte im Rechenzentrum

Dr. Markus Ohlenroth und Werner Bauer, Rechenzentrum

CD-ROM Brenngerät

Wie schon in **connect** 2/1996 ausführlich berichtet, bietet das Rechenzentrum sowohl Universitätsangehörigen als auch Studenten die Möglichkeit, zum Selbstkostenpreis CD-ROMs zu brennen. Hierzu besitzt das Rechenzentrum einen Yamaha CDR 100 CD-ROM Brenner. Damit können CD-ROMs für verschiedene Computersysteme in verschiedenen Formaten gebrannt werden. Auf eine CD passen, je nach Format, bis zu 650 MB an Daten, bzw. 74 Minuten Audio-Spuren. Als Brennsoftware wird das Astarte Toast CD-ROM Pro Programm für Apple Macintosh verwendet.

Die von der Astarte Toast CD-ROM Pro Software unterstützten Formate sind: Macintosh HFS, Macintosh HFS Multisession, ISO 9660, ISO 9660 XA Multisession, Macintosh/ISO Hybrid, Audio CD, Mixed Mode, Photo CD, Photo CD Portfolio, CD-i, Video CD, Generic CD und Generic CD XA.

Achtung! Die unterstützten Formate können zwar gebrannt werden, aber die Daten müssen im richtigen Format vorliegen. Das Brennen einer CD inklusive Rohling kostet 20.– DM. Für Anmeldung und Informationen wenden Sie sich bitte an Herrn Bauer im Rechenzentrum. eMail: Werner.Bauer@RZ.Uni-Augsburg.DE

Scanner

Das Scannersystem „Kurzweil K-5200“ steht für Praktikums-, Diplom-, oder Doktorarbeiten im Raum 1028 des Rechenzentrums zur Verfügung. Es besteht aus:

- Scanner für Papierformate $\leq$ A4 mit automatischem Einzelblatteinzug
- RISC Komponente
- Windows Software zur Ansteuerung des Scanners

Das Scannersystem ist vorrangig für Texterkennung (OCR) ausgelegt, es können jedoch auch Grafiken (schwarz/weiß) und gemischte Vorlagen verarbeitet werden.

Um Doppelbelegungen zu vermeiden, muß der Scanner beim Rechenzentrum reserviert werden. Die notwendige Voranmeldung nehmen Frau Beer oder Frau Kötterle gern entgegen.

E. Datennetz der Universität Augsburg

Siegfried Stindl, Planung Kommunikationssysteme

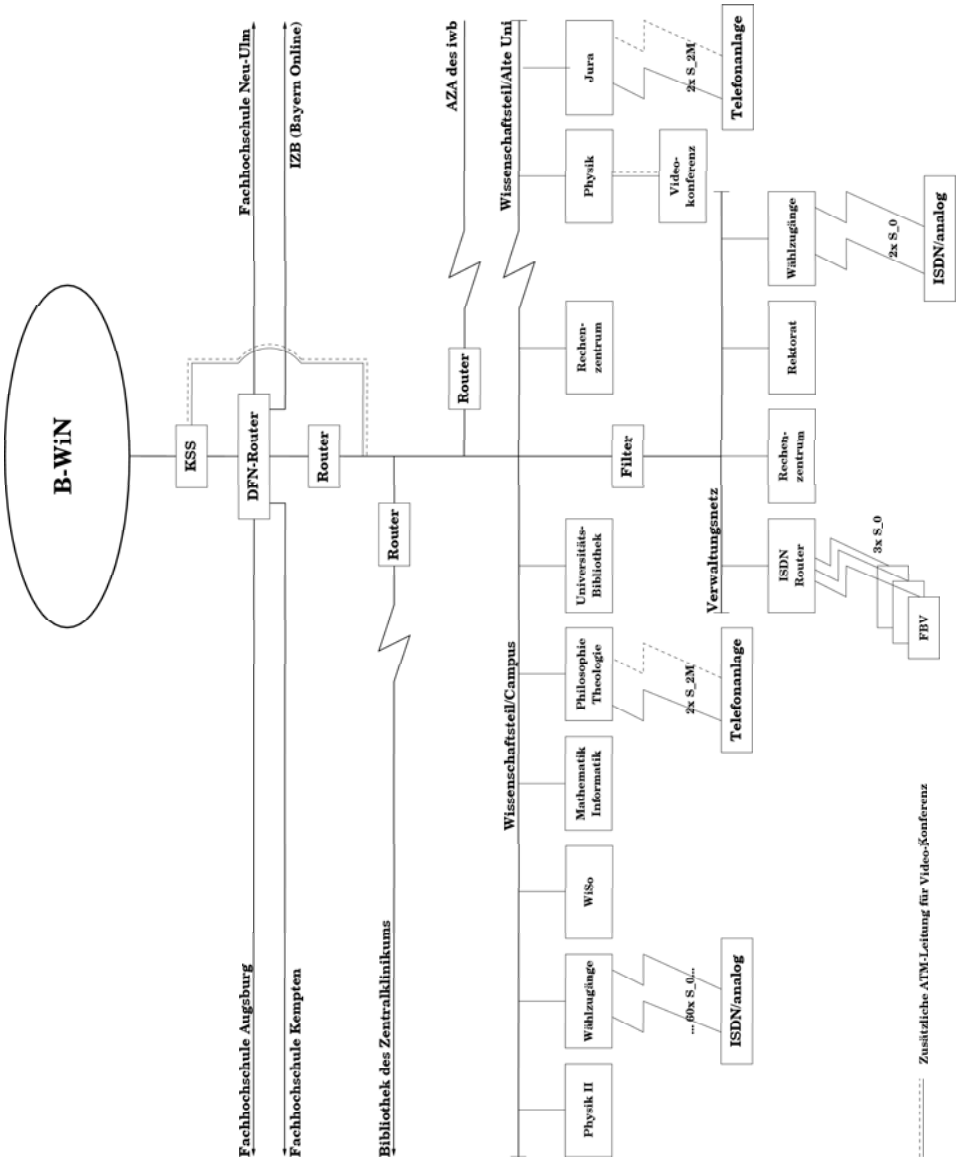


Abbildung E.1.: B-WiN-Anschluß

Beendigung des X.25-Betriebes

Der X.25-WiN-Betrieb wurde zum 31.12.1996 eingestellt. Für Bibliotheksanwendungen, die noch nicht umgestellt werden konnten, steht ein X.25-Tunnel zur Generaldirektion der bayerischen staatlichen Bibliotheken zur Verfügung. Für Benutzer, die früher über X.25 Rechner im WiN erreicht haben, steht meist ein Telnetzugang zur Verfügung. Beispielhaft seien folgende Datenbankrechner aufgeführt:

Datenbank	Telnet
DIMDI	grips.dimdi.de
ECHO	echo.lu
eLib	elib.zib.de
GPS	no5.leipzig.ifag.de
Juris	juris-sb.de
MerKoWi	über 129.143.3.27
STN	stn.fiz-karlsruhe.de

Für X.25-WiN-Rechner, die nicht über Telnet erreichbar sind, gibt es folgendes Gateway:

WiN-DTE-Adresse:	45050966003
IP-Adresse:	129.143.3.1

Für Datex-P-Rechner wird gerade in München bzw. in Erlangen ein kostenpflichtiges Gateway installiert. Bei Bedarf wenden Sie sich bitte an die Informationsstelle des Rechenzentrums, oder senden uns eine eMail.

Impressum

connect wird herausgegeben im Auftrag des Rechenzentrums der Universität Augsburg

Auflage: 1 000 Exemplare

Ausgabe: 5. Ausgabe

Redaktion: Professor Dr. Hans-Joachim Töpfer (verantwortlich), Annja Huber, Markus Zahn

Layout und Satz: Annja Huber, Markus Zahn

Redaktionsanschrift:

Redaktion **connect**
Rechenzentrum der Universität Augsburg
D – 86 135 Augsburg
connect@RZ.Uni-Augsburg.DE
http://www.RZ.Uni-Augsburg.DE/connect/

Die nächste Ausgabe des Mitteilungsblatts **connect** erscheint im Juli 1997, Redaktionsschluß ist der 30. Mai 1997.