

Brandschutzmauer für das Internet?!

**Erfahrungsbericht der UB Hohenheim über die Einrichtung
von Internet-Arbeitsplätzen für Benutzer ¹⁾**

Elisabeth Niggemeyer

Sie wissen, was das Internet ist? Sicherlich! Nachdem jede gute Tageszeitung im Feuilleton die Internet-Spalte eingeführt hat, gibt es für die Wörter Internet, Intranet, WWW, Netscape wahrscheinlich keinen Erklärungsbedarf.

Auch muß an dieser Stelle keine Neuauflage der Definition *Benutzer einer Bibliothek* erfolgen. Was aber will eine Bibliothek ihren Benutzern bieten?

Nehmen wir die Sichtweise des Benutzers an:

Er stellt sich vor, „ein Maximum an Information aus der Bibliothek mitzunehmen.... Er möchte sich darüber informieren, welche Veröffentlichungen in seinem Fachgebiet interessant sind, möchte dieser idealerweise in digitaler Form erhalten oder zumindest den Standort lokalisieren und den Bestell-/Ausleihvorgang einleiten. Daneben ist es praktisch für ihn, den Informationsaustausch per E-Mail zu pflegen, seine Literaturliste per Datenbank zu verwalten und seine Texte mit einem Textverarbeitungssystem zu bearbeiten.“²⁾

Daher bieten wir an der UB Hohenheim, an einem PC alle zur Zeit möglichen Bibliotheksangebote an. In der Praxis ist das ein Angebot von E-Mail bis OPAC, von WWW bis CD-ROM, von Windows-Anwendungen bis Hosts. Ich möchte mich im weiteren auf den Aspekt des Internet-Zuganges be-

schränken. Der Internet-Zugang ist eine Ressource, deren Aspekte uns niemals 100% bekannt sein werden und deren Zwiespalt zwischen populär und wissenschaftlich ständig gegeben ist.

Während die University of Westminster in einem Erfahrungsbericht über eine ähnliche Ausstattung und Konzeption schreibt: „Internet access in the library computer room ... was not as well used“,³⁾ kann ich für die Universität Hohenheim nur feststellen: Internet ist der Renner. Eine Benutzerin mailt dazu: „Einfach toll, was die UB Hohenheim an elektronischen Angeboten zur Verfügung stellt“. Wir vertrauen bei der Bereitstellung des Internet „auf die Verantwortung des ‘guten’ Teilnehmers im Internet“.⁴⁾ Für die Benutzer der UB Hohenheim ist der Zugang zum Internet zur Zeit kostenfrei. Surfen im Internet ist erlaubt, selbstverständlich in den Grenzen, die die Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste auferlegt. Dort wird z.B. aufgeführt, daß die Nutzung der DFN-Dienste dann mißbräuchlich ist, wenn das Verhalten der Benutzer gegen einschlägige Schutzvorschriften (u.a. Strafgesetz, Jugendschutzgesetz, Datenschutzrecht) verstößt. Weiter heißt es: „Aufgrund ihrer Fachkunde ist bei den Benutzern der Kommunikationsdienste die jeweilige, insbesondere strafrechtliche Relevanz etwa der Computerkriminalität, des Vertriebs pornographischer Bilder und Schriften oder des Diebstahls, der Veränderung oder sonstige Manipulation von bzw. an Daten und Programmen als bekannt vorauszusetzen. Diese Fachkenntnis bezieht sich auf die Sensibilität der Übertragung von Daten, die geeignet sind, das Persönlichkeitsrecht anderer und /oder deren Privatsphäre zu beeinträchtigen oder bestehende Urheberrechte bzw. auf diesen gründende Lizenzen zu verletzen“.⁵⁾ Die DFN Benutzungsrichtlinien haben wir durch eigene Sicherheitsrichtlinien⁶⁾ konkretisiert.

Im Internet ist als Verhaltenskodex die „Netiquette“ üblich. Dabei handelt es sich leider nicht um ein Standardwerk mit juristisch einwandfreier Grundlage, sondern um ein Regelwerk, das in ca 50 verschiedenen Versionen im Internet vorliegt. Die Netiquette gibt Sitten und Gebräuche wieder, die sich allgemein einbürgert haben.⁷⁾

Die Frage, die sich nun stellt, ist: Halten sich unsere Benutzer daran? Genau an diesem Punkt tauchen Zweifel auf: „Studenten gucken dreckige Internet-Pornos“ berichtet ein Blatt mit hoher Auflage. Weiter heißt es: „Für den Benutzer ist es ein Vergnügen, für den Steuerzahler ärgerlicher Mißbrauch, der Geld kostet.“⁸⁾ Höchstwahrscheinlich handelt es sich hier um eine fingierte Schlagzeile. Wir kontrollieren regelmäßig, was an den multifunktionalen Benutzerplätzen läuft. In erster Linie werden die Rechner genutzt für die CD-ROM Recherche, für OPAC, für Recherche in Verbundkatalogen über WWW, für Recherchen, die über unsere Homepage gelinkt sind. Die Struktur unserer

PC-Arbeitsoberfläche ist auf die bibliothekarischen Bedürfnisse abgestimmt. Nur der PC- und Interneterfahrene Benutzer geht über unsere Angebote hinaus und öffnet weitere Web-Pages. Und genau an diesem Punkt kann natürlich auch ein Fünkchen Wahrheit an obiger Schlagzeile dran sein, denn es gibt immer den Benutzer, der meint, Gebote sind dazu da, nicht beachtet zu werden.

Als wir Mitte 1994 den Web-Service zur Verfügung stellten, haben wir dies nur auf dem Campus publik gemacht. Wir konnten sicher sein, es nur mit Universitätsangehörigen zu tun zu haben, die auch noch sehr unbedarft mit diesem Medium umgegangen sind. Inzwischen hat die Stuttgarter Presse unser Angebot HELL = Hohenheim Electronic Library publik gemacht: „In der Hölle brennt Tag und Nacht das Licht.“⁹⁾ Unter die Universitätsangehörigen mischen sich nun Benutzer, die den PC-Raum der Universitätsbibliothek in den verschiedensten Varianten nutzen.

Nun haben wir einen echten Handlungsbedarf, die Benutzer exakt zu identifizieren. Daher müssen wir der Frage nachgehen:

Welche Möglichkeiten eröffnet ein Internet-Zugang einem Benutzer?

Welche Maßnahmen können wir ergreifen, um mißbräuchliche Nutzung des Internet zu vermeiden?

Computerkriminalität

Grundsätzlich können Benutzer die PC-Konfiguration zerstören, Dateien beschädigen, Viren aufsetzen. Könnten wir dies einem Benutzer nachweisen, so könnten wir das deutsche Recht in Anspruch nehmen: § 303b StGB „Computersabotage“.

In der täglichen Arbeit erleichtert uns ein Backup-Konzept, die entstandenen Schäden problemlos zu beheben.

Benutzer könnten den PC der UB nutzen, um sich als Hacker zu betätigen: Dazu aus „Sicherheit im Internet: Die weitaus größte Zahl der Einbruchversuche (nicht von erfolgreichen Einbrüchen) wird von Studenten und Schülern aus dem Universitäts- und Schulumfeld begangen. Leistungsfähige, für Studenten kostenlos verfügbare Computer-Systeme mit Internet-Zugang, genaue Kenntnisse über Betriebssysteme und Protokolle sowie unbegrenzt zur Verfügung stehende Zeit, verbunden mit einer gehörigen Portion Spieltrieb, - diese für viele Informatikstudenten zutreffenden Eigenschaften stellen die idealen Voraussetzungen dar, sich zumindest gelegentlich als Hacker zu versuchen. Die Motivation für diese „Hacks“ ist in den meisten Fällen eine Kombination aus Neugier, Spieltrieb, Selbstbestätigung und Orwell -1984-

Lebensgefühl. Gesucht wird weniger nach spezifischen Informationen, wichtiger ist es, erfolgreich einzubrechen....“¹⁰⁾

Könnten wir das einem Benutzer nachweisen, so käme § 202a StGB „Ausspähen von Daten“ und § 303a StGB „Datenveränderung“ bzw. §303b StGB „Computersabotage“ zum Vollzug.

Internet-Kriminalität

Nicht-wissenschaftlich motiviertes Surfen im Internet ist grundsätzlich über die DFN-Benutzungsordnung nicht erlaubt. Aktives Einbringen und Verbreitung pornographischer Schriften ist strafbar nach § 184 StGB.

„Besonders streng ist in Deutschland das Strafrecht, wenn rassistische und nationalistische Äußerungen verbreitet werden. § 130 StGB sieht Freiheitsstrafen bis zu 5 Jahren vor.“¹¹⁾

Die Strafvorschriften aus dem Gesetz über die Verbreitung jugendgefährdender Schriften können im Netz nicht einfach angewendet werden. Der Gesetzgeber plant daher eine Anpassung der Gesetze.

Doch auch hier gilt: Worte oder Gesetze sind Schall und Rauch. Daher brauchen wir technische Beschränkungen.

Unter dem Stichwort „Kindersicherung - jugendfreies Internet“¹²⁾ gibt es Ergänzungssoftware, wie NetNanny und Cybersitter. Diese Programme ermöglichen Eltern eine Zugangskontrolle zum Internet. Wesentlicher Bestandteil der Programme ist eine Liste mit identifizierten Web-Pages zu den Themen Sex, Porno, Gewalt, sowie einem Begriffslexikon, dessen Einträge mit den Inhalten der zu ladenden Web-Pages abgeglichen werden. Teilweise können auch eigene Erweiterungen vorgenommen werden. Ein solches Programm kann allerdings für eine Bibliothek nicht ernsthaft erwogen werden. Selbst für die angestrebte Zielgruppe stuft DIE ZEIT solche Programme als „hilflose Hüter“¹³⁾ ein.

In den USA hat Bill Clinton am 8. Febr. 96 die Reform des Telekom-Gesetzes unterzeichnet. „Seither ist jeder amerikanische Internet-Provider voll für die Inhalte zuständig, die er zugänglich macht. Er hat dafür zu sorgen, daß über ihn keine anstößigen Inhalte erreichbar sind.“¹⁴⁾ Es wirkt eher hilflos, als Gesetzgeber, „Einfluß auf die Inhalte des Internets“¹⁵⁾ ausüben zu wollen. „Es liegt in der Struktur des Netzwerks, daß es immer einen Weg vorbei an der Zensur gibt.“¹⁶⁾ Auch in Bonn wird seit geraumer Zeit ein Gesetzentwurf diskutiert, der unter anderem die Verschlüsselung von Daten reglementieren soll.¹⁷⁾

Eine beliebte Form der Internet-Kriminalität ist auch das Versenden von E-Mails mit falscher Adresse. Selbstverständlich kann die E-Mail zurückverfolgt werden an den Absendeort. Ansätze, wie die Aktivitäten eines Benutzers über ein Logbuch zu protokollieren, verlieren ihre Wirksamkeit, wenn sich Benutzer nicht vorher grundsätzlich anmelden müssen. Daher haben wir bislang keine Möglichkeit, den Verfasser einer E-Mail ausfindig zu machen. Bei einigen Explorern ist es mittlerweile möglich, die E-Mailfunktion abzustellen.

Urheberrecht

Wichtig ist es auch, sich mit dem Urheberrecht auseinanderzusetzen. *Susan Singleton* führt in ihrem Artikel: „The Internet- whose law is it, anyway“ zum Thema Copyright aus: Informationen, die im Internet verteilt sind und von jedem Net-Surfer kostenfrei gelesen werden können, berechtigen nicht automatisch dazu, Kopien davon zu machen, wenn der Autor keine explizite Erlaubnis dazu erteilt. Die Konsequenz ist, daß Drucken und Downloaden schon ein Bruch des Copyrights darstellt. Dies aber wird wohl kaum strafrechtlich verfolgt. Wenn aber ein Benutzer das geladene Material in seine eigenen Arbeiten einarbeitet, dann ist das Urheberrecht verletzt worden.¹⁸⁾ Hier wirkt dann §106 Urbergesetz.¹⁹⁾

Können wir unter diesen Bedingungen das Internet überhaupt zulassen? Aber sicher doch, denn Kriminalität ist der Ausnahmefall und wir werden doch nicht den Ausnahmefall zur Regel erklären und einen Service, der für die wissenschaftliche Arbeit hervorragend ist, wieder schließen. Denken Sie nur an die Internet-Zugänge der Verbundsysteme, an die Fachforen usw.

Wir sind aber in einer Situation, in der wir nicht nur Sicherheitsrichtlinien brauchen, sondern in der auch Sicherheitsstandards geschaffen werden müssen. Einiges ist heute schon möglich, anderes muß speziell auf öffentliche Internet-Benutzerarbeitsplätze zugeschnitten sein.

Internet-Cafe

So könnten wir uns z.B. als Internet-Cafe verstehen. Das kann ganz einfach gelöst werden. Die Stromversorgung muß so eingerichtet sein, daß eine zentrale Stelle die Schalter bedienen kann. Grundsätzlich ist der Bildschirm schwarz. Beahlt ein Benutzer für eine bestimmte Zeit, so wird Strom auf den Bildschirm geschaltet. Dieses Verfahren wird in den USA teilweise praktiziert. In der Bundesrepublik würde dieses Verfahren eindeutig gegen die Ziele der Bundesregierung verstoßen, die mit dem Wandel Deutschlands auch den Wandel zur Informationsgesellschaft sichern will und vorgibt, „von staatlicher Seite darauf zu achten, daß gleiche Zugangschancen für alle gewährleistet

sind. Der Entwicklung einer Gesellschaft, in der viele die neuen Techniken nutzen können und andere dazu nicht befähigt sind, soll entgegengewirkt werden...“²⁰⁾

Zugangsprovider

Wir brauchen also ein Benutzer-Authentifikationssystem. Vorstellbar ist, daß die Universität sich als Zugangsprovider versteht und ebenso wie bei T-Online oder anderen Zugangs Providern erst einmal die Authentifikation des Benutzers verlangt. Doch wie kann ein solches System in der Praxis aussehen? Die Technik für einen Zugangsprovider ist dort angesiedelt, wo wir es eigentlich nicht vermuten, nämlich bei den Abwehrsystemen. Dies möchte ich nun skizzieren, visualisieren. In der Praxis gibt es das, soweit mir bekannt ist, nur in Ansätzen:

Vorerst aber möchte ich mich eines Beispiels bedienen:

Im Mittelalter wurden Stadtmauern errichtet. Diese dienten dazu, Angreifer von außen abzuhalten. Angreifer mit Feuer konnten die Stadt erst dann mit Feuer vernichten, wenn das Feuer die Mauer durchdringen oder überwinden konnte. Die Mauer war also auch Brandschutzmauer. In der modernen Welt des Internet schottet sich ein Unternehmen, das wertvolle Datengebäude zu verteidigen hat, durch eine elektronische Brandschutzmauer, dem Firewall, ab.

Andererseits, wer innerhalb solcher Mauern lebte, der mochte auch die Welt außen sehen. Im Mittelalter gab es Menschen, die nie die Stadttore nach außen passieren konnten und andere, die einen Passierschein hatten und die Stadt verlassen konnten.

Die moderne Bibliothek von heute ist eine Durchgangsstadt. Ihre Datengebäude können ohne weiteres abgebrannt werden, z.B. Ausleih-Server auf Internet-Basis, OPAC-Server, CD-ROM-Server, WWW-Server. Die Gefahr des Ab Brennens wird als gering erachtet und meines Erachtens unterschätzt. Andererseits können Benutzer einer Bibliothek in die internetweite Welt ziehen, ohne Passierscheine und Mautgebühren. Das Internet selbst hat keine Schutzmechanismen, it „was never designed as a secure system“.²¹⁾ In dieser Situation ergibt sich die Forderung nach einem Firewallsystem für Bibliotheken.

Firewall

Die in der Literatur vorgestellten Firewall-Systeme beschäftigen sich vorrangig mit dem Aspekt des Schutzes vor Angreifern. „Generally, firewalls are configu-

red to protect against unauthenticated interactive logins from the 'outside' world" ²²⁾ Ihre Konzeption ist noch unzureichend, was den Aspekt der kontrollierten Reise in die internetweite Welt angeht.

Doch seitdem Unternehmen das Internet entdeckt haben, haben Firewalls Passierwege bekommen in Form von *application gateways*, „to let people inside get out“ ²³⁾.

Im elektronischen System ist der Firewall ein Rechner, der zwischen dem lokalen Netz und dem Internet angesiedelt ist. Jede Kommunikation von innen nach außen muß über diesen Firewall geführt werden. Auf dem Firewall-Rechner müssen bestimmte Services definiert werden nach einem der beiden folgenden Vorgehensweisen:

„Alles, was nicht explizit erlaubt ist, ist erst einmal verboten -
Alles, was nicht explizit verboten ist, ist zunächst einmal erlaubt“ ²⁴⁾

Für den Kommunikationsweg von außen nach innen empfiehlt sich die erste Regel: Keine Internet-Adresse von außen hat Zugang zum internen Netz, außer es ist explizit erlaubt.

Für die Kommunikation von innen nach außen wird das *application gateway* notwendig.

Es gibt zwei verschiedene Varianten: Zum einen können Accounts auf dem Firewall eingerichtet werden und zum anderen können die gängigen Anwendungen wie TELNET, FTP, HTTP als „Proxy-Server“ auf dem Firewall eingerichtet sein, d.h. startet ein lokaler Rechner eine TELNET-Session, dann übernimmt der TELNET Proxy Server des Firewalls den Prozeß zur Kommunikation ins Internet. Meines Erachtens brauchen Bibliotheken eine Kombination und Erweiterung beider Dienste. Ist auf dem Firewall ein HTTP-Proxy Server in Betrieb, dann ist weiterhin internetweites Surfen möglich. Hat ein solcher Proxy-Server aber auch noch Elemente aus Programmen wie NetNanny oder Cybersitter, dann besteht die Möglichkeit, Internet-Suche auf wissenschaftliches Suchen einzugrenzen.

Daher ist die Authentifizierung der Internet-Anwender über User-ID und Paßwort sinnvoll. Zum Einsatz kommen muß allerdings die zentral vergebene User-ID. Eine eigene Benutzerverwaltung zu führen ist einfach zu aufwendig. „Die Sicherheit bei der Verwendung von User-IDs kann durch den Einsatz von SmartCards erhöht werden“ ²⁵⁾ Die universelle SmartCard, wie sie z.B. an der Universität Bochum ²⁶⁾ bereits eingeführt wurde, müßte auch im Internet zu Abrechnungszwecken eingesetzt werden können. Sie erhält Informationen, die die „nutzbaren Dienstleistungen, z.B. nach anfordernder Person..., Datum, Art der Aktion und Gebührenabrechnung der angeforderten“ Dienste beschränkt. ²⁷⁾ Über eine SmartCard haben wir die Möglichkeit, die Bibliothek

generell allen zu öffnen; die Internet-Dienste könnten wir aber einschränken auf Universitätsangehörige. Mit der „Einführung einer intelligenten Chipkarte für Bibliotheksdienste“²⁸⁾ haben wir das Modell: Information on demand oder Pay Library.

Schlußfolgerung

Ein Firewall mit dem noch zu entwickelnden intelligenten HTTP-Proxy-Server und das Modell *Information on demand* sind eine Garantie dafür, daß wissenschaftliches Arbeiten in der Universitätsbibliothek für Universitätsangehörige frei bleibt und schiebt all denen einen Riegel vor, die in der Unibibliothek ein billiges Internet-Cafe sehen.

Anmerkungen

- 1) Dieser Vortrag wurde am 20.09.96 anlässlich des 5. SWB-Nutzerrates gehalten.
- 2) Elisabeth Niggemeyer: König Kunde - oder was bietet die Bibliothek ihren Benutzern und Benutzerinnen, in ZfBB, 43. Jg, Heft 3 1996
- 3) Barry B. Blinlo: Academic staff, students and the Internet: the experience at the University of Westminster, in: The Electronic Library, Vo. 14, No 2, April 1996, S. 111 - 116
- 4) Karanjit Siyan, Chris Hare: Internet firewalls & Netzwerksicherheit : [alle Hintergrundinformationen zur Sicherheit und TCP/IP firewalls und andere Modelle zur Datensicherheit ; Herstellerübersichten und Produktbeschreibungen], 1995
- 5) Benutzungsordnung für das Zusammenwirken der Anwender der DFN-Kommunikationsdienste, in: GWDG-Nachrichten 7/94, ISSN 0940-4686 (Original lag nicht vor)
- 6) HELL- Sicherheitsrichtlinien vom 1.7.1996
- 7) Thomas Hoeren: Internationale Netze und das Wettbewerbsrecht, in: Rechtsprobleme internationaler Datennetze, hrsg. Jürgen Becker, S. 35 - 56
- 8) BILD Stuttgart v. 23.5.1996
- 9) Stuttgarter Zeitung v. 22.2.1996
- 10) Othmar Kyas: Sicherheit im Internet, DATACOM Fachbuchreihe, 1996
- 11) Straftaten im Netz, in: c't 9/96 S. 123
- 12) Axel Kossel: Kindersicherung - jugendfreies Internet, in: c't 9/96 S. 120-121
- 13) Detlef Borchers: Hilflöse Hüter in: DIE ZEIT Nr 29 v. 12.7.96, S. 58
- 14) Report: Zensur im Internet, Freiheit, Zensur oder freiwillige Selbstkontrolle? Selbstreinigung, in: DOS 5/96 S24-30
- 15) Report: Zensur im Internet - Verlorene Liebesmüh, in: MACup Hamburg, 1996, Band 12, Heft 4, S. 146-147

- 16) Report: Zensur im Internet - Verlorene Liebesmüh, in: MACup Hamburg, 1996, Band 12, Heft 4, S. 146-147
- 17) Ulrich Schmitz, Kommunikationssperre, in: iX 2/1996 S. 28
- 18) Susan Singleton: The Internet - whose law is it, anyway?, in: Administrator - London 1996, Band 1996, Heft April
- 19) Straftaten im Netz, in: c't 9/96 S. 123
- 20) Bericht der Bundesregierung Info 2000 - Deutschlands Weg in die Informationsgesellschaft, Drucksache 13/4000 v. 07.03.96
- 21) Chris Leiby and Mark Konkol: Security issues on the internet, in: Aslib Proceedings, vol 48, no. 5 May 1996, pp 123-127
- 22) Vance McCarthy: Building a Firewall, in: DATAMATION May 15, 1996, S. 74 - 76
- 23) Vance McCarthy: Building a Firewall, in: DATAMATION May 15, 1996, S. 74 - 76
- 24) Joachim Schlette. Internet Sicherheit durch Firewalls, in: DATACOM 1/96 S. 62-66
- 25) Joachim Schlette. Internet Sicherheit durch Firewalls, in: DATACOM 1/96 S. 62-66
- 26) Sesam öffne dich - Die neue Chipkarte wird Studentenausweis, Bahnticket, Mensamarke und Kreditkarte zugleich, aus: Quelle liegt nicht vor
- 27) Ruth Marzi, Tilo Schürer: Sicherheitsprobleme bei Anschluß von lokalen Netzen an das Internet, in: DV Management 4/95, S. 176- 179
- 28) Jürgen Hänle, Die intelligente Chipkarte in einem offenen Bibliotheksverbund, in: ABI-Technik 1, 1995, Nr. 3, S. 205-206

