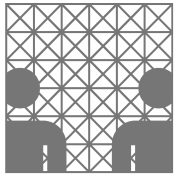
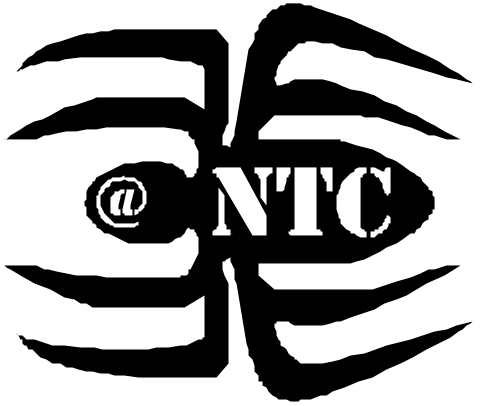
Impressum
Universität Hamburg
FachbereichInformatik
Network-Test-Center
Vogt-Kölln-Straße 30
22527 Hamburg

Telefon: ☎040 / 42883 - 2234 (Labor)
☎040 / 42883 - 2405 (Sekretariat)

Fax: ☎040 / 42883 - 2226

Web-Seite: http://agn-www.informatik.uni-hamburg.de





Network Test Center

Sicherer ins Internet

Einführung und Informationen zur Konfiguration gängiger Browser und Betriebssysteme

von Lutz Feldmann, Heiko Gerlach, Rainer Herzog, Martin Johns, Sibel Mutlu, Axel Schnell, Marc Schönberg, Emine Yueksel und Karim „Kasi Mir“ Senoucci

Impressum
Universität Hamburg
FachbereichInformatik
Network-Test-Center
Vogt-Kölln-Straße 30
22527 Hamburg

Telefon: ☎040 / 42883 - 2234 (Labor)
☎040 / 42883 - 2405 (Sekretariat)

Fax: ☎040 / 42883 - 2226

Web-Seite: http://agn-www.informatik.uni-hamburg.de

Spenden an das Network-Test-Center bitte an die
Landeshauptkasse Hamburg, Kto-Nr. 101 600
Hamburgische Landesbank, BLZ 200 500 00
Stichwort: 34013 Prof. Brunnstein / FB Informatik

Copyright ©2000-2002 Lutz Feldmann, Karim „Kasi Mir“ Senoucci (Hrsg.)

Entstanden unter Verwendung von „Sicherer ins Internet unter Windows 98 und Windows 98 SE“ von Andreas G. Lessig (mit freundlicher Genehmigung des Autors)

Alle Rechte an Text und Abbildungen sind vorbehalten. Kein Teil des Werkes darf in irgendeiner Form ohne schriftliche Genehmigung reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder weiterverbreitet werden.

Vorwort

Eine der bedeutendsten Entwicklungen im Bereich der Kommunikationsmedien ist das Internet. Das Internet verbindet Millionen von Menschen auf der ganzen Welt, durch zahlreiche Internet Service Provider kann es von nahezu jedem genutzt werden. Schon heute hat das Internet einen festenundunverzichtbarenPlatzinunseremtäglichenLebeneingenommen.

Die Benutzung des Internets bringt aber auch Gefahren mit sich. Hat man bei Ihnen schon mal in die Wohnung ein gebrochen? Oder Ihr Auto aufgebrochen? Haben Sie sich dann vielleicht gefragt, was Sie falsch gemacht haben, oder sich informiert, was Sie hätten besser machen können? Für uns ist es selbstverständlich geworden, das Auto oder die Wohnung nach Verlassen abzuschließen. Auch das Einrasten des Lenkradschlosses, das Abnehmen des Bedienteiles vom Autoradio oder das Einhängen der Kette oder des Riegels vor die Wohnungstür, wenn man beim Klingeln keinen Besuch erwartet, ist für viele von uns ein Muß. Natürlich bedeuten alle diese Sicherheitsmaßnahmen einen zusätzlichen Aufwand. Und nach einem Wohnungseinbruch denken viele über einen komplizierteren Schließzylinder, abschließbare Fenstergriffe oder ähnliches nach. Über die Möglichkeiten, sich beim Umgang mit dem Internet vor fremden Übergriffen zu schützen, soll die folgende Broschüre informieren. Viele der hier beschriebenen Methoden über einen sichereren Umgang werden Sie in Ihrer Bequemlichkeit einschränken, werden zu zusätzlichem Aufwand führen oder Ihnen nahelegen, von einigen der Ihnen liebgewonnenen Vorgehensweisen besser abzusehen. Am Ende werden immer Sie entscheiden, wie wichtig Ihnen Ihre Sicherheit ist, wir machen Ihnen in der folgenden Broschüre lediglich Vorschläge, was Sie möglicherweise verbessernkönnen.

Dabei geben wir detaillierte Hinweise zur Konfiguration von Windows 95/98/ME und gehen auf die sicherheitsrelevanten Einstellungen der gängigen Internet-Browser von Netscape und Microsoft ein. Aber auch Nutzer anderer Browser oder Betriebssysteme werden in diesen Abschnitten nützliche Hinweise zur besseren Einrichtung Ihres Rechnersystems finden. Im hinteren Teil schließlich gehen wir kurz auf Linux-Installationen sowie allgemeine, systemunabhängige Maßnahmen zur Sicherung des eigenen Computers ein. All diese Themen können wir in der Kürze dieser Broschüre natürlich nur anreißen; für tiefergehend an der Materie Interessierte bieten wir jedoch am Ende eine kleine Sammlung informativer Anlaufstellen für weiteres Studium.

Grundkonfiguration von Windows 95/98/ME

Auch wenn man Windows 95/98/ME prinzipiell ziemlich sicher konfigurieren kann, so ist es doch nicht möglich, einen hundertprozentigen Schutz zu garantieren. Gelingt es aber einem Angreifer, erst einmal „einen Fuß in die Tür zu bekommen“, so existierenkeineweiterenSchutzmechanismen, die ihn daran hindern, die totale Kontrolle über den Rechner zu erlangen. Aus diesem Grunde empfiehlt es sich, auf dem zum Surfen benutzten System keine Anwendungen zu benutzen, bei denen man einen Ausfall oder Verlust aller Daten nicht ohne Probleme verschmerzen kann. Die genaue Einschätzung muß natürlich dem Anwender überlassen bleiben, typischerweise fallen in diese Kategorie jedoch zum Beispiel Textverarbeitungs- und Tabellenkalkulationssysteme, die man für die private und berufliche Korrespondenz bzw. die Haushaltsführung einsetzt, aber auch Steuerabrechnungshilfen oder Datenbankprogramme; mit denen man z.B. die private Videosammlung katalogisiert hat. Bei diesen Programmen sollte man sich immer zweierlei fragen:

1. Wie groß ist der Aufwand, die Programme im Schadensfall neu zu installieren? Dies kann sich schwieriger gestalten, als man zunächst denkt, vor allem, wenn man das Rechnersystem bereits vorinstalliert gekauft hat und manche Programme nicht auf einem sicheren Datenträger (z.B. CD-ROM) zur Installation vorliegen.
2. Wie groß ist der Aufwand, im Schadensfall die selbsterstellten Daten wieder zu erhalten? Eine Backup-Strategie kann diesen Aufwand in der Regel stark reduzieren – wer schon einmal eine umfangreiche Sammlung von Videokassetten, Comic-Heften oder Firmenkontakten neu eingeben mußte, wird dies sicherlich bestätigen können.

Schätzt man auch nur bei einer dieser Fragen den Aufwand als hoch ein, so sollte man für das

Surfen im Internet ein eigenes Rechnersystem einsetzen. Der einfachste Weg, eine Trennung der Systeme zu erreichen, besteht sicherlich darin, zwei Rechner zu benutzen, von denen der eine dem Surfen vorbehalten ist, während der andere für alle sonstigen Anwendungen benutzt wird. Obwohl dies die sauberste Lösung ist, kommt sie aber wohl nur dann in Frage, wenn schon ein zusätzlicher Rechner vorhanden ist, der zu diesem Zweck umgerüstet werden kann. Ist dies nicht der Fall, so bietet es sich an, die Festplatten des Rechners in Wechselrahmen einzubauen und eine weitere Platte samt Einschub für den Wechselrahmen anzuschaffen. Auf diese Weise ist es möglich, vor dem Besuch des Internets alle „normalen" Platten zu entfernen und die „Surfplatte" einzubauen. Dabei ist allerdings zu beachten, daß im BIOS der Plattentyp aller Plattenals „Auto" eingetragen ist, so daß es beim Start selbständig erkennt, welche Platten vorhanden sind.

Nachdem nun die Hardware für das Surfen vorbereitet ist, gilt es Windows 95/98/ME sowie die für den Zugang nötige Software zu installieren. Dies ist nicht weiter problematisch und soll hier nicht erklärt werden. Es ist allerdings zu beachten, daß Windows ohne den *Windows Scripting Host*, den *Personal Webserver* und *Frontpage Express* installiert wird, bzw., daß diese nach der Installation über die *Start->Systemsteuerung->Software->Windows Setup->Zubehör* bzw. *Start->Systemsteuerung->Software->Windows Setup->Internet Programme* entfernt werden. Dieser Vorgang wird in der folgenden Abbildung dargestellt.

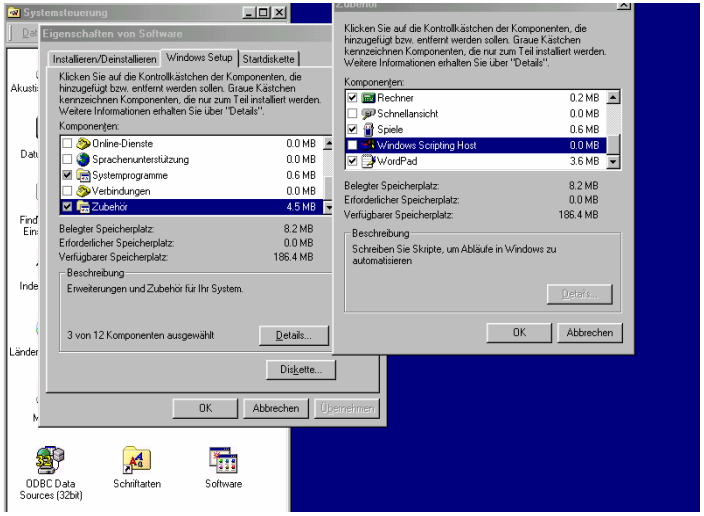


Abbildung 1: Deinstallation des *WindowsScriptingHost*

Der *Windows Scripting Host* ist dabei besonders wichtig, da er gerne als Einfallstor für HTML-Viren benutzt wird. Unter Windows ME wird der *Windows Scripting Host* allerdings standardmäßig installiert und läßt sich auch nicht mehr einfach nachträglich entfernen. Aus ähnlichen Gründen sollte daher auch kein Office-Paket installiert werden. Sollen Word-Dokumente aus dem Internet betrachtet werden, so ist dies in der Regel auch mit der *Schnellansicht*, dem *Wordpad* (beide in Windows 95/98/ME enthalten) oder dem *Word-Betrachter* (unter **`http://www.microsoft.de/`** erhältlich) möglich. Auf diese Weise wird die Verseuchung des Systems mit Makroviren vermieden. Für den *Personal Webserver* sind dagegen noch keine Angriffe bekannt. Er ist aber im Grunde unnötig, es sei denn, es sollen Webseiten mit *Frontpage Express* erstellt werden. Wird er installiert, so stellt der Windows-Rechner einen richtigen Webserver dar, der von jedem Rechner im Internet abgefragt werden kann. Nun ist aber eines der wichtigsten Prinzipien der Internet-Sicherheit, keine unnötigen Serverdienste auf dem Rechner zu installieren, da sie immer einen Ansatzpunkt für mögliche Angriffe darstellen. Aus diesem Grund scheint es ratsam, ihn zu

Linkliste

Überprüfung der Browsereinstellungen, Überblick über Informationen, die der Website vom Browser geliefert werden, Demonstration von Sicherheitslücken:
`http://www.privacy.net/analyze/`
`http://www.heise.de/ct/browsercheck/`

Test der Verschlüsselungstärke des Browsers:
`https://www.fortify.net/sslcheck.html`

Aktuelle Sicherheitslücken und Ratschläge:
`http://www.securityfocus.com`, Mailingliste Bugtraq
`http://www.insecure.org`, Security Tools: `http://www.insecure.org/tools.html`
`http://www.guninski.com/`
`http://www.cert.org/advisories/`

Allgemeine Sicherheitsinformationen und Tests von aktuellen Virenscannern:
`http://agn-www.informatik.uni-hamburg.de/` (siehe Virus-Test-Center)

Hinweise zum Konfigurieren von Linux-Firewalls
`http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html`

deinstallieren. *Frontpage Express* ist damit nicht mehr benutzbar und kann ebenfalls deinstalliert werden.

Um die Grundkonfiguration abzuschließen, sollte noch sichergestellt werden, daß der *Explorer* auch alle Dateien in einem Verzeichnis anzeigt. Standardmäßig werden als „versteckt" markierte Dateien nicht und Dateien mit bekannten Endungen ohne dieselbe angezeigt. Beide Tatsachen können dazu genutzt werden, daß eine Datei im *Explorer* nicht angezeigt wird. Um dies zu vermeiden, sollte in einem *Explorer*-Fenster unter *Ansicht->Ordneroptionen->Ansicht* (bei Windows ME unter *Extras->Ordneroptionen->Ansicht* der Punkt „Dateinamenerweiterung bei bekannten Dateitypen ausblenden" abgestellt werden. Außerdem sollte unter „Versteckte Dateien" der Punkt „Alle Dateien anzeigen" angewählt werden.

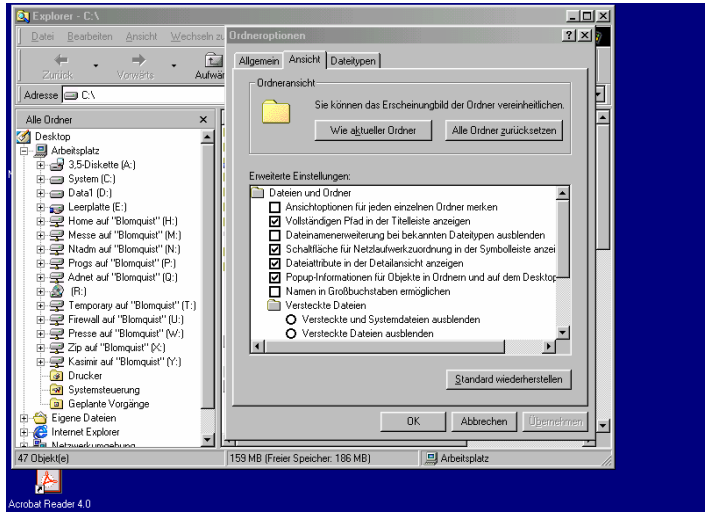


Abbildung 2: Ordneroptionen (hier unter Windows 98)

Netzwerkfreigaben

Generell sollte ein guter Grund vorliegen, falls auf einem Surfsystem Freigabedienste installiert werden. Läßt sich dies nicht vermeiden, so sollte sichergestellt werden, daß diese Dienste nicht in das Internet exportiert werden.

Um dies zu erreichen, müssen als erstes die Bindungen von TCP/IP überprüft werden. Dazu wählt man in der *Systemsteuerung* die Karte *Netzwerk* und sucht das TCP/IP-Protokoll. Dieses sollte zweimal vorhanden sein; einmal ist es an die Netzwerkkarte gebunden, einmal an das DFÜ-Netzwerk. Uns interessiert der letztere Eintrag. Nach einem Klick auf Eigenschaften und der Anwahl der Karte Bindungen ergibt sich folgendes Bild:

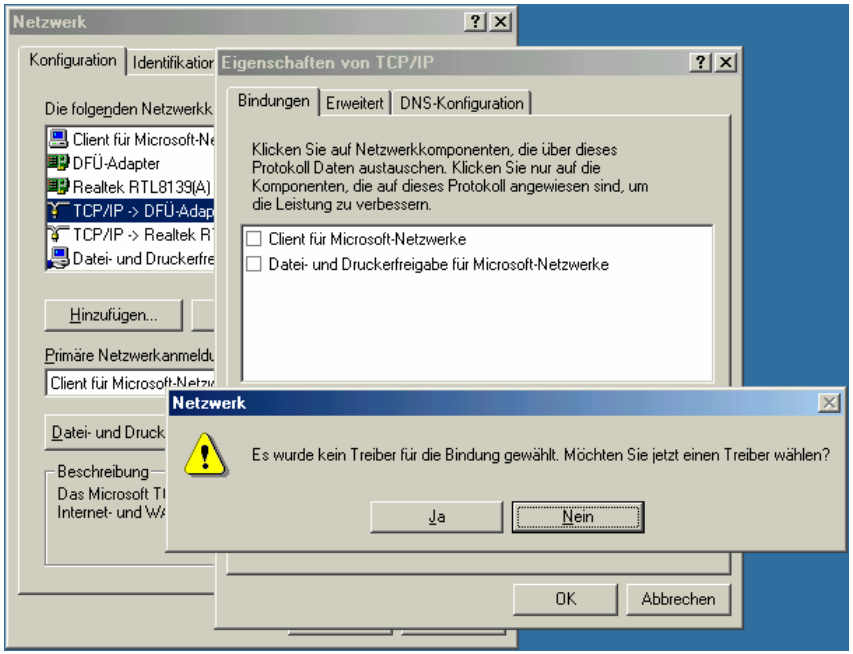


Abbildung 3: TCP/IP-Eigenschaften

Insbesondere das Kästchen „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ sollte leer sein. Als nächstes sollten noch die Einstellungen der im DFÜ-Netzwerk eingetragenen Verbindungen überprüft werden. Dazu klickt man nacheinander mit der rechten Maustaste auf die einzelnen Einträge und wählt im nun erscheinenden Kontextmenü den Punkt *Eigenschaften*. In dem sich nun öffnenden Fenster wählt man die Karte Servertypen. Hier sollte sich der folgende Anblick ergeben:

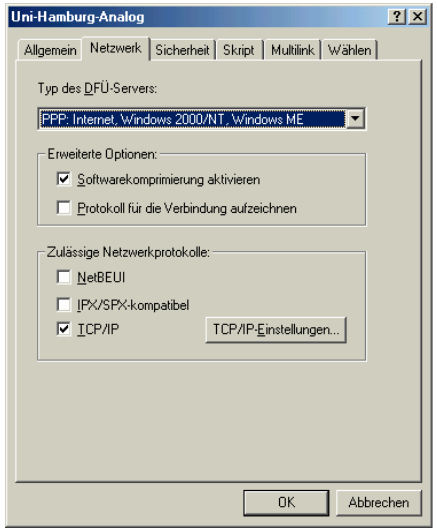


Abbildung 4: Verbindungseigenschaften

wahrt seine Sicherheit, indem man die eigenen Schlüssel/Geheimnummern für andere unzugänglich verwahrt und für das Internet-Banking die neuesten Internet-Browser verwendet. Näheres unter Updates. Manche Institute verwenden darüber hinaus noch eine zusätzliche Verschlüsselung, hier gibt es teilweise große Unterschiede.

Updates

Softwarehersteller beheben bekannt gewordene Sicherheitslücken in ihren Programmen oft recht schnell, da sie um ihr Image fürchten. Anwender, die anonym bleiben möchten, müssen sich aber selbst um die Beschaffung der Updates oder Patches bemühen.

- Updates für MS Windows: **`http://www.microsoft.com`**
- für Windows 2000: **`http://www.microsoft.com/windows2000/downloads/`**
- für Windows NT 4: **`http://www.microsoft.com/downloads/`**
- für Windows 95: **`http://www.microsoft.com/windows95/downloads/`**
- für Windows 98: **`http://www.microsoft.com/windows98/downloads/corporate.asp`**

Für Linux bieten die führenden Anbieter komplette Updates ihrer Distributionen an, je nach eigener Distribution findet man unter **`http://www.suse.de`**, **`http://www.redhat.de`**, **`http://www.caldera.com`** oder der Webseite anderer Linux-Vertreiber passende Updates.

Entscheidend ist auch die Wahl des neuesten Internet-Browsers, da alleine durch die verbesserten Verschlüsselungsalgorithmen von zur Zeit 128 Bit, die bei Netscape ab Version 4.73, beim MS Internet Explorer ab Version 5.01 angeboten wird. Man kann die Verschlüsselungsstärke des eigenen Browsers unter **`https://www.fortify.net/sslcheck.html`** testen.

Den neuesten *Microsoft Internet Explorer* findet man unter **`http://www.microsoft.com`**, *Netscape Communicator* unter **`http://www.netscape.com/download`**.

http://www.kernel.org. Für die folgenden Firewall-Einstellungen sind bei der Kernel-Konfiguration unter ‘Networking options‘ folgende Einstellungen zu setzen, andere nicht:

```
[*] Network firewalls
[*] Socket filtering
[*] Unix domain sockets
[*] TCP/lP networking
[*] lP: firewalling
[*] lP: masquerading
[*] IP: Allow large windows
```

Mit dem Befehl **ipchains** wird für ein- und ausgehende Netzwerkpakete bestimmt, wie diese zu handhaben sind. Sinnvollerweise legt man die folgenden Regeln in einem Shell-Skript an, das bei Systemstart ausgeführt wird.

Zunächst sperrt man für sämtliche Pakete beide Richtungen:

```
/sbin/ipchains –F
/sbin/ipchains -P input DENY
/sbin/ipchains -P output REJECT
/sbin/ipchains -P forward REJECT
```

Dann gibt man nur für die gewünschten A nforderungen die Pakete wieder frei:

```
/sbin/ipchains -A input  -i lo -j ACCEPT
/sbin/ipchains -A output -i lo –j ACCEPT
```

wobei mit „lo“ das Loopback-lnterface gemeint ist, über das alle Verbindungen abgewickelt werden, die der Rechner mit sich selbst aufba ut. Mit den obigen zwei Regeln läuft z.B. der X-Server wieder (der normalerweise auf einem Firewall-Rechner nichts zu suchen hat) Mit:

```
/sbin/ipchains -A output -i ippp0 -p tcp -s EXIP 1024:65535 \
--destination-port 80 -j ACCEPT

/sbin/ipchains -A input -i ippp0 -p tcp ! -y --source-port 80 \
-d EXIP 1024:65535 -j ACCEPT
```

schaltet man nun den Datenfluß ins Internet frei, unterbindet jedoch den Aufbau einer Verbindung eines Rechners im Internet mit dem eigenem. In den letzten Regeln stellt ein „\“ jeweils die Fortsetzung der Befehlszeilen in der nächsten Textzeile dar, EXIP steht für die IP-Adresse, die dem eigenem Rechner während des lnternet-Aufenthaltes zugeordnet wird; diese wird bei kurzfristigem Aufenthalt i.d.R. für jede Verbindung neu vergeben und ist nach dem Verbindungsaufbau z.B. über

```
/sbin/ifconfig ippp0 | grep “inet addr“ | awk -F: ‘{print $2}‘ \
< awk ‘{print $1}‘
```

abzurufen.

Diese beiden Beispiele sollten nicht den Eindruck erwecken, daß sie vollständig sind, sondern eher als Anregung dienen, hierauf aufzubauen und das eigene System individuell abzusichern.

Sichererer Umgang mit Online-Banking

Das zur Zeit sicherste Verfahren auf dem Markt nennt sich HBCI, und wird z. Zt. von einigen Sparkassen unterstützt. Über eine zunächst recht umständliche Vergabe von Schlüsseln identifizieren sich Geldinstitut und Kunde miteinander. Dann wird anhand dieser Schlüssel eine sichere Datenübertragung initiiert. Ein weiteres Verfahren ist die PIN/TAN-Absicherung. Mit einer geheimen Persönlichen Identifikationsnummer (PIN) identifiziert sich der Kunde, mit einer Transaktionsnummer (TAN), die nur einmal gültig ist, wird jeder einzelne Auftrag bestätigt. Man

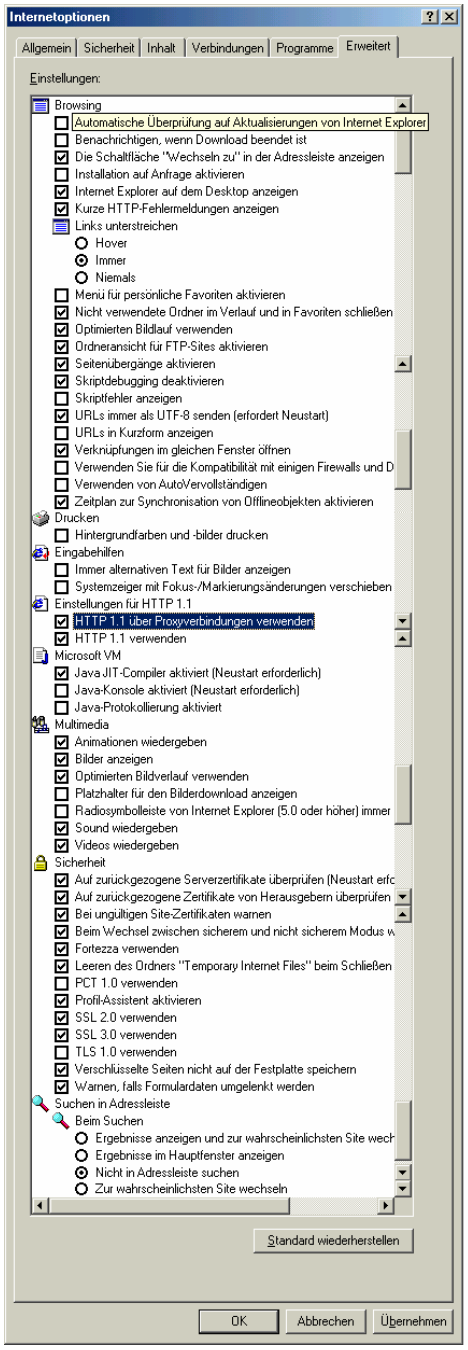


Abbildung5:Internetoptionen

Die Einstellungen sollten nun an obige Abbildung angepaßt werden; insbesondere sollten unter „Zulässige Netzwerkprotokolle“ „NetBEUI“ sowie „IPX/SPX-kompatibel“ abgewähltwerden.

Browserkonfiguration

Der neben den Netzwerkfreigaben (s.o.) wichtigste Ansatzpunkt für Angriffe ist der Browser. Täglich werden neue Methoden bekannt, ihn zu Aktionen zu überreden, die für den Benutzer gelinde gesagt unvorteilhaft sind. Bekannten Angriffen sollte entgegengetreten werden, indem jeweils die aktuellen Patches, bzw. die neueste Version des Browsers installiert wird.

Darüber hinaus läßt sich sagen, daß die überwiegende Anzahl von Angriffen nur mit sogenannten aktiven Seiteninhalten (Java, JavaScript, VBScript, ActiveX etc.) funktioniert. Da diese Inhalte aber auch von „normalen“ Webseiten benutzt werden, fällt die Entscheidung schwer, wie die Sicherheits- und Funktionalitätsanforderungen unter einen Hut zu bringen sind. Wir beschreiben in diesem Dokument zunächst den sicheren Weg und geben Konfigurationen an, die die Sicherheit des Rechners klar in den Vordergrund stellen. Wer unbedingt Webseiten mit aktiven Inhalten benutzen will oder muß, dem wird im weiteren Hilfestellung geboten, diese gezielt und einzeln zu aktivieren.

Im folgenden Abschnitt werden Konfigurationsanleitungen für den Internet Explorer 5.5 und den Netscape Communicator 4.7x aufgeführt. Sie gelten im Wesentlichen auch für andere Versionen der jeweiligen Browser; die genaue Bezeichnung und Positionierung der jeweiligen Einstellungsoptionen kann allerdings von Version zu Version variieren.

Internet Explorer 5.5

Der Internet Explorer kennt das Konzept unterschiedlicher Sicherheitszonen, in denen unterschiedliche Sicherheitseinstellungen gelten. So gelten für auf dem lokalen Rechner liegende Seiten andere Zugriffsbeschränkungen als für solche, die von einem Rechner im Internet heruntergeladen werden. Dies erscheint auf den ersten Blick sehr sinnvoll, da man lokalen Seiten

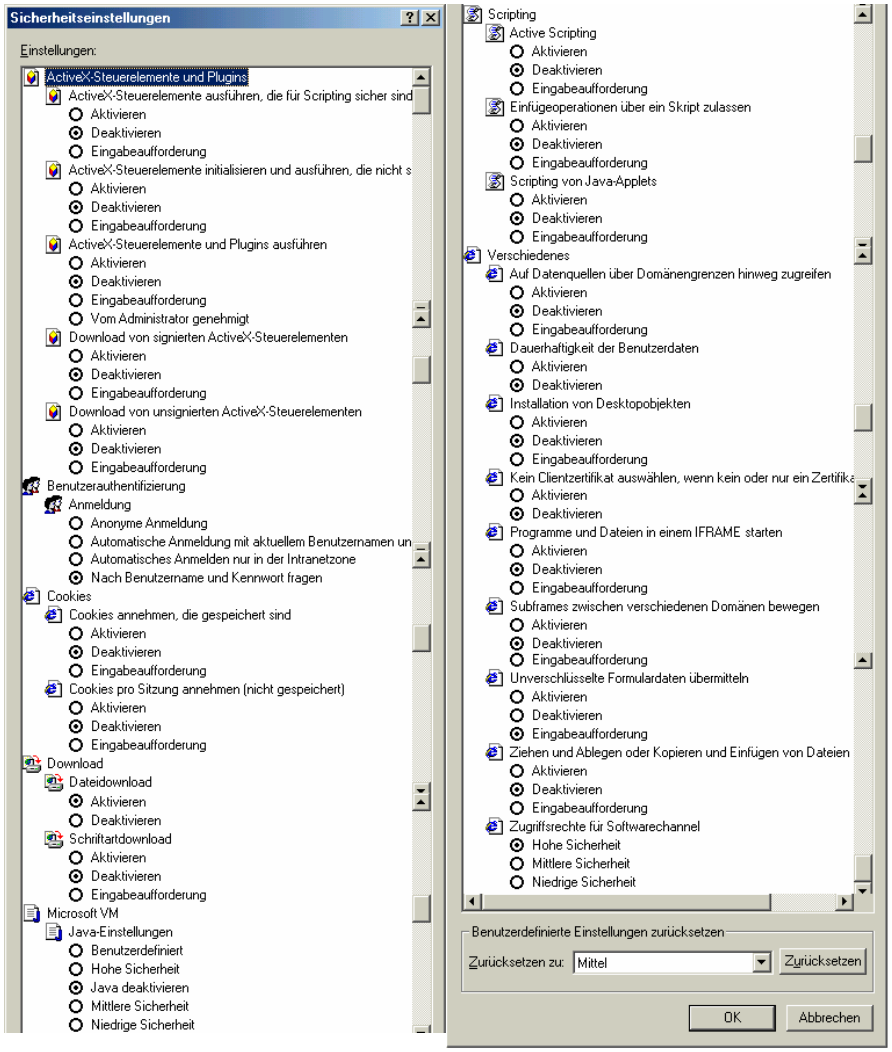


Abbildung6:Sicherheitseinstellungen

sicherlich mehr Vertrauen entgegenbringt, als solchen, die von einem unbekannten Rechner im Internet stammen. Leider hat sich aber gezeigt, daß dieser Einteilung nicht vertraut werden kann. Es gibt sogar HTML-Viren, die es schaffen, diese zu umgehen. Es empfiehlt sich daher, für alle Zonen die restriktivsten Einstellungen zu treffen.

Um dies zu tun, wählt man im Menü „Extras“ den Unterpunkt „Internetoptionen“ aus. In dem nun erscheinenden Fenster wählt man die Karte „Sicherheit“, auf dieser kann für jede Zone eine Sicherheitsstufe ausgewählt werden.

Der im folgenden beschriebene Vorgang muß nun für jede Sicherheitszone wiederholt werden. Man wählt zunächst die Einstellung „Angepasst“ und klickt auf „Einstellungen“. Die Abbildung 6 sollte in etwa dem sich Ihnen bietenden Bild entsprechen. Um nicht jede Einstellung einzeln korrigieren

einfachen Benutzerrechten anzulegen und nur diesen für die tägliche Arbeit und den Besuch im Internet zu verwenden.

Sicherer ins Internet unter Linux

Da sich ein Linux-System bis in kleinste Details konfigurieren läßt, kann es zu einem sehr sicheren System gestaltet werden. Leider entspricht die Grundkonfiguration, in der die meisten Linux-Systeme installiert werden, eher dem Gegenteil davon. Da es „das“ Linux nicht gibt, sondern Linux-Systeme sich extrem unterscheiden können, kann hier nur eine kurze, allgemeine Beschreibung für zwei Möglichkeiten, Linux sicherer zu machen, wiedergegeben werden:

Deaktivieren nicht benötigter Dienste

Werden Dienste wie Telnet, FTP, RSH, RLogin, TaIk, NTalk, POP etc. wirklich gebraucht? Wenn nicht, sollte man sie deaktivieren. Gemeint sind hier zunächst so genannte Server-Dienste; der Telnet-Dienst z.B. erlaubt es anderen, sich über das Netzwerk bei Ihrem Rechner anzumelden. Was die „Clients“ betrifft, also die Programme, mit denen man sich selbst bei anderen Rechnern anmeldet, ist der gesonderte Abschnitt darüber zu beachten.

Jeder dieser Dienste wird über einen sog. „Port“ (eine jedem Dienst eindeutig zugeordnete Zahl) bedient, bei Telnet ist das z.B. Port 21. Ports, an denen Dienste angeschlossen sind, sind potentielle Ansatzpunkte für Angriffe.
Mit dem Befehl **`netstat -a | less`** spürt man alle Dienste auf, die an die Ports angeschlossen sind; davon sind alle kritisch zu beurteilen, die in der Spalte „State“ als „Listen“ aufgeführt sind. Die meisten Dienste werden über die Datei „inetd.conf“ aufgerufen, die sich im Verzeichnis „/etc“ befinden sollte. Hier genügt bei nicht gebrauchten Diensten ein „#“ vor die entsprechende Zeile zu schreiben, um sie zu deaktivieren.

Andere Dienste werden direkt gestartet, hier soll nur exemplarisch der Webserver *Apache* genannt werden, der unter *SuSE-Linux* auch zum Anzeigen der *SuSE*-Hilfsseiten dient, die beim Start von *Netscape* angezeigt werden. Den automatischen Start von *Apache* unterbindet man – soweit möglich – über das mit dem Linux-System mitgeliefertem Konfigurationsprogramm (z.B. *Yast* bei *SuSE*), oder direkt über die „Runlevel“, die das Starten und Beenden verschiedener Programme bei verschiedenen Systemzuständen beschreiben (unter *SuSE* unter „/etc/rc.d/“, hier löscht man unter „rc2.d“ den Link auf **`apache`**). Will man auf den *Apache* nicht ganz verzichten, so kann man ihn bei Bedarf von Hand starten, über „**`/usr/local/apache/bin/apachectl start`**“, bei *SuSE* mit „**`etc/rc.d/apache start`**“; vor der Einwahl ins Internet hält man ihn mit „... **`stop`**“ an.

„Firewall“-Konfiguration

Unter einer Firewall versteht man ein System, das zwischen dem Internet und dem lokalem Netzwerk geschaltet ist, das erwünschte Verbindungen durchläßt und unerwünschte blockiert.

Um Arbeitsplätze ohne zusätzlichen Rechner zu sichern, kann man sog. Personal-Firewalls oder Desktop-Firewalls verwenden. Mit diesen Systemen erreicht man nicht die Sicherheit von „echten“ Firewalls, genießt bei ***richtiger*** Konfiguration zumindest einen gewissen Schutz und kann Angriffsversuche entdecken. (Siehe hierzu: „Die Gefahren des Internet meistern, Report“, **`http://www.heise.de/ct/00/20/116/default.shtml`** und „Elf Personal Firewalls im Test“, c't 20/00, Seite 126)

Eine „echte“ Firewall unter Linux läuft auf einem eigenen Rechner, ist nicht in wenigen Stunden konfiguriert und bedarf ständiger Kontrolle, hier kann daher nur auf eine knappe Grundkonfiguration eingegangen werden, die man noch lange nicht als „sicher“ bezeichnen kann, immerhin aber als „sicherer“.

Der Kernel, also der Betriebssystemkern, kann und sollte unter Linux immer dem Computer angepaßt werden, auf dem Linux läuft. Wie das geht, erfährt man in den Handbüchern oder unter

unverschlüsselt über das Netz übertragen. Wie schützt man sich davor? Bei Telnet, rsh und rlogin ist das ganz einfach: Diese Dienste sind nicht mehr zu benutzen, denn es gibt die Alternative: SSH, die Secure Shell. Unter Unix/Linux wird einem in der Bedienung kein Unterschied auffallen, die verschlüsselten Dienste heißen hier einfach ssh und slogin.

Als Administrationstool für entfernt stehende Linux- oder Unix-Rechner erfreut sich „Webmin“ (`http://www.webmin.com`) großer Beliebtheit (SSL-verschlüsselt) Unter Windows, wo man i.a. den Umgang mit graphischen Umgebungen gewohnt ist, gibt es für den Privatgebrauch kostenlos den *SSH Client* (also den Teil von SSH, mit dem man sich auf einem anderem Computer anmeldet) unter `http://www.ssh.com`. Mit dem *Secure File Transfer Client* ist gleichzeitig eine sichere Dateiübertragung möglich, sie ersetzt den FTP-Clienten. Unter Unix/Linux kommt man mit 'scp' statt 'rcp' ans Ziel. Voraussetzung ist immer auch der andere Teil von SSH, der SSH-Server, der auf dem Computer laufen muß, auf dem Sie sich anmelden möchten. Ist ein Anmelden nicht möglich, weil der Server fehlt, sprechen Sie die zuständigen Personen ruhig darauf an, es sollte auch in deren Interesse liegen!

Unbedenklicher dagegen ist die Benutzung des sog. Anonymous FTP. Man meldet sich mit dem Benutzernamen „anonymous“ an, als Paßwortersatz ist die eigene E-Mail-Adresse vorgesehen, davon ist jedoch in aller Regel abzuraten, wie im Abschnitt zum *Netscape Communicator* schon genauer ausgeführt wurde. Wenn im Internet-Browser in der Adreßzeile ganz links „FTP://“ steht, handelt es sich um Anonymous FTP.

Paßwörter

Einen sinnvollen Schutz durch Paßwörter erreicht man nur, wenn diese auch gut gewählt sind. Einfache Wörter, wie sie im Duden vorkommen, sind sehr leicht auszumachen, professionelle Angreifer verwenden hierzu Programme, die mit einem Wörterbuch hinterlegt sind. Ein sicheres Paßwort sollte nicht kürzer als sechs Zeichen sein und aus einer unsystematischen Folge aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen bestehen. Ein sehr gutes Beispiel wäre z.B. `7hB$2y8G`. Abhängig vom zum Paßwortaustausch mit dem Server verwandten Verfahren kann auch eine wesentlich größere Paßwortlänge notwendig sein; für Windows-Netzwerke gibt hierzu `http://www.l0pht.com/l0phtcrack/` Auskunft. Wichtig ist auch die Benutzung verschiedener Paßwörter für verschiedene Anwendungen. Oder möchten Sie, daß evtl. der Administrator eines Ihrer freien Mail-Konten mit dem gleichem Paßwort auch Zugriff auf Ihr Konto hat? Auch sollte man sich die Paßwörter gut merken; auf keinen Fall darf man der Bequemlichkeit verfallen und das Angebot z.B. des eigenen Browsers oder Betriebssystems annehmen, es auf der Festplatte zu speichern.

Paßwort vergessen? Kein Problem!

Auf solche Seiten stößt man oft im Internet. Meistens werden einem in diesem Fall eine von zwei Möglichkeiten angeboten: Man hat bei der Erstellung seines Accounts beim Anbieter der Seite seine E-Mail-Adresse hinterlegt und wird manchmal um eine Ausweichfrage gebeten, die in diesem Fall angezeigt wird und die einem entweder bei der Erinnerung an das Paßwort behilflich sein soll oder zur Eingabe eines anderen, vorher festgelegtem Paßwortes auffordert. Diese an sich gute Variante wird oft zu einem Sicherheitsloch, wenn die Antwort auf die Frage zu leicht ist. „Welche Farbe/Marke hat mein Auto?“ kann sicherlich auch von vielen Arbeitskollegen beantwortet werden. Die zweite Variante ist die Zusendung des Paßwortes per E-Mail. Bei ungesicherter Übertragung kann allerdings jeder das Paßwort mitlesen. Näheres kann man im Abschnitt über den sicheren Umgang mit E-Mails nachlesen.

Benutzeraccounts/ -rechte auf dem eigenem Rechner

Professionellere Betriebssysteme wie *Windows NT, Windows 2000* oder *Linux* richten bei der Installation zunächst nur den Benutzer „Administrator“ oder „root“ ein. Wer unter diesem Namen angemeldet ist, hat alle Rechte eines Systemverwalters, daher sollte er auch nur der Systemverwaltung vorbehalten bleiben. Sicherer ist es, von Anfang an einen weiteren Benutzer mit

zu müssen, bietet es sich an, zuerst einmal unter „Zurücksetzen auf“ den Punkt „Hohe Sicherheit“ zu wählen und die Schaltfläche „Zurücksetzen“ anzuklicken. Nun müssen noch eine Reihe von Einstellungen überprüft werden; wir bieten Ihnen zunächst einmal eine Grundkonfiguration, mit der die größtmögliche Sicherheit vor bekannten Angriffen aus dem Internet gegeben ist. Dazu wählen Sie bitte alle Einstellungen wie in Abbildung 6 beschrieben.

Nachdem Sie diesen Vorgang für alle Zonen wiederholt haben, bleiben nur noch ein paar generelle Einstellungspunkte übrig, die sich auf der Karte „Erweitert“ befinden (siehe Abbildung 5). Auch hier sollten Sie wieder die in Abbildung 5 beschriebenen Einstellungen übernehmen.

In dieser sicheren Grundkonfiguration kann es leider vorkommen, daß bestimmte Webseiten nicht oder nicht richtig angezeigt werden oder einzelne Elemente nicht richtig bedienbar sind. Daher kann es in der Praxis notwendig sein, diese restriktiven Einstellungen fallweise zu lockern. Um eine gezielte Lockerung zu ermöglichen, werden nachfolgend die auffälligsten Einschränkungen dieser Konfiguration zusammen mit den Einstellungen aufgeführt, die diese wieder aufheben; dabei sollten Sie allerdings die ebenfalls beschriebenen Sicherheitsprobleme, die sich aus einer solchen Lockerung ergeben, genau beachten.

- ***ActiveX-Steuerelemente und Plugins ausführen, die sicher für Scripting sind***
- ***ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind***
- ***ActiveX-Steuerelemente und Plugins ausführen***
- ***Java-Einstellungen***

Wenn Sie beim Abruf einer Webseite diese Fehlermeldung auf dem Bildschirm sehen:

Abbildung 7: Fehlermeldung – Der Internet Explorer darf aktive Elemente nicht anzeigen

dann benutzt die Seite zur Darstellung Hilfsprogramme, sogenannte ActiveX-Steuerelemente oder Plugins, ohne die Teile der Seite u.U. fehlen oder nicht richtig angezeigt werden können. ***Entgegen der angezeigten Fehlermeldung kann es aber auch sein, daß sich kein ActiveX-Steuerelement auf der Seite befindet, sondern ein in der Programmiersprache Java geschriebenes Programm (ein sog. Java-Applet)***. Es gibt leider keine Möglichkeit, herauszufinden, ob ActiveX-Komponenten oder Java-Applets verwendet werden, ohne die jeweiligen Einschränkungen aufzuheben, welche die Grundkonfiguration setzt. Sollten Sie die fehlenden Elemente für so wichtig erachten, daß Sie die mit der Aufhebung der Sicherheitsrestriktionen verbundenen Risiken in Kauf nehmen wollen, so ist aufgrund des geringeren Gefährdungspotentials zu empfehlen, daß mit der Aktivierung von Java zu beginnen.

Bevor Sie Java aktivieren, sollten Sie sich auf jeden Fall vergewissern, daß Sie den aktuellsten Java-Interpreter installiert haben. Um die auf Ihrem Rechner installierte Build-Nummer zu ermitteln, geben Sie an der Eingabe-Aufforderung "JVIEW" ein. Angezeigt wird z.B. 5.00.3316, die letzten vier Stellen sind maßgeblich, hier 3316. Vergleichen Sie diese mit der unter `http://www.microsoft.com/java/` angegebenen Nummer und laden Sie gegebenenfalls von dort eine aktualisierte Version herunter. Danach können Sie Java aktivieren, indem Sie die Java-Einstellungen auf „hohe Sicherheit“ ändern. Sollte bei der erneuten Seitenanforderung abermals obige Fehlermeldung erscheinen, so verwendet die Seite tatsächlich ActiveX-Steuerelemente oder Plugins.

In diesem Fall kann das Aktivieren von „ActiveX-Steuerelemente und Plugins ausführen“ Abhilfe schaffen; der Webseite wird damit allerdings gestattet, Programme auf Ihrem Rechner

auszuführen, die auch zu bösartigen Zwecken mißbraucht werden können. Mit der Aktivierung des ersten Punktes „ActiveX-Steuerelemente und Plugins ausführen, die sicher für Scripting sind“ erlauben Sie auch dazu geeigneten E-Mail-Programmen wie Microsoft Outlook (Express), diese Hilfsprogramme zum Anzeigen von E-Mail zu benutzen; dies ist jedoch in der Praxis so gut wie nie notwendig und wird vor allem von E-Mail-Viren ausgenutzt, um Schaden anzurichten. Von der Aktivierung des zweiten Punktes „ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind“ können wir nur abraten, da man damit eventuellen bösartigen E-Mails und Webseiten quasi freie Hand läßt, jeden beliebigen Schaden anzurichten.

- ***Active Scripting***

  Auch ohne die obige Fehlermeldung kann es passieren, daß gewisse Elemente einer Webseite, z.B. das Anklicken einiger Links, offensichtlich nicht funktionieren. In diesem Fall ist es wahrscheinlich, daß diese Elemente skriptgesteuert sind. Skripte sind direkt in die Webseite eingebettete Ablaufanweisungen, die – idealerweise benutzergesteuert – Aktionen im Browser ausführen können, ohne neue Elemente herunterladen zu müssen. Diese finden gerne z.B. bei dynamisch aufklappbaren Menüstrukturen, Laufbändern oder kleineren optischen Effekten Anwendung. Es gibt mehrere Varianten dieser Skriptsprachen (z.B. Javascript und VBScript), allen ist jedoch zweierlei gemeinsam: sie werden auf dem lokalen Rechner ausgeführt und können direkt und unbehindert auf das Betriebssystem zugreifen. Die damit einhergehenden Sicherheitsprobleme lassen es wenig ratsam erscheinen, die Verwendung von Skriptsprachen unkritisch zu aktivieren. Bestenfalls bei speziellen Seiten, auf die man unbedingt angewiesen ist, könnte man eine Aktivierung gestatten. Will man nicht regelmäßig die Sicherheitseinstellungen ändern, so gibt es noch die Möglichkeit, „Active Scripting“ auf „Eingabeaufforderung“ zu stellen; dadurch wird man jedesmal gefragt, bevor ein Skript ausgeführt werden soll; die in dieser Mitteilung:

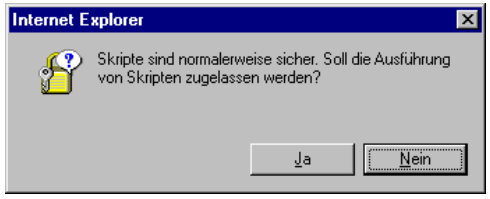


Abbildung 8: Irreführende Abfrage

aufgestellte Behauptung über die Sicherheit von Skripten sollte man aber besser nicht als Entscheidungsgrundlage verwenden.

- ***Cookies annehmen, die gespeichert sind***
- ***Cookies pro Sitzung annehmen (nicht gespeichert)***

  Wenn sich Webseiten darüber beschweren, daß Ihr Browser keine Cookies annimmt, dann müssen Sie sich entscheiden, wie weit Sie dem Betreiber der Webseite (und ggf. dessen Geschäftspartnern) vertrauen wollen. Die Webseite möchte dann nämlich in der Regel Ihren Rechner mit Hilfe eines Cookies eindeutig markieren, um ihn bei späteren Besuchen auf derselben Webseite wiederzuerkennen. Damit wird Ihr Rechner für den Betreiber – und all jene, die diese Markierung ebenfalls entziffern können (das könnten z.B. die Werbepartner der Webseite sein) - identifizierbar, und wenn Sie nur auf einer Seite, die diese Markierung erkennt, persönliche Daten (z.B. für eine Online-Bestellung) eingeben, dann sind Sie im Internet persönlich erkennbar!

  Firmen, die Kontakt zu vielen Webseiten haben, z.B. Online-Werbeanbieter, können damit u.U. ein Profil Ihrer Aktivitäten im Internet erstellen. Wenn Sie eine Webseite, die Cookies verlangt, unbedingt benutzen können möchten - z.B. weil Sie einen Online-Einkauf tätigen wollen - dann empfiehlt es sich, zunächst nur „Cookies pro Sitzung annehmen“ zu aktivieren. Damit sollten

werden können. Bei *Microsoft Outlook* fordert man dazu über *Extras->Optionen->Sicherheit* eine 'Digitale ID' an, beim *Messenger* erreicht man über *Communicator->Extras->Sicherheitsinformationen->Zertifikate->Eigene->Zertifikat anfordern* das Gleiche. Profis schätzen das kostenlose Programm PGP (`http://www.pgpi.org`), das mit einer 4096-Bit-Verschlüsselung nach heutigem Maßstab als wirklich sicher bezeichnet werden kann. PGP läßt sich unterdessen einfach bedienen und über Plugins in viele Mail-Programme integrieren. PGP ist für viele Betriebssysteme verfügbar.

Schutz vor Viren

Zum einen können Viren über sog. „aktive Inhalte“ auf Ihren Rechner gelangen; darunter versteht man in HTML-Mails (die übrigens bei Profis verpönt sind) untergebrachten Programme wie ActiveX, Java- oder VBScript. Diese können bei Aufruf Kontakt mit anderen Rechnern im Internet aufnehmen, oder bereits auf Ihrem Rechner vorhandene Viren in Aktion setzen. Sicherer ist die Deaktivierung aktiver Inhalte in E-Mails, wie sie bei allen führenden E-Mail-Programmen möglich ist; leider ist per Voreinstellung alles aktiviert.

Zum anderen besteht die wohl unterdessen größte Bedrohung in virenbelasteten Attachments. Attachments können harmlose Dateianhänge an E-Mails sein, aber auch z.B. *Microsoft-Word*-Dateien mit Makroviren oder eigenständige Virenprogramme. Allgemein ist die Empfehlung, ein Attachment niemals direkt zu öffnen, sondern auf der Festplatte zu speichern und sofort mit einem (hoffentlich installiertem) aktuellem Virenscanner zu überprüfen. Das gleiche gilt im übrigen auch für den Download von Dateien, die direkt von Webseiten abgerufen werden. Entscheidungshilfe zur Auswahl eines guten Virenscanners (den es für Privatpersonen teilweise sogar kostenlos gibt) findet sich unter `http://agn-www.informatik.uni-hamburg.de` (siehe Virus-Test-Center). Eine Virenprüfung kann je nach Virenscanner und dessen Einstellung entweder automatisch bereits beim Download, beim Empfang von E-Mail, bei jedem Dateizugriff, oder rein manuell nur nach Benutzereingriff vorgenommen werden.

Da Virenscanner neue Virentypen häufig nicht mit der eingebauten Heuristik (eine programmspezifische Sammlung von Methoden, Viren über deren übliche Verhaltensweisen zu finden) erkennen, ist es notwendig, regelmäßig die Virensignaturen des eingesetzten Scanners auf den neuesten Stand zu bringen.

Vor Makroviren, wie sie häufig in *Microsoft-Word*-Dateien auftreten – vor denen aber auch andere Office-Pakete nicht sicher sind – schützt man sich (neben dem Einsatz von Virenscannern) auch durch Öffnen in Texteditoren oder nicht makrofähigen Anzeige-Programmen. *Microsoft Office* bietet zudem die Möglichkeit, vor dem Öffnen von Dateien mit Makros den Benutzer zu warnen, allerdings sagt das nichts darüber aus, ob in dem Makro wirklich ein Virus ist. *Visual Basic Script* Dateien, die Viren enthalten können, erkennt man an der Endung .vbs, sofern man die Anzeige der Dateiendungen (s.o.) aktiviert hat. Deaktiviert man den *Windows Scripting Host*, kann auch ein unbedarfter Doppelklick auf diese Anhänge keine Gefahr bedeuten. Näheres dazu unter dem Abschnitt „Grundkonfiguration unter Windows 95/98/ME“. Für viele heute selbstverständlich ist eine mögliche Bedrohung durch Dateien mit den Endungen .bat, .exe oder .com; garantierte Sicherheit gibt es aber bei keinen Dateien, selbst wenn Sie von Ihnen gut bekannten Absendern stammen. Hat nämlich erst einmal ein Virus die Kontrolle über das Mail-Programm der betreffenden Person übernommen, kann dieses virenbehaftete E-Mails an alle Personen verschicken, die es im Adreßbuch findet. Aus diesem Grunde muß hier auch von der Benutzung des beliebten Programmes *Microsoft Outlook* abgeraten werden, denn es ist das am meisten verbreitete Programm, und die Autoren von Viren suchen sich genau dieses Programm für ihre Zwecke heraus, da sie somit den größten Schaden anrichten können.

FTP & Telnet

FTP, das „File Transfer Protocol“ dient zur Datenübertragung, Telnet dient zum Login auf entfernt stehenden Rechnern, wie auch Remote Login (rlogin) oder die Remote Shell (rsh). Bei der Anmeldung an diese Dienste wird der Benutzername (das sog. Login) und das Paßwort

Im mittleren Bereich „Server für ausgehende Mail“ haben Sie die Möglichkeit, Ihre ausgehende Mail über einen verschlüsselten Kanal zum Mail-Server zu übertragen. Fragen Sie ggf. bei Ihrem

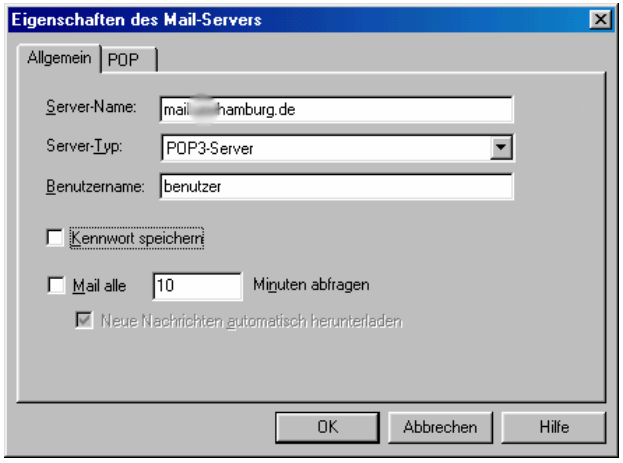


Abbildung 12: Detaileinstellungen für den E-Mail-Transport

Provider nach, ob Sie dieses Merkmal nutzen können. Oder probieren Sie es einfach mal aus! Bedenken Sie hier jedoch, daß damit nur der Transport bis zum Mail-Server Ihres E-Mail-Diensteanbieters verschlüsselt erfolgt – danach wird die E-Mail vermutlich, wie im Internet üblich unverschlüsselt weitergeleitet. Wenn Sie also sicherstellen wollen, daß niemand unbefugt die Nachricht mitliest, so müssen Sie andere Maßnahmen ergreifen. Dazu gibt es im nächsten Kapitel einige allgemeine Hinweise.

Sichererer Umgang mit weiteren Internet-Diensten

Verschlüsseln? Warum?

Nur in den allerseltensten Fällen findet die Datenübertragung im Internet direkt zwischen Ihrem und dem Rechner statt, auf den Sie zugreifen möchten; eine Internetverbindung zwischen Hamburg und München kann also durchaus über Tokio, Los Angeles und New York laufen. Alle Rechner auf dem Weg können Datenpakete auslesen.

E-Mail

Hierbei geht es nicht um das Lesen der E-Mails im Browser wie z.B. unter **`http://www.gmx.de`**, **`http://www.hotmail.com`** oder **`http://www.web.de`**, sondern um das Abholen mit einem E-Mail-Programm wie den an die Browser gebundenen *Microsoft Outlook* oder *Netscape Messenger*, auch Programme wie *Qualcomm Eudora* oder *Pegasus*. Zum Abholen und Senden sollte immer die SSL-Verschlüsselung aktiviert sein, sonst ist auch hier beim Anmelden auf dem Server die Paßwortübertragung ungeschützt. Leider ist die SSL-Übertragung unter *Netscape Messenger* nicht bei POP-Servern möglich, hier sollte auf jeden Fall auf einen IMAP-Server ausgewichen werden. (i.d.R. werden immer beide Dienste angeboten, fragen Sie im Zweifel bitte Ihren Provider.)

Diese Einstellungen betreffen nur die geschützte Übertragung zu Ihrem Provider und zurück; im weiteren Verlauf sind die Mails ohne weitere Einstellungen (siehe gesonderten E-Mail-Abschnitt) weiterhin ungeschützt!

E-Mails werden meistens völlig unverschlüsselt übers Netz geschickt, diese können fast so einfach wie Postkarten mitgelesen werden. Wesentlich sichererer ist eine Übertragung von 128 Bit RC2-verschlüsselter Mails, wie sie mit *Microsoft Outlook* oder dem *Netscape Messenger* verschlüsselt

die meisten Warenkorb-Systeme der einschlägigen Anbieter funktionieren, alle Markierungen werden jedoch nach dem Beenden des Internet Explorers wieder gelöscht. Desweiteren haben Sie noch die Möglichkeit, vor Annahme eines jeden Cookies gefragt zu werden, ob Sie dies zulassen; dies geht - sowohl pro Sitzung als auch dauerhaft - indem Sie die obigen Punkte auf „Eingabeaufforderung“ setzen. Allerdings müssen Sie dann damit rechnen, eine Vielzahl von Anfragen auf Cookie-Übermittlung zu erhalten, die dem Bedienkomfort auf bestimmten Seiten ziemlich abträglich sind.

Netscape Communicator 4.7x

Die Einstellungen für Cookies, Java/JavaScript etc. lassen sich in den *Netscape*-Browsern der Reihe 4.7x einfach vornehmen. Hierfür gibt es ein eigenes *Einstellungen*-Fenster, das man über das Menü *Bearbeiten* und den Punkt *Einstellungen* erreicht.

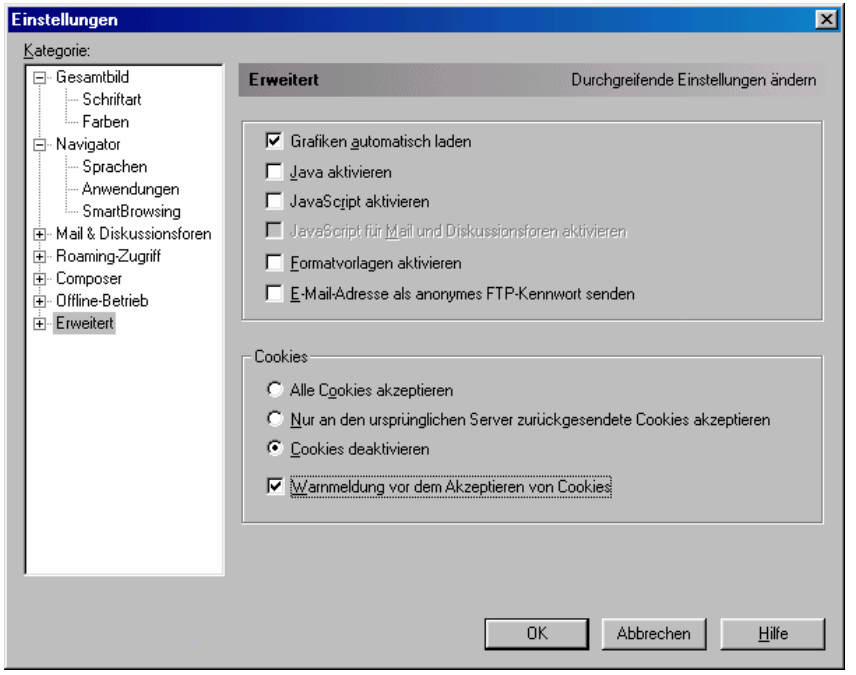


Abbildung 9: Das erweitere Einstellungs-Menü des *NetscapeCommunicator*

Im linken Teil des nun erscheinenden Fensters befindet sich eine Leiste mit Kategorien und Unterkategorien. Die Wichtigste für unsere Belange ist *Erweitert*. Dort befinden sich alle Einstellungsmöglichkeiten zu den Punkten Cookies und Java bzw. JavaScript. Die quadratischen Felder links der einzelnen Punkte sollten für:

- „Java aktivieren“
- „JavaScript aktivieren“
- „Automatische Installationsoption aktivieren“
- „E-Mail-Adresse als anonymes FTP-Kennwort senden“

frei sein und keine Häkchen enthalten. Früher hatte man beim anonymen FTP bei der

Paßwortabfrage seine E-Mail-Adresse aus Höflichkeit angegeben, damit der Betreiber am anderen Ende wußte, wer sein System benutzt. Heutzutage ist von dieser Höflichkeit stark abzuraten. Von Firmen wird die E-Mail-Adresse prompt zur E-Mail-Reklame ausgenutzt, und außerdem lassen sich im Verbund mit anderen Systemen, auf denen Sie dieselbe Adresse angegeben haben, wieder Profile erstellen; zu deutsch: Man kann Ihre Bewegungen im Netz ausspähen.

Wie Cookies funktionieren und ob sie immer gut schmecken, ist bereits im Abschnitt zum *Internet Explorer* genauer beschrieben. Zu Ihrem Schutz sollten Sie Cookies hier auch gleich deaktivieren. Zuvor sollten Sie noch zusätzlich „Warnmeldung vor dem Akzeptieren von Cookies“ mit einem Häkchen anwählen.

Eine Besonderheit stellt unter *Netscape* das sog. *Smart Browsing* dar. In der Kategorie *Navigator* gibt es eine Unterkategorie *Smart Browsing*. Wird diese angewählt, so erscheint folgender Dialog:

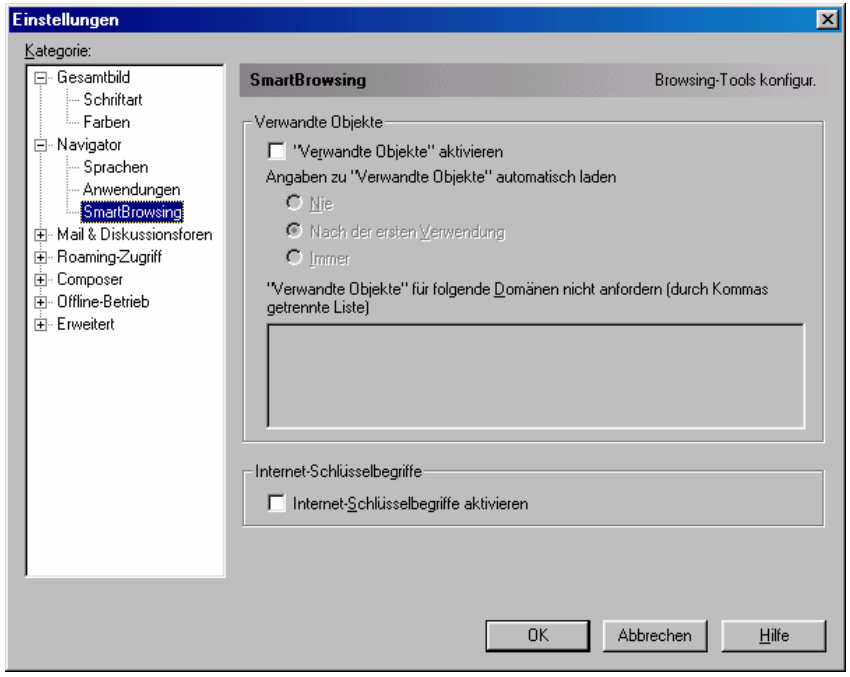


Abbildung 10: *Smart Browsing* unter *Netscape Communicator 4.7x*

Wie aus der Abbildung ersichtlich, teilt sich *Smart Browsing* in die beiden Bereiche *Verwandte Objekte* und *Internet Schlüsselbegriffe* auf. Ersterer beschreibt das Verhalten bezüglich der Übermittlung von Uniform Resource Locators (URL), also Webadressen, an den Internet-Suchdienst der Firma Netscape, deren System dann nach weiteren URL zum selben Thema sucht. Die Standardeinstellung ist „Nach der ersten Verwendung“. Dies bedeutet: nachdem in der bestehenden Sitzung einmal eine URL an Netscape übermittelt wurde – etwa um sie zu vervollständigen –, wird jede URL jeder nachfolgend besuchten Seite an Netscape übermittelt. Dies stellt einen erheblichen Eingriff in die Privatsphäre dar, denn somit werden Ihre Bewegungen im WWW eigentlich von fremder Seite protokolliert! Um sich davor zu schützen, sollten Sie entweder die Option "Nie" auswählen, oder das Häkchen vor "Verwandte Objekte aktivieren" entfernen. Im ersteren Fall wird nur dann eine Anfrage losgeschickt, wenn der Benutzer tatsächlich darum gebeten hat.

Der zweite Bereich *Internet-Schlüsselbegriffe* steht für eine automatische Suchanfrage des *Netscape Communicator* bei der Eingabe einer unvollständigen Adresse zwecks Vervollständigung derselben. Da dies wiederum eine Anfrage an den Netscape-Suchserver bedeutet, die grundsätzlich ohne Rückfrage an den Benutzer erfolgt, sollten Sie auch diesen Punkt deaktivieren.

Nun noch ein letzter Punkt zum *Netscape Communicator*, falls Sie Ihre E-Mail mit dem *Netscape Messenger*, dem E-Mail-Programm des *Communicators*, lesen. Es gibt dort die Möglichkeit, das Kennwort zum Abrufen der E-Mail speichern zu lassen, d.h., Sie geben es nur einmal beim Einrichten des *Communicator* ein und brauchen es dann nicht mehr einzugeben. Bedenken Sie bitte, daß gespeicherte Daten von Angreifern ggf. ausgelesen werden können. Es könnte also auch Ihr Paßwort treffen. Aus Sicherheitsgründen sollten Sie daher darauf verzichten, es speichern zu lassen. Aber keine Angst! Sie müssen nun nicht jedesmal Ihr Paßwort eingeben, wenn Sie nach neuer Mail schauen – jedenfalls nicht, solange Sie den Netscape Communicator nicht beenden. Die Paßworteingabe ist lediglich einmal pro Sitzung erforderlich. Außerdem schützt die regelmäßige Eingabe auch ein wenig davor, das Paßwort zu vergessen.

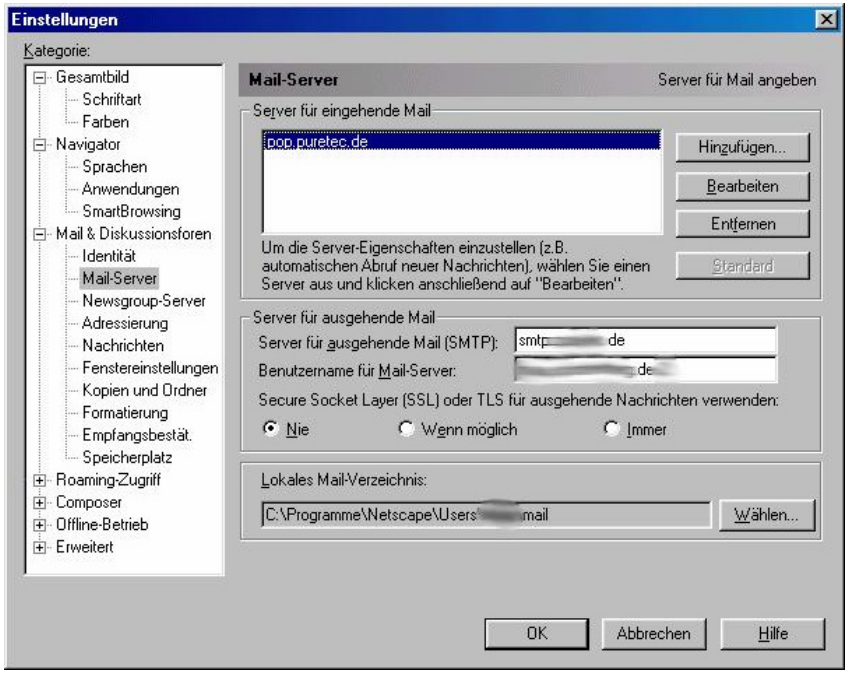


Abbildung 11: Mail-Server-Einstellungen mit dem Netscape Communicator 4.7x

Die entsprechende Einstellung nehmen Sie in *Mail & Diskussionsforen*, Unterkategorie *Mail-Server* vor. Doppelklicken Sie den Mail-Server und ein entsprechendes Fenster erscheint. Hier können Sie wählen, ob Ihr E-Mail-Kennwort gespeichert werden soll oder nicht. Klicken Sie anschließend auf OK.