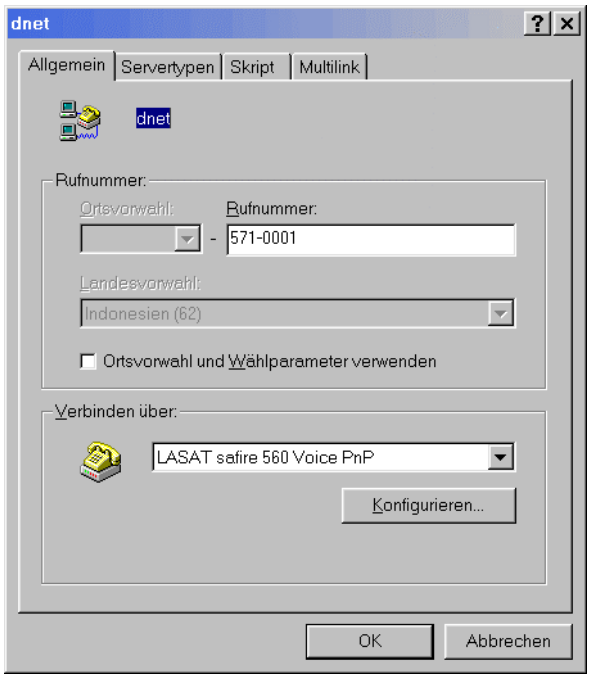
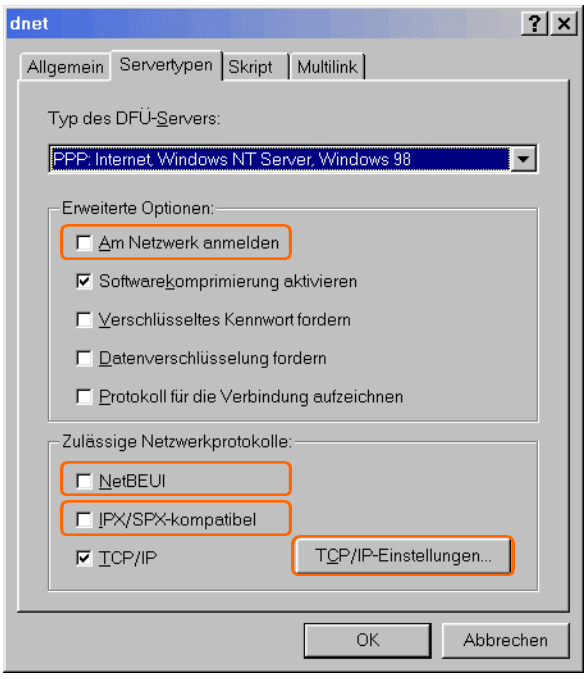
1. Den Internetzugang optimieren

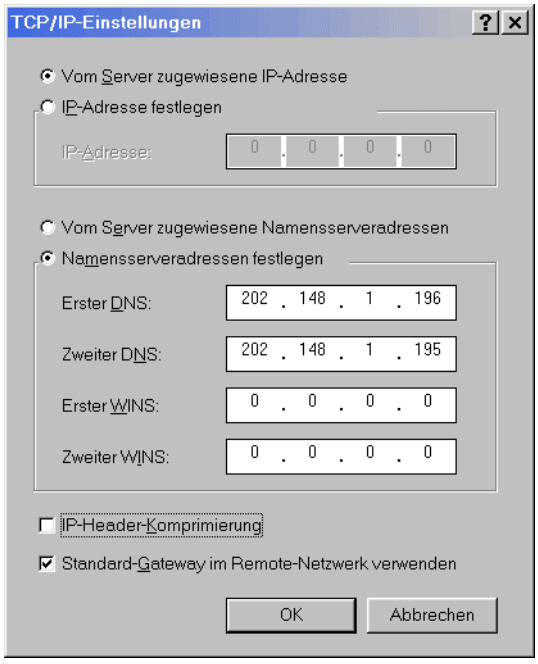
Einträge im DFÜ-Netzwerk überprüfen

Auf dem Desktop doppelklickt man auf „Arbeitsplatz“ und dort auf „DFÜ-Netzwerk“. (DFÜ heißt **D**aten**F**ern-**Ü**bertragung). Ist bei dem Computer schon eine Verbindung mit einem Internet-Provider eingerichtet, klickt man mit der rechten Maustaste auf diese Verbindung und wählt das „Eigenschaften“-Menü.
Wer noch keine Internet-Verbindung hat, bekommt in der Regel vom Internet-Provider eine entsprechende Anleitung, wie man eine „Neue Verbindung erstellen“ soll.
Im folgenden soll anhand des Providers „dnet“ gezeigt werden, welche Einstellungen für einen optimalen Zugang nötig sind.





Unter „Allgemein“ ist auf die richtige Telefonnummer zu achten. Einige Provider haben unterschiedlich schnelle Modems an verschieden Telefonleitungen hängen – dieses ist meist irgendwo auf den Internet-Seiten des Provider vermerkt.
Beispiel Dnet: 571-0001; 572-1110; 251-3001; 251-3002; 251-3601; 251-3602; 251-3603 - alle „langsam“
Centrin: 252-3777; 252-3888; 252-5333 sind „langsame“ Modems
5299-4222 und 2351-8888 schnelle 56K Flex/V.90–Modems

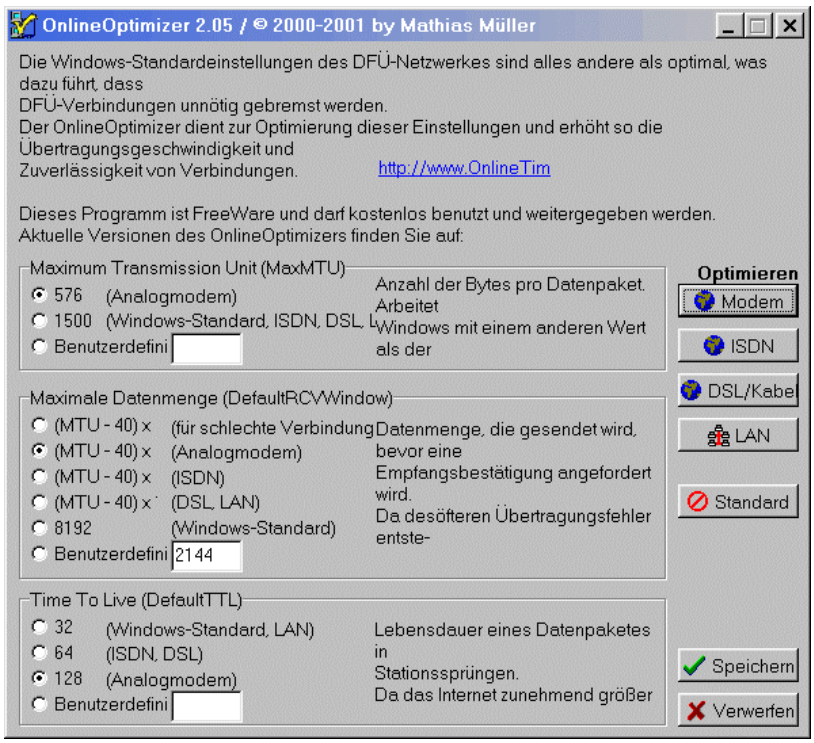


Unter „Servertypen“ muss „Am Netzwerk anmelden“, „NetBEUI“ und „IPX/SPX-kompatibel“ deaktiviert werden (also „ohne Häkchen“). Das erste kostet unnötig Zeit beim Einwählen, die Aktivierung fürs Internet unnötiger Netzwerkprotokolle schafft Zugangsmöglichkeiten für Angreifer aus dem Internet.
Unter „Skript“ und „Multilink“ ist in der Regel nichts zu ändern.

Wichtig ist allerdings, dass man bei „Servertypen“ auf die Schaltfläche „TCP/IP-Einstellungen“ klickt und dort überprüft, ob die richtigen DNS-Nummern eingetragen sind.
Diese Nummern kennzeichnen die Zugangsadressen des Providers, für den jeweiligen Provider muss man die erste und zweite DNS in Erfahrung bringen und eintragen – sonst dauert das Einwählen länger als nötig oder klappt überhaupt nicht.
Centrin:
1.DNS 202.146.255.3
2.DNS 202.146.255.5
Dnet:
1.DNS 202.148.1.196
2.DNS 202.148.1.195

Datendurchsatz optimieren

Eine weitere Optimierung betrifft die Art und Weise, wie Windows die Daten auf die Reise schickt. Da diese drei Einstellungen tief in der Windows-Datenbank verborgen sind, ist das zum Ändern dieser Parameter das Hilfsprogramm „OnlineOptimizer“ sinnvoll.



2. Programme zum Benutzen des Internets

Das Internet ist „nur“ eine Vielfalt von Kabeln, die einigermaßen intelligent genutzt werden. Zwei Arten der Nutzung sind besonders populär : Das Versenden von EMails und die Hyperlink-Struktur des „www“ (World Wide Web). Daneben kann des Internet u.a. zur reinen Datenübertragung genutzt werden (ftp) oder zur Fernbedienung von Computern (Telnet).
Wir beschränken uns auf die Nutzung des „www“ und „EMail“.

„http://www…“ und „URL[1]“ benutzen : Ein Browser zur Nutzung des World Wide Web

Zur Nutzung des www benötigt man einen „Browser“ – ein Programm, das per Hand eingegebene Adressen („URL“) verstehen kann und beim Klicken auf besondere Markierungen („hyperlinks“) ebenfalls bestimmte Aktionen durchführt. Die bekanntesten Browser sind

- der Microsoft Internet-Explorer,
- der Netscape Navigator (bzw. Mozilla),
- Opera.

Während der Internet-Explorer ungefragt auf dem Windows-Computer installiert wird, müssen die anderen beiden extra installiert werden.
Da der Netscape Navigator technisch veraltet ist, beim Internet-Explorer sehr viele Sicherheitslücken existieren und die Abschottung des Computers gegen Angriffe aus dem Internet selbst für Fortgeschrittene nicht einfach ist, möchte ich mit dem werbefinanzierten[2] „Opera“-Browser arbeiten.
Hervorzuheben sind bei Opera

- die „Hotlist“ (die den „Favoriten“ im Explorer entspricht),
- die leichten Anfragen an Suchportale (wie z.B. google.de),
- die Taste (F11) für „Vollbildsurfen“
- die Tasten (+) und (-) auf der numerischen Tastatur für Schriftvergrößerung/ -verkleinerung
- die übersichtlichen „Einstellungen“ (Sicherheit !) im Menü „Datei“ mit einer meist verständlichen Hilfe
- der Möglichkeit des Löschens aller persönlichen Daten am Ende einer Internet-Sitzung unter „Private Informationen löschen“
- und vieles, was man im Lauf der Zeit entdeckt (und sich bestimmt oft über sinnvolle Details freuen wird …)

[1]) URL : Uniform Resource Locator
[2]) ein kleines Werbefenster rechts oben mit geringer Datenmenge (für 39 US$ zu entfernen), Opera ist *keine* Spyware

„@“ benutzen : Ein Programm zum Empfangen und Senden von EMails

Es gibt zwei Arten EMails zu benutzen:

- Eigentliche EMail-Programme wie „Outlook Express“, „Pegasus“, „The Bat“, „Eudora“, oder auch die beim Netscape Navigator und Opera integrierten Mail-Programme
- oder Email-Programme, die im www *per Browser* zu bedienen sind („webmail“). Zu dieser Kategorie gehören die Programme, die man beim Benutzen von Diensten wie „Hotmail“ benutzt.

Die zweite Kategorie von Programmen bietet den Vorteil, dass man kein zusätzliches Programm auf dem Rechner installieren muss und – das ist für viele entscheidend – problemlos von jedem Internet-Cafe seine Mails abrufen kann (die allerdings bei einiger Unvorsichtigkeit vom nächsten Benutzer des Computers gelesen werden können). Nachteilig ist allerdings, dass die Mails von fremden Händen verwaltet werden .

Eine vernünftige Korrespondenzverwaltung geht nur mit Programmen der ersten Art.
Auch hier gilt leider wieder, dass das Microsoft Programm „Outlook Express“ sehr unsicher ist. Dies liegt nicht so sehr daran, dass Microsoft zu dumm ist, sondern ist hauptsächlich darin begründet, dass Microsoft die Benutzer nicht mit Unbequemlichkeiten verschrecken möchte. Deshalb sind die Grundeinstellungen dieses Email-Programms so, dass viele vom Absender erwünschte Dinge auch in dieser Form auf unserem Computer ankommen. Da es leider nicht nur wohlmeinende Zeitgenossen gibt, können aber auch die „bösen Hacker“ (die „echten Hacker“ sind für Privatleute keine Bedrohung) und „Script-Kiddies“ einiges mit unserem Computer anstellen …
Der Einfachheit halber würde ich als Anfänger das in Opera integrierte Email-Programm benutzen, als erfahrener Computerbenutzer ist es ratsam, die Email in einer umfassenderen Korrespondenz-, Aufgaben- und Terminverwaltung zu integrieren.

3. Sicherheit im Netz

Gefahrenarten

Es gibt zwei Kategorien von Gefahren
1) Beschädigung von Daten auf der Festplatte
2) Ungewollte Übermittlung persönlicher Daten

Die erste Gefahr ist ärgerlich, aber zu meistern, wenn man täglich Sicherheitskopien der eigenen Dateien anfertigt. Die zweite Gefahr ist heimtückischer, da man meist nichts von der Datenspionage merkt – oder erst dann, wenn die Dateien aus dem Ordner „Eigene Dateien“ wahllos an EMail-Partner verschickt wurden. Insbesondere können Anhänge an EMails getarnte Programme enthalten, die Schadensroutinen auf dem Computer in Gang setzen. Hier gilt es, Anhängsel NIEMALS ohne ausdrückliche Unbedenklichkeitsversicherung des Absenders (in einer Extra-EMail!) zu aktivieren. Insbesondere Dateien mit den mit den folgenden Endungen (kein Anspruch auf Vollständigkeit!) enthalten aktive Inhalte und können deshalb gefährlich sein:

- EXE, COM, BAT — ausführbare Programme
- REG, INF — Registry-Datei, Install-Datei
- VBS, VBE JS, JSE — Visual Basic Script Java Script
- WSH — Windows Scripting Host
- HTM, HTA — kann auf Scripte verweisen
- PIF — Program Information File
- SCR — Bildschirmschoner
- DOC, XLS, PPT, MDB, MDE — Office-Dokument (Makroviren)

Das Virenschutzprogramm »AntiVir« untersucht folgende Dateien: .386 .ACM .APP .ASP .AWX .AX .BAT .BIN .CDF .CHM .CLASS .CMD .CNV .COM .CPL .CSH .DLL .DLO .DO? .DRV .EML .EXE .FLT .FOT .HLP .HT* .INI .JS .LNK .MDB .MOD .NWS .OBJ .OCX .OLB .OSD .OV? .PDR .PGM .PIF .PKG .POT .PPS .PPT .PRG .RPL .RTF .SCR .SCRIPT .SH .SHA .SHB .SHS .SHTM* .SPL .SWF .SYS .TLB .TSP .TTF .VB? .VLM .VXD .VXO .WIZ .WLL .WPC .WWK .XL? .XML

Achtung: Im Windows-Explorer (nicht Internet Explorer) unter Ansicht–Ordneroptionen–Ansicht „Dateinamenerweiterung bei bekannten Dateitypen ausblenden“ nicht aktivieren!
Leider bestehen auch durch html-(bzw. htm-, hta-) Dateien Gefahren, weswegen auch solche Dateien nicht automatisch durch das EMail-Programm geöffnet werden sollten (was der „Outlook Express“ meines Wissens macht)

Abwehr der Gefahren

- Einstellungen des Browsers bzw. Emailprogramms überprüfen.
- Virenscanner installieren und wöchentlich aktualisieren.
- Programme und ausführbare Dateien (s.o.) aus dem Internet zuerst auf der Festplatte speichern, dann mit dem Virenscanner untersuchen und erst dann starten.
- Gesundes Misstrauen gegenüber seltsamen EMails auch von guten Bekannten.
- Dokumente (doc, pdf, ...) nur mit nicht-makrofähigen Viewern öffnen.
- Bei erhöhter Bedrohung (insbesondere bei permanenter Verbindung mit dem Internet) zusätzliche Benutzung eines Firewalls

Schutzprogramme und genauere Informationen finden sich auf der CD-ROM …