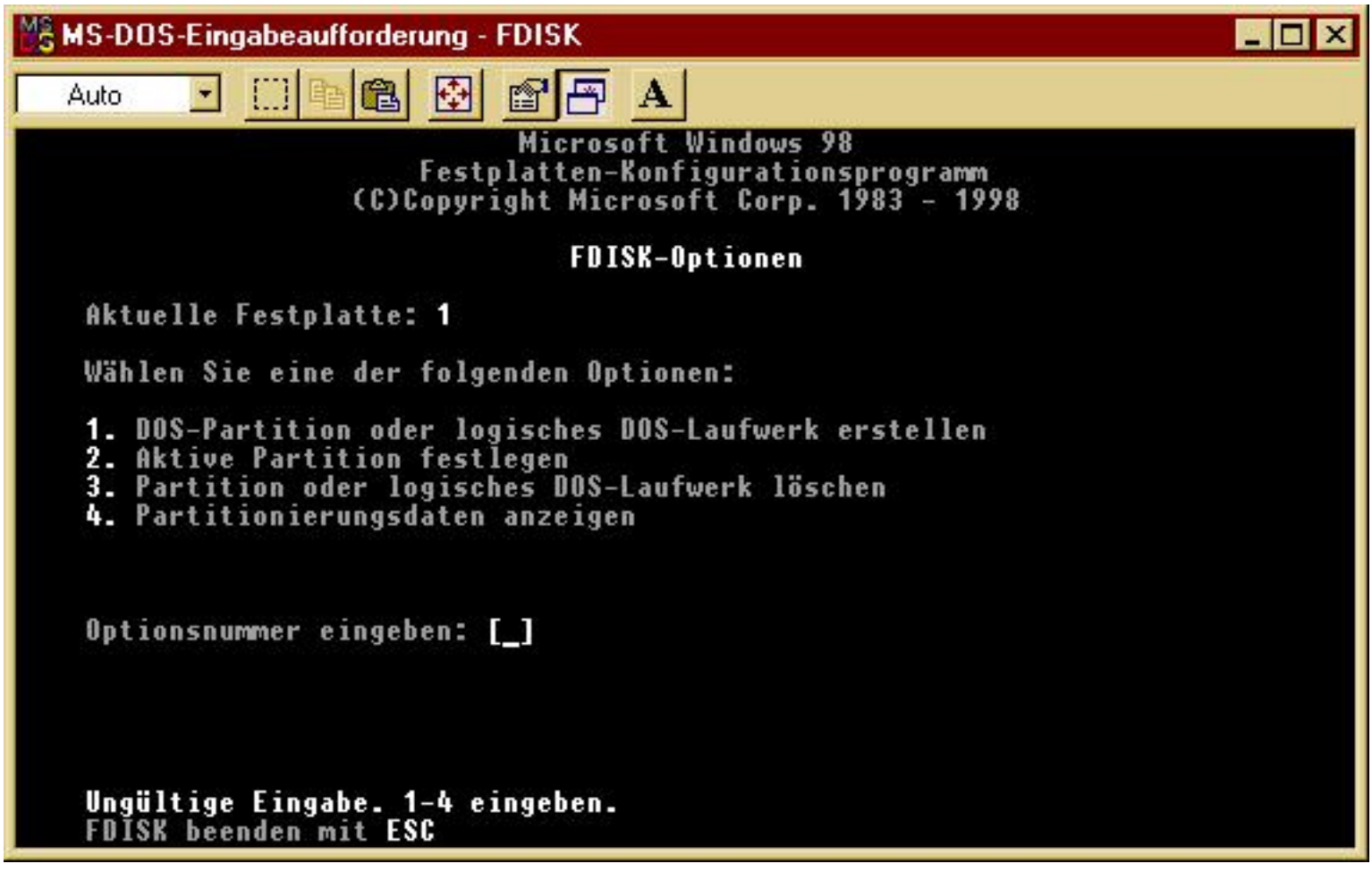
Windows Home Security

Ich möchte hiermit die Grundeinstellungsmöglichkeiten für Windows in Verbindung mit dem Explorer, Internet Explorer und einigen kleinen Hilfsprogrammen aufzeigen.
Da Windows98 nicht mehr so oft im Einsatz ist, werde ich hier verstärkt auf WindowsXP eingehen und kleine Veränderungen die zur Sicherheit vorgenommen werden können.
Dieses Dokument ist eine Weiterentwicklung des bereits veröffentlichten Schriftstücks "Windows absichern".

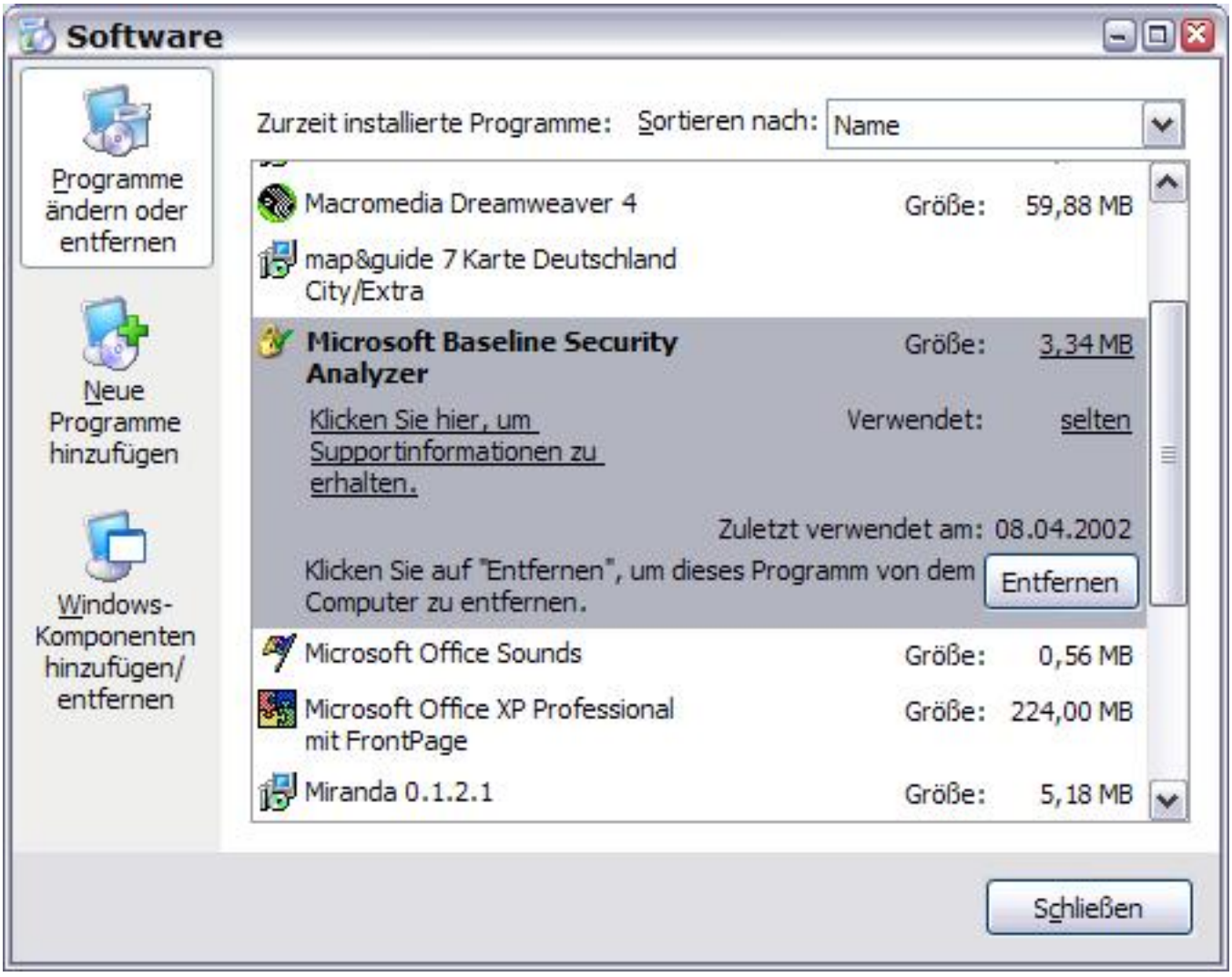
Windows Installation: Allgemeine Hinweise.

Zunächst einmal möchte ich damit beginnen, daß man wie schon oft beschrieben Windows bei der Installation nicht auf dem vorgeschriebenen Pfad installieren muß.
Standartinstallationspfad für Windows ist C:\WINDOWS.
Sie können wärend der Installation von Windows den Pfad frei wählen und somit schon im Ansatz des Betriebssystems eine weitere Sicherheitsstufe erzeugen.
Windows fragt Sie auf welchem Pfad Windows installiert werden soll und hier können frei wählen und tragen als Beispiel nachfolgende Daten ein: F:\WINDOWS oder C:\Files\ etc.
Beachten Sie jedoch vorher, daß Windows kurz vor der Installation eine geeignete Partition anlegt, die mindesten über 1 GByte Größe verfügt. Sie können natürlich auch manuell eine Partition erstellen.
Alternativ können Sie auch eine Windows98 Startdiskette verwenden, diese in das Diskettenlaufwerk einlegen und eine freie Partition mit dem Programm FDISK.exe erzeugen.
Sie brauchen hierfür keine fachlichen Kenntnisse, da das Programm selbsterklärend arbeitet.



Hier sehen Sie den Startbildschirm und haben die Auswahl welche Funktion ausgeführt werden soll.
Bei jeglichen Arbeiten sollten nachfolgende Ratschläge beachtet werden, wenn man auf die eigene Sicherheit bedacht ist:
- lassen Sie niemanden bei der Einrichtung des Computers zuschauen, wenn Sie sich allein dazu in der Lage fühlen
- achten Sie grundlegend darauf, daß der Monitor nicht von einem anderen Fenster einsehbar ist
- Festplatten können verschließbar sein, Kartenleser oder andere computergestützte Systeme sollten nicht frei zugänglich sein

Bedenken Sie: Die Standartinstallation von Windows erfolgt in einem vordefiniertem Rahmen der von Windows angelegt wird und nicht direkt zu kontrollieren ist.
Windows installiert entsprechend seinen eigenen Vorgaben Hilfsprogramme und unnötige Applikationen, die zum einen Speicherplatz belegen und die Performance beeinträchtigen.



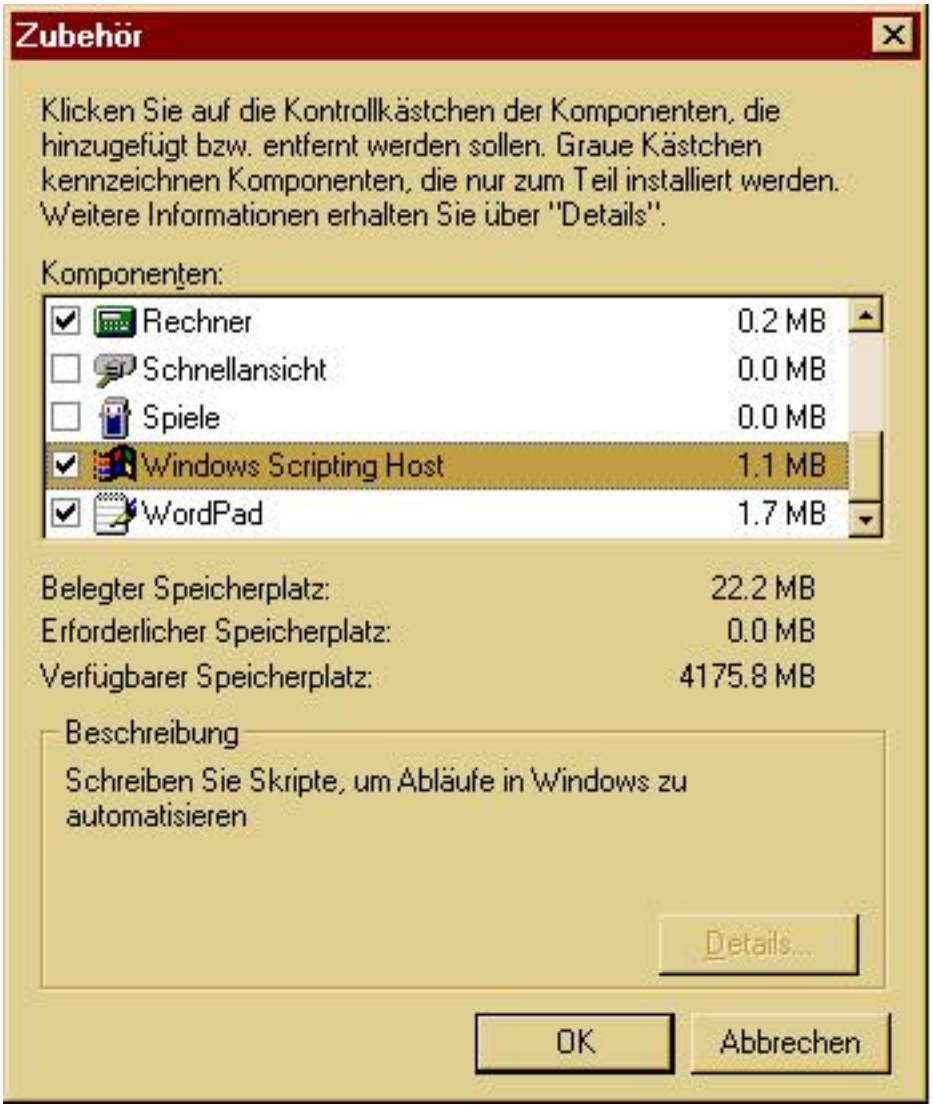
Sie erhalten eine Übersicht über die installierten Programme durch folgende Eingabe:
Klicken Sie: Start - Einstellungen - Systemsteuerung - Software.
Nun zeigt die Windows Systemsteuerung die bereits installierten Komponenten an und Sie können wählen welche Sie weiterhin auf dem Computer verwenden wollen.
Wenn Sie nun einige Windows Komponenten deinstallieren möchten die Sie nicht brauchen, so wählen Sie in der linken Leiste den Button Windows-Komponenten hinzufügen/entfernen.

Aber wählen Sie bitte mit bedacht, da einige Programme benötigt werden.
Folgende Programme empfehle ich zu deinstallieren, solange Sie den Computer für private Anwendungen verwenden wollen:
- Windows Webserver kann deinstalliert werden, dieser wird nur dann benötigt wenn Sie anderen Benutzern aus dem Internet gestatten wollen, auf Ihrem Computer HTML Seiten anzuschauen.
Den Webserver finden Sie ebenfalls unter den Windows-Setup und dann im Unterpunkt Internet-Programme.
Bei Windows Professional Versionen finden Sie den bekannten IIS von Microsoft, der den gleichen Zweck unter Windows NT, Windows2000 oder WindowsXP erfüllt wie der Webserver.
Hinweis: Für Windows2000, daß nach wie vor ein sehr weit verbreitetes Betriebssystem ist, hat Marc Ruef ein sehr gutes Kompetendum geschrieben: Sicherheit unter Windows2000.
IIS ist der Internet-Information-Server von Microsoft, der HTML Seiten für entfernte Benutzer im Internet zur Verfügung stellt.
Weitere Dienste sind hier möglich auf die ich jedoch nicht näher eingehen möchte, da es für diese Zwecke unerheblich ist. (FTP, EMail etc.)
Sehen Sie hier im Beispiel, den deinstallierten IIS unter WindowsXP Professional:

Durch das entfernen oder setzen des Haken können dann die Applikationen installiert oder entfernt werden.
Sie sehen schon, daß einige Dienste mit bis zu 15 Mbyte oder mehr auf die Festplatte installiert werden.
Hier können Sie die nicht gewünschten Softwarebestandteile von Windows entfernen, die Sie nicht mehr benötigen.

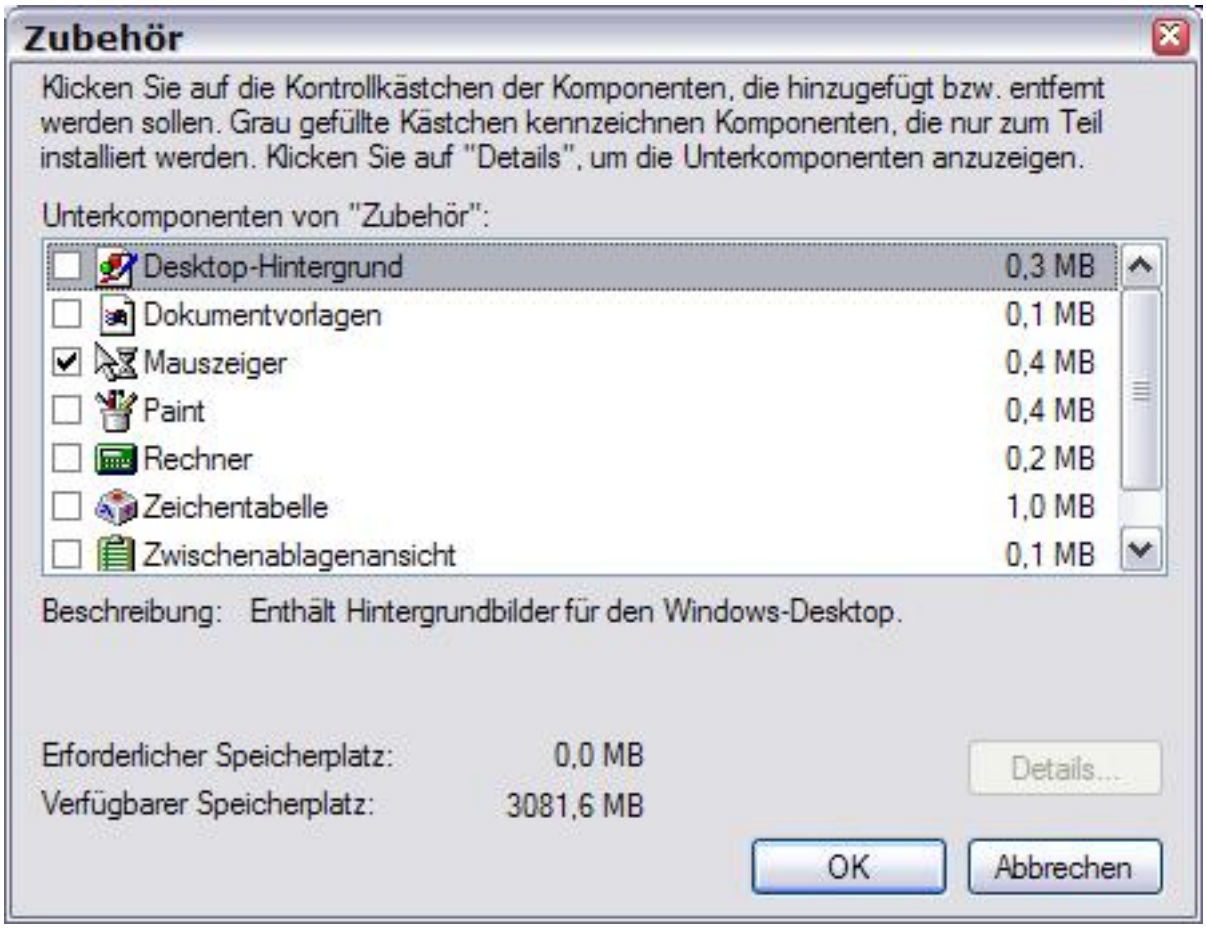
- Ebenfalls muß nicht installiert sein der Windows DFÜ-Server, da hierdurch andere Benutzer die Möglichkeit haben, sich über eine DFÜ-Verbindung mit Ihrem Computer zu verbinden.
Der Windows DFÜ-Server befindet sich ebenfalls im Windows Setup im Untermenü Verbindungen.

- Wenn Sie auf Ihrem Computer keine automatisierten Aufgaben über Visual Basic Script steuern möchten, so ist es ratsam Windows Script Hosting zu deinstallieren.
Windows Script Hosting finden Sie im Windows Setup im Untermenü Zubehör wo Sie auf Details klicken und dann einen Haken bei entfernen machen können.
Sie finden Windows Script Hosting unter Windows98 noch im Menü: Start - Einstellungen - Systemsteuerung - Windows-Setup - Zubehör.



Eine Platzeinsparung auf der Festplatte von 1.1 MByte ist das Ergebnis.
Im Normalfall kann man den Taschenrechner und die Bildschirmschoner entfernen, da diese nicht verwendet werden.
Bildschirmschoner wurden bei alten Generationen von Bildschirmen verwendet, damit sich das

letzte Bild nicht auf dem Bildschirm einbrennt und somit dauerhaft den Bildschrim untauglich macht oder beschädigt.
Verwenden Sie aus Sicherheitsgründen einen Bildschirmschoner, so sollte dieser natürlich installiert bleiben und mit einem Passwort zum Schutz versehen sein.
Unter WindowsXP sieht das Untermenü Zubehör etwas umfangreicher aus, beinhaltet nach der Standartinstallation jedoch nicht bedeutend mehr Programme als Windows98 oder Windows2000:

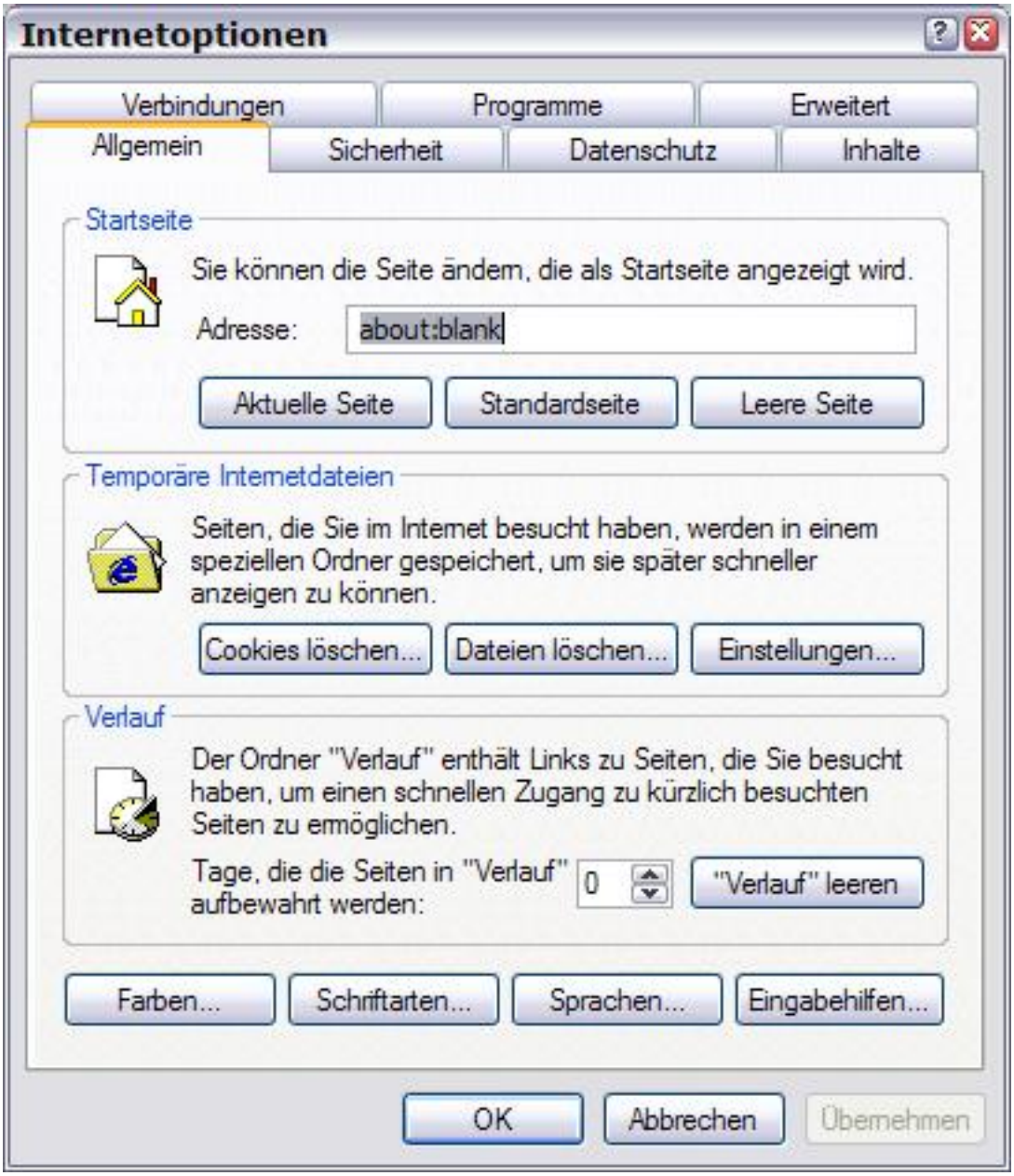


Windows und sein Startverhalten: Booten.

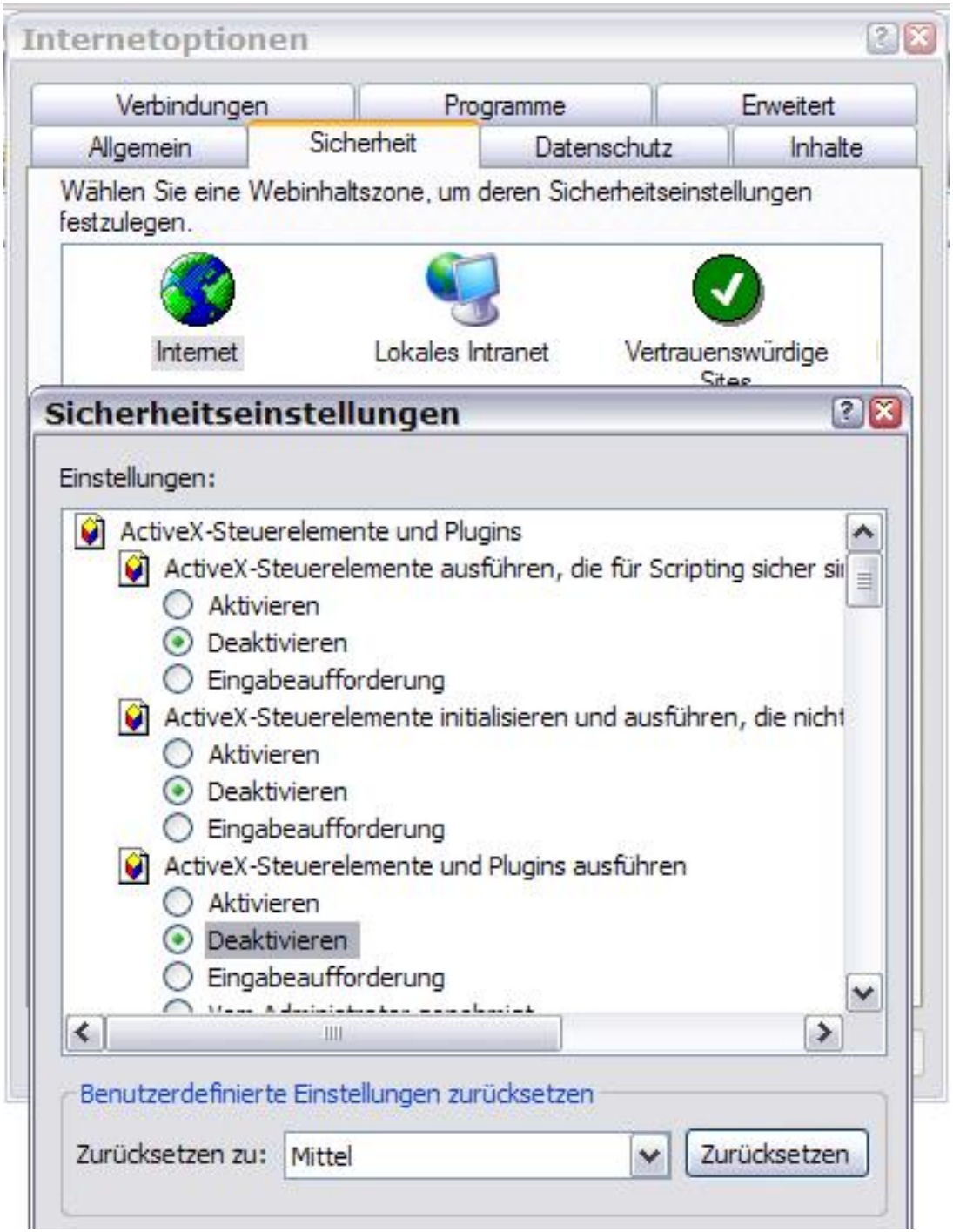
Sie allein können mit ein wenig Aufmerksamkeit und Aufwand bestimmen, wie Windows gestarten werden soll und was genau für Daten und Dateien geladen werden.
Entscheident ist das BIOS eines Computers beim booten.
Für Ihre eigene Sicherheit sollten Sie nach der ersten Systeminstallation das BIOS Ihres Computers mit einem Passwort absichern, sodaß niemand unberechtigt Zugriff darauf hat.
Ebenfalls ist im BIOS einstellbar, in welcher Reihenfolge das BIOS den Startvorgang abfragen soll.
Einstellungen sind hierbei meistens, daß BIOS die Abfrage nach C:, CD-ROM, A: absucht und dort ein Betriebssystem gesucht wird um es vom BIOS zu starten.
Lassen Sie von einem Fachman prüfen, ob Ihr BIOS über einen Jumper verfügt, der einen Schreibschutz aktiviert.
Sollte dieser nicht gesetzt sein, so kann man das dann nachholen.

Windows Internet Explorer: Das Internet sicher betrachten.

Öffnen Sie den Internet Explorer von Microsoft und klicken anschliessend auf Menü - Extras - Internetoptionen.
Es öffnet sich ein neues Fenster mit verschiedenen Schaltflächen, hier WindowsXP:



Die wichtigsten Einstellungen finden Sie in der Schaltfläche Sicherheit und dann Internetzone. Hier haben Sie die Möglichkeiten, diverse Einstellungen vorzunehmen um nicht Opfer von Attacken aus dem Internet zu werden bzw. das Risiko bereits im Ansatz hier minimieren.
Die Möglichkeiten die sich hier finden sind bereits sehr vielseitig und nicht mehr mit Windows 98 vergleichbar.
Daher gehe ich wieder etwas detaillierter auf WindowsXP Professional ein.
Beginnend bei den Grundeinstellungen klicken Sie auf die Schaltfläche "Stufe anpassen" und gelangen nun zum Fenster um ActiveX, Java und Co. einzustellen.



Hier sehen Sie bereits, daß ActiveX Steuerelemente aus dem Internet nicht zugelassen sind und entsprechend nicht bei Ihnen auf dem Computer ausführbar sind.
Ich empfehle bei allen ActiveX Steuerelementen die Deativierung, gleich ob es sich um signierte oder unsignierte handelt.
PlugIns oder Downloads von ActiveX sollten ebenfalls deaktiviert sein, da diesen Zustand 0190er Dialer ausnutzen könnten um sich im Hintergrund zu installieren.
Gleiche Einstellungen gelten hierbei natürlich auf für Java Applets.
Diese sollten ebenfalls entweder gesperrt / deaktiviert sein oder entsprechend die Eingabeaufforderung erfolgen.
Empfehlenswert ist hierbei die Sicherheitseinstellung auf Hoch zu setzen, um eine möglichst hohe Sicherheit zu garantieren.

Im Untermenü Verbindungen kann man dann wie gewohnt einstellen, welche Verbindung als Standart gesetzt werden soll wenn sich der Computer ins Internet einwählt.
Hierbei besteht dann ebenfalls die Möglichkeit, daß Sie die Verbindung nachträglich noch einstellen können:

Ebenfalls von hier aus erreichbar, der Internet-Verbindungsassistent.
Dieser führt Sie sehr einfach durch die Einstellungen bei einer Internetverbindung, falls Sie manuell noch keine eingerichtet haben.
Neu ist unter WindowsXP die interne Firewall, die wie nachfolgend zu sehen ist.

Sie sehen den Menüpunkt Internetverbindungsfirewall, die für jede einzelne Verbindung aktiviert oder deaktiviert werden kann.
Diverse Zeitschriften haben bereits darüber berichtet und auch ich kann Ihnen nicht empfehlen, diese Firewall von WindowsXP einzusetzen um sich zu schützen.
Sehr gute Firewalls für den Einsatz am Homecomputer laufen unter WindowsXP oder Windows2000 und sind sehr leicht zu handhaben.
Daher empfehle ich Ihnen in diesem Bereich eine geeignete Desktopfirewall, die in vielen Fällen sogar für Heimbenutzer kostenlos zur Verfügung steht.
Ich werde später für Sie noch etwas genauer auf die Firewalls eingehen.

Ein neues Highlight ist die Cookieverwaltung von WindowsXP unter dem Menüpunkt Datenschutz.
Hier haben Sie die Möglichkeit das Cookieverhalten des Computers ein wenig besser zu kontrollieren:

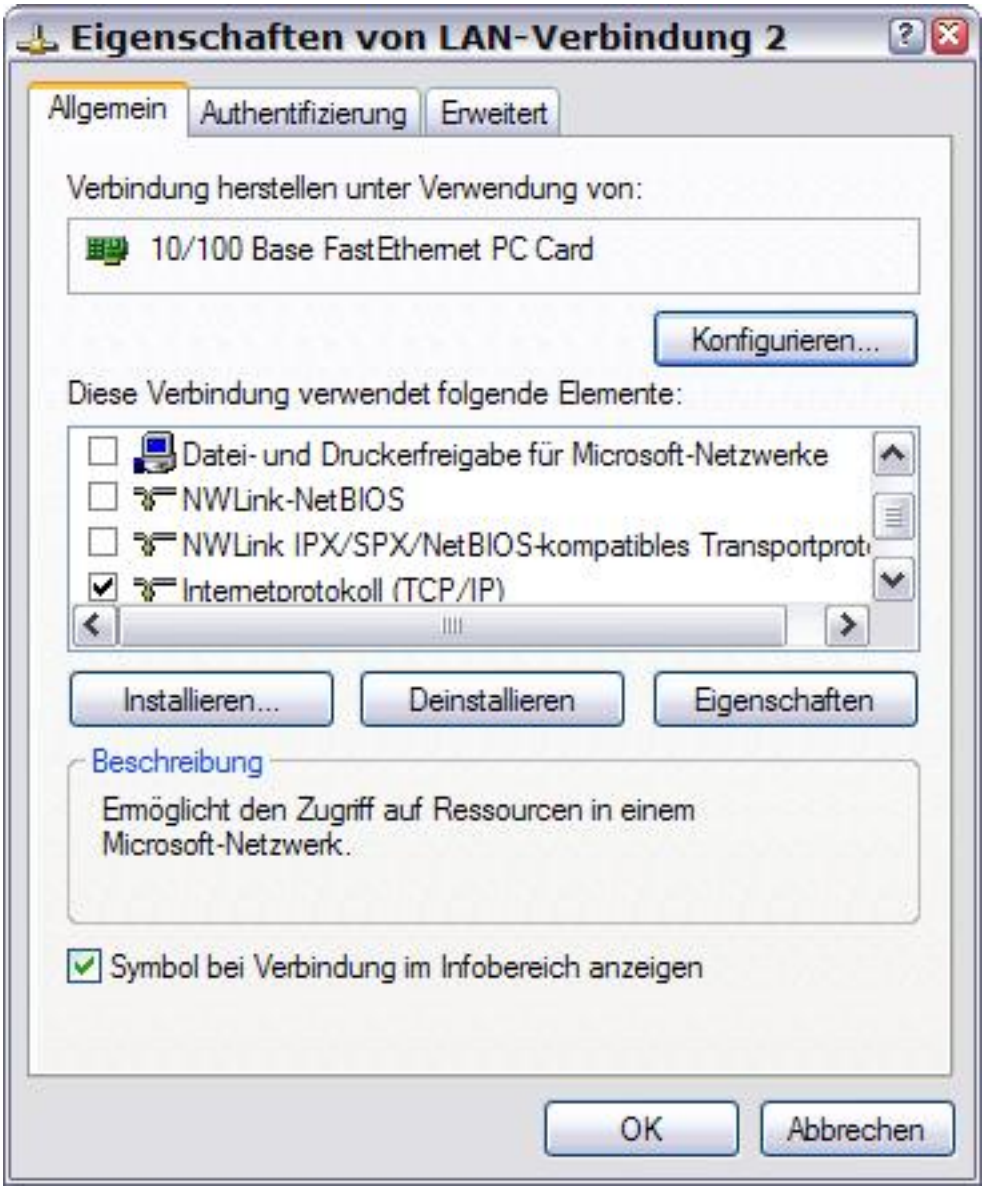
Empfehlenswert ist hierbei eine Eingabeaufforderung, bei der Sie bestimmen was mit dem Cookie geschehen soll.
Wenn Sie nun also eine Internetseite aufsuchen, wird der Internet Explorer Sie fragen ob der Cookie gesetzt werden darf oder nicht.
Wenn Sie sich jedoch unsicher sind ob Sie es einschätzen können, so sollten Sie den Punkt auf Sperren setzen.
Dabei ist zu beachten, daß einige Internetseiten Cookies benötigen, aber dafür minder gefährlich für Sie sind.
Große Internetseiten die personalisiert sind zähle ich dazu, da hierbei Ihre Daten und eine Sessionnummer gespeichert werden.
Das weitere Browserverhalten kann nach meinen Erfahrungen wie folgt eingestellt werden:

Allgemeine Einstellungen und Scripting:

Microsoft VM - Hohe Sicherheit
Einfügeoperation über ein Script zulassen - Deaktivieren
Active Scripting - Deaktivieren
Scripting von Java-Applets - Deaktivieren
Auf Datenquellen über Domänengrenzen hinweg zugreifen - Deaktivieren
Dauerhaftigkeit der Benutzerdaten - Deaktivieren
Gemischte Inhalte anzeigen - Eingabeaufforderung
Installation von Desktopobjekten - Deaktivieren oder Eingabeaufforderung
Keine Aufforderung bei Clientzertifikatauswahl wenn .... - Deaktivieren
META-Refresh zulassen - Eingabeaufforderung
Programme und Dateien in einem IFRAME starten - Deaktivieren
Subframes zwischen verschiedenen Domänen bewegen - Deaktivieren
Unverschlüsselte Formulardaten - Eingabeaufforderung oder Deaktivieren
Ziehen, Ablegen, Kopieren, Einfügen von Dateien - Eingabeaufforderung oder Deaktivieren
Zugriffsrechte für Softwarechannel - Hohe Sicherheit
Automatische Überprüfung auf Aktualisierungen - Deaktivieren
Installation auf Anfrage aktivieren - Deaktivieren
Zählen der übertragenen Seiten - Deaktivieren

Java-Protokollierung - Aktivieren
Auf zurückgezogene Zertifikate überprüfen - Aktivieren
Bei ungültigen Site-Zertifikaten warnen - Aktivieren
Beim Wechsel zwischen sicher und undsicherem Modus warnen - Aktivieren
PCT 1.0 verwenden - Deaktivieren
Profil-Assistent aktivieren - Deaktivieren
SSL 2.0 verwenden - Deaktivieren
SSL 3.0 verwenden - Aktivieren
TLS 1.0 verwenden - Aktivieren
Verschlüsselte Seiten nicht auf der Festplatte speichern - Aktivieren
Warnen, falls Formulardaten umgelenkt werden - Aktivieren

Weitere Einstellungen für das surfen im Internet mit Windows und Internet Explorer:
Sie sollten bei den Verbindungen darauf achten, daß nicht alle Protokolle geladen sind auf einer Verbindung.
Für einen Homecomputer der nicht in einem Netzwerk integriert ist und nicht auf andere Daten von Netzwerkcomputern zugreifen muß, sollte DFÜ-Netzwerk sowie TCP/IP installiert sein.



Weitere Komponenten sind hierbei nicht erforderlich und steigern das Sicherheitsrisiko.
Der Haken bei Symbol bei Verbindung im Inforbereich anzeigen sollte drin sein, da Sie so

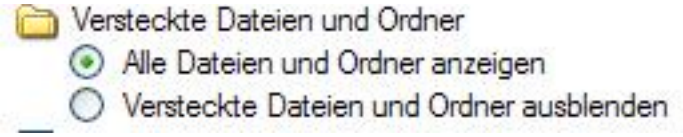
sehen können ob eine Netzverbindung besteht oder nicht.

In diesem Beispiel ist keine Verbindung aktiviert.

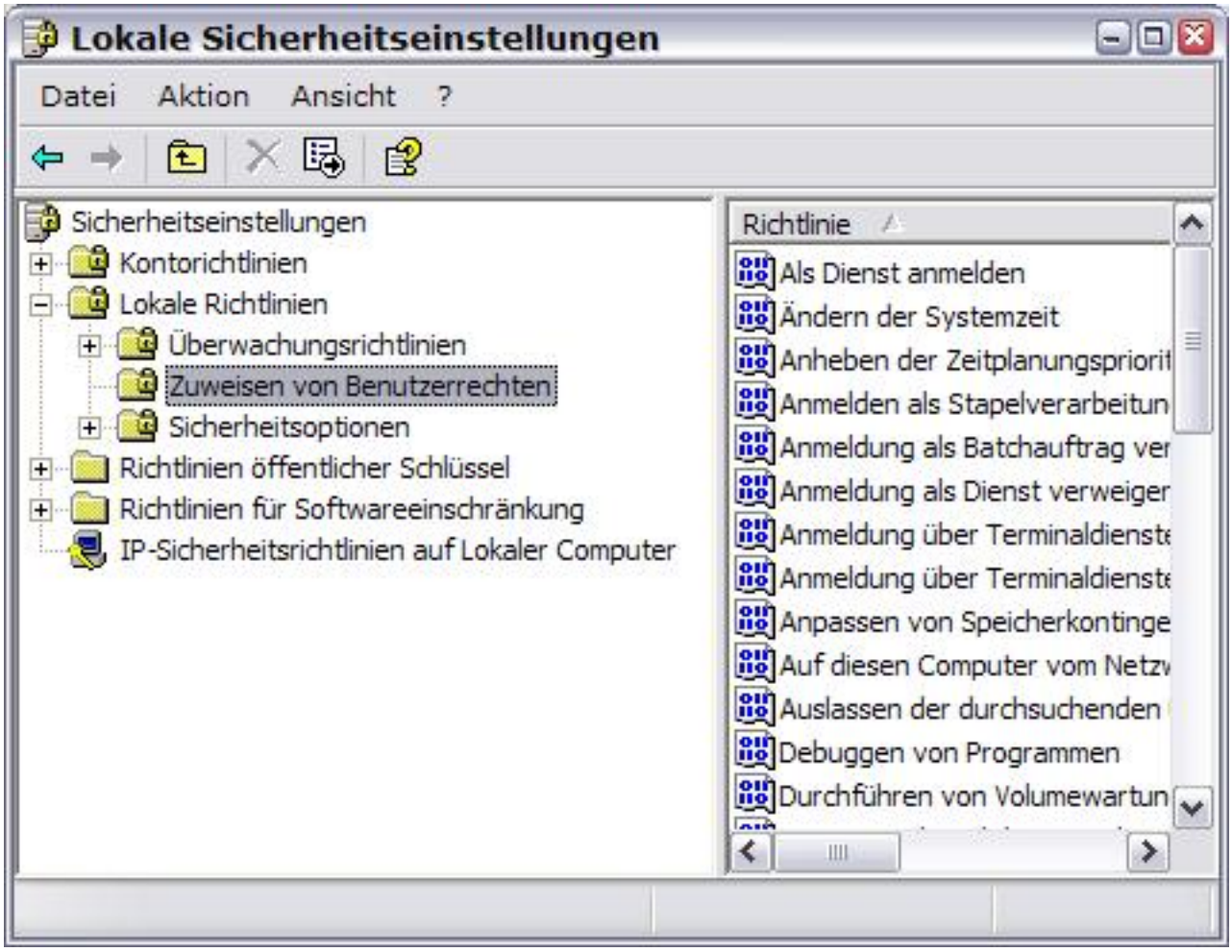
Sollten Sie die Protokollierung aktiviert haben, können Sie davon ausgehen das Ihre Zugangsdaten in einer Logdatei gespeichert werden.
Diese dort abgelegten Daten sind nicht verschlüsselt und das Passwort ist für jederman lesbar.

Sollten Sie vorhaben über einen Proxyserver anonym zu surfen kann ich Ihnen nur davon abraten.
Warum rate ich Ihnen davon ab, wenn doch Proxyserver die Anonymität angeblich unterstützen und die IP-Adresse bei der Einwahl verschleiert wird?!
Alle Programme die bisher auf Windows Betriebssystemen arbeiten sind nicht 100% zuverlässig und Sie als Benutzer haben keine Kontrolle darüber, was auf dem Proxyserver mit Ihren Daten geschieht.
Sicher arbeiten Sie mit einem Proxyserver dann, wenn Sie diesen als Ihr Eigentum bezeichnen können.

Hier noch einige Ratschläge und Sicherheitshinweise von mir, die ich für durchaus sinnvoll erachte wenn es um die Sicherheit von Windows geht.
Zunächst einmal bleiben wir in der Systemsteuerung und gehen in das Untermenü Ordneroptionen / Ansicht.
Dort finden Sie wie nachfolgend die Einstellung, daß alle Dateien und Ordner angezeigt werden sollen:



Somit haben Sie mittels des Windows Explorer immer die Möglichkeit, alle Dateien und Ordner zu sehen.
Wichtig erscheinen mir ebenfalls die Einstellungen in der Computerverwaltung der Systemsteuerung.
Hier ist jedoch VORSICHT geboten, denn einige Einstellungen können Schäden führen die Sie nicht mehr korriegieren können.
Die Sicherheitsrichtlinien stellen hierbei einen besonderen Bereich da, der sensibel zu betrachten ist und ohne Fachkenntnisse nicht bearbeitet werden sollte.
Sie können hier Einstellungen vornehmen, welcher Benutzer oder welche Benutzergruppe welche Operationen ausführen darf oder welche Programme für welche Gruppe zugänglich sind.



Seien Sie also VORSICHTIG wenn Sie in der Verwaltungsebene von WindowsXP oder Windows2000 arbeiten.
Beide Betriebssysteme von Microsoft sind sich dort sehr ähnlich.
Was können Sie weiterhin tun, um sich entsprechend im Internet zu schützen:
Hierbei empfehle ich Ihnen eine gute Kombination aus einem Anti-Viren Programm, einer Firewall und bei hohem Bedarf an Security ebenfalls einen Anti-Trojan Programm.
Die Erkennungsraten von Anti-Virenscanner für Trojaner ist nicht so hoch, daß man komplett auf einen Trojaner Scaner verzichten sollte.
Eine Desktop Firewall ist ebenso ein recht nützlicher Helfer wenn es um die Sicherheit Ihres Computers geht.

Anti-Virensoftware sollte schnell arbeiten können, permanent mit dem Internet arbeiten um gefährliche Scripte abzuwehren, E-Mails sofort mit Outlook scanen wenn Sie damit arbeiten.
Hierfür empfehle ich:
- McAfee Virus Scan: http://www.mcafee.com
- TrendMicros PC Cillin: http://www.trendmicro.de

Anti-Trojaner Programme sollten bei Bedarf einsetzbar sein und nicht zu teuer:
- Anti-Trojan Network: http://www.anti-trojan.net

Firewallsysteme für Homebenutzer:
- OutPost Firewall: http://www.agnitum.com
- Tiny Firewall: http://www.tinysoftware.com
- Norton Internet Security: http://www.symantec.com / Nachfolger der bekannten AT-Guard Firewall

Referenz:

- Hacking Intern :: Das Buch mit dem Kapitel "Projekt sicheres Windows".

Ich möchte mich nachfolgend für die Veröffentlichung bei Marc Ruef bedanken.
Kritisch und konsequent beurteilt er nach wie vor meine Arbeiten und ist immer wieder hilfreich bei der Umsetzung meiner Ideen.
Weiterhin danke ich:
Meiner Familie, Martin J. Muench, Sven Bast, Snakebyte, Roland Brecht und den vielen anderen Menschen und Kollegen der Branche, die es mir ermöglichen meine Arbeiten zu verwirklich.

Sie möchten WindowsXP optimal auf Sie abstimmen? Dann lesen Sie den WindowsXP Optimized Bericht Version 2.0!

Marko Rogge, Brain-Pro Security // www.brain-pro.de
Kontakt E-M@il: mr@brain-pro dot de