Handbuch

Computersicherheit

Ein kleines Handbuch...

Version 1.1

Inhaltsverzeichnis

1 Inhalt

Überblick

Dieses Kapitel gibt dir einen ganz kurzen Überblick zum Inhalt dieses Handbuchs.

Du findest folgende Infos:

- Allgemeines zu diesem Handbuch
- Was dich so erwartet
- Benötigte Vorkenntnisse zur Verwendung des Handbuchs
- Was gibt es Neues in dieser Version (im Vergleich zur alten Version 1.0 des Handbuchs)
- Eine Liste der in diesem Handbuch behandelten Programme
- Einen Hinweis, dass oft einiges ein bisschen anders als erwartet kommt
- Eine Erklärung der verwendeten Symbole
- Eine kurze Beschreibung der einzelnen Kapitel in diesem Handbuch

1.1 Beschreibung des Handbuchs

Dieses kleine Handbuch...

Das ist eine kleines Handbuch zum Thema Computersicherheit und was mensch an einfachen Maßnahmen treffen kann, um den eigenen Computer und vor allem die Daten darauf sicherer vor unbefugtem Zugriff zu machen.

Dieses Handbuch beschränkt sich auf die wichtigsten Punkte und bietet einfache Erklärungen. Es ist für Menschen gedacht, die keine Lust und/oder keine Zeit haben, sich durch Berge von Computerzeitschriften, Internetseiten und Tausende Seiten von oft schwer verständlichen Dokumentationen durchzukämpfen, ihren Computer und die Daten darauf aber weitgehend gegen unbefugten Zugriff absichern wollen.

Zurück zum Inhalt dieses Kapitels

Was erwartet dich?

Du erhältst einen kurzen Überblick über die wichtigsten Problembereiche bezüglich Computersicherheit. Dazu gibt's dann Beschreibungen von Programmen (siehe Liste unten), die deinen Computer und die Daten darauf sicherer machen. Zu diesen Programmen findest du Installationsanleitungen und die wichtigsten Handgriffe zur Bedienung.

Wenn du dich für einzelne Programme näher interessierst, findest du einige Handbücher auf der zugehörigen CD, außerdem findest du bei den Links Verweise zu Internetseiten, wo es detailliertere Informationen gibt.

Den größten Teil des Handbuchs bilden die ausführlichen Installationsanleitungen der behandelten Programme. Mit diesen Anleitungen solltest du die behandelten Programme problemlos selbst installieren und bedienen können.

Zurück zum Inhalt dieses Kapitels

Benötigte Kenntnisse

Zum Lesen dieses Handbuchs brauchst du zwar keine „Computer-SpezialistIn“ sein, du solltest jedoch Grundkenntnisse zu deinem Betriebssystem haben und auch schon mal Windows aus der Nähe gesehen haben.

Zu diesen benötigten Grundkenntnissen gehören z.B. das Starten von Programmen, das Anlegen von Ordnern, in Windows die Verwendung des Windows Explorer u.ä.

Zurück zum Inhalt dieses Kapitels

Was gibt es Neues in dieser Version

Wenn du die erste Version des Handbuchs kennst (Version 1.0), musst du nicht alles noch einmal durchstöbern. Bei den in der ersten Version behandelten Kapiteln hat sich nichts Wesentliches geändert.

Hinzugekommen sind:

- Eine etwas genauere Beschreibung zur Verwendung des Programms JAP (Java Anon Proxy) zum anonymen Surfen. Die Ergänzungen findest du unter Die Verwendung von JAP.
- Eine kurze Beschreibung des Problems „Spyware“ (Spionage-Programme) und die Beseitigung des Problems mit den Programmen XP Antispy für Windows XP BenutzerInnen, Lavasoft Ad-Aware zum Auffinden und Beseitigen von Spyware und Webwasher zur Wahrung der Privatsphäre beim Surfen.
- Aktualisierte Programmversionen auf der zugehörigen CD. Zu allen beschriebenen Programmen findest du die aktuellen Versionen auf der zugehörigen CD.

Zurück zum Inhalt dieses Kapitels

In diesem Handbuch behandelte Programme

- PGP: Pretty Good Privacy, zum Ver- und Entschlüsseln von Texten, z.B. von Mails
- PGP Disk: Teil des Programms PGP, zum Verschlüsseln von Festplattenbereichen
- Zone Alarm: Firewall, zum Schutz vor Zugriffen von außen bei Internetverbindungen, nur für das Betriebssystem Windows
- Window Washer: Zum Aufräumen von Müll auf der Festplatte, nur für das Betriebssystem Windows
- JAP: Java Anon Proxy, zum anonymen Surfen
- Ad-Aware: Gegen Spyware (Spionageprogramme) auf deinem Computer
- XP AntiSpy: Gegen Spyware und bedenkliche Einstellungen von Windows XP
- Webwasher: Zum Schutz deiner Privatsphäre beim Surfen
- H+BEDV AntiVir: Anti-Virenprogramm, nur für das Betriebssystem Windows

Zurück zum Inhalt dieses Kapitels

Alles immer ein bisschen anders als erwartet...

Leider sehen die angeführten (aber nicht nur die) Programme in jeder Version ein wenig anders aus, auch die Installationsvorgänge und die Handhabung der Programme hängen von der Version und vom verwendeten Betriebssystem ab. Für die meisten Beispiele in diesem Handbuch wurde das weit verbreitete Windows 98 Second Edition verwendet.

In anderen Windows Versionen ist das Ganze aber sehr ähnlich. BenutzerInnen von MacOS, Linux o.a. müssen ein wenig Phantasie walten lassen und die Angaben zu Windows auf das jeweilige Betriebssystem umlegen.

Aber es wären natürlich nicht Computer und zugehörige Programme, wenn nicht immer wieder Probleme auftauchen könnten. Alle diese möglichen Probleme aufzulisten, würde den Rahmen dieses Handbuchs sprengen. In diesem Fall lese mal die jeweilige Dokumentation durch und/oder wende dich an deine fachkundigen FreundInnen oder schau mal ins Internet. Es ist immer wieder erfreulich, was mensch im Internet so alles an Tipps und Ratschlägen findet.

Zurück zum Inhalt dieses Kapitels

In diesem Handbuch verwendete Symbole

Folgende Symbole werden im Handbuch verwendet:

Verweis zu weiterführenden Informationen

Hinweis, besonders zu beachten

Angaben zur zugehörigen CD (Dokumentationen oder Programme)

Verzeichnisangabe (Ordner) auf der zugehörigen CD

Dateiname einer Dokumentation auf der zugehörigen CD

Programm auf der zugehörigen CD (mit Doppelklick Installationsvorgang starten)

Zurück zum Inhalt dieses Kapitels

1.2 Die einzelnen Kapitel im Überblick

Hier findest du einen kurzen Überblick über die einzelnen Hauptkapitel in diesem Handbuch:

Die wichtigsten Problembereiche	Beinhaltet eine ganz kurze Beschreibung der wichtigsten Problembereiche bezüglich Computersicherheit, die in diesem Handbuch behandelt werden
Was tun zur Sicherheit?	Beinhaltet eine ebenfalls kurze Beschreibung der Lösungsmöglichkeiten zu den im vorigen Kapitel aufgelisteten Problembereichen
PGP (Pretty Good Privacy)	Beinhaltet eine Beschreibung, was PGP ist und wie es funktioniert
PGP Installation und Schlüsselverwaltung	Beinhaltet eine detaillierte Anleitung zur Installation von PGP, außerdem zur Erstellung und Verwaltung von Schlüsseln, die zur Ver- und Entschlüsselung von Texten (z.B. Mails) benötigt werden
Die Verwendung von PGP mit Mailprogrammen	Beinhaltet detaillierte Anleitungen, wie PGP mit den Mailprogrammen Eudora, Outlook und anderen Programmen zu verwenden ist, um Mails zu ver- bzw. entschlüsseln
PGP Disk	Beinhaltet eine Anleitung, wie Festplattenbereiche mit PGP Disk verschlüsselt werden können
Zone Alarm (Firewall für Windows)	Beinhaltet eine Installationsanleitung und eine Beschreibung, wie mensch Zone Alarm als Firewall verwendet

Window Washer (Datenmüll aufräumen für Windows und MacOS)	Beinhaltet eine Installationsanleitung und eine Beschreibung, wie mensch mit Window Washer (bzw. MacWasher für MacOS) Datenmüll auf der Festplatte aufräumt
JAP (Java Anon Proxy zum anonymen Surfen)	Beinhaltet eine Beschreibung und eine Installationsanleitung des Programms
Ad-Aware	Sucht und beseitigt Spionageprogramme, die Informationen auf deinem Computer ausspionieren (für alle Windows Versionen)
XP Antispy	Hilft bei der Beseitigung von Windows XP Programmen/Einstellungen, die Informationen auf deinem Computer ausspionieren
Webwasher	Filterprogramm für Internet-Seiten: verhindert beim Aufruf von Webseiten Web-Käfer, Werbebanner u.v.m. (für Windows und Linux)
AntiVir (Viren-Schutzprogramm für Windows)	Beinhaltet eine Erklärung von AntiVir, eine Installationsanleitung und eine Beschreibung, wie mensch AntiVir verwendet
Tipps für Passwörter/Passphrases	Beinhaltet einige Tipps, wie mensch Passwörter oder ganze Passwort-Sätze am besten gestaltet
Lexikon	Beinhaltet einige in diesem Handbuch verwendete Begriffe mit deren Bedeutung
Die CD	Beinhaltet eine Auflistung und Kurzbeschreibung, was die zugehörige CD alles beinhaltet

Quellen/Verweise/Weitere Infos	Beinhaltet einige Verweise auf Dokumente auf der CD und Webseiten mit weiterführenden Informationen

Zurück zum Inhalt dieses Kapitels

2 Die wichtigsten Problembereiche

Überblick

In diesem Kapitel findest du eine Kurzbeschreibung der wichtigsten Problembereiche von Computern die Sicherheit der Daten betreffend.

Du findest Infos zu folgenden Bereichen:

- Datenverkehr im Internet - Mails
- Gespeicherte Daten auf dem Computer
- Gelöschte Daten
- Von Programmen verursachter „interessanter“ Datenschrott
- Verbindung zum Internet
- Anonymes Surfen
- Spionageprogramme (Spyware)
- Webkäfer, Werbebanner etc.
- Computerviren
- Passwörter

2.1 Die Problembereiche

Datenverkehr im Internet - Mails

Ohne Verschlüsselung reisen Mails völlig ungesichert quer durchs Netzwerk. Für Fachleute ist es sehr leicht, Mails abzufangen und darin herumzustöbern. Mails werden zeitweise auch vollautomatisch nach sogenannten „Reizwörtern“ durchsucht und bei Auffinden eines der Wörter automatisch irgendwo gespeichert (siehe ECHELON) und bei Bedarf hervorgekramt.

Schutz davor bietet nur die Verschlüsselung von Mails, das derzeit beste Programm dazu ist PGP, das im Internet kostenlos erhältlich ist.

Jeder Inhalt ist für neugierige Menschen unter Umständen von Interesse, auch völlig harmlose Mails. Sie können erfahrungsgemäß dazu verwendet werden, abenteuerliche Konstrukte zu erfinden.

Von Interesse ist aber auch, mit wem du wie oft kommunizierst, also z.B. wem du Mails schickst. Davor gibt es leider kaum Schutz.

Weiteres zur Lösung dieses Problems findest du im Kapitel PGP (Pretty Good Privacy)

Zurück zum Inhalt dieses Kapitels

Gespeicherte Daten auf dem Computer

Es ist sicher nachvollziehbar, dass auf deinem Computer gespeicherte Daten für neugierige Menschen furchtbar interessant sind. Schutz vor unberechtigtem Zugriff auf diese Daten bietet ebenfalls ein Teilprogramm von PGP, das „PGP Disk“ heißt. Damit werden ganze Festplatten- oder Diskettenbereiche verschlüsselt.

Weiteres zur Lösung dieses Problems findest du im Kapitel PGP (Pretty Good Privacy)

Zurück zum Inhalt dieses Kapitels

Gelöschte Daten

Selbst wenn du glaubst, Daten gelöscht zu haben, sind sie doch meist wiederherstellbar, auch wenn du den Windows-Papierkorb brav geleert hast und die Daten für dich nicht mehr sichtbar sind.

Durch Restmagnetismus auf den Speichermedien (z.B. auf der Festplatte) können diese „gelöschten“ Daten oft wiederhergestellt werden.

Schutz davor bietet ein Teilprogramm von PGP, das „Wipe“ bzw. „Free Space Wipe“ heisst. Dieses Programm bearbeitet die Festplatte derart, dass kein Restmagnetismus der ursprünglichen Daten mehr vorhanden ist.

Weiteres zur Lösung dieses Problems findest du im Kapitel PGP (Pretty Good Privacy)

Zurück zum Inhalt dieses Kapitels

Von Programmen verursachter „interessanter“ Datenschrott

Vor allem Windows-Programme haben die unangenehme Angewohnheit, eine Vielzahl von temporären Dateien anzulegen, die meist, aber nicht immer, nach Beenden der Programme wieder „gelöscht“ werden (siehe aber auch Kapitel „gelöschte Daten“).

Außerdem werden von Programmen im gesamten System des Computers Informationen abgelegt. Z.B. welche Internetseiten du geladen hast, welche Bilder du angezeigt bekommen hast, welche Dateien du zuletzt geöffnet hast etc.

Im Fall einer Internetverbindung dienen diese Informationen auch dazu, dir das nächste Mal eine Internetseite schneller auf den Bildschirm zaubern zu können. Der Nachteil daran ist, dass auch neugierige Menschen begierig darauf sind zu erfahren, was du mit deinem Computer so treibst.

Abhilfe bietet das Programm „Window Washer“, das diesen Datenschrott aufräumt.

Weiteres zur Lösung dieses Problems findest du im Kapitel Window Washer

Zurück zum Inhalt dieses Kapitels

Verbindung zum Internet

Sobald du mit dem Internet verbunden bist, können neugierige Menschen mit ein paar Tricks auf die Daten deines Computers zugreifen, wenn er nicht dagegen abgesichert ist.

Einen gewissen Schutz davor bieten sogenannte Firewalls. Ganz besonders empfehlenswert ist so eine Firewall für alle BenutzerInnen von permanenten Internetverbindungen (wie z.B. bei Chello), da sie über lange Zeiträume mit dem Internet verbunden sind.

Weiteres zur Lösung dieses Problems findest du im Kapitel Zone Alarm (Firewall)

Zurück zum Inhalt dieses Kapitels

Anonymes Surfen

Auch wenn es dir vorgegaukelt wird, das Surfen im Internet ist nie wirklich anonym. Es ist über eine weltweit eindeutige Nummer, die IP-Adresse, immer rückverfolgbar, auf welchem Computer zu welcher Zeit was getan wurde (z.B. welche Webseite aufgerufen wurde oder woher eine Mail gekommen ist).

In diesem Handbuch wird das Programm JAP (Java Anon Proxy) beschrieben, mit dessen Verwendung du wirklich anonym surfen kannst.

Weiteres zur Lösung dieses Problems findest du in Kapitel JAP (Java Anon Proxy)

Zurück zum Inhalt dieses Kapitels

Spionageprogramme (Spyware)

Es gibt eine Vielzahl von Programmen, die so ganz nebenbei alles mögliche auf deinem Computer ausspionieren und unter Umständen unauffällig an irgendwen verschicken. Besonders fleissig dabei sind natürlich Windows-Programme - schon die Installation von Windows XP bringt dir eine Reihe von bedenklichen Programmen und Einstellungen.

Zum Beseitigen dieser Programme und Einstellungen werden 2 kostenlose Programme vorgestellt:

- Das Programm Ad-Aware durchsucht deinen Computer nach solchen Spionageprogrammen und beseitigt bzw. entschärft sie auf Wunsch
- Das Programm XP Antispy speziell für Windows XP Systemprogramme und Einstellungen

Weiteres zur Lösung dieses Problems findest du in den Kapiteln Ad-Aware und XP Antispy

Zurück zum Inhalt dieses Kapitels

Webkäfer, Werbebanner etc.

Ist schon nervig – mensch ruft irgendeine Webseite auf und findet dann oft kaum die gewünschte Information, weil die Seiten mit Werbebannern, Pop-Up Fenstern, Animationen etc. zugepflastert sind.

Weiters können auf Webseiten kleine, unsichtbare Grafiken eingebaut sein, die in Dokumenten versteckt sind und Rückmeldungen an Dritte auslösen. Diese sog. „Web Bugs“ (Webkäfer) werden von Datensammlern benutzt, um aus dem Surfverhalten der AnwenderIn Profile zu erstellen.

Diese und einige andere Probleme beseitigt das Gratis-Programm Webwasher, das es für Windows, MacOS und Linux gibt. Für MacOS X gibt es leider keine eigene Version. BenutzerInnen von Mac OS X wird geraten, das Programm in der Bluebox laufen zu lassen

Weiteres zur Lösung dieses Problems findest du im Kapitel Webwasher

Zurück zum Inhalt dieses Kapitels

Computerviren

Es passt zwar nicht ganz zu diesem Handbuch, ein weiteres leidliches Thema sind aber Computerviren. Viren sind kleine Programme, die eigenständig arbeiten oder sich unauffällig an andere bestehende normale Programme anhängen und irgendwelchen Mist auf deinem Computer veranstalten. Dieser durchgeführte Mist kann bis zur Ausspionierung deiner Passwörter oder der Zerstörung der Festplatte gehen.

Die meisten Viren sind aber „nur“ sehr lästig und zerstören nichts wirklich. Trotzdem ist es ungemein wichtig, ein Viren-Schutzprogramm auf dem Computer zu haben.

Viren haben auch die Angewohnheit, sich selbst „fortzupflanzen“. Wenn sich z.B. ein Virus auf deinem Computer befindet und du kopierst eine Datei auf eine Diskette, kommt der Virus gleich mit. Eine andere Person, welche die Diskette auf ihrem Computer öffnet, wird dann auch gleich vom Virus beglückt. Das funktioniert z.B. bestens mit Microsoft Word-Dateien, die sogenannte „Makro-Viren“ beinhalten können.

Daher gehört auch zu den Grundregeln beim Mailverkehr, nur in wirklich notwendigen Fällen Word-Dateien oder andere Anhänge mitzuschicken.

Normalerweise solltest du Mails ausschließlich mit Text verschicken (so wie du ihn mit deinem Mailprogramm eintippst), reine Texte können nämlich keine Viren enthalten.

Wenn du ein Word-Dokument verschicken musst, sollte es vorher ins RTF-Format umgewandelt werden, es können zwar einige Formatierungen verloren gehen, dafür sind diese Dateien garantiert virenfrei.

Abgesehen davon werden es dir alle EmpfängerInnen danken, die keinen Internet-Kabelanschluss haben, bei einem Modemanschluss dauert es nämlich furchtbar lange, bis z.B. so eine meist sehr große Word-Datei aus dem Internet (vom Mailserver) geladen ist.

Weiteres zur Lösung dieses Problems findest du im Kapitel AntiVir – Viren-Schutzprogramm

Zurück zum Inhalt dieses Kapitels

Passwörter

Diese ganzen tollen hier vorgestellen Programme nützen oft nichts, wenn du deine Daten nicht durch gute Passwörter schützt. Passwörter sind auch bei der Verwendung dieser Programme meist der einzige Schutz vor unbefugtem Zugriff auf deine Daten.

Daher findest du in einem eigenen Kapitel ein paar Tipps zur Verwendung von guten Passwörtern.

Weiteres zur Lösung dieses Problems findest du im Kapitel Passwörter und Passphrases

Zurück zum Inhalt dieses Kapitels

3 Was tun zur Sicherheit?

Überblick

Das Thema „Computersicherheit“ ist unerschöpflich, als Mensch wie du und ich ist mensch manchmal etwas überfordert, sich unter den vielen angesprochenen Problemen und Lösungen zurechtzufinden, vieles wird erst verständlich, wenn mensch sich lange damit beschäftigt und detailliertes technisches Wissen angeeignet hat.

Es gibt jedoch einige grundlegende Dinge, die jedeR beachten kann/soll/muss, um eine Grundsicherheit zu erreichen. Und ein paar dieser grundlegenden Dinge werden nachfolgend ganz kurz erklärt. In den späteren Kapiteln findest du dann detailliertere Beschreibungen.

Alle angeführten Programm findest du auch auf der zugehörigen CD, Window Washer (und MacWasher für MacOS) als 30-Tage-Version. Folgende Programme werden beschrieben:

Du findest Infos zu folgenden Programmen:

- PGP (Pretty Good Privacy) (Ver- und Entschlüsseln von Daten)
- Window Washer (Aufräumen mit Datenschrott)
- Zone Alarm (Firewall) (Schutz im Internet)
- JAP (Java Anon Proxy) (Anonymes Surfen im Internet)
- Ad-Aware (Gegen diverse Spionageprogramme von Windows)
- XP Antispy (Gegen Spionageprogramme und bedenkliche Einstellungen von Windows XP)
- Webwasher (Gegen Spionage und Werbung beim Surfen)
- AntiVir – Viren-Schutzprogramm

Ausserdem findest du einige Tipps für die Wahl von guten Passwörtern:

- Passwörter und Passphrases

3.1 Lösungsansätze

PGP (Pretty Good Privacy)

Eines der wichtigsten Dinge zum Schutz vor unbefugtem Zugriff auf deine Daten ist das Verschlüsseln von Nachrichten, die du übers Internet versendest, und die Verschlüsselung von Daten, die auf dem Computer gespeichert sind. PGP ist ein Programm dazu, das mensch gratis im Internet herunterladen kann. Es dient zum

- Ver- und Entschlüsseln von Texten (z.B. Mails)
- Verwalten der zugehörigen Schlüssel
- Nichtwiederherstellbaren Löschen von Dateien bzw. Festplattenbereichen
- Verschlüsseln von Daten auf Speichermedien (z.B. Festplatte, Disketten etc.) mit PGP Disk

Mittlerweile wird die Verschlüsselung von Mails ja sogar vom Europäischen Parlament empfohlen, nachdem die USA zugegeben haben, was die ganze Welt seit langem weiß: dass seit der Nachkriegszeit mittels dem System ECHELON (das wahrscheinlich jetzt anders heißt) Nachrichten nach „Reizwörtern“ durchsucht und bei Auffinden eines der Reizwörter auf speziellen Computern gespeichert werden, um bei Bedarf angefordert werden zu können.

Detailliertere Informationen zu PGP findest du im Kapitel PGP (Pretty Good Privacy).

Zurück zum Inhalt dieses Kapitels

Window Washer (bzw. MacWasher)

Window Washer ist ein lizenzpflichtiges (=kostenpflichtiges) Programm für Windows, das den Datenschrott auf der Festplatte aufräumt (die Version für MacOS heisst MacWasher).

Vor allem bei Verwendung von Windows-Programmen werden oft von dir unbemerkt zahlreiche temporäre Dateien, Registry-Einträge etc. angelegt. Window Washer hilft, diesen für neugierige Menschen sehr interessanten Datenschrott wieder loszuwerden.

Detailliertere Information zu Window Washer findest du im Kapitel Window Washer.

Zurück zum Inhalt dieses Kapitels

Zone Alarm (Firewall)

Sobald du mit dem Internet verbunden bist, besteht die Gefahr, dass andere Personen auf deinen Computer zugreifen. Zone Alarm ist eine sogenannte Firewall, die kontrolliert, was bei einer Verbindung zum Internet von deinem Computer nach außen geht und was von außen zu deinem Computer kommt.

Dieses einfach zu installierende und zu bedienende Programm ist für Windows wie PGP kostenlos im Internet erhältlich.

Detailliertere Informationen zu Zone Alarm findest du im Kapitel Zone Alarm (Firewall)

Zurück zum Inhalt dieses Kapitels

JAP (Java Anon Proxy)

Das Programm JAP dient dazu, wirklich anonym im Internet surfen zu können. Es ist normalerweise über eine weltweit eindeutige Nummer deines Computers, die IP-Adresse (siehe unten), immer rückverfolgbar, auf welchem Computer zu welcher Zeit was getan wurde (z.B. welche Webseite aufgerufen wurde oder woher eine Mail gekommen ist).

„IP“ bedeutet „Internet Protocol“, es ist die Art und Weise (das Protokoll), wie Daten im Internet (aber nicht nur dort) verschickt werden. Es gibt auch andere Protokolle, im Internet hat sich aber dieses Protokoll durchgesetzt.

Diese IP-Adresse wird von deinem Provider entweder fix für deinen Computer vergeben (bleibt also zumindest eine Zeit lang gleich) oder dynamisch bei jeder Verbindung zugeteilt (ist also immer eine andere). Zum Zeitpunkt der Verbindung mit dem Internet ist sie in jedem Fall weltweit eindeutig.

Diese IP-Adresse ist keine Boshaftigkeit der Internet-BetreiberInnen, sondern sie ist notwendig, um die von dir gewünschten Daten (z.B. eine Internetseite) über das Netzwerk des Internets genau an deinen Computer zu senden.

Beim Programm JAP werden diese IP-Adressen unter den JAP-BenutzerInnen auf einem oder mehreren Computern bunt durcheinandergewürfelt. Es ist dann nicht mehr rückverfolgbar, an welchem Computer was getan wurde.

Nur auf diesen Computern ist deine Originaladresse zum Zeitpunkt der Verbindung bekannt, so können die für dich bestimmten Daten über diese Computer wieder zu dir geschickt werden.

Detailliertere Informationen zu JAP findest du im Kapitel JAP (Java Anon Proxy)

Zurück zum Inhalt dieses Kapitels

Ad-Aware

Das Programm Ad-Aware durchsucht deinen Computer nach sogenannter Spyware (Spionageprogrammen). Solche Spionageprogramme sind immer in Programmen integriert, sie spionieren deinen Computer aus senden diese Informationen unbemerkt nach aussen.

Ad-Aware ist ein sehr einfach zu installierendes und zu bedienendes Gratis-Programm. Es hilft dir dabei, diese Programme oder Programmteile wieder loszuwerden.

Detailliertere Informationen zu Ad-Aware findest du im Kapitel Ad-Aware

Zurück zum Inhalt dieses Kapitels

XP Antispy

So wie Ad-Aware eine Vielzahl von Spionageprogrammen findet und beseitigen kann, ist XP Antispy speziell für BenutzerInnen von Windows XP gemacht. Schon bei der Installation von Windows XP handelst du dir eine ganze Reihe von bedenklichen Programmen und Einstellungen ein.

SP Antispy ist wie Ad-Aware sehr einfach aufzurufen und zu bedienen.

Detailliertere Informationen zu XP Antispy findest du im Kapitel XP Antispy

Zurück zum Inhalt dieses Kapitels

Webwasher

Selbst wenn du mit Hilfe von JAP oder anderen Anonymisierungsdiensten arbeitest, können Internetseiten bedenkliche Teile beinhalten. Dazu gehören z.B. Webkäfer (Web Bugs), das sind kleine, unsichtbare Grafiken, die in Dokumenten versteckt sind und Rückmeldungen an Dritte auslösen. Web Bugs werden von DatensammlerInnen benutzt, um aus dem Surfverhalten von AnwenderInnen Profile zu erstellen.

Sehr nervig können auf Webseiten auch die Vielzahl von Werbebanners, animierten Grafiken, Pop-Up Fenster u.ä. sein.

Gegen diese und einige andere Probleme beim Surfen hilft Webwasher, ein Gratisprogramm für Windows, MacOS und Linux.

Detailliertere Informationen zu Webwasher findest du im Kapitel Webwasher

Zurück zum Inhalt dieses Kapitels

AntiVir – Viren-Schutzprogramm

Computerviren sind ein äußerst lästiges Kapitel, sie können einigen Ärger bereiten. Wenn du ein Viren-Schutzprogramm installiert hast und damit immer auf dem neuesten Stand bleibst (dir regelmäßig Updates im Internet herunterladest), hast du einen sehr hohen Schutz vor Computerviren.

Diese Viren-Schutzprogramme wachen ständig im Hintergrund, damit du dir nicht irgendwie einen Computervirus einfängst. In diesem Handbuch stellen wir eines der Gratis-Viren-Schutzprogramme für Windows vor (AntiVir von der Firma H+BEDV). Es gibt aber eine ganze Menge dieser Programme, vielleicht auch bessere. Jedenfalls gilt: irgendein aktueller Virenschutz ist viel besser als kein Virenschutz.

So ein Viren-Schutzprogramm ist u.a. auch wichtig für den Gebrauch von PGP. Der wichtigste Schutz vor unbefugtem Zugriff auf deine Daten ist nämlich das Passwort (die Passphrase), mit dem du PGP absicherst. Und es gibt spezielle Computerviren, sogenannte Trojanische Pferde, die dein System inklusive Passwörtern ausspionieren, davor musst du dich natürlich schützen.

Detailliertere Informationen zu AntiVir findest du im Kapitel AntiVir (Viren-Schutzprogramm)

Zurück zum Inhalt dieses Kapitels

Passwörter und Passphrases

Passwörter (oder ganze Passwort-Sätze – Passphrases) sind der wichtigste und oft einzige Schutz vor unbefugtem Zugriff auf deine Daten. Deine ganzen tollen Schutzprogramme sind mehr oder weniger nutzlos, wenn du schlechte, d.h. leicht herauszufindende Passwörter wählst.

Bei der Wahl von Passwörtern sollte mensch daher einige Dinge beachten und ein Passwort auswählen, das nicht so leicht zu knacken ist.

Einige Tipps zu Passwörtern und Passphrases findest du im Kapitel Tipps für Passwörter/Passphrases

Zurück zum Inhalt dieses Kapitels

4 PGP (Pretty Good Privacy)

Überblick

In diesem Kapitel findest du einiges zu PGP, dem Programm zum Ver- und Entschlüsseln von Daten.

Du findest folgende Infos zu PGP:

- eine Beschreibung, was PGP eigentlich ist
- wie Texte (z.B. Mails) ver- und entschlüsselt werden mit einem Beispiel
- über das Verschlüsseln von Festplattenbereichen mit PGP Disk
- eine Zusammenfassung des ganzen Kapitels

In diesem Handbuch werden aber nur die wichtigsten Punkte oberflächlich erklärt. Eine ausführliche Dokumentation von PGP findest du auf der CD, u.a.:

PGP\Doku

IntroToCrypto.pdf (Einführung in die Kryptographie)

PGPWinUsersGuide.pdf (BenutzerInnen-Handbuch)

Pgpfaq.html (Fragen und Antworten zu PGP)

Einfach auf die Dateien doppelklicken, sie öffnen sich mit dem zugehörigen Programm automatisch.

Für die html-Dateien benötigst du einen Internet-Browser (z.B. Internet Explorer oder Netscape), für die pdf-Dateien benötigst du das Programm Adobe Acrobat Reader.

PGP Versionen und Hinweis für Windows XP

In diesem Handbuch wird die PGP Version 6 (6.5.8) vorgestellt. Seit einiger Zeit gibt es die PGP Version 7. Aus verschiedenen Gründen wird jedoch empfohlen, diese Version 7 nicht zu verwenden.

Den Grund für diese Empfehlung findest du in beiliegenden Dokumenten auf der CD (siehe Dokument unter Warum nicht Version 7).

Zum Zeitpunkt der Erstellung dieses Handbuchs ist gerade die allerneueste PGP Version 8.0 erschienen. Du findest diese neue Version auch schon auf der zugehörigen CD.

Ein paar Infos zur Version 8

Der Mensch, der als erster PGP auf einem Internetserver zur Verfügung gestellt hat und sich damit einigen Ärger mit den US-Amerikanischen Behörden eingehandelt hat, nämlich Philip Zimmermann (ein paar Infos zu ihm findest du unter http://www.philzimmermann.com/), war nach dem Ausstieg bei Version 7 bei dieser neuen Version wieder als Berater tätig. Und Zimmermann gilt noch immer als Garant für die Integrität des Programms.

Windows XP BenutzerInnen, die auch PGP Disk verwenden wollen, kommen um diese neue Version 8 sowieso nicht herum, da ältere Versionen unter Windows XP nicht wirklich funktionieren. Das merkt mensch entweder schon beim Installationsversuch, oder spätestens bei der Erstellung von PGP Disks (z.B. Fehlermeldung „Windows konnte die Formatierung nicht abschließen“).

Das Programm Adobe Acrobat Reader

Falls du Adobe Acrobat Reader noch nicht auf deinem Computer installiert hast, installiere es durch Doppelklick auf die jeweilige Datei auf der CD, abhängig vom von dir verwendeten Betriebssystem (in Windows z.B. im Windows Explorer):


Adobe Acrobat Reader\Windows


ar500deu.exe


Adobe Acrobat Reader\MacOS


ar500deu.bin


Adobe Acrobat Reader\Linux


linux-ar-405.tar.gz

Die neueste Version des Adobe Acrobat Reader kannst du dir auch immer gratis aus dem Internet laden:

Herunterladen von Adobe Acrobat Reader

4.1 Was ist PGP

Das Programm

PGP ist ein kostenloses Programm für das

- Ver- und Entschlüsseln von Texten, z.B. von Mails (Encrypt und Decrypt)
- Verwalten der dazu benötigten Schlüssel (PGP Keys)
- Verschlüsseln von Festplattenbereichen. (PGP Disk)
- nichtwiederherstellbare Löschen von Dateien und Bereichen z.B. auf einer Festplatte oder Diskette (PGP Wipe, PGP Freespace Wipe)

Zurück zum Inhalt dieses Kapitels

Was ist Verschlüsseln

Verschlüsseln von Texten heißt, aus einem Text einen lustigen unlesbaren Haufen von Zeichen zu erzeugen, dieser Text kann dann von niemandem außer der Person, für die der Text verschlüsselt wurde, wieder entschlüsselt und damit gelesen werden.

Verschlüsseln von Festplattenbereichen heißt, aus allen Daten eines Teils der (je nach Belieben auch fast der ganzen) Festplatte einen ebenso lustigen unlesbaren Haufen von Zeichen zu erzeugen. Nach Eingabe des richtigen Passworts kannst du diesen Bereich aber mit allen darauffliegenden Dateien ganz normal und wie gewohnt benutzen.

In den „internationalen“ Versionen (außerhalb USA und Canada) fehlt das Programm „PGP Disk“ zum Verschlüsseln von Festplattenbereichen. Auf der CD findest du jedoch eine (nicht ganz offizielle) Vollversion inkl. PGP Disk (Version 6.5.8).

Zu den älteren PGP-Versionen auf der CD ohne PGP Disk (Versionen 6.5.1 und 6.5.3) findest du zusätzlich ein zugehöriges Programm, einen sogenannten Crack (pgpdiskhack.exe). Dieser Crack zaubert PGP Disk aus dem Programm PGP hervor. Der Trick ist, dass es eigentlich auch in den internationalen Versionen enthalten ist, es ist nur gesperrt, die Sperre wird von diesem Crack-Programm aufgehoben und PGP Disk dazuinstalliert.

Windows XP BenutzerInnen sollten die neueste PGP Version 8 verwenden, da es bei älteren Versionen meist Probleme gibt. Um auch PGP Disk zu erhalten, ist jedoch eine kommerzielle Version notwendig, die Gratis-Version enthält nicht PGP Disk.

Zurück zum Inhalt dieses Kapitels

Voraussetzungen zum Ver- und Entschlüsseln von Texten

Alle beteiligten Personen (SenderIn und EmpfängerIn) benötigen das installierte Programm PGP und ihren Schlüsselbund. Für Menschen, die zu Hause einen Computer haben und mit ihrem Computer arbeiten, ist das kein Problem, PGP installieren und schon geht's los.

Befindest du dich aber bei einem anderen Computer, auf dem PGP nicht installiert ist, kannst du auch nicht Ver- und Entschlüsseln. Ist auf diesem anderen Computer jedoch das Programm PGP installiert, kannst du deinen sogenannten Schlüsselbund auf Diskette oder CD mitnehmen und mit ihm auch auf dem anderen Computer Ver- und Entschlüsseln.

Zurück zum Inhalt dieses Kapitels

4.2 Das Verschlüsseln von Texten (z.B. Mails)

Private und öffentliche Schlüssel auf dem Schlüsselbund

Das Schlüsselpaar

Zum Ver- und Entschlüsseln von Texten benötigt mensch ein Schlüsselpaar, das gleich nach der Installation des Programms PGP erstellt werden kann. Das Schlüsselpaar besteht aus

- deinem privaten Schlüssel (secret key, private key)
- deinem öffentlichen Schlüssel (public key)

Der Schlüsselbund

Diese Schlüssel hängen wie im wirklichen Leben an einem sogenannte „Schlüsselbund“ (Keyring), der um weitere Schlüssel erweitert werden kann.

An diesen Schlüsselbund werden später z.B. die öffentlichen Schlüssel von anderen Personen gehängt, um ihnen verschlüsselte Nachrichten senden zu können.

Der private Schlüssel

Deinen privaten Schlüssel benötigst du, um für dich verschlüsselte Mails entschlüsseln zu können. Er ist durch ein Passwort (eine „Passphrase“) geschützt.

Die öffentlichen Schlüssel

Die öffentlichen Schlüssel anderer Personen benötigst du, um für diese anderen Personen Texte verschlüsseln zu können. Genauso brauchen andere Personen deinen öffentlichen Schlüssel, um für dich Texte verschlüsseln zu können.

Diese öffentlichen Schlüssel sind, wie der Name sagt, öffentlich, d.h. jeder Mensch kann deinen öffentlichen Schlüssel haben, auch neugierige Menschen. Er ermöglicht ja nur, dir für dich verschlüsselte Texte zu schicken.

Zurück zum Inhalt dieses Kapitels

Das Austauschen der öffentlichen Schlüssel

Als Beispiel werden hier 2 Personen, Maxi und Josefine, angenommen. Mit dem öffentlichen Schlüssel von Maxi kann Josefine an Maxi verschlüsselte Texte schicken. Nur die BesitzerIn des privaten Schlüssels kann diesen Text entschlüsseln, in diesem Fall also Maxi. Maxi muss vorher seinen öffentlichen Schlüssel an Josefine schicken, damit diese Mails für Maxi verschlüsseln kann.

Verschlüsselt z.B. Josefine eine Mail für Maxi, kann nicht einmal sie selbst diese Mail jemals wieder entschlüsseln, sie wurde ja für Maxi und nur für Maxi verschlüsselt

Umgekehrt geht's natürlich auch: Josefine schickt ihren öffentlichen Schlüssel an Maxi, dann kann Maxi verschlüsselte Texte an Josefine schicken.

Du kannst deinen öffentlichen Schlüssel ganz offen verschicken bzw. hinterlegen, prinzipiell kann ihn jeder Mensch haben, auch neugierige Menschen. Er berechtigt ja nur dazu, dir verschlüsselte Nachrichten zu schicken.

Siehe auch das zugehörige Beispiel

Zurück zum Inhalt dieses Kapitels

Das Hinterlegen der öffentlichen Schlüssel auf einem Key-Server

Die beste Möglichkeit, anderen deinen öffentlichen Schlüssel zukommen zu lassen, ist das Hinterlegen des öffentlichen Schlüssels auf einem sogenannten Key-Server.

Diese Computer, die über das Internet erreichbar sind, dienen nur dazu, öffentliche Schlüssel von Personen auf der ganzen Welt zu speichern. Andere Personen können dann jederzeit deinen öffentlichen Schlüssel von diesem Computer herunterladen und dir dann verschlüsselte Nachrichten senden. Wie das funktioniert, wird im Kapitel Das Versenden deines öffentlichen Schlüssels an den Key-Server beschrieben.

Besser ist diese Vorgangsweise auch deshalb, weil die andere Person ganz sicher sein muss, dass dieser öffentliche Schlüssel auch wirklich von dir ist bzw. umgekehrt.

Theoretisch könnte ja ein neugieriger Mensch z.B. deine Mail mit dem öffentlichen Schlüssel abfangen, deinen Schlüssel mit seinem eigenen vertauschen, und diesen eigenen Schlüssel weitersenden. Dieser neugierige Mensch könnte dann jede Mail von dir an die andere Person abfangen, entschlüsseln, für deine Zielperson neu verschlüsseln und weiterschicken. So ein Angriff wird als „man-in-the-middle-attack“ („Mann-in-der-Mitte-Attacke") bezeichnet. Aber das ist wie gesagt wirklich nur eine theoretische Möglichkeit, also keine Panik.

Zurück zum Inhalt dieses Kapitels

Das Schützen des privaten Schlüssels mittels Passwort

Dein privater Schlüssel ist natürlich durch ein Passwort geschützt, bei PGP sogar durch eine sogenannte „Passphrase“, nämlich einen ganzen „Passwort-Satz“.

Tipps zur Wahl eines guten Passworts (bzw. einer guten Passphrase) findest du im Kapitel Tipps für Passwörter/Passphrases.

Zurück zum Inhalt dieses Kapitels

Das Sichern deines privaten Schlüssels

Du solltest deinen privaten Schlüssel irgendwo sichern, d.h. auf eine Diskette oder eine CD kopieren. Kommt dir dein privater Schlüssel abhanden (z.B. wenn deine Festplatte eingeht) und du hast ihn nicht gesichert, kannst du nie mehr die alten für dich verschlüsselten Mails lesen.

Sollte einer anderen Person dein privater Schlüssel in die Hände fallen, so ist das nicht allzu schlimm, solange sie dein Passwort nicht herausfindet. Diese andere Person kann dann nur Personen verschlüsselte Texte zusenden und sich dabei als du ausgeben.

Zur Absicherung dagegen kann mensch Texte sowohl ohne Passwort-Eingabe (unsigned) oder mit Passwort-Eingabe (signed) verschicken. Die EmpfängerIn sieht im verschlüsselten Text, ob bei der Verschlüsselung das Passwort angegeben wurde oder nicht (ob die Nachricht „signed“ oder „unsigned“ ist). Daher also Texte immer mit Passwort-Eingabe verschlüsseln.

Zurück zum Inhalt dieses Kapitels

Beispiel

Nachfolgend findest du eine Beschreibung des prinzipiellen Ablaufs des Schlüsselpaar-Erstellens, des Ver- und Entschlüsseln und des Verschickens von verschlüsselten Mails.

Angenommen werden zwei Personen, Maxi und Josefine, die beide

- PGP installiert haben
- Je ein erstes Schlüsselpaar erstellen
- Den eigenen öffentlichen Schlüssel an die jeweils andere Person schicken bzw. auf einem Key-Server hinterlegen
- Für die jeweils andere Person eine verschlüsselte Nachricht schreiben und verschicken.
- Die Nachricht der jeweils anderen Person entschlüsseln und lesen

Maxi		Josefine
M. installiert PGP auf seinem Computer		J. installiert PGP auf ihrem Computer
M. erstellt ein Schlüsselpaar mit seinem privatem und seinem öffentlichem Schlüssel		J. erstellt ein Schlüsselpaar mit ihrem privatem und ihrem öffentlichem Schlüssel
M. hat seinen privaten und seinen öffentlichen Schlüssel auf seinem Computer		J. hat ihren privaten und ihren öffentlichen Schlüssel auf ihrem Computer
M. schickt eine Kopie seines öffentlichen Schlüssels an Josefine oder hinterlegt ihn auf einem Key-Server	→	J. nimmt den öffentlichen Schlüssel von Maxi in ihren Schlüsselbund auf und kann jetzt verschlüsselte Texte an Maxi schicken

Maxi		Josefine
M. nimmt den öffentlichen Schlüssel von Josefine in seinen Schlüsselbund auf und kann jetzt verschlüsselte Texte an Josefine schicken	←	J. schickt eine Kopie ihres öffentlichen Schlüssels an Maxi oder hinterlegt ihn auf einem Key-Server
		J. schreibt eine Mail für Maxi
		J. verschlüsselt die Mail an Maxi mit Maxis öffentlichem Schlüssel, der bereits an ihrem Schlüsselbund hängt
		J. kann diese Mail nun selbst nicht mehr lesen, sie wurde für Maxi und nur für Maxi verschlüsselt
M. erhält die für ihn von Josefine verschlüsselte Mail	←	J. schickt die verschlüsselte Mail an Maxi
M. entschlüsselt die Mail mit seinem privaten Schlüssel		
M. kann die Mail lesen		
M. schreibt eine Antwort für Josefine		
M. verschlüsselt die Mail an Josefine mit Josefines öffentlichem Schlüssel, der bereits an seinem Schlüsselbund hängt		
M. kann diese Mail nun selbst nicht mehr lesen, sie wurde für Josefine und nur für Josefine verschlüsselt		
M. schickt die verschlüsselte Mail an Josefine	→	J. erhält die für sie von Maxi verschlüsselte Mail
		J. entschlüsselt die Mail mit ihrem privaten Schlüssel
		J. kann die Mail lesen

Detaillierte Angaben zur Installation von PGP und zur Schlüsselverwaltung findest du im Kapitel PGP – Installation und Schlüsselverwaltung.

Zurück zum Inhalt dieses Kapitels

4.3 Das Verschlüsseln von Festplatten-bereichen mit PGP Disk

Was ist PGP Disk?

Mit PGP kann mensch nicht nur einzelne Texte (z.B. Mails) verschlüsseln, mit dem zugehörigen Programm „PGP Disk“ kann mensch auch ganze Festplatten oder Teile davon verschlüsseln (wenn hier von Festplatten die Rede ist, sind auch Disketten, Zip-Disketten u.ä. gemeint).

Dazu werden ein oder mehrere Teile deiner Festplatte für die Verschlüsselung reserviert, diese Teile werden dann wie eine eigene Festplatte, eine CD oder eine Diskette behandelt, sie erhalten einen eigenen Laufwerksbuchstaben (wie C:\ für deine Hauptfestplatte), du kannst dann problemlos auf die Dateien dieser (virtuellen, nicht real existierenden) Laufwerke zugreifen, natürlich nur, wenn du die Passphrase zu diesem Laufwerk weißt.

Diese Festplattenbereiche sind dann für neugierige Menschen genauso unlesbar wie eine verschlüsselte Mail.

Zurück zum Inhalt dieses Kapitels

Hintergrund

Auf deiner Festplatte (bzw. einer deiner Festplatten) wird eine eigene Datei angelegt, welche dann die Informationen deiner verschlüsselten Daten (Dateien) enthält.

Nach dem Öffnen mit der Eingabe des Passworts verhält sie sich wie ein eigenes Laufwerk (eine Partition), hat dann also z.B. in Windows die gleiche Erscheinungsform wie eine Diskette oder eine CD, sie besitzt nämlich einen eigenen Laufwerksbuchstaben (z.B. F). Diesen Buchstaben kannst du unter noch nicht benutzten Laufwerksbuchstaben aussuchen.

Zum Lesen der Dateien auf diesem „virtuellen“ (nicht real existierenden) Laufwerk (dieser Partition) muss das Laufwerk zuerst gemountet werden. Mounten heißt, es wird zu deinem Dateisystem dazugehängt, vorher siehst du z.B. im Windows Explorer den Laufwerksbuchstaben nicht. „Virtuell“ (nicht real existierend deshalb, weil es ja nicht wirklich eine neue Festplatte oder ähnliches ist, du kannst es aber genauso behandeln wie eine eigene Festplatte).

Genauso wie mounten kannst du das Laufwerk auch un-mounten (abhängen). Der Laufwerksbuchstabe verschwindet dann wieder aus deinem Dateisystem, die Dateien dieses Laufwerks sind dann nicht sicht- oder lesbar.

Während dieses Laufwerk gemountet ist, haben auch neugierige Menschen Zugriff darauf, also den Computer bei Verlassen immer abdrehen oder zumindest vorher das verschlüsselte Laufwerk unmounten.

Mehr zu PGP Disk erfährst du im Kapitel PGP Disk.

Zurück zum Inhalt dieses Kapitels

4.4 Zusammenfassung

Eine der wichtigsten Funktionen von PGP ist das Verschlüsseln von Texten, wie z.B. Mails. Der Vorgang ist:

- Du und alle Personen, die mit PGP verschlüsselte Nachrichten austauschen, müssen das Programm PGP installieren.
- Du musst ein Schlüsselpaar mit öffentlichem und privatem Schlüssel erstellen.
- Du verschickst deinen öffentlichen Schlüssel an Personen, die verschlüsselte Mails an dich versenden wollen (bzw. hinterlegst du deinen öffentlichen Schlüssel auf einem Key-Server).
- Du nimmst die öffentlichen Schlüssel von anderen Personen, an die du verschlüsselte Mails schicken willst, in deinen Schlüsselbund auf.
- Wenn du eine verschlüsselte Nachricht an eine andere Person verschicken willst, musst du sie für diese Person verschlüsseln. Keine andere als diese EmpfängerIn mit ihrem privaten Schlüssel kann dann die Nachricht entschlüsseln, nicht einmal du selbst.
- Der private Schlüssel muss gut aufgehoben und z.B. auf einer Diskette (besser auf mehreren Disketten) oder einer CD gesichert werden
- Der einzige Schutz deines privaten Schlüssels ist das zugehörige Passwort (die „Passphrase“).
- Kommt dir dein privater Schlüssel abhanden (z.B. hast du ihn nicht gesichert und deine Festplatte geht kaputt), kannst du bisherige an dich verschlüsselt geschickte Mails nie mehr lesen. Also irgendwo (z.B. auf Disketten oder CD) sichern und gut aufpassen darauf.
- Du kannst nicht nur einzelne Texte (Mails) verschlüsseln, du kannst mit PGP auch Teile oder fast die ganze Festplatte verschlüsseln. Dazu dient das inkludierte Teil-Programm PGP Disk.

Zurück zum Inhalt dieses Kapitels

5 PGP – Installation und Schlüssel-verwaltung

Überblick

In diesem Kapitel werden die Installation von PGP und die Erstellung, Verwaltung, Hinterlegung und Sicherung von Schlüsseln erklärt.

Du findest folgende Infos zu folgenden Bereichen:

- Die Installation von PGP
- Einen kurzen Überblick über die verschiedenen Teilprogramme von PGP
- Die Erstellung des ersten Schlüsselpaars
- Das Versenden deines öffentlichen Schlüssels an den Key-Server
- Das Finden eines öffentlichen Schlüssels auf dem Key–Server und die Aufnahme in den Schlüsselbund
- Das Exportieren des öffentlichen Schlüssels für jemanden anderen
- Das Importieren eines öffentlichen Schlüssels von jemandem anderen
- Das Sichern des Schlüsselpaares
- Problembehebung: nach der PGP Installation keine Verbindung zum Internet

PGP Programme ⇔ Schlüssel ⇔ verschlüsselte Laufwerke

Bei PGP ist immer zwischen dem Programm PGP und den mit PGP erstellten Schlüsseln und verschlüsselten Laufwerken zu unterscheiden.

Selbst wenn du das Programm PGP löschst (deinstallierst), mehrmals installierst (z.B. später andere Versionen installierst) u.a., gehen deine mit dem Programm PGP erstellten Schlüssel und verschlüsselten Laufwerke nicht verloren.

Du benötigst jedoch das Programm PGP, um deine mit PGP erstellten Schlüssel und verschlüsselten Laufwerke verwenden zu können.

Nach einer Neuinstallation musst du nur angeben, wo sich deine Schlüssel befinden, bzw. wo sich die Dateien mit deinen verschlüsselten Laufwerken befinden.

Zurück zum Inhalt dieses Kapitels

5.1 Die Installation des Programms

Die Deinstallation von bereits installierten PGP Versionen

Hast du bereits eine Version von PGP installiert, musst du diese vor der neuen Installation deinstallieren. Das machst du am Besten durch Wählen von

- „Start ⇨ Einstellungen ⇨ Systemsteuerung ⇨ Software ⇨ PGP“ suchen und markieren ⇨ „Ändern/Entfernen ⇨ PGP“

oder in Windows98

- „Start ⇨ Einstellungen ⇨ Systemsteuerung ⇨ Hinzufügen/Entfernen von Programmen“ ⇨ PGP suchen und markieren ⇨ „Ändern/Entfernen ⇨ PGP“

oder in Englisch

- „Start ⇨ Settings ⇨ Control Panel ⇨ Add/Remove Programs“ ⇨ PGP suchen und markieren ⇨ „Add/Remove ⇨ PGP“

oder so ähnlich. Du musst nach der Deinstallation wie verlangt den Computer neu starten.

Zurück zum Inhalt dieses Kapitels

Das PGP Installationsprogramm

Auf der CD im Verzeichnis PGP findest du PGP-Versionen für Windows, MacOS und verschiedene Unix-Versionen (z.B. Linux). Als Beispiel wird hier die Windows-Installation der Vollversion 6.5.8 (inkl. PGP Disk) auf Windows 98 angeführt. Bei anderen Betriebssystemen ist der Installationsvorgang ganz ähnlich bis genauso.

Es gibt PGP-Versionen für eine Vielzahl von Unix-Derivaten (z.B. Linux), du findest sie auf der CD unter PGP\Unix in den jeweiligen Verzeichnissen.

Für Windows öffne den Windows Explorer, wechsle auf der CD ins Verzeichnis PGP/Windows/6.5.8 und doppelklicke auf die Datei pgp658ckt02.exe. Das Installationsprogramm wird gestartet.

PGP\Windows\6.5.8

pgp658ckt02.exe

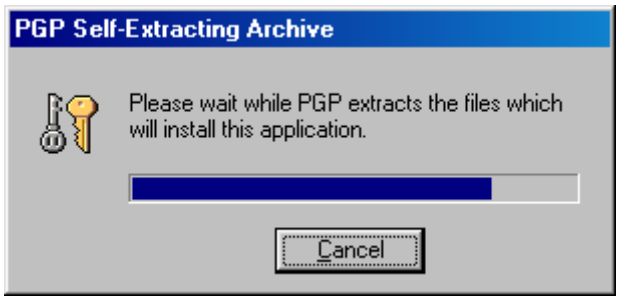
PGP\MacOS\6.5.8

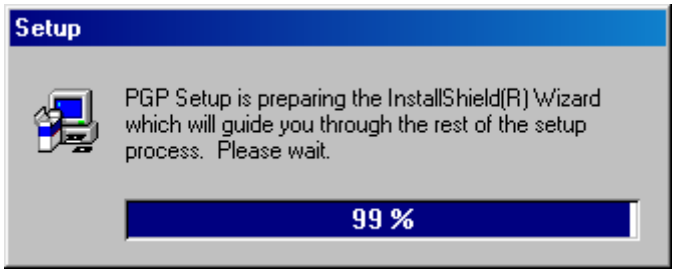
PGPFW658Mac.sit.bin

PGP\Unix\…

Zurück zum Inhalt dieses Kapitels

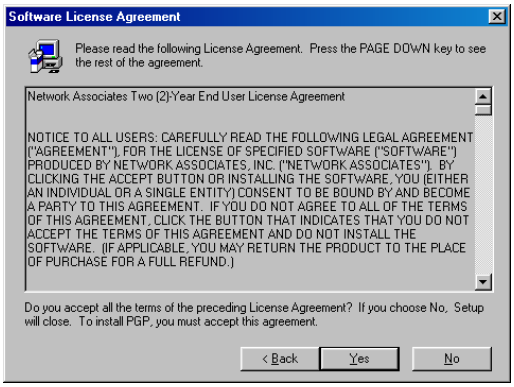
Die Vorbereitung des Installationsprogramms beginnt:

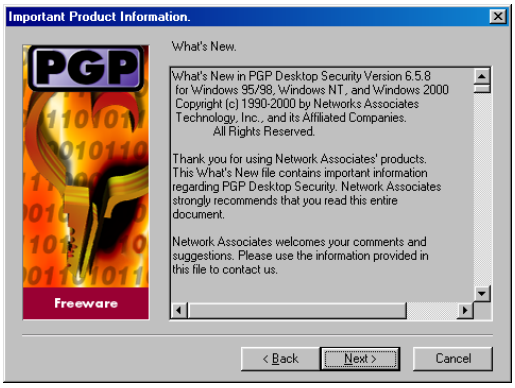


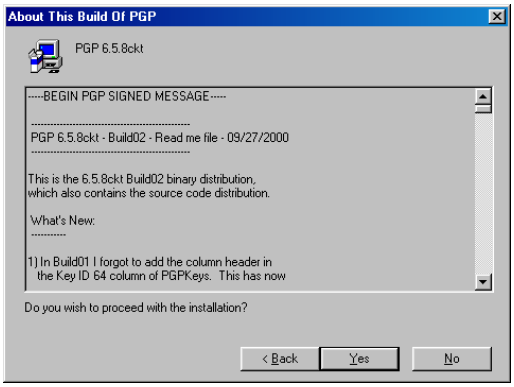


Zurück zum Inhalt dieses Kapitels

Zu Beginn erscheinen diverse Begrüßungen und Bestätigungen von Lizenzverträgen. Einfach immer „Next“, „Yes“, „Ja“ o.ä. drücken.

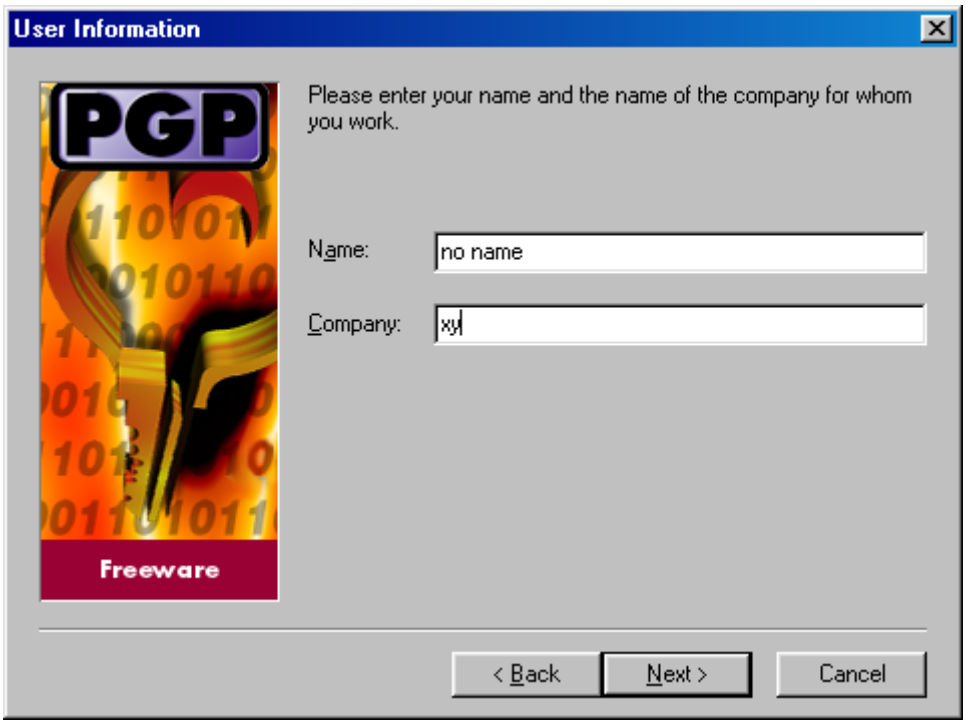






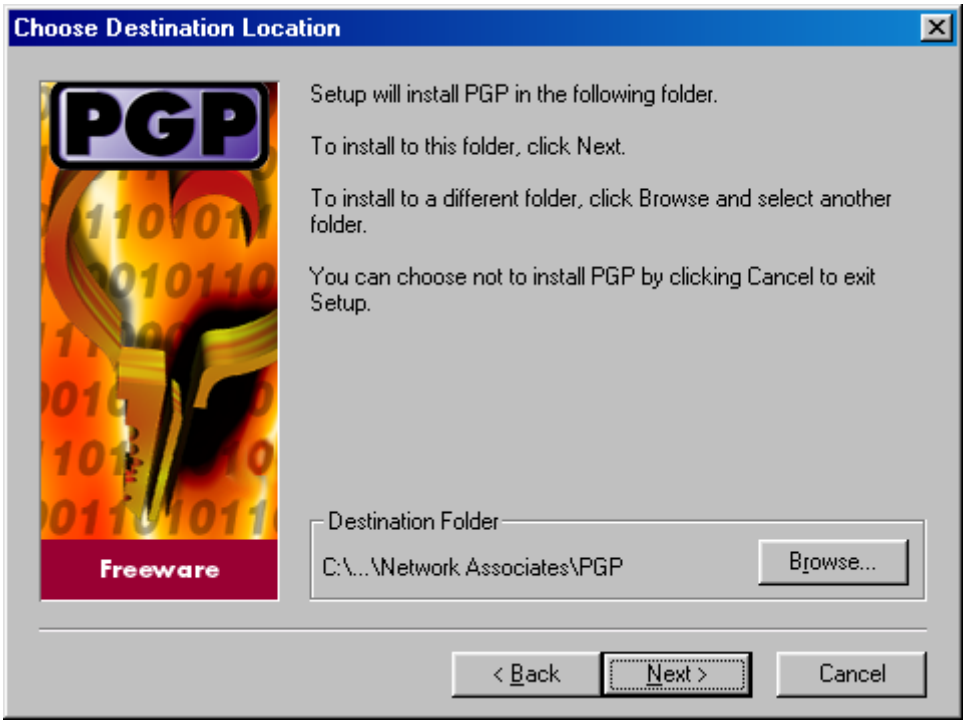
Zurück zum Inhalt dieses Kapitels

Dann werden einige Dinge abgefragt. Den Namen und die eigene wirkliche E-Mail Adresse muss mensch nicht angeben, geht ja eigentlich niemanden etwas an.



Zurück zum Inhalt dieses Kapitels

Jetzt musst du das Verzeichnis angeben, in das PGP installiert werden soll. Du kannst ruhig das vorgeschlagene Verzeichnis akzeptieren und einfach „Next“ drücken. Wenn du willst, kannst du natürlich mit „Browse“ auch ein anderes Verzeichnis wählen.



Zurück zum Inhalt dieses Kapitels

Dann wird abgefragt, was du installieren möchtest (Abbildung auf nächster Seite). Du möchtest aber ziemlich sicher nicht, wie vorgeschlagen, alles installieren.

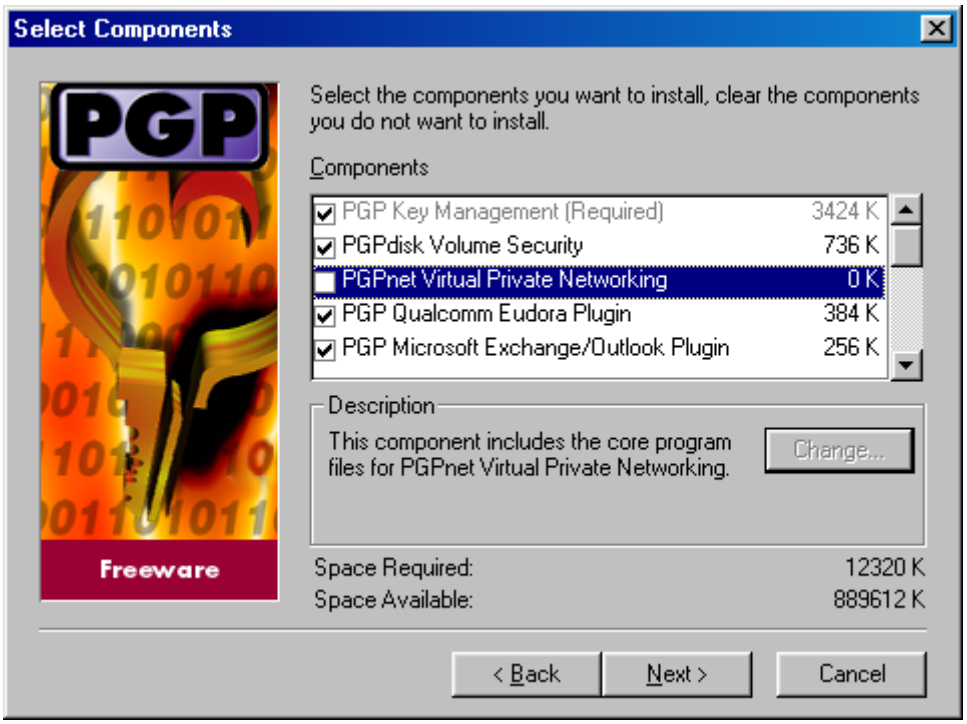
„PGPnet Virtual Private Networking" dient vor allem für den Datenverkehr innerhalb eines (z.B. Firmen-) Netzwerkes. Dazu müssen alle Computer innerhalb dieses Netzwerkes konfiguriert werden. Für den Normalgebrauch benötigen wir dieses Programm nicht.

Wichtig: wenn du vergisst, dieses Programm wegzukreuzeln, kannst du nach der Installation von PGP keine Verbindung mehr zum Internet herstellen!

Falls dir das passiert, siehe dazu Problembehebung: nach PGP Installation keine Verbindung zum Internet

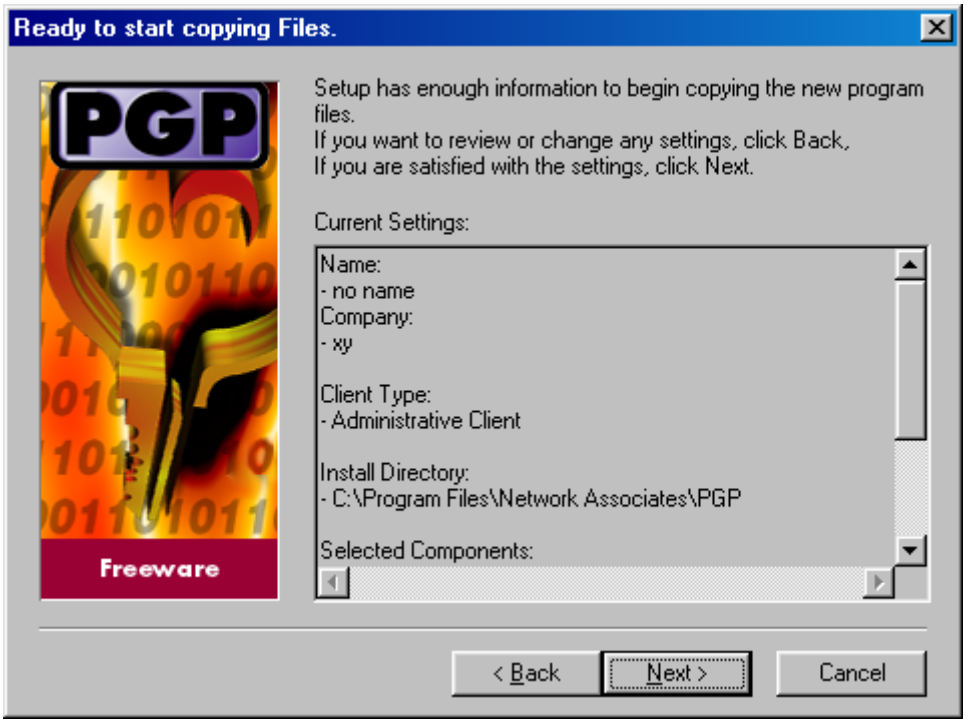
Die Liste hängt von auf deinem Computer installierten Mail-Programmen ab. Im Beispiel unten werden Integrationsprogramme für Eudora und Microsoft Outlook mit installiert. Das macht das spätere Ver- und Entschlüsseln von Texten viel komfortabler.

Also, falls es sich in der Liste befindet, keinesfalls vergessen, PGPnet Virtual Private Networking zu entmarkieren (entkreuzeln = nicht installieren), den Rest kannst du angekreuzt lassen.



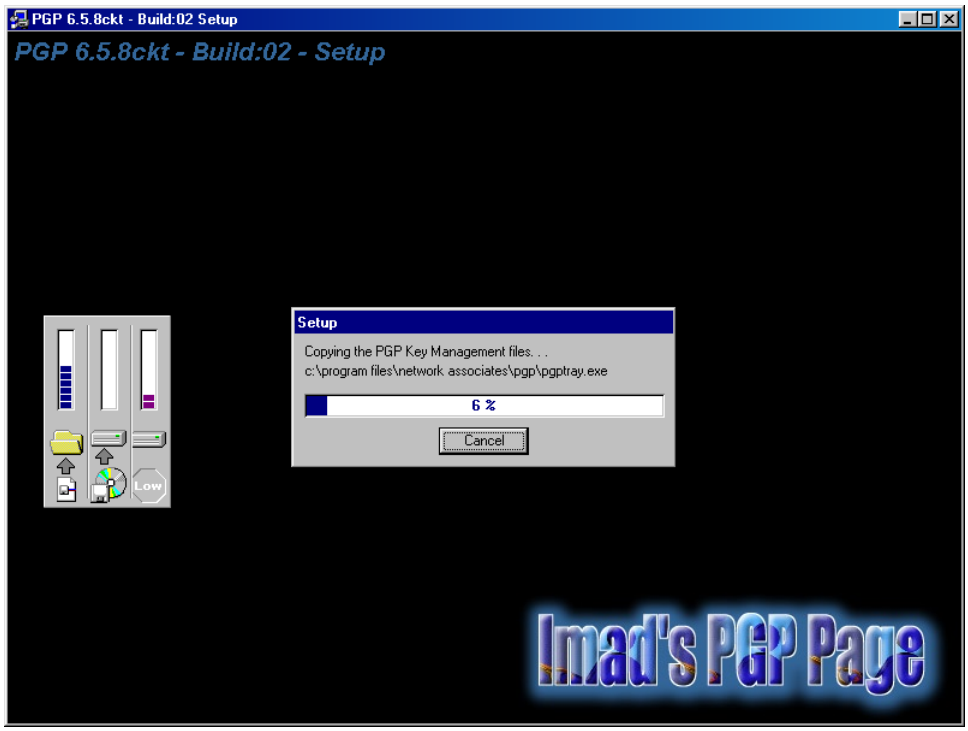
Zurück zum Inhalt dieses Kapitels

So, nun hat das Installationsprogramm alle nötigen Informationen. Noch ein Click auf „Next“ und die eigentliche Installation beginnt.



Zurück zum Inhalt dieses Kapitels

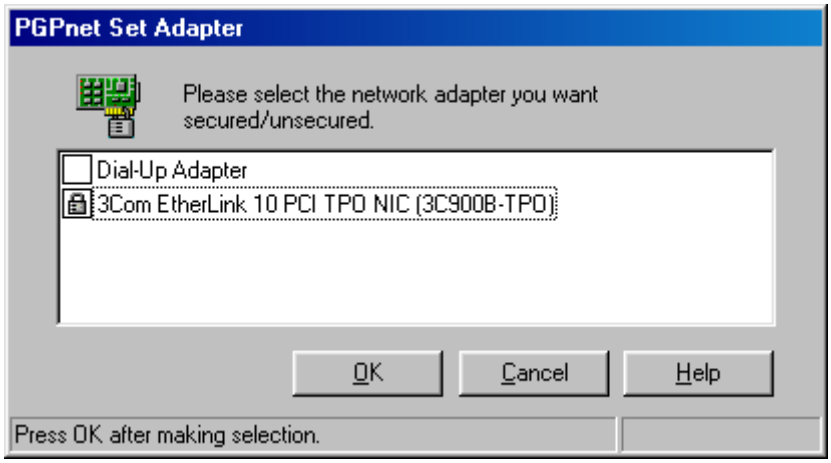
Jetzt beginnt die eigentliche Installation des Programms, die nicht allzu lange dauert.



Zurück zum Inhalt dieses Kapitels

Wenn du vergessen hast, das Teilprogramm PGPnet Virtual Private Networking“ zu entmarkieren, erhältst du noch folgende Abfrage. Klick einfach irgendwas an (du musst leider irgendwas markieren, sonst ist der Button „OK“ nicht aktiviert) und schaue dann im Kapitel Problembehebung: nach PGP Installation keine Verbindung zum Internet nach, was du nachher machen musst, um wieder eine Internetverbindung herzustellen.

Diejenigen, die das erwähnte Programm wie empfohlen entmarkiert haben (= nicht installiert haben), sehen die folgende Abfrage nicht.

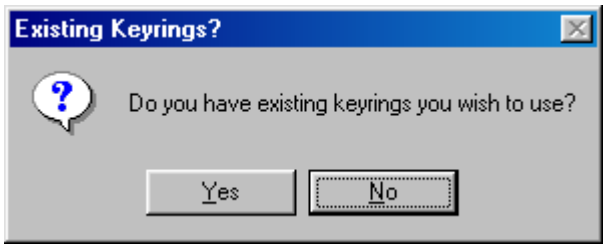


Zurück zum Inhalt dieses Kapitels

Zum Abschluss musst du noch angeben, ob du einen bereits existierenden Schlüsselbund hast. Beim ersten Installieren von PGP hast du natürlich noch keine und wirst sie später erzeugen.

Falls du bereits einen Schlüsselbund hast, dann kannst du „Yes“ wählen und dann die Dateien mit den Schlüsseln angeben.

Hast du noch keinen existierenden Schlüsselbund, wähle „No“.



Zurück zum Inhalt dieses Kapitels

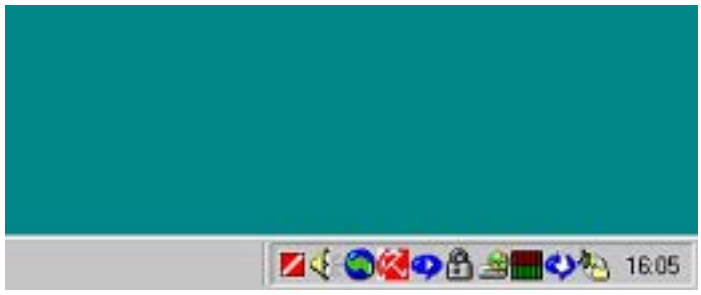
Nach dem Ende der Installation muss der Computer neu gestartet werden.

Nun ist die Installation abgeschlossen, nach dem Neustart des Computers kannst du gleich dein erstes Schlüsselpaar erstellen.

Zurück zum Inhalt dieses Kapitels

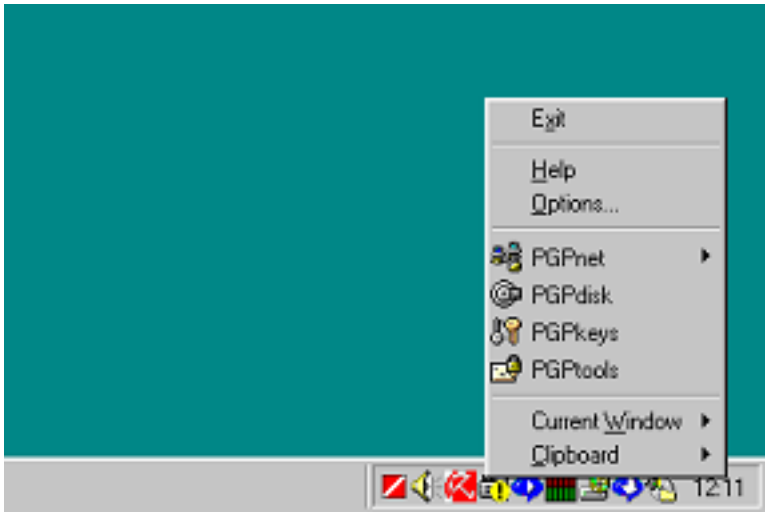
5.2 Die PGP Programme

Nach der Installation von PGP und dem Neustart des Computers siehst du auf deinem Desktop rechts unten ein neu hinzugekommenes Symbol, das wie ein Schloss aussieht (6. Symbol von links, 5. von rechts).



Wenn du mit dem Mauszeiger auf das Schloss-Symbol zeigst und die rechte Maustaste drückst, siehst du ein paar PGP Programme aufgelistet, z.B.:

- PGPdisk (zu diesem Programm kommen wir noch)
- PGPkeys (das wirst du gleich kennenlernen)
- PGPtools (ein Fensterchen mit allen PGP Programmen)



Zurück zum Inhalt dieses Kapitels

Wenn du PGPtools auswählst, geht folgendes Fenster mit fast allen PGP-Programmen auf (PGP Disk fehlt leider, ist halt doch keine richtige Vollversion)

Die Programme sind von links nach rechts:

- PGPkeys (Schlüsselverwaltung)
- Encrypt (Verschlüsseln)
- Sign (Signieren)
- Encrypt Sign (Verschlüsseln und Signieren)
- Decrypt/Verify (Entschlüsseln)
- Wipe (einzelne Dateien nicht wiederherstellbar löschen)
- Freespace Wipe (freigegebenen Speicherplatz nicht wiederherstellbar machen)

Die meisten der einzelnen Programme wirst du in den folgenden Kapiteln kennenlernen. Wie bereits erwähnt, fehlt bei diesem Fenster nur das Programm „PGP Disk“, das findest du aber im Kontextmenü, wenn du mit der rechten Maustaste auf das Schloss-Symbol am rechten unteren Rand deines Bildschirms klickst (siehe Abbildung auf der vorherigen Seite).

Zurück zum Inhalt dieses Kapitels

5.3 Die Erstellung des ersten Schlüsselpaars

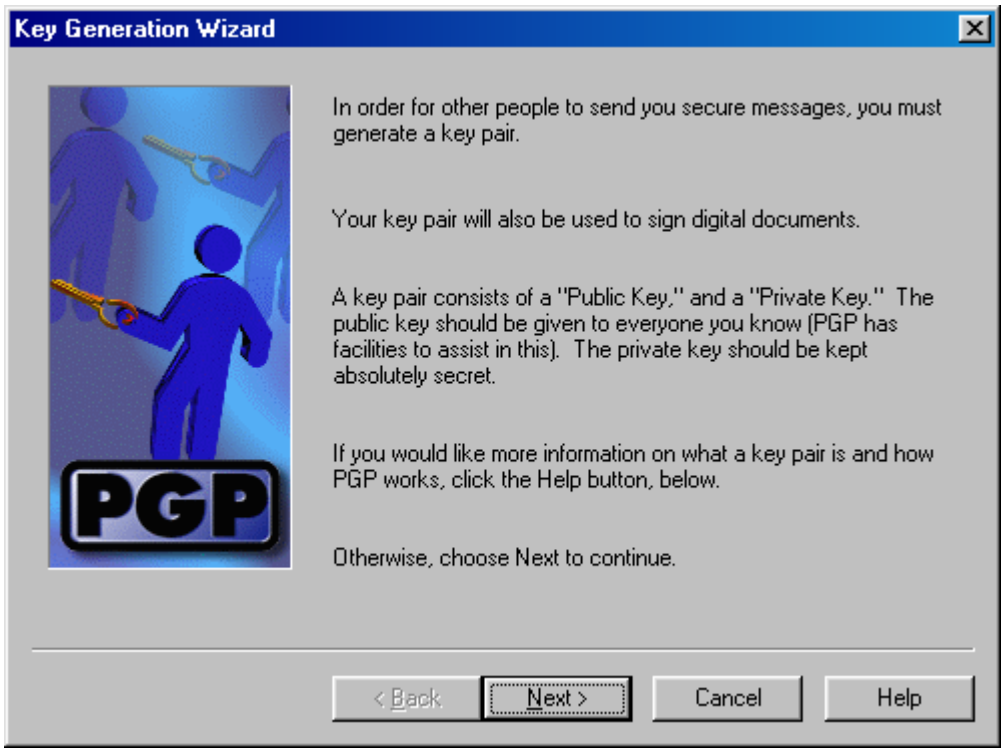
Das Programm PGPkeys dient der Schlüsselerstellung und Schlüsselverwaltung. Du kannst damit dein eigenes Schlüsselpaar erstellen und dann die öffentlichen Schlüssel von anderen Personen an deinen Schlüsselbund hängen.

Jetzt beginnst du mal mit der Erstellung deines ersten eigenen Schlüsselpaars, das aus deinem privaten (private key, secret key) und deinem öffentlichen (public key) besteht.

Wenn du das Programm PGPtools gewählt hast, drücke auf den ganz linken Button PGPkeys. Ohne das Fenster mit den PGPtools kannst du auch direkt mit der rechten Maustaste auf dem Schloss-Symbol rechts unten auf deinem Bildschirm das Programm PGPkeys wählen. Ist einfach das Gleiche, mach es, wie es dir sympathischer ist.

Hast du bei der Installation angegeben, noch keinen Schlüsselbund zu besitzen, geht beim ersten Start des Programms PGPkeys folgendes Fenster auf, das dich darauf hinweist, dass du jetzt ein Schlüsselpaar erstellen musst, um anderen Personen verschlüsselte Nachrichten senden zu können.

Drücke einfach „Next“.



Zurück zum Inhalt dieses Kapitels

Dann wirst du wieder mal nach deinem Namen und deiner E-Mail Adresse gefragt. Diese Information wird auch bei verschlüsselten Informationen immer unverschlüsselt mitgeschickt, ist also für jeden Menschen sichtbar. Eine Empfehlung ist, hier nicht deinen wirklichen Namen anzugeben, auch deine E-Mail Adresse geht niemanden etwas an.

Das Problem ist, dass die Verbindung von Namen und e-mail Adresse natürlich für neugierige Menschen äußerst interessant ist. Also einfach irgendwas angeben.

Eine Empfehlung ist allerdings, einen ausgefallenen und irgendwie merkbaren Phantasienamen anzugeben (nicht unbedingt wie im Beispiel unten), das erleichtert später anderen das Auffinden deines Schlüssels auf einem Key-Server ungemein.

Bei der E-Mail Adresse kannst du einfach irgendwas hinschreiben (sollte aber doch wie eine E-Mail Adresse aussehen, mit dem Klammeraffen in der Mitte).

Zurück zum Inhalt dieses Kapitels

Du kannst zu einem späteren Zeitpunkt auch andere Namen und E-Mail Adressen für deinen öffentlichen PGP-Key angeben.

Die Angabe deiner richtigen E-Mail Adresse würde anderen Leuten später das Verschlüsseln von Texten an dich erleichtern, weil dann fast alles automatisch ginge...

Andererseits könnte deine richtige E-Mail Adresse z.B. am Key-Server von lästigen Menschen eingesammelt werden und zum Versenden von Junk Mail (nicht bestellten Massenmails) verwendet werden.

Zurück zum Inhalt dieses Kapitels

Dann wirst du gefragt, welchen Schlüsseltyp du wünscht, nimm Diffie-Hellmann/DSS, das ist der neuere und bietet laut PGP Dokumentation größere Sicherheit und mehr Möglichkeiten.

Allerdings kennen sehr alte Versionen von PGP diesen Schlüsseltyp nicht, wenn du mit Leuten elektronisch kommunizierst, die nur eine Uralt-Version von PGP haben, nimm den RSA-Typ.

Zurück zum Inhalt dieses Kapitels

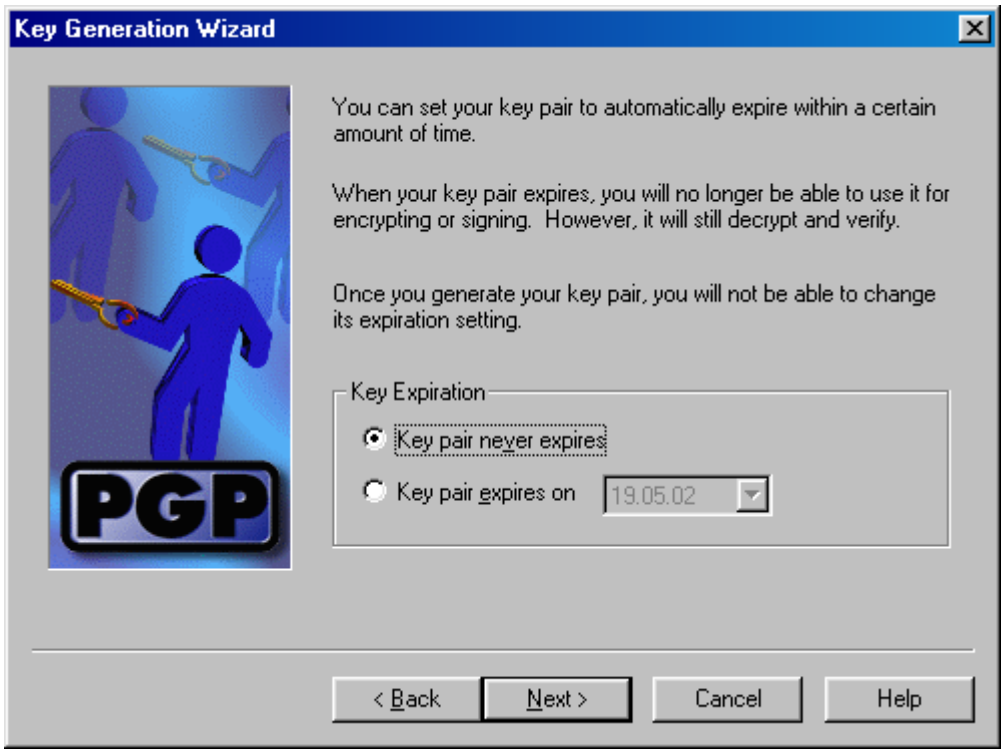
Nun wirst du gefragt, wie groß (=sicher) dein Schlüssel werden soll. Je größer die Schlüsselgröße, desto größer ist die Sicherheit, allerdings dauert das Verschlüsseln dann auch etwas länger, vor allem die erste Schlüsselerstellung dauert bei sehr großen Schlüsseln sogar sehr lange.

4096 Bits bieten eine ausreichend große Sicherheit, wenn du gerade sehr viel Zeit hast (z.B. vor dem Schlafengehen), kannst du auch eine noch höhere Sicherheit wählen (bis 8192 Bits), die nachfolgende Schlüsselerstellung dauert dann jedoch sehr lange.

Gib also 4096 bits oder mehr an und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du angeben, wann dein Schlüssel ungültig wird, diese Angabe ist nach der Schlüsselerstellung nicht mehr korrigierbar. Wähle wie vorgeschlagen „Key pair never expires“, das heißt, dass dein Schlüssel für immer gültig ist (bis du ihn löschst).

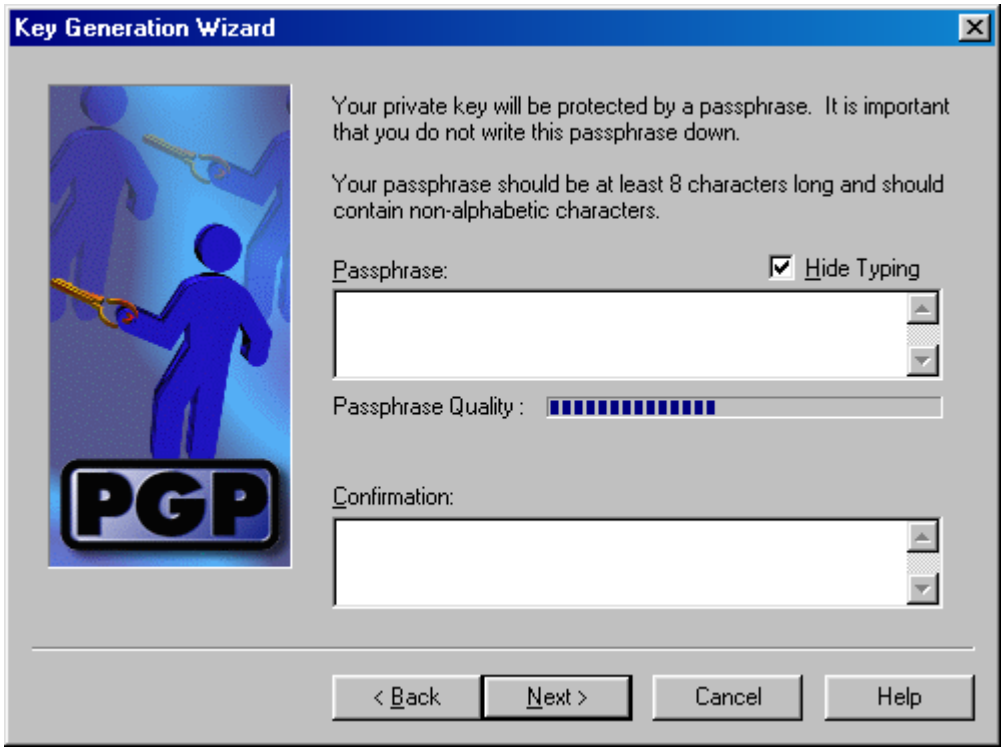


Zurück zum Inhalt dieses Kapitels

Nun musst du eine ausgeklügelte „Passphrase“ (einen „Passwort-Satz“) angeben. Das ist der wichtigste Teil der Schlüsselerstellung, die ganze Sicherheit von PGP ist nur so gut wie das Passwort bzw. die Passphrase, welche das Ganze schützt. Tipps zum Erfinden guter Passwörter findest du im Kapitel Tipps für Passwörter und Passphrases.

Passphrase heißt das deshalb, weil du nicht nur ein einzelnes Passwort angeben kannst, sondern ganze Sätze.

Du musst deine „Passprase“ zwei Mal angeben, um Tippfehler auszuschließen, drücke dann den Button „Next“.

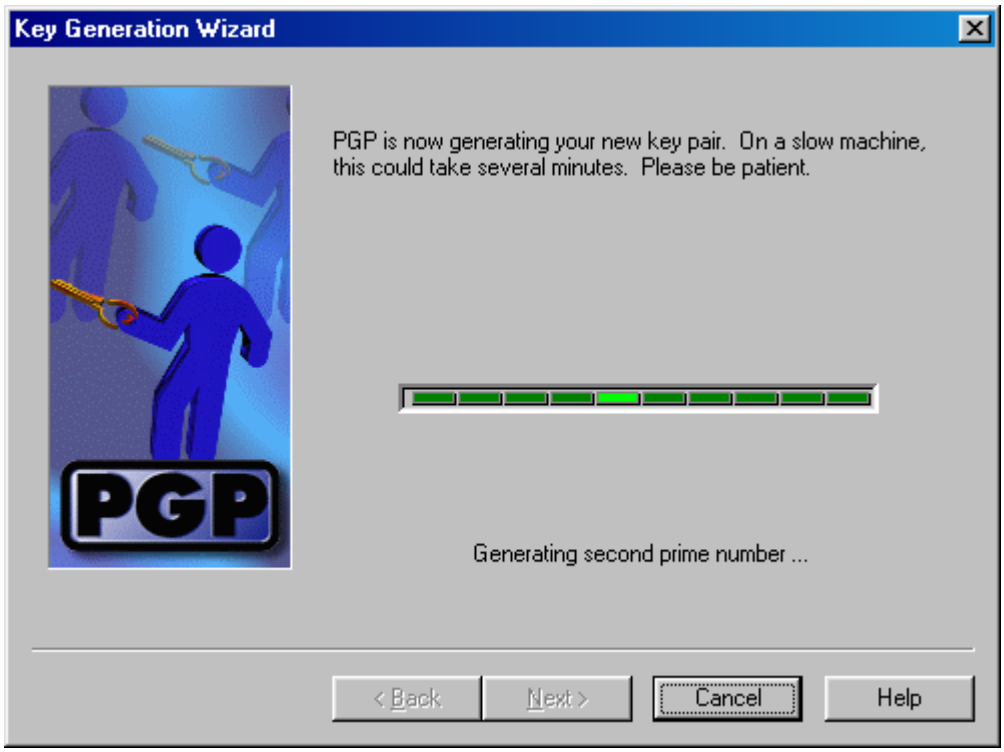


Zurück zum Inhalt dieses Kapitels

Nun heißt es ein bisschen warten, während dein erstes Schlüsselpaar mit einem ausgeklügelten Algorithmus erstellt wird.

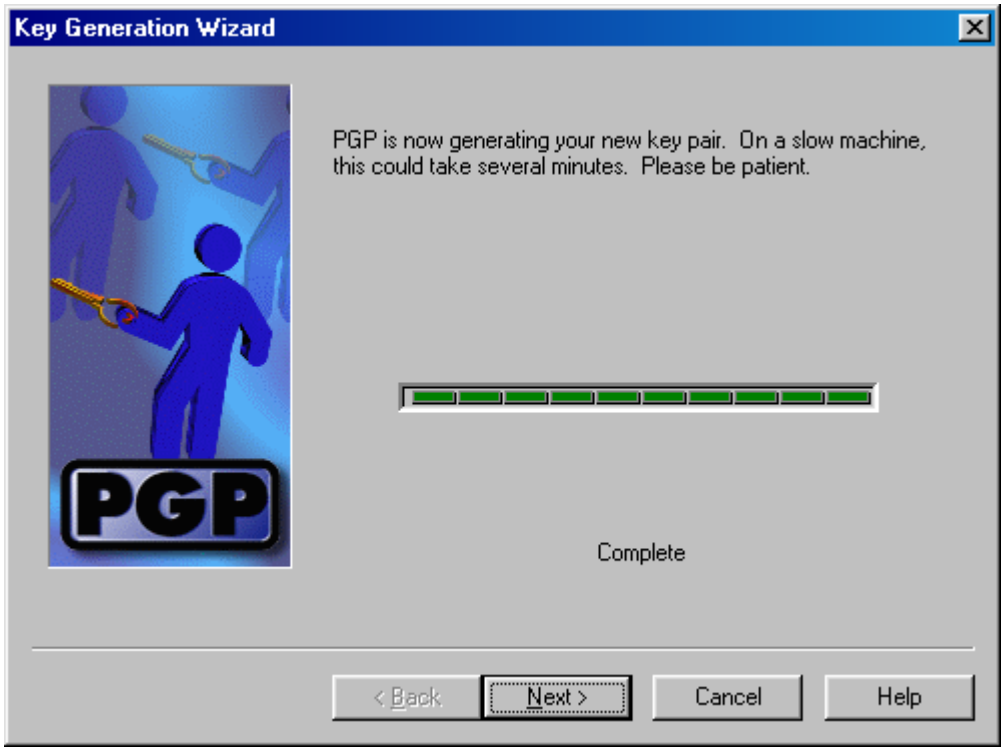
Wie das intern gemacht wird, findest du in den PGP Dokumentationen, der Algorithmus selbst ist öffentlich, jeder Mensch kann ihn sehen. Trotzdem ist dein Schlüssel in dieser Form nie wieder herstellbar. Das heißt auch, dass du auf deinen Schlüssel gut aufpassen musst, mehr dazu findest du im Kapitel „Sichern des Schlüssels“.

Also jetzt bitte um ein wenig Geduld, der Computer ist nicht abgestürzt, es dauert nur ein wenig...



Zurück zum Inhalt dieses Kapitels

Wenn der Schlüssel endlich erstellt ist, siehst du die Mitteilung „Complete“ auf dem Fenster, drücke dann „Next“.



Zurück zum Inhalt dieses Kapitels

Dann wirst du gefragt, ob du deinen öffentlichen Schlüssel auf einem Key-Server hinterlegen willst. Falls du gerade eine Verbindung zum Internet hast, kannst du das Feld „Send my key to the root server now“ anhaken, diesen Vorgang kannst du aber auch jederzeit später machen. Wie das geht, erfährst du im Kapitel Das Versenden des öffentlichen Schlüssels an einen Key-Server“.

Das Hinterlegen deines öffentlichen Schlüssels auf so einem Key-Server hat den Vorteil, dass ihn andere Menschen leicht finden und in ihren Schlüsselbund aufnehmen können (so sie deinen vorher gewählten phantasievollen Namen kennen, den kannst du ihnen aber ja mitteilen). So erspart mensch sich das mühsame Herumschicken von öffentlichen Schlüsseln per Diskette, Mail o.ä.

Außerdem können dann andere Personen sicher sein, dass dieser öffentliche Schlüssel wirklich von dir ist und ihn niemand auf dem Weg übers Internet unbemerkt ausgetauscht hat (was eine sehr theoretische Möglichkeit ist, die aber doch existiert).

Zurück zum Inhalt dieses Kapitels

Wenn du bei der vorherigen Abfrage das Kästchen mit „Send my key to the root server now“ angehakt hast, wird er gleich zu diesem Key-Server gesendet.

Hast du das Kästchen vorher nicht angehakt, siehst du die folgenden beiden Fenster nicht, hast es schon angehakt, erscheint folgendes Fenster:

Zurück zum Inhalt dieses Kapitels

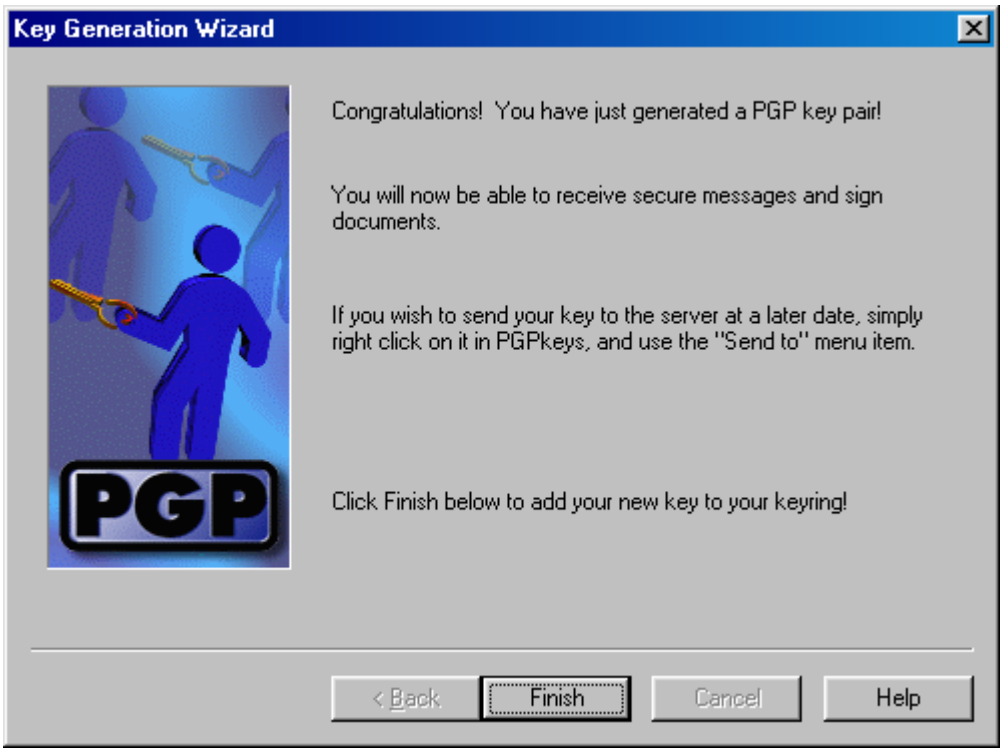
Wenn du aber gerade keine Verbindung zum Internet hast oder sonst was schief geht, erhältst du eine Fehlermeldung. Das macht aber nichts, du kannst dieses Hinterlegen des Schlüssels auch später erledigen (siehe Kapitel „Das Versenden des öffentlichen Schlüssels an einen Key-Server“).

Eine eventuelle Fehlermeldung, wenn keine Verbindung zum Internet vorhanden ist (oder sonst etwas schief geht, was beim Hinterlegen auf einem Key-Server häufig vorkommt), sieht so aus („An error has occurred: host not found“, drücke einfach „Next“).

Zurück zum Inhalt dieses Kapitels

So, jetzt hast du es geschafft, du hast PGP installiert, dein erstes Schlüsselpaar erstellt und eventuell sogar schon deinen öffentlichen Schlüssel auf einem Key-Server hinterlegt.

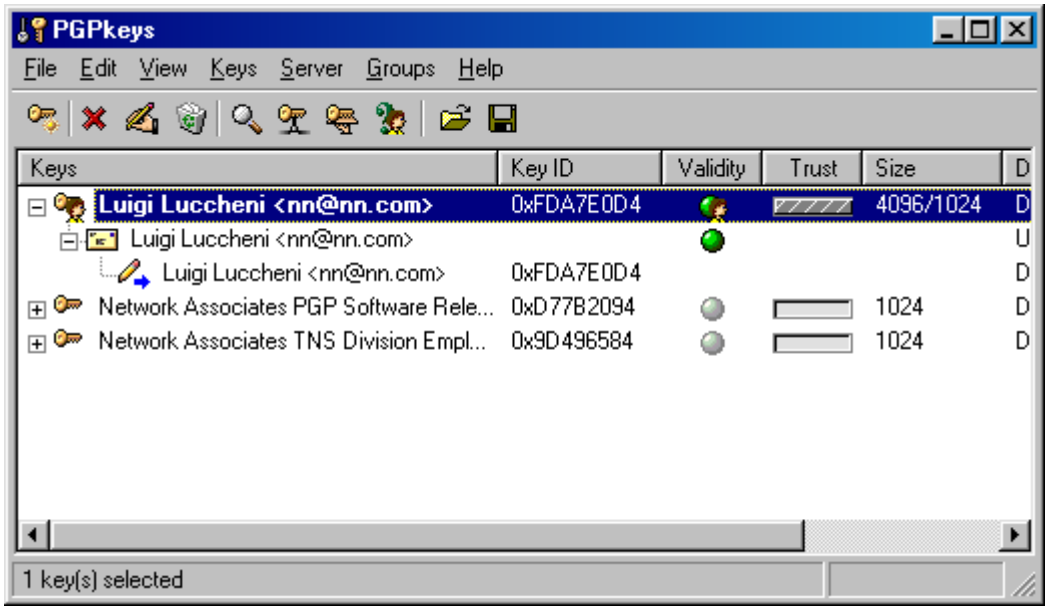
Daher siehst du auch folgenden Gratulations-Dialog auf dem Bildschirm. Einfach mit „Finish“ bestätigen.



Zurück zum Inhalt dieses Kapitels

Nun siehst du gleich das Standardfenster von PGPkeys vor dir, dieses Fenster wird in Zukunft jedes Mal aufgehen, wenn du das Programm PGPkeys wählst.

Hier kannst du alle Schlüssel verwalten, neue öffentliche Schlüssel von anderen aufnehmen, deinen beim Schlüssel erscheinenden Namen ändern, Schlüssel löschen, deinen Schlüssel zum Key-Server schicken u.a (mehr dazu erfährst du in den nächsten Kapiteln)

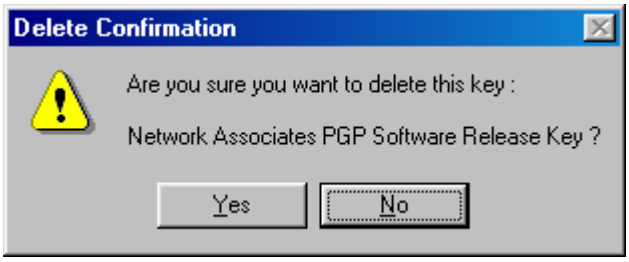


Zurück zum Inhalt dieses Kapitels

Die beiden Einträge mit den Namen „Network Associates ...“ kannst du gleich löschen, die wirst du wahrscheinlich nicht brauchen, außer du willst unbedingt verschlüsselte Mails an die Firma Network Associates schicken.

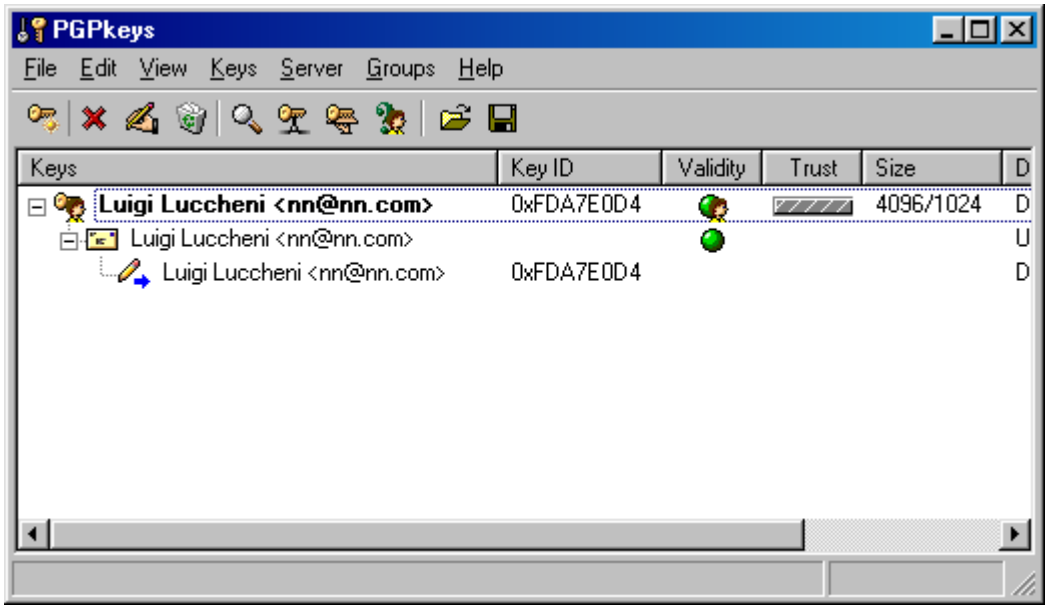
Markiere zum Löschen die entsprechenden Einträge und drücke die Taste „Entf“ wie Entfernen, oder wähle im Menü Edit ⇨ Delete. Aber nicht vergessen, vorher den richtigen Schlüssel zu markieren (nach dem Markieren meist blau hinterlegt), sonst löscht du aus Versehen deinen eigenen Schlüssel.

Bestätige die entsprechende Sicherheitsabfrage mit „Yes“ (= du willst den Schlüssel wirklich löschen, der Name des Schlüssels (hier z.B. „Network Associates“ ist zur Prüfung des Löschvorgangs nochmals angegeben).



Zurück zum Inhalt dieses Kapitels

Nach dem Löschen der beiden nicht benötigten Schlüssel ist nur mehr dein eigenes Schlüsselpaar sichtbar. Jede Änderung bei den Schlüsseln ist natürlich nur nach Eingabe deiner Passphrase, die du bei der Schlüsselerstellung angegeben hast, möglich.



Zurück zum Inhalt dieses Kapitels

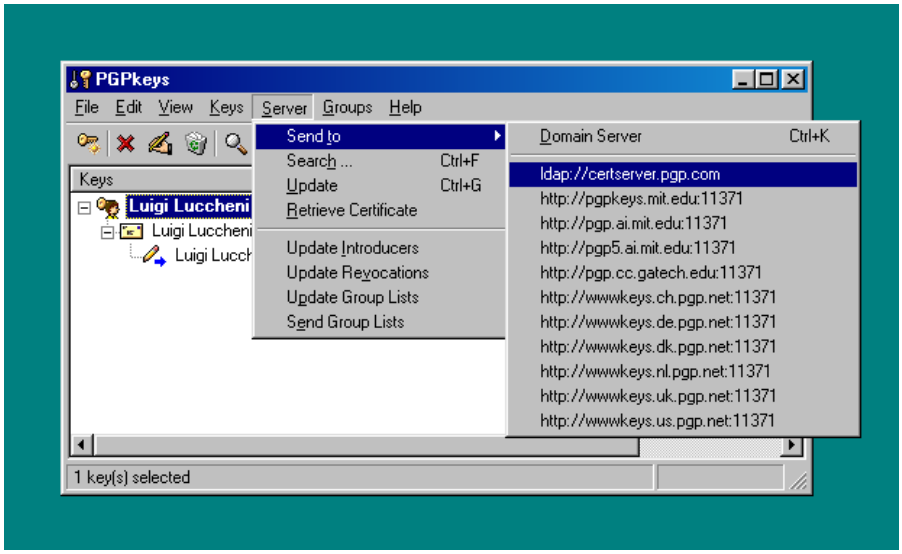
5.4 Das Versenden deines öffentlichen Schlüssels an den Key-Server

Wie schon erwähnt, ist das Hinterlegen des eigenen öffentlichen Schlüssels die beste Möglichkeit, anderen das Aufnehmen deines Schlüssels in ihren Schlüsselbund zu ermöglichen.

Andere Personen benötigen deinen öffentlichen Schlüssel, um dir verschlüsselte Nachrichten schicken zu können.

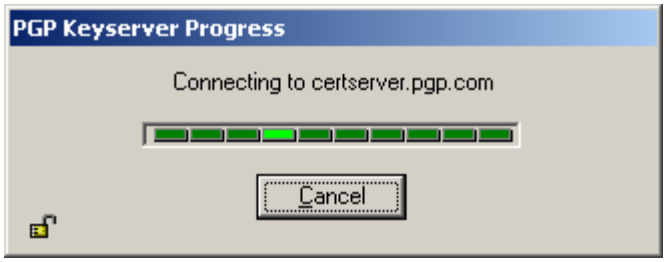
Stelle eine Verbindung zum Internet her (Modem oder Kabel), starte dann das Programm PGPkeys (auf dem Schlüssel-Symbol rechts unten auf deinem Bildschirm mit dem Mauszeiger darauf, rechte Maustaste drücken, PGPkeys wählen, oder PGPtools wählen und den Button ganz links für PGPkeys drücken.

Markiere deinen Schlüssel und wähle im Menü von PGPkeys den Punkt „Server“ ⇨ Send to ⇨ ldap://certserver.pgp.com.

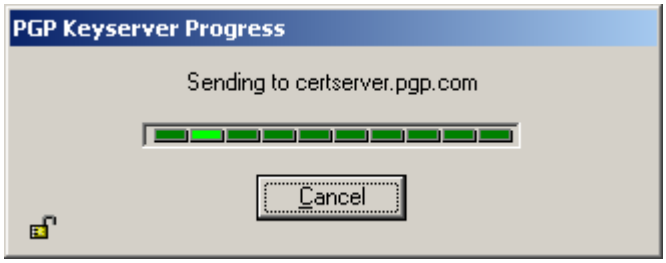


Zurück zum Inhalt dieses Kapitels

Danach wird die Verbindung zum Key-Server hergestellt.

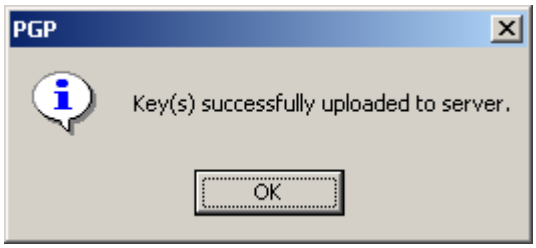


Konnte die Verbindung hergestellt werden, wird dein öffentlicher Schlüssel zum Key-Server geschickt.



Zurück zum Inhalt dieses Kapitels

Wurde der Schlüssel erfolgreich zum Key-Server gesendet, erhältst du folgende Meldung:



Hast den Schlüssel bereits früher auf den Key-Server hinterlegt, erhältst du folgenden Hinweis:

Wenn du den Namen und/oder die E-Mail Adresse zum Schlüssel änderst, kannst du den Schlüssel neuerlich mit dem neuen Namen und einer neuen E-Mail Adresse auf dem Key-Server hinterlegen.

Jetzt kann jede Person auf der Welt, die deinen bei der Schlüsselerstellung angegebenen oder nachher hinzugefügten bzw. geänderten (Phantasie-)Namen kennt, den Schlüssel auf diesem Key-Server finden. Siehe dazu das nächste Kapitel.

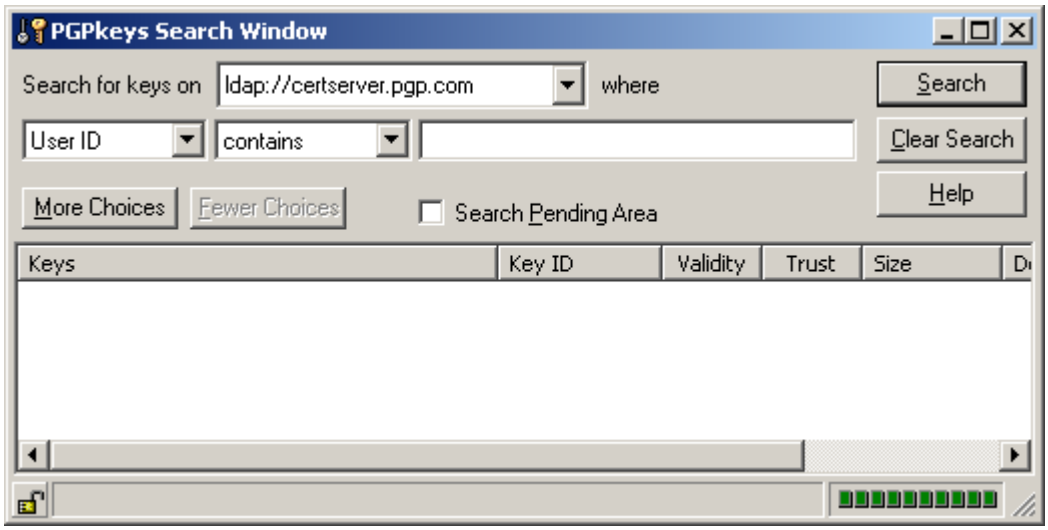
Zurück zum Inhalt dieses Kapitels

5.5 Das Finden eines öffentlichen Schlüssels auf dem Key–Server und die Aufnahme in den Schlüsselbund

Wenn jemand den öffentlichen Schlüssel auf einem Key-Server hinterlegt hat, kannst du ihn dort auch wiederfinden und in deinen Schlüsselbund aufnehmen.

Am einfachsten ist es, wenn du den (Phantasie-)Namen zum Schlüssel kennst. In unserem Beispiel haben wir den Namen Luigi Luccheni angegeben und den Schlüssel zum Key-Server gesendet.

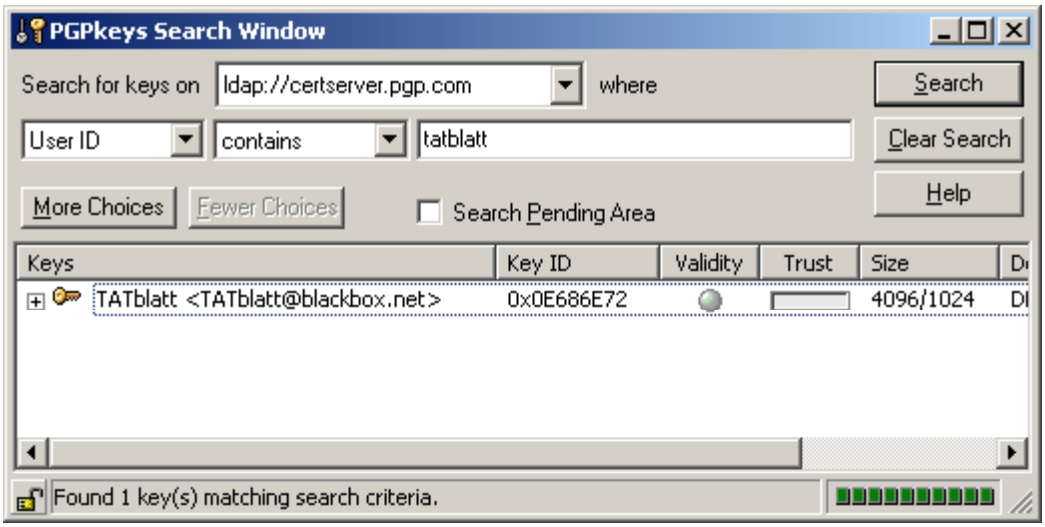
Wenn du das Programm PGPkeys startest, findest du im Menü den Punkt „Server ⇨ Search“. Dann geht folgendes Such-Fenster auf:



Zurück zum Inhalt dieses Kapitels

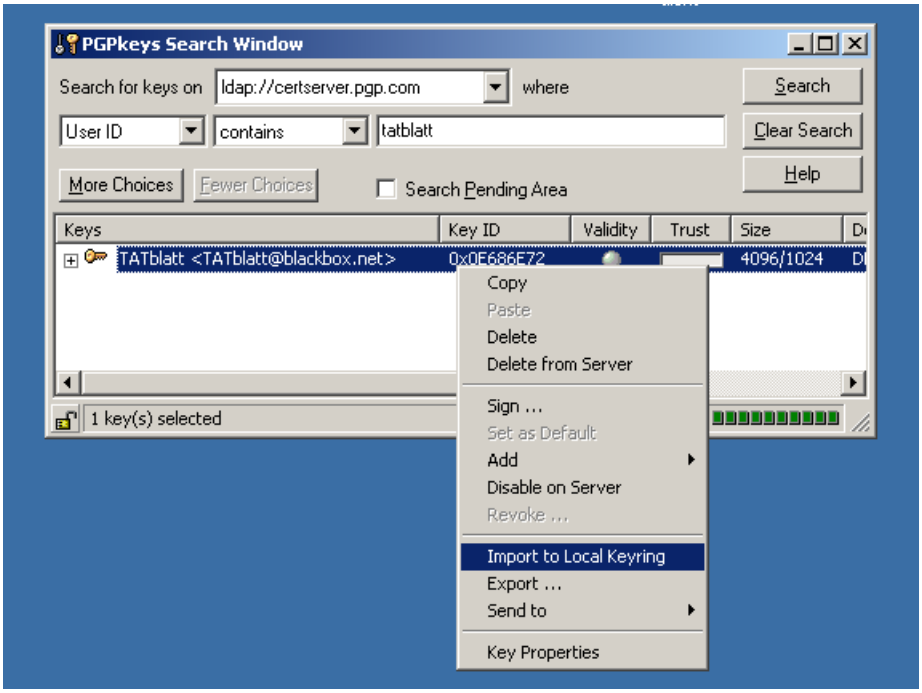
Wenn du nun bei User ID einen Namen eingibst und auf den Button „Search“ drückst, wird der öffentliche Schlüssel mit diesem Namen auf dem Key-Server gesucht und nach dem Auffinden angezeigt. Im Beispiel unten wird der öffentlichen Schlüssel des TATblatt gesucht:

Gib bei User ID contains „tatblatt“ an und drücke den Button „Search“, nach kurzer Zeit wird der öffentliche Schlüssel des TATblatt im Fenster unten unter „Keys“ angezeigt.



Zurück zum Inhalt dieses Kapitels

Um den Schlüssel des TATblatt in deinen Schlüsselbund aufzunehmen, zeige mit dem Mauszeiger darauf und drücke die rechte Maustaste. Im aufgehenden Kontextmenü findest du den Punkt „Import to Local Keyring“. Wähle diesen Menüpunkt und schließe dann das Fenster (drücke das „x“ rechts oben).



Du findest dann den TATblatt-Schlüssel in deinem Schlüsselbund und kannst jetzt verschlüsselte Nachrichten ans TATblatt schicken. Aber bitte nicht zum Spaß ausprobieren, schick dir zum Testen lieber einfach selbst eine verschlüsselte Nachricht oder wechsle Nachrichten mit einer FreundIn aus.

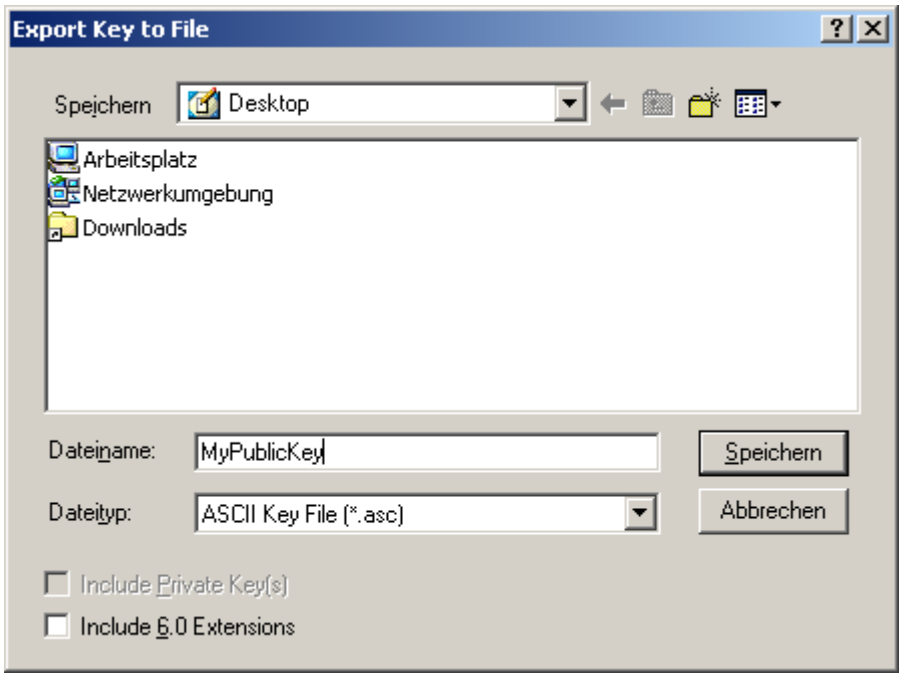
Zurück zum Inhalt dieses Kapitels

5.6 Das Exportieren des öffentlichen Schlüssels für jemanden anderen

Du musst deinen Schlüssel aber auch nicht unbedingt auf einem Key-Server hinterlegen, du kannst deinen öffentlichen Schlüssel jemandem auch per Diskette oder Mail zukommen lassen.

Dazu kannst du eine Datei, die deinen Schlüssel beinhaltet, anlegen. Starte das Programm PGPkeys und wähle im Menü „Keys ⇨ Export“.

Im erscheinenden Fenster kannst du ein Verzeichnis und einen Dateinamen wählen, unter dem dein Schlüssel gespeichert wird.



Drücke nach der Wahl des Verzeichnisses und des Dateinamens auf den Button „Speichern“.

Es wird dann eine Datei mit dem angegebenen Dateinamen angelegt, die deinen Schlüssel enthält. Diese Datei kannst du anderen Personen per Diskette oder per Mail geben bzw. schicken.

Zurück zum Inhalt dieses Kapitels

Nur zur Info, dein Schlüssel sieht in Textform (auch in der Datei) dann ungefähr so aus (auch verschlüsselte Texte haben ein ähnliches Erscheinungsbild):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 6.5.8ckt xxxx://irfaiad.virtualave.net/

mQGiBDnCfEURBAD2yZ10DCEEgtnl+PQz7hnIZIrWPaFgqS1hLZ/5E1Vbq+RQkNEv
2p/3ZPrCACG7A+ADDGkclk/nfcrhR2wh+8+IvYjwJj7M86SIGJkfQrX5Eti4cgVj
TVTn8GjNAVAV3AfsB0Vk2qK54nFh5+7KlIF5IjrGCrRCEvSl/zD858/kswCg/zkL
FiDQmmi8PtYEbkVMN6ee3FMD/RQyALeLuZ4gui3mHozraPrd2Sf+T1l6sUyMzDlP
2OZBssn0Nh47fIvAP675x7VlF2XA81EaX8uigRmWCYR0rpRxRQZKpRg9E9kavYq1
z0FP53dIZoVM3vmG3xM4z9aBAszeWErs2yj0gToo2lfyoq/Gn+nWWemal8EP0uW1
Axm9A/0anOdttZ47b/VW/Fa0bcKjmIGXnirIovFdVlBccR6Bs1tIUpWfAlhWhvSP
rRK/23SmB+YekRoNT2otx78QAJwbF951SJX49AWN12dh4ZGHbeF5XEDF/1n96jrt
Sx5+MgnI3ld4fOwaDQw0sd+HXo5m8W+VBR93l92PKrafKo/31bQgVEFUYmxhdHQg
PFRBVGJsYXR0QGJsYWNrYm94Lm5ldD6JAJwEEAEBAAYFAjnCfcMACgkQqQb5ywwt
nzUUxQQArSvw9IYgOpG0tmQ8MEFty3U793Hpl59fhGzMSurp/d7cdE/5zASSW9cG
DFgx9suadwmcyN7SCNGwDBqcoWtN2SO3zmGFWg2vQ2Zf7ao/q1axn1Tcp3TkvXhA
ofX2bUUp9Zobrldq1QQ3T0qWBOJvELMEEsGCf50dWubfa1g4sdWJAE4EEBECAA4F
AjnCfEUECwMCAQIZAQAKCRAgXTeTDmhucsy0AKDuMLHjC8ez4H48SpTLjcvwSsze
0wCg3T7toPKC4r2TjvEuLpp+NjKwGiiJAEYEEBECAAYFAjp/o8gACgkQTjb2vjSP
z30gkQCfftHz9xm3WZbYm2YETBISppQerRQAoLPm5s58Wtqg2i8FGinphZ//HCN+
uQQNBDnCfEcQEAD5GKB+WgZhekOQldwFbIeG7GHszUUfDtjgo3nGydx6C6zkP+NG
lLYwSlPXfAIWSIC1FeUpmamfB3TT/+OhxZYgTphluNgN7hBdq7YXHFHYUMoiV0Mp
vpXoVis4eFwL2/hMTdXjqkbM+84X6CqdFGHjhKlP0YOEqHm274+nQ0YIxswdd1ck
Ve0Xs8K2OizX
=Np63
-----END PGP PUBLIC KEY BLOCK-----
```

Nett, oder? Wie mensch so einen Schlüssel in den Schlüsselbund aufnimmt, erfährst du im folgenden Kapitel.

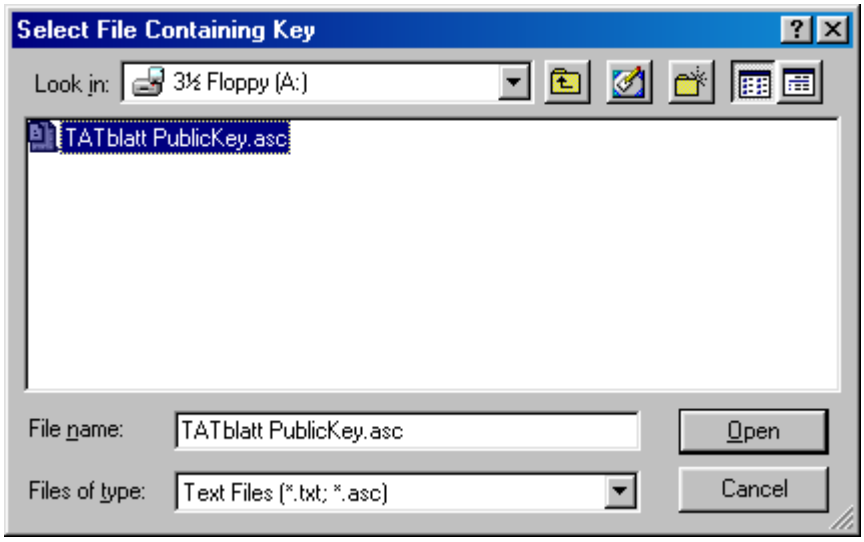
Zurück zum Inhalt dieses Kapitels

5.7 Das Importieren eines öffentlichen Schlüssels von jemandem anderen

Erhältst du einen Schlüssel nicht über den Key-Server, sondern per Herunterladen aus dem Internet, Diskette oder Mail, musst du den Schlüssel mittels Importieren in deinen Schlüsselbund aufnehmen.

Starte das Programm PGPkeys und wähle im Menü „Keys ⇨ Import“.

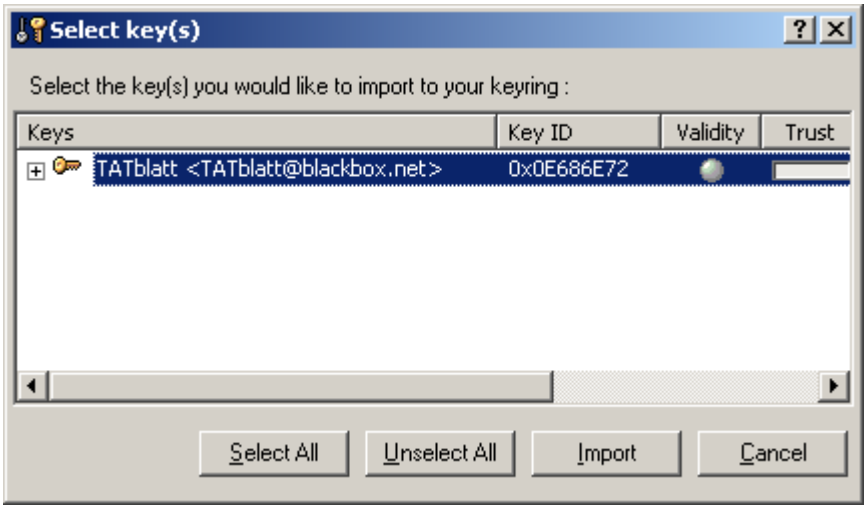
Im erscheinenden Fenster kannst du ein Verzeichnis und einen Dateinamen wählen, unter dem der aufzunehmende Schlüssel gespeichert ist (die Dateien mit einem PGP-Schlüssel haben standardmässig die Endung asc, das muss aber nicht so sein, sie können z.B. genauso die Endung txt o.a. haben).



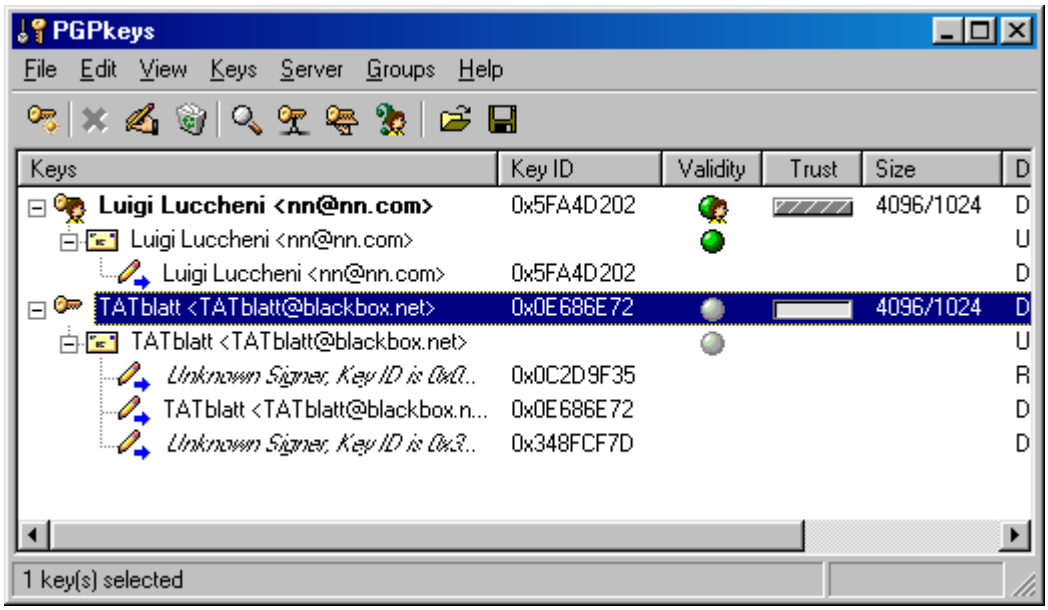
Markiere die Datei mit dem Schlüssel und drücke den Button „Open“.

Zurück zum Inhalt dieses Kapitels

Du siehst dann ein Fenster mit dem Schlüssel in der Liste:



Markiere den Eintrag und drücke den Button „Import“, der Schlüssel befindet sich dann auf deinem Schlüsselbund und du kannst der BesitzerIn des Schlüssels verschlüsselte Nachrichten senden.



Zurück zum Inhalt dieses Kapitels

5.8 Das Sichern des Schlüsselpaares

Ohne deinen privaten Schlüssel kannst du an dich geschickte verschlüsselte Texte nicht lesen. Verlierst du deinen Schlüssel, wirst du bestehende verschlüsselte Texte nie wieder lesen können, „Aufsperrdienst“ wie bei verlorenen Wohnungsschlüsseln gibt’s hier keinen. Es ist daher ungemein wichtig, den Schlüssel zu sichern.

Dieses Sichern kann auf einer Diskette erfolgen (am besten auf mehreren, da Disketten die Angewohnheit haben, ziemlich schnell defekt zu werden), oder besser auf einer CD oder einer etwaigen 2. Festplatte.

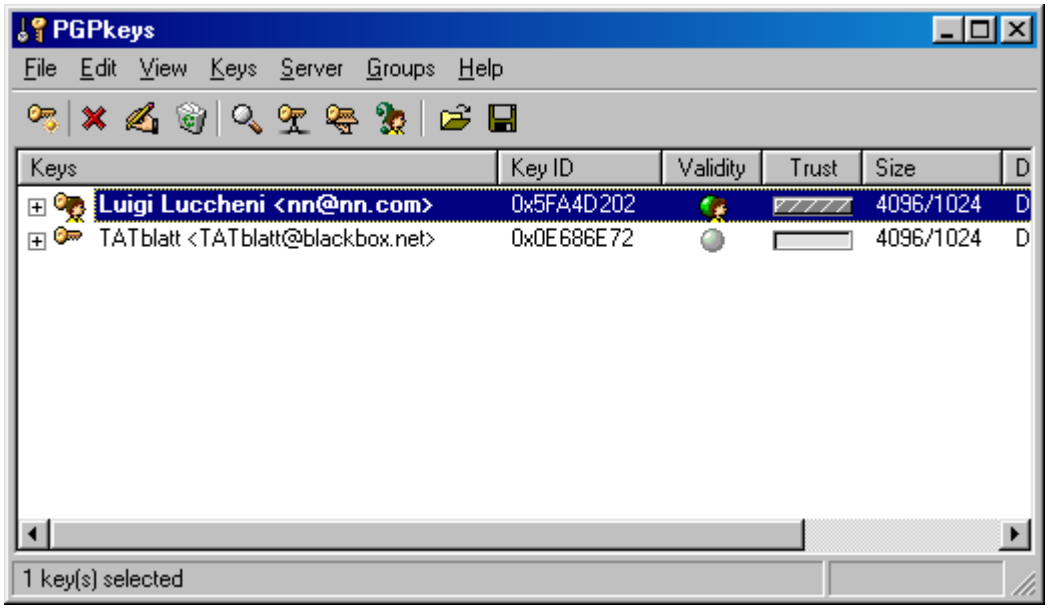
Wenn dir eine Kopie deines privaten Schlüssels abhanden kommt, ist das nicht ganz so schlimm – sofern du noch das Original oder eine andere Kopie davon hast. Er ist ja noch immer durch deine „Passphrase“ geschützt, und diese Passphrase ist ja sicherlich so ausgeklügelt, dass sie niemand knacken kann...

Eine ganz besonders gute Idee ist natürlich, den Schlüssel auf einer PGP Disk verschlüsselt zu sichern.

Zurück zum Inhalt dieses Kapitels

So wie du deinen öffentlichen Schlüssel für andere exportieren kannst, kannst du auch dein ganzes Schlüsselpaar inklusive deinem privaten Schlüssel exportieren (in einer Datei speichern).

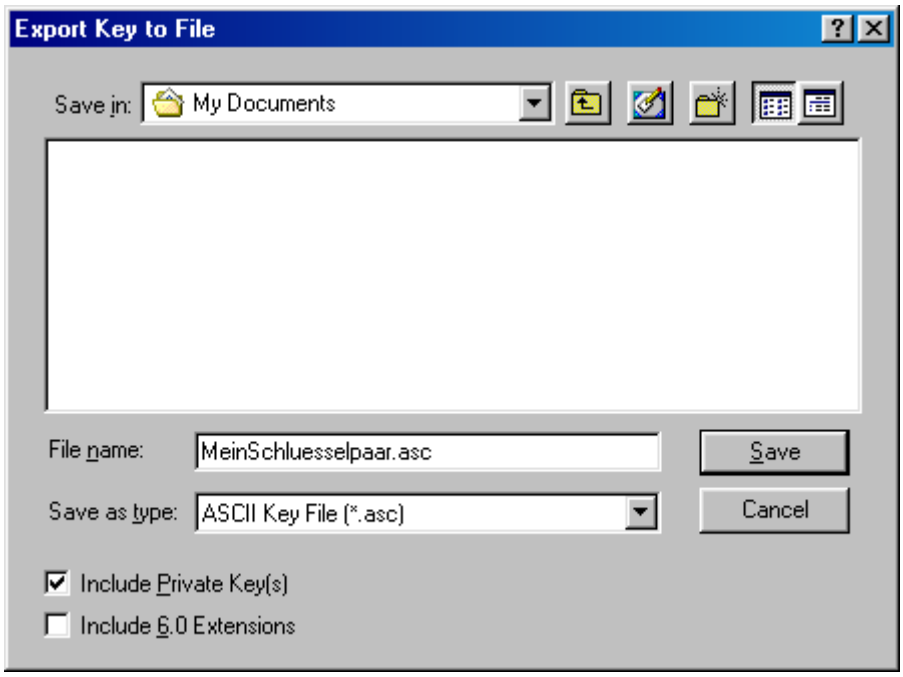
Starte das Programm PGPkeys, markiere deinen eigenen Schlüssel und wähle im Menü „Keys ⇨ Export“.



Zurück zum Inhalt dieses Kapitels

Im daraufhin erscheinenden Fenster kannst du ein Verzeichnis und einen Dateinamen wählen, unter dem dein Schlüssel gespeichert wird.

Markiere links unten den Punkt „Include Private Key(s)“, d.h. dass nicht nur dein öffentlicher Schlüssel, sondern auch dein privater Schlüssel in einer Datei gespeichert wird. Drücke nach der Wahl des Verzeichnisses und des Dateinamens auf den Button „Speichern“.



Es wird dann eine Datei mit dem angegebenen Dateinamen angelegt, die dein ganzes Schlüsselpaar enthält. Diese Datei solltest du dann irgendwo sicher speichern, also wie gesagt z.B. auf eine CD, auf eine 2. Festplatte, auf mehrere Disketten oder auf ein ZIP-Laufwerk kopieren.

Falls dein Originalschlüssel auf deiner Festplatte verloren geht, kannst du den gesicherten Schlüssel z.B. von der Diskette wieder importieren und so alle für dich verschlüsselten Texte weiterhin lesen.

Zurück zum Inhalt dieses Kapitels

5.9 Problembehebung: nach PGP Installation keine Verbindung zum Internet

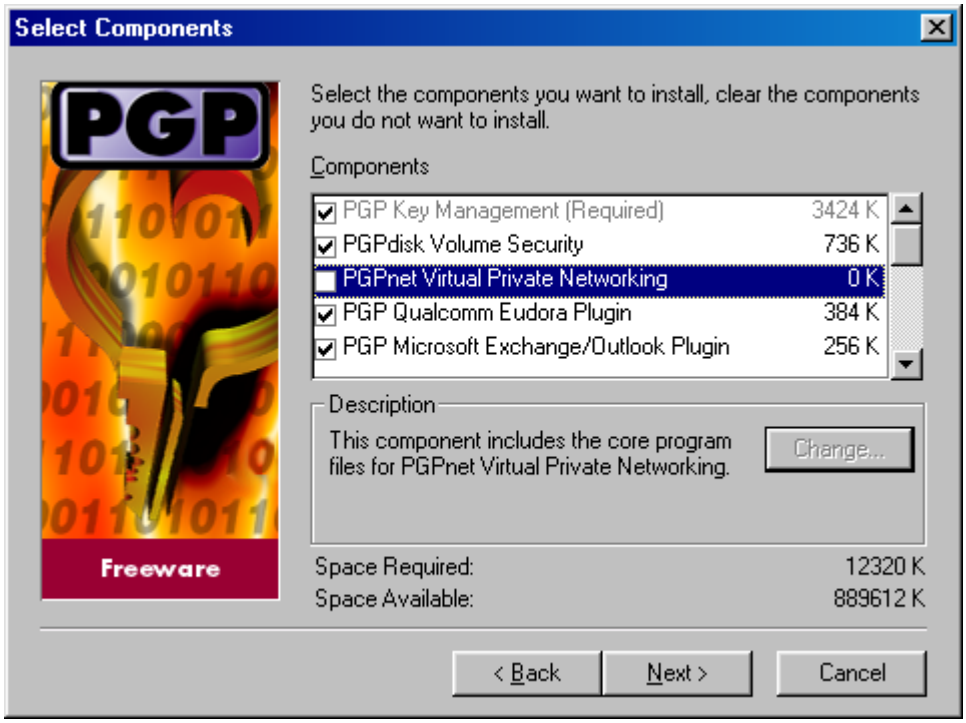
Problem

Du hast PGP installiert, vorher hattest du eine funktionierende Verbindung zum Internet, nach der PGP Installation nicht mehr.

Grund

Höchstwahrscheinlich hast du bei der PGP Installation vergessen, PGPnet Virtual Private Networking zu entmarkieren, d.h. du hast es irrtümlich dazuinstalliert.

Zur Erinnerung: bei der Auswahl der Komponenten wurde empfohlen, diesen Punkt zu entmarkieren.



Zurück zum Inhalt dieses Kapitels

Prüfung und Behebung

Starte in der Systemsteuerung die Netzwerkeinstellungen:

- Start ⇨ Einstellungen ⇨ Systemsteuerung ⇨ Netzwerk oder
- Start ⇨ Settings ⇨ Control Panel ⇨ Network

oder so ähnlich.

Du siehst eine Liste von diversen Einträgen. Lösche alle Einträge, die PGP beinhalten. Starte dann den Computer neu, anschliessend sollte wieder alles ganz normal funktionieren.

Zurück zum Inhalt dieses Kapitels

6 Die Verwendung von PGP mit Mailprogrammen

Überblick

In diesem Kapitel erfährst du, wie du mit diversen Mailprogrammen verschlüsselte Nachrichten versenden kannst.

Du findest Beschreibungen zu folgenden Mail-Programmen:

- Eudora
- Microsoft Outlook
- Andere Mailprogramme und Web-Mail

6.1 Eudora

In diesem Kapitel erfährst du, wie du mit dem Mailprogramm Eudora Mails ver- und entschlüsselst.

Dieses Mail-Programm kannst du auch von der CD aus installieren. Auf der CD befindet sich die derzeit aktuelle Version 5.1. Das Programm Eudora selbst wird aber hier nicht erklärt, sondern nur die Integration von PGP.

Installation von Eudora

Hast du Eudora noch nicht installiert, willst es aber in Zukunft verwenden, kannst du es mit dem Installationsprogramm auf der CD vor der Installation von PGP installieren.


Eudora\Windows\5.1


Eudora51.exe


Eudora\MacOS\5.1


Eudora5.1_installer.hqx

Zurück zum Inhalt dieses Kapitels

Installation Eudora ⇔ PGP

Ein Problem bei der Installation von PGP in Zusammenhang mit Eudora ist, dass

- Eudora vor der PGP-Installation installiert sein muss, um die PGP-Integration durchführen zu können
- PGP vor Eudora installiert sein muss, um alle Eudora-Daten auf ein verschlüsseltes Laufwerk speichern zu können

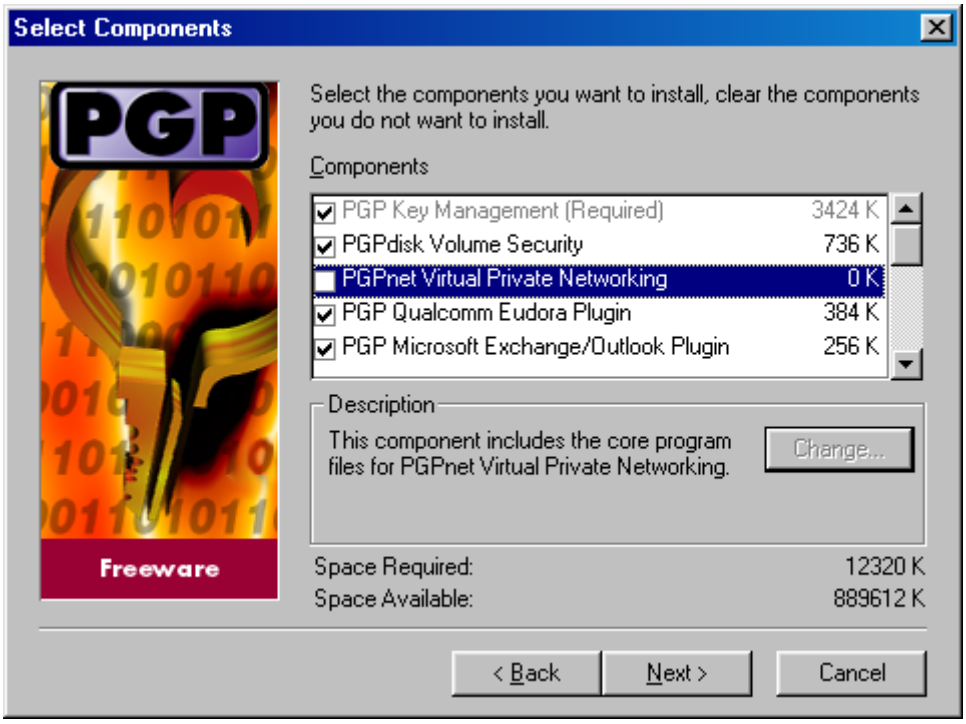
Beides gleichzeitig geht aber halt leider nicht. In der unten angegebenen Reihenfolge funktioniert's jedenfalls, auch wenn's ein wenig mühsam ist:

- PGP installieren und ein verschlüsseltes Laufwerk erzeugen
- Eudora installieren, als Ordner für die Eudora-Daten einen Ordner auf einem verschlüsselten Laufwerk angeben
- PGP deinstallieren und nochmals installieren, um es in Eudora zu integrieren

Zurück zum Inhalt dieses Kapitels

Vorbereitung

Mit Eudora ist die Ver- und Entschlüsselung besonders komfortabel. Grund dafür ist, dass PGP in Eudora voll integriert ist, wenn du die Option bei der Installation von PGP gewählt hast. Zur Erinnerung die diesbezügliche Liste bei der Installation von PGP, du siehst auch die Integration in Eudora dabei (PGP Qualcomm Eudora Plugin):

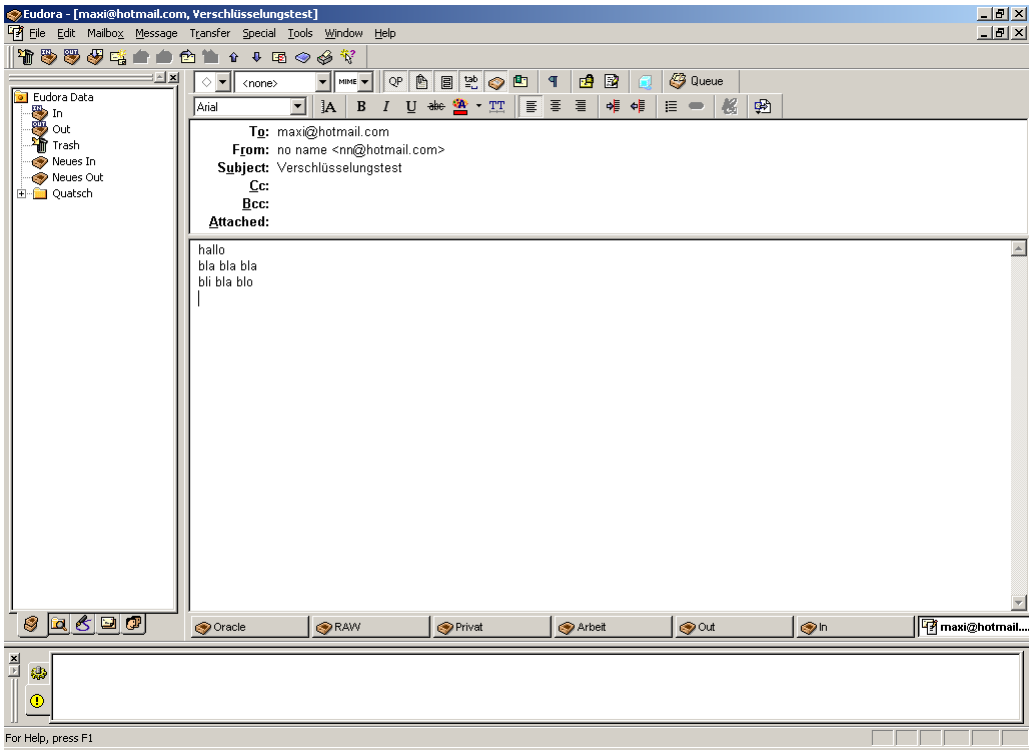


Hattest du Eudora zum Zeitpunkt der PGP-Installation noch nicht auf deinem Computer, kannst du jederzeit das Zusatzprogramm für Eudora nachträglich dazuinstallieren.

Zurück zum Inhalt dieses Kapitels

Das Verschlüsseln

Wenn du nun eine Mail in Eudora geschrieben hast, sieht das ungefähr so aus:



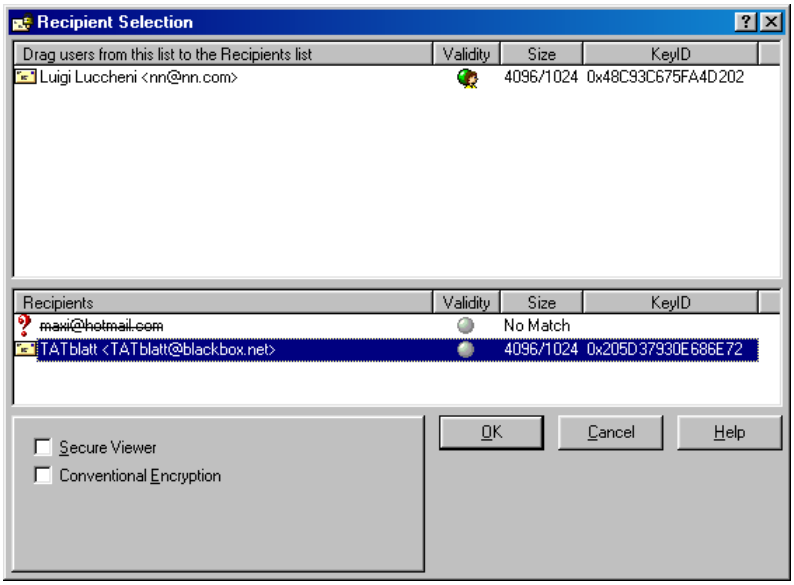
Zurück zum Inhalt dieses Kapitels

Drücke nun irgendwo im Fenstern mit der Nachricht auf die rechte Maustaste und wähle aus dem Kontextmenü „Message Plug-ins ⇨ PGP Encrypt & Sign“, du kannst auch einfach im normalen Menü „Edit ⇨ Message Plug-ins ⇨ PGP Encrypt & Sign“ wählen.

Ein Fenster mit allen deinen Schlüsseln erscheint. Wenn sich die von dir in der Mail angegebene Adresse exakt mit der Adresse eines der Schlüssel deckt, siehst du ihn gleich im unteren Teil des Fensters bei Recipients (EmpfängerInnen). Findet das Programm die Mailadresse nicht, ist sie bei Recipients durchgestrichen.

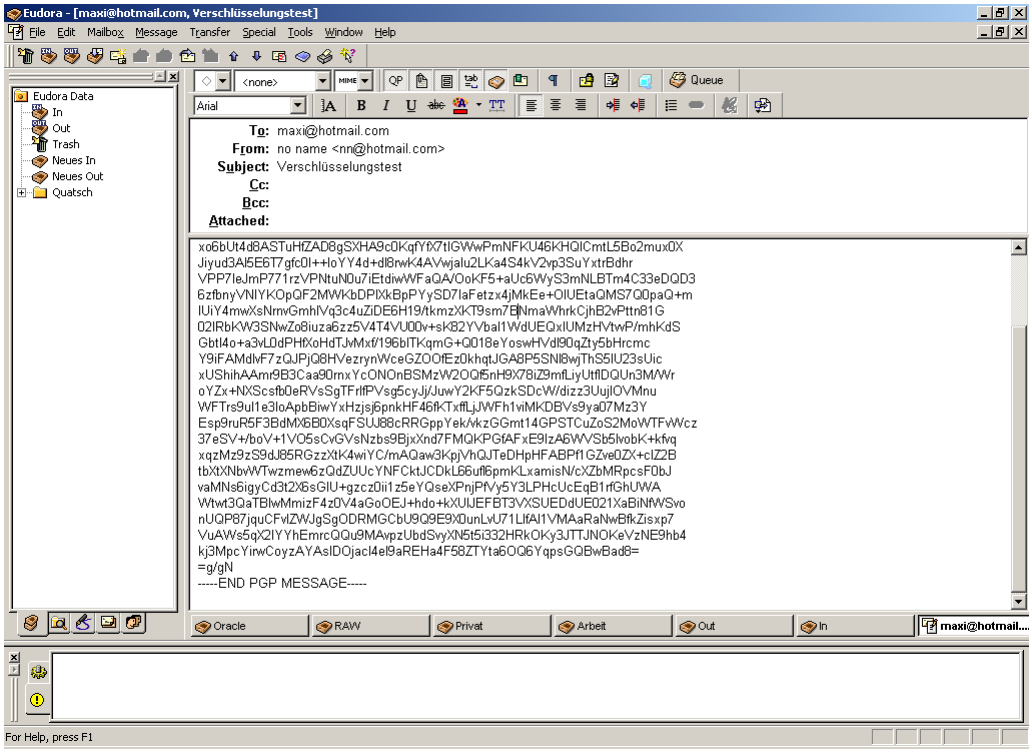
Ist die EmpfängerInnen-Adresse noch nicht bei den Recipients angeführt, doppelklicke im oberen Teil auf die richtige EmpfängerIn, sie wandert dann zu den Recipients nach unten.

Markiere die richtige Adresse im unteren Teil und drücken den Button „OK“.



Zurück zum Inhalt dieses Kapitels

Wenn du nun (bei Wahl von „Encrypt & Sign“ nach der Eingabe des Passworts) zu Eudora zurückkehrst, sieht dein ursprünglicher Nachrichtentext etwas verändert aus.

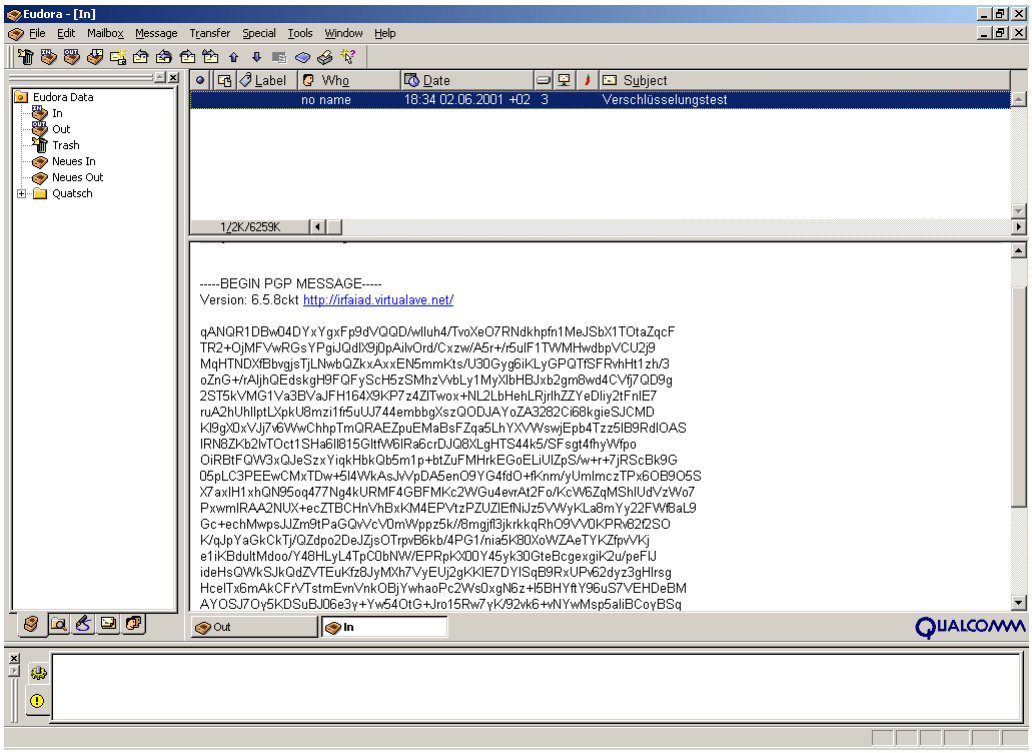


Du kannst nun die verschlüsselte Nachricht versenden.

Zurück zum Inhalt dieses Kapitels

Das Entschlüsseln

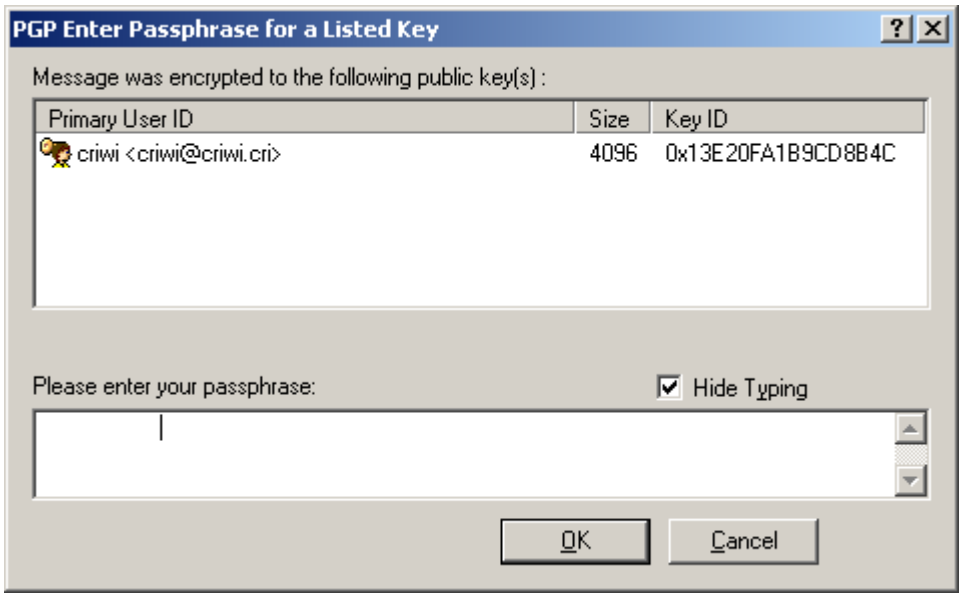
Wenn du eine verschlüsselte Nachricht erhältst, sieht das in Eudora ungefähr so aus:



Zurück zum Inhalt dieses Kapitels

Öffne die Mail durch Doppelklick auf den Inhaltstext im oberen Teil. Drücke mit dem Mauszeiger irgendwo im Nachrichtenfenster die rechte Maustaste und wähle aus dem Kontextmenü „Message Plug-ins ⇨ PGP Decrypt & Verify“. Das Fenster mit deinem eigenen Schlüssel geht auf, gib deine Passphrase an, die du bei der Schlüsselerstellung gewählt hast und drücken den Button „OK“.

Wurde die Nachricht (z.B. irrtümlich) für eine andere Person verschlüsselt, erscheint eine entsprechende Fehlermeldung.



Zurück zum Inhalt dieses Kapitels

Wenn du nun zu Eudora zurückkehrst, siehst du den entschlüsselten Text.

Beim Schließen des Fensters wirst du gefragt, ob du den geänderten (hier entschlüsselten) Text speichern willst oder den Originalzustand (hier verschlüsselt) lassen willst.

Du kannst den Text ruhigen Gewissens in entschlüsselter Form speichern, wenn du deine Eudora-Daten auf einem verschlüsselten Festplattenbereich speicherst (siehe die Kapitel PGP Disk und Das Speichern von Eudora-Daten auf einem verschlüsselten Laufwerk).

Tust du das nicht, belasse die Nachricht lieber in verschlüsselter Form, du kannst sie ja bei Bedarf jederzeit wieder entschlüsseln.

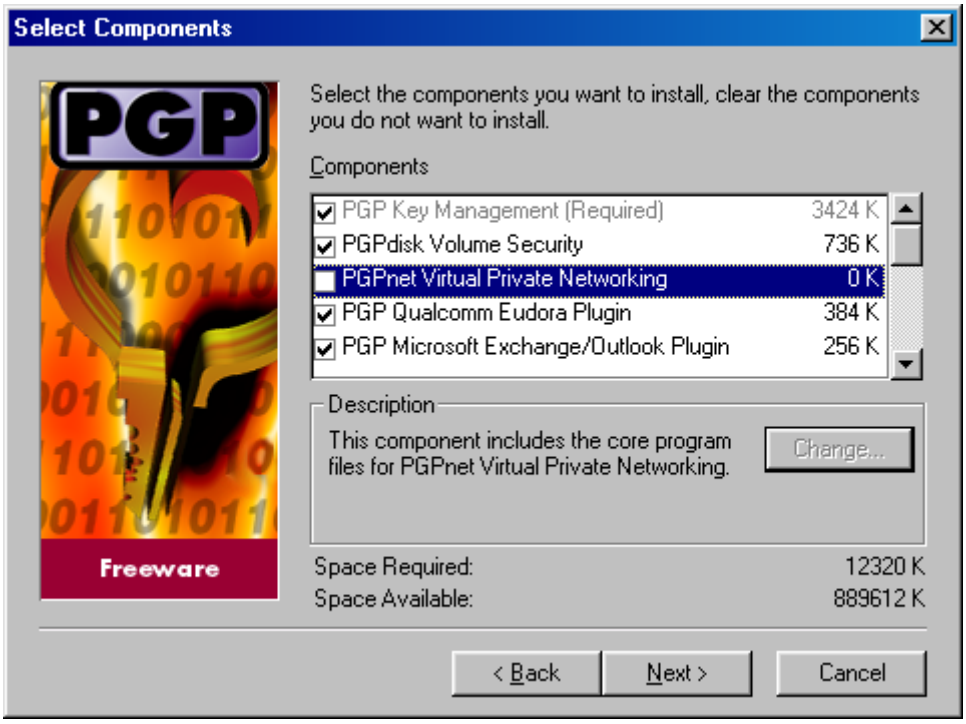
Grund ist, dass neugierige Menschen natürlich sehr interessiert an deinen Mails sind. Beim Übersenden war diese Mail zwar nicht lesbar, kommt dir dein Computer jedoch irgendwie abhanden, können natürlich auch neugierige Menschen deinen Computer starten und seelenruhig alle deine unverschlüsselten Mails lesen, wenn sie nicht auf einem verschlüsselten Teil der Festplatte untergebracht wurden.

Zurück zum Inhalt dieses Kapitels

6.2 Microsoft Outlook

Hier erfährst du, wie du bei Verwendung von Microsoft Outlook Mails ver- und entschlüsseln kannst.

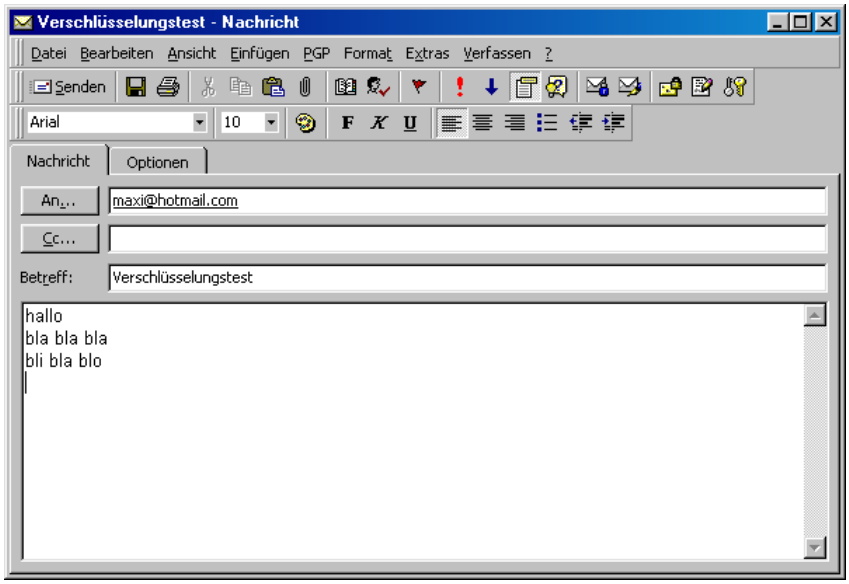
Auch in Outlook ist PGP integriert, wenn du die Option bei der Installation von PGP gewählt hast. Zur Erinnerung die diesbezügliche Liste bei der Installation von PGP, du siehst auch die Integration in Outlook dabei (PGP Microsoft Exchange/Outlook Plugin):



Zurück zum Inhalt dieses Kapitels

Das Verschlüsseln

Wenn du nun eine Mail in Outlook geschrieben hast, sieht das ungefähr so aus:



Zurück zum Inhalt dieses Kapitels

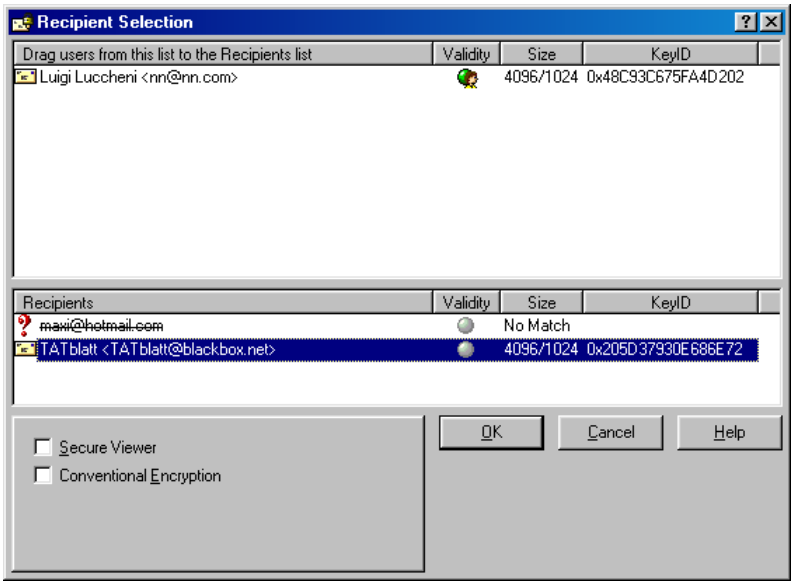
Mit etwas Glück findest du in der Menüleiste den Menüpunkt „PGP“. Nach manchen Installationen ist der Menüpunkt in Outlook nicht sichtbar. Ist dies der Fall, lese im nachfolgenden Kapitel Andere Mailprogramme und Web-Mail, wie du trotzdem mit PGP arbeiten kannst.

Ist der Menüpunkt „PGP“ sichtbar, markiere den geschriebenen Text und wähle dann den Punkt „PGP ⇨ Encrypt and sign now“.

Ein Fenster mit allen deinen Schlüsseln erscheint. Wenn sich die von dir in der Mail angegebene Adresse exakt mit der Adresse eines der Schlüssel deckt, siehst du ihn gleich im unteren Teil des Fensters bei Recipients (EmpfängerInnen). Findet das Programm die Mailadresse nicht, ist sie bei Recipients durchgestrichen.

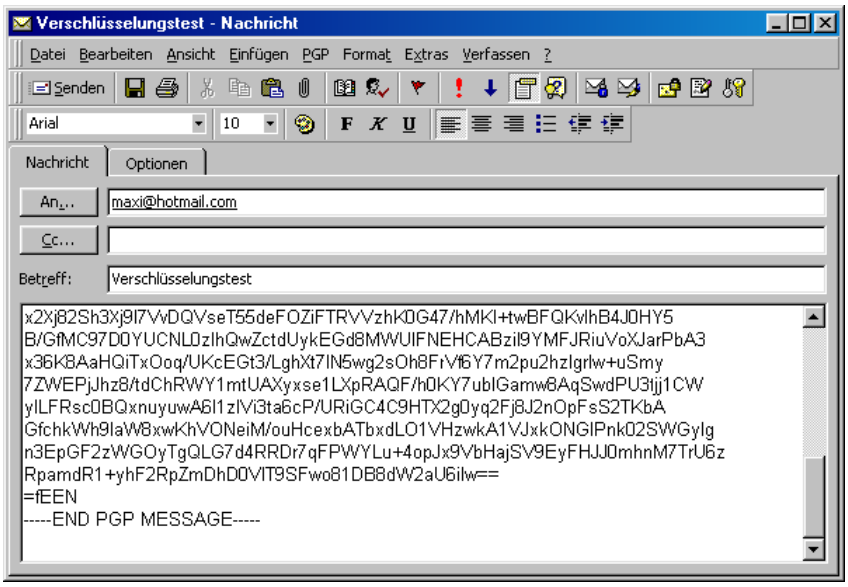
Ist die EmpfängerInnen-Adresse noch nicht bei den Recipients angeführt, doppelklicke im oberen Teil auf die richtige EmpfängerIn, sie wandert dann zu den Recipients nach unten.

Markiere die richtige Adresse im unteren Teil und drücken den Button „OK“.



Zurück zum Inhalt dieses Kapitels

Wenn du nun (bei Wahl von „Encrypt & Sign“ nach der Eingabe des Passworts) zu Outlook zurückkehrst, sieht dein Nachrichtentext etwas verändert aus.

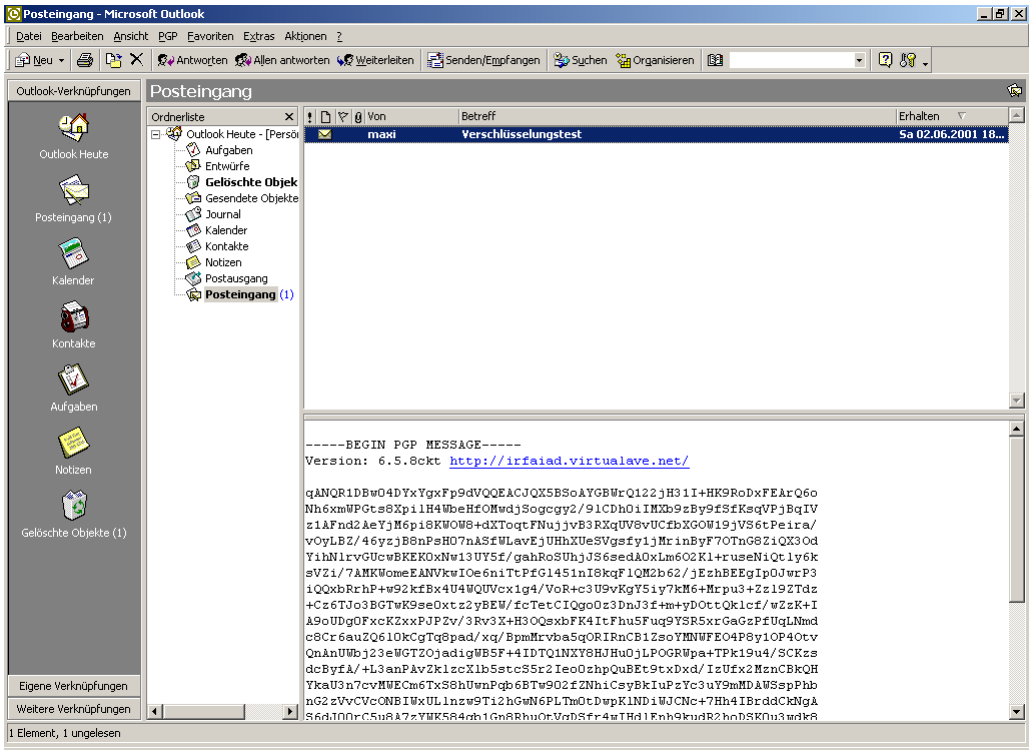


Du kannst nun die verschlüsselte Nachricht versenden.

Zurück zum Inhalt dieses Kapitels

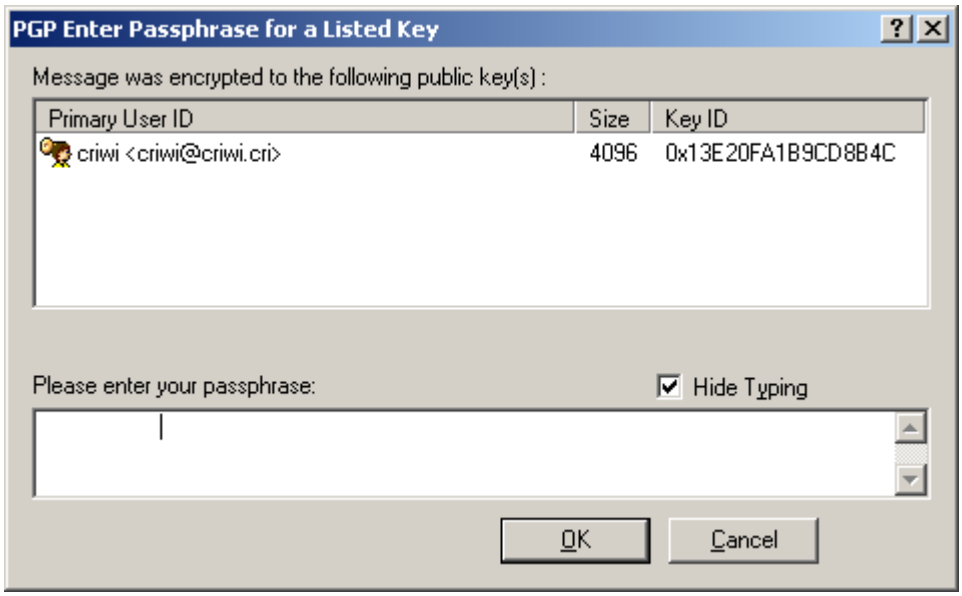
Das Entschlüsseln

Wenn du eine verschlüsselte Nachricht erhältst, sieht das in Outlook ungefähr so aus:



Zurück zum Inhalt dieses Kapitels

Doppelklicke auf die Zeile im oberen Fenster, die Mail wird dann in einem eigenen Fenster geöffnet. Wähle im Menü „PGP ⇨ Decrypt/Verify“, das Fenster mit deinem eigenen Schlüssel geht auf, gib deine Passphrase an, die du bei der Schlüsselerstellung gewählt hast und drücken den Button „OK“.



Zurück zum Inhalt dieses Kapitels

Wenn du nun zu Outlook zurückkehrst, siehst du den entschlüsselten Text.

Beim Schließen des Fensters wirst du gefragt, ob du den Text in entschlüsselter Form speichern willst. Du kannst den Text ruhigen Gewissens in entschlüsselter Form speichern, wenn du deine Outlook-Daten auf einem verschlüsselten Festplattenbereich speicherst (siehe die Kapitel PGP Disk und Das Speichern von Outlook-Daten auf einem verschlüsselten Laufwerk).

Tust du das nicht, belasse die Nachricht lieber in verschlüsselter Form, du kannst sie ja bei Bedarf jederzeit wieder entschlüsseln.

Grund ist, dass neugierige Menschen natürlich sehr interessiert an deinen Mails sind. Beim Übersenden war diese Mail zwar nicht lesbar, kommt dir dein Computer jedoch irgendwie abhanden, können natürlich auch neugierige Menschen deinen Computer starten und seelenruhig alle deine unverschlüsselten Mails lesen, wenn sie nicht auf einem verschlüsselten Teil der Festplatte untergebracht wurden.

Zurück zum Inhalt dieses Kapitels

6.3 Andere Mailprogramme und Web-Mail

Wenn du weder Eudora noch Outlook als Mailprogramm verwendest und z.B. über eine Internetseite zu deinen Mails kommst (z.B. bei Hotmail), ist PGP nicht ins Mailprogramm integriert.

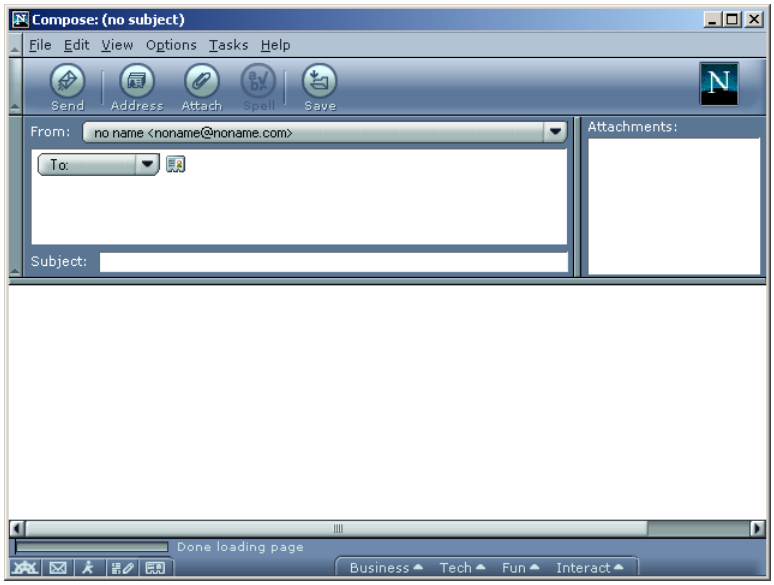
Du kannst aber trotzdem deine Nachrichten ver- und entschlüsseln, wenn PGP auf dem Computer installiert ist. Du musst einfach den Text in die Zwischenablage kopieren, ver- bzw. entschlüsseln und wieder in die Mail zurückkopieren.

Das Beispiel zeigt anhand von Netscape, wie mensch das macht, so geht das aber mit allen Texten, die du schreibst, nicht nur mit Netscape Mail.

Zurück zum Inhalt dieses Kapitels

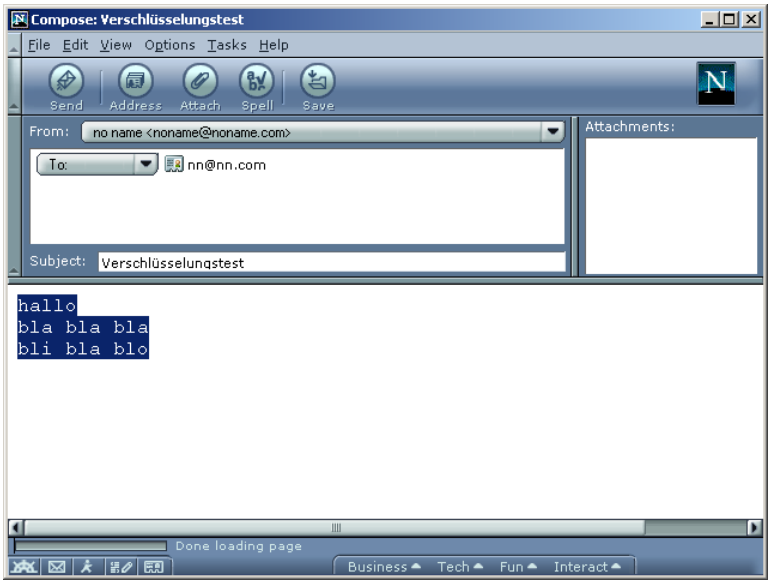
Das Verschlüsseln

Wähle das Mailprogramm, in Netscape 4.7 und 6.0 gibt es den Menüpunkt „File ⇨ New ⇨ Message“. Wenn Netscape Mail gestartet wird, sieht das bei der Version 6.0 so aus:



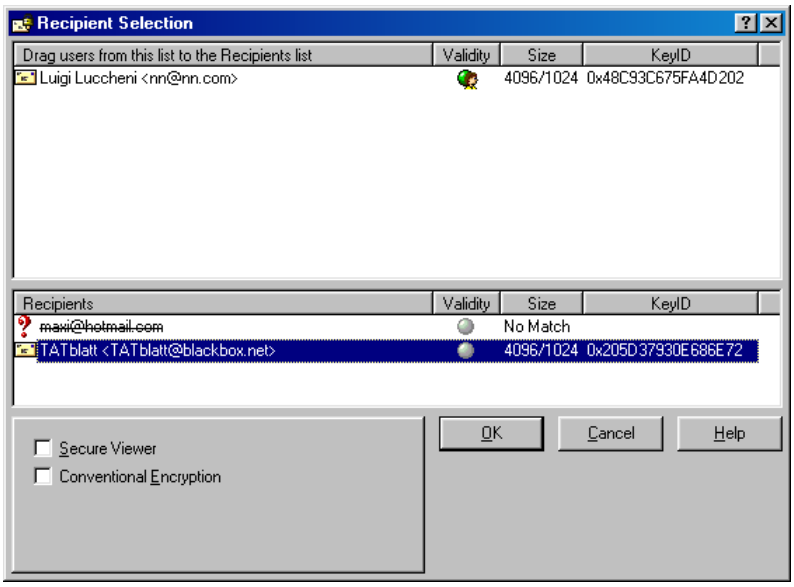
Zurück zum Inhalt dieses Kapitels

Schreibe einen Empfänger, ein Subject und einen Text in die einzelnen Felder. Markiere dann deinen eigentlichen Nachrichtentext und wähle im Menü „Edit ⇨ Copy“ bzw. bei deutschsprachigen Versionen „Bearbeiten ⇨ Kopieren“.



Zurück zum Inhalt dieses Kapitels

Zeige mit dem Mauszeiger auf das Schloss-Symbol von PGP am rechten unteren Rand deines Bildschirms und drücke die rechte Maustaste. Wähle aus dem Menü „Clipboard ⇨ Encrypt & Sign“. Ein Fenster wie das unten mit den Schlüsseln deines Schlüsselbundes geht auf:



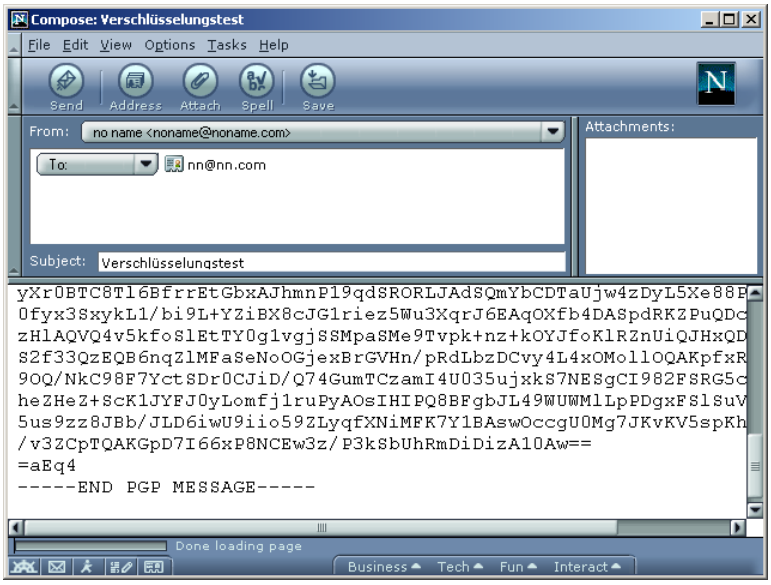
Zurück zum Inhalt dieses Kapitels

Doppelklicke auf den Schlüssel der EmpfängerIn, er wandert dann vom oberen zum unteren Teil des Fensters. Drücke dann den Button „OK“.

Nun ist der Text in der Zwischenablage (im Clipboard) verschlüsselt worden, wenn du den Text nun irgendwo einfügst, erhältst du nicht mehr den Originaltext, sondern den unlesbaren verschlüsselten Text.

Kehre nun zum Nachrichten-Fenster von Netscape zurück, dein ursprünglicher unverschlüsselte Text sollte noch markiert sein. Ist er das nicht, markiere ihn (so überschreibst du dann gleich den ursprünglichen Text, was ja in diesem Fall erwünscht ist).

Wähle im Menü „Edit ⇨ Paste“ oder in deutschsprachigen Versionen „Bearbeiten ⇨ Einfügen“. Nun wird der verschlüsselte Text aus der Zwischenablage (aus dem Clipboard) eingefügt.



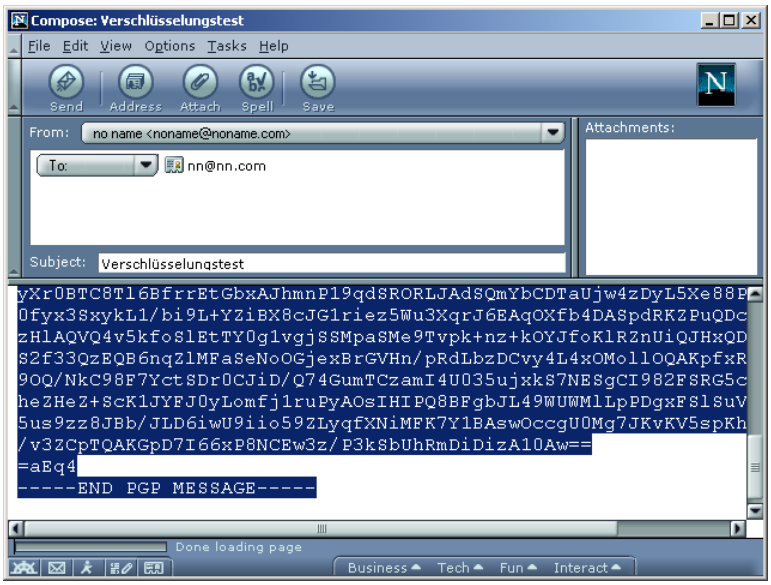
Und schon kannst du den verschlüsselten Text verschicken. Und diese Methode mit dem händischen Kopieren und Einfügen über die Zwischenablage (das Clipboard) funktioniert immer, egal, welches Programm du verwendest.

Zurück zum Inhalt dieses Kapitels

Das Entschlüsseln

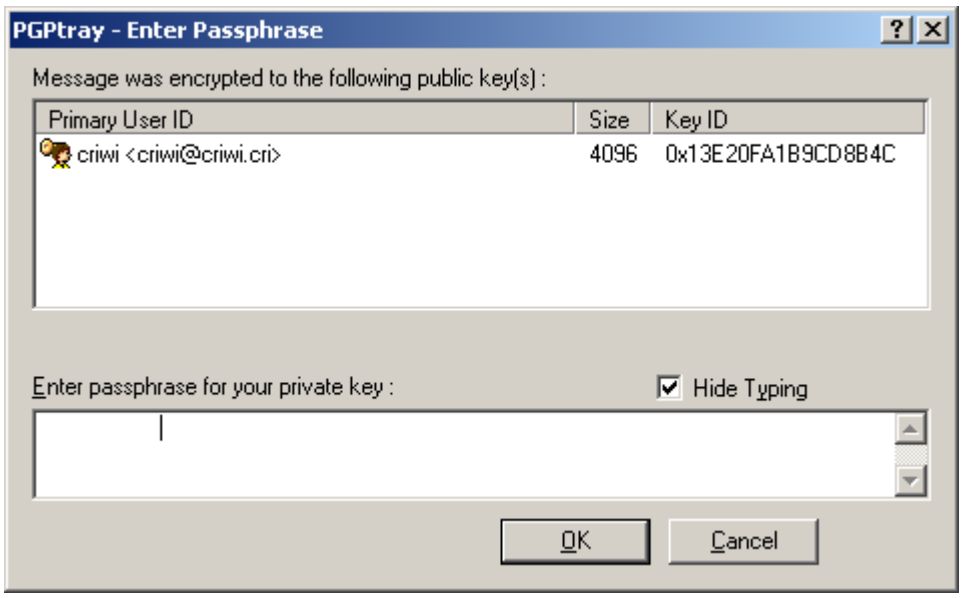
Umgekehrt geht's natürlich genauso, wenn du eine verschlüsselte Mail erhältst, kannst du sie auch über die Zwischenablage (über das Clipboard) entschlüsseln.

Markiere den verschlüsselten Text (von -----BEGIN PGP MESSAGE----- bis -----END PGP MESSAGE-----, alles inklusive). Wähle dann im Menü „Edit ⇨ Copy" bzw. bei deutschsprachigen Versionen „Bearbeiten ⇨ Kopieren".



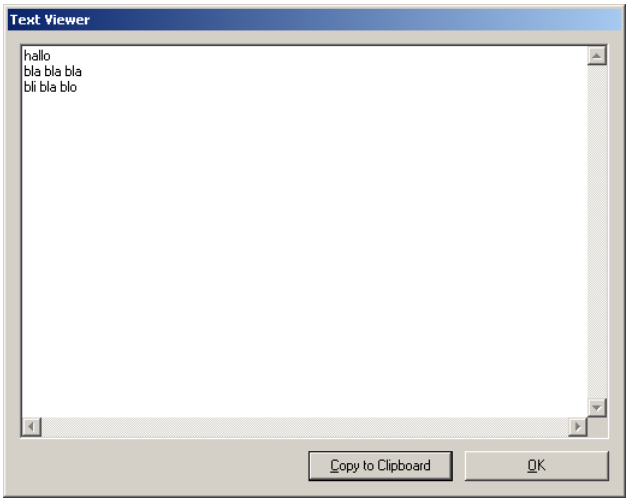
Zurück zum Inhalt dieses Kapitels

Zeige mit dem Mauszeiger auf das Schloss-Symbol von PGP am rechten unteren Rand deines Bildschirms und drücke die rechte Maustaste. Wähle aus dem Menü „Clipboard ⇨ Decrypt & Verify“. Ein Fenster mit deinem eigenen Schlüssel geht auf, im unteren Teil des Fensters musst du deine Passphrase, die du bei der Schlüsselerstellung gewählt hast, eingeben. Drücke anschließend den Button „OK“.



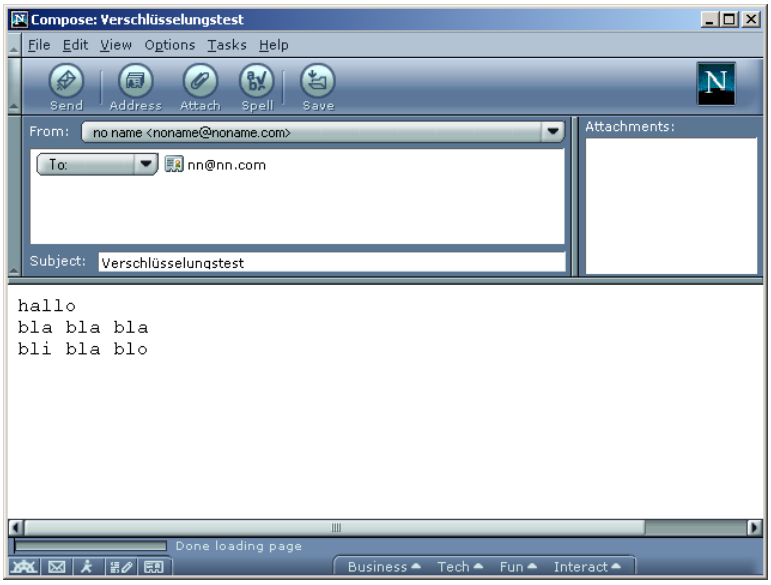
Zurück zum Inhalt dieses Kapitels

Nun geht der „Text Viewer“ mit dem entschlüsselten Text auf. Du kannst den Text nun mit dem Button „Copy to Clipboard“ in die Zwischenablage kopieren. Wenn du den entschlüsselten Text nicht speichern willst, drücke einfach „OK“.



Zurück zum Inhalt dieses Kapitels

Hast du „Copy to Clipboard“ gedrückt, kannst du zum Mailprogramm zurückkehren und im Menü „Edit ⇨ Paste“ bzw. in deutschsprachigen Programmen „Bearbeiten ⇨ Einfügen“ wählen. Der entschlüsselte Text wird dann eingefügt:



Wenn du deine Nachrichten auf einem verschlüsselten Teil der Festplatte speicherst, kannst du ruhig den entschlüsselten Text speichern (siehe Kapitel PGP Disk). Ist dies nicht der Fall, belasse ihn lieber in verschlüsselter Form, du kannst ihn ja jederzeit bei Bedarf wieder entschlüsseln.

Grund ist, dass neugierige Menschen natürlich sehr interessiert an deinen Mails sind. Beim Übersenden war diese Mail zwar nicht lesbar, kommt dir dein Computer jedoch irgendwie abhanden, können natürlich auch neugierige Menschen deinen Computer starten und seelenruhig alle deine unverschlüsselten Mails lesen, wenn sie nicht auf einem verschlüsselten Teil der Festplatte untergebracht wurden.

Zurück zum Inhalt dieses Kapitels

7 PGP Disk

Überblick

In diesem Kapitel erfährst du Näheres zu einem Teilprogramm von PGP, dem Programm PGP Disk.

Es dient zum Verschlüsseln von Festplattenbereichen. Alle Dateien, die du auf diesem Bereich (auf dieser Partition, auf diesem „Laufwerk“) speicherst, werden verschlüsselt gespeichert, nur nach Eingabe der Passphrase kann mensch die Daten wieder lesen.

Du findest Beschreibungen zu folgenden Bereichen:

- Die prinzipielle Funktionsweise von PGP Disk
- PGP Disk unter Windows XP
- Das Starten von PGP Disk
- Das Mounten und Unmounten von angelegten PGP Disks (An- und Abhängen der verschlüsselten Partitionen („Laufwerke“) an bzw. von deinem Dateisystem)
- Das Sichern von verschlüsselten Daten
- Das Speichern von Eudora-Daten auf einem verschlüsselten Laufwerk
- Das Speichern von Outlook-Daten auf einem verschlüsselten Laufwerk

Auf das Kapitel Das Sichern von verschlüsselten Daten möchten wir hier besonders hinweisen, da es dabei immer wieder Missverständnisse gibt. Es nützt einfach nichts, auf dem Computer die Daten fein verschlüsselt zu haben, neben dem Computer aber die Sicherungs-CDs mit unverschlüsselten Daten liegen zu haben.

7.1 Wie funktioniert das?

Auf deiner Festplatte (oder Diskette o.ä.) wird eine Datei angelegt, die Größe kannst du bei der Einrichtung bestimmen. Diese Datei erhält einen Laufwerksbuchstaben, so wie deine Festplatte den Laufwerksbuchstaben C besitzt.

In dieser Datei werden von dir mehr oder weniger unbemerkt deine eigentlichen Dateien (z.B. ein Word Dokument, Bilder, Mails etc.) verschlüsselt gespeichert. Für dich macht das aber kaum einen Unterschied, statt auf der Festplatte C speicherst du deine Dateien auf einem anderen Laufwerk, dessen Buchstaben du dir bei der Einrichtung von PGP Disk aussuchen kannst (also z.B. F).

Jeder Mensch mit Zugang zu deinem Computer kann diese Datei sehen, aber erst nach Eingabe des Passworts werden die verschlüsselten Daten sichtbar.

Mensch spricht hier von einem „virtuellen Laufwerk“, das ist ein Laufwerk, das nicht wirklich als Laufwerk existiert (du hast ja keine weitere Festplatte oder sonst irgendwas eingebaut). Trotzdem ist für dich die Handhabung genauso einfach wie mit einer zusätzlichen Festplatte oder einem Diskettenlaufwerk.

Technisch korrekt ist die Bezeichnung „Partition“, das ist eine logische Unterteilung deiner Festplatte(n).

Dieses Laufwerk wird auf deinen Wunsch und nach Eingabe der Passphrase zu deinem Dateisystem „dazugemountet“, das heißt dazugehängt. Es ist dann z.B. im Windows Explorer wie eine zusätzliche Festplatte oder ein Diskettenlaufwerk mit einem eigenen Laufwerksbuchstaben sichtbar.

Speichere dann deine Dateien einfach auf diesem Laufwerksbuchstaben ab, genauso wie du es bisher auf C getan hast. Du kannst natürlich auch auf deinem verschlüsselten Laufwerk Ordner erstellen, Dateien umbenennen etc., einfach alles, was du auch auf anderen Laufwerken tust.

Wenn du ganze Ordner und Unterordner von C auf dieses Laufwerk kopierst, werden natürlich auch die Ordner und Unterordner genauso erstellt. Es macht also für dich wirklich keinen Unterschied.

Der einzige Unterschied ist, dass die Daten auf diesem Laufwerk verschlüsselt sind und von keiner Person, welche die Passphrase nicht kennt, entschlüsselt werden können.

Am Ende des Kapitels findest du noch einen kleinen Tipp, wie du dieses Laufwerk jedes Mal beim Starten von Windows automatisch mounten kannst, die Passphrase musst du dabei natürlich trotzdem eingeben. Das erspart dir bei Starten des Computers einige Handgriffe.

Zurück zum Inhalt dieses Kapitels

7.2 PGP Disk unter Windows XP

Leider funktionieren die bisherigen PGP Versionen (bis einschließlich Version 7.x) nicht unter Windows XP. Für Windows XP ist erst die Version 8 freigegeben und funktionstüchtig.

Die älteren Versionen lassen sich entweder gar nicht installieren, oder speziell bei der Erstellung einer PGP Disk erscheint beim Formatieren die Fehlermeldung „Windows konnte die Formatierung nicht abschließen“.

Es gibt auch weiterhin kostenlose Versionen von PGP, die beinhalten aber leider nicht PGP Disk. D.h., die einzige legale Möglichkeit, eine vollständige PGP Version inklusive PGP Disk für Windows XP zu erhalten, ist, sie käuflich zu erwerben.

Die Gratis-Version der Version 8 findest du auf der CD und kannst sie durch Doppelklick auf die Datei „PGP8-Win32-Beta“ installieren.



PGP\Windows\8.0

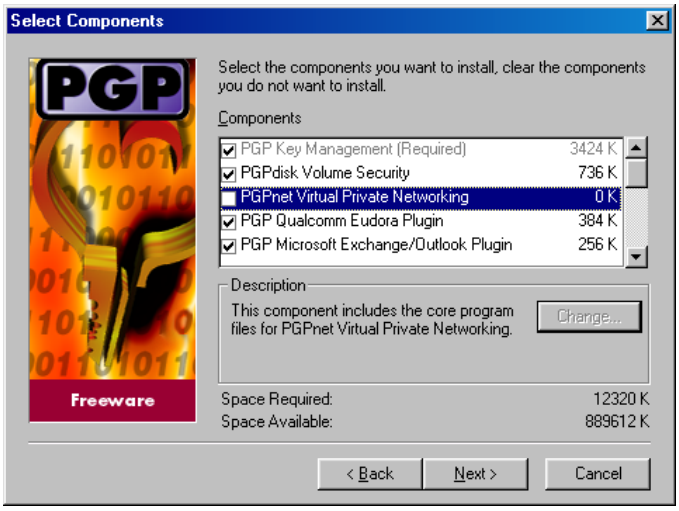

PGP8.exe

Hier noch die guten Nachrichten: im Unterschied zu einem Teil der 6er-Versionen und der Version 7 von PGP ist die Version 8 wieder ein sogenanntes Open Source Programm, d.h. der Programmcode wird völlig offen gelegt. Wenn dich der Source Code interessiert, kannst du ihn von der Webseite von PGP (http://www.pgp.com/) herunterladen. Das ermöglicht Leuten auf der ganzen Welt, eventuelle Sicherheitslücken im Programm zu finden, die dann in einem Update oder einer neuen Version beseitigt werden können.

Nachdem er bei Version 7 ausgestiegen ist (siehe Artikel „warum nicht v7 – erklaerung“ auf der CD), war bei Version 8 auch wieder Phil Zimmermann (das ist der Mann, der PGP zum ersten Mal öffentlich zugängig gemacht hat und sich damit auch einigen Ärger mit den US-Behörden eingehandelt hat) als Berater tätig, was doch auf einen Strategiewechsel bezüglich PGP hoffen lässt.

7.3 Das Starten von PGP Disk

Nach der Installation von PGP 6.5.8 hast du auch PGP Disk installiert. Das war im Installationsdialog auszuwählen. Zur Erinnerung die Auswahlliste bei der Installation:



In der 2. Zeile von oben findest du PGPdisk Volume Security, das ist das Programm PGP Disk.

Falls du eine andere Version von PGP ohne das Teilprogramm PGP Disk installiert hast (6.5.1 oder 6.5.3), musst du PGP Disk dazuinstallieren:

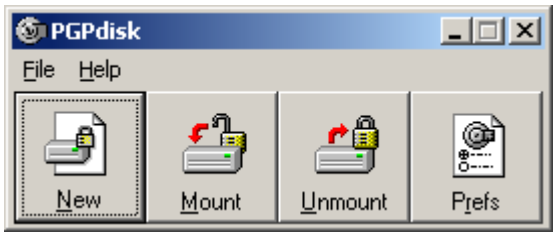
PGP\Windows\6.5.1(6.5.3)\DiskHack

pgpdiskhack.exe

Zurück zum Inhalt dieses Kapitels

Zeige nun mit dem Mauszeiger auf das PGP Schloss-Symbol am rechten unteren Rand des Bildschirms und drücke die rechte Maustaste. Unter dem sich öffnenden Kontextmenü befindet sich auch der Punkt „PGPdisk“, wähle diesen Menüpunkt.

Eine Leiste mit dem PGPdisk-Menü geht auf:



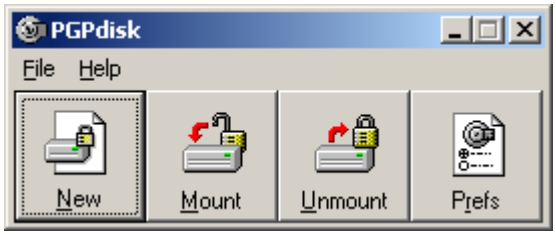
Du siehst nun alle für PGPdisk benötigten Menüpunkte:

- New: zum Erstellen einer neuen Partition
- Mount: zum Dazuhängen einer Partition in dein Dateisystem
- Unmount: zum Abhängen einer Partition von deinem Dateisystem
- Prefs: zum Setzen deiner Preferenzen

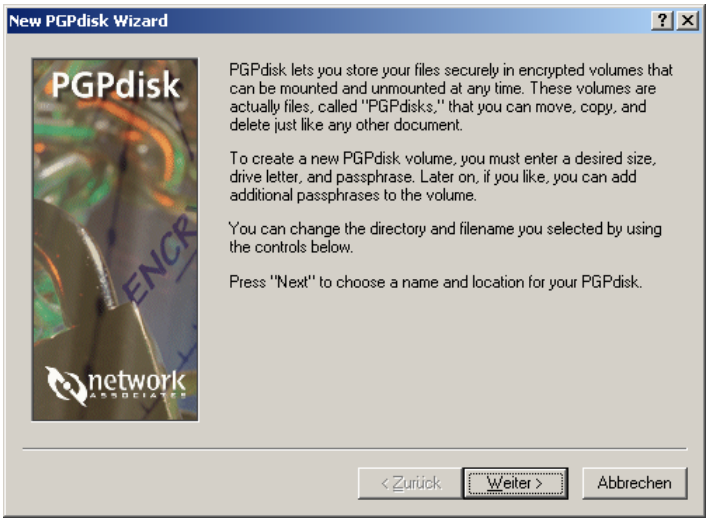
Zurück zum Inhalt dieses Kapitels

Das Erstellen eines verschlüsselten Bereichs (Partition) auf der Festplatte

Zum Einrichten einer neuen Partition starte PGPdisk, wie im vorherigen Kapitel beschrieben und wähle in der Menüleiste den Button „New“ zum Erstellen einer neuen verschlüsselten Partition.



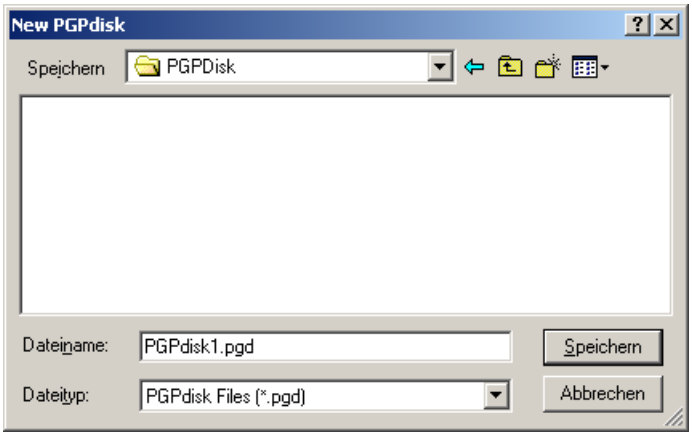
Der Begrüßungsdialog erscheint dann am Bildschirm:



Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann erscheint ein Fenster, in dem du dir das Verzeichnis (den Ordner) und den Dateinamen aussuchen kannst, unter dem deine neue Partition gespeichert wird. Du kannst z.B. wie im Beispiel einen neuen Ordner „PGPDisk“ anlegen und dem Dateinamen die Nummer 1 geben, falls du möglicherweise weitere Partitionen erstellen wirst. Du kannst den Namen aber ganz frei wählen.



Drücke dann den Button „Speichern“.

Zurück zum Inhalt dieses Kapitels

Nun kannst du die gewünschte Größe des Festplattenbereichs angeben, der für die Datei mit den verschlüsselten Daten reserviert wird. Diese Größe hängt natürlich von der Größe deiner Festplatte ab, wie viel freien Speicherplatz du noch hast und wie viele Daten du verschlüsselt speichern willst.

Eine gute Idee ist sicherlich, einfach alle deine eigenen Daten verschlüsselt abzuspeichern (also deine Word-Dokumente, Bilder, Mails etc.). So ersparst du dir eventuell mühsames Suchen deiner Dateien.

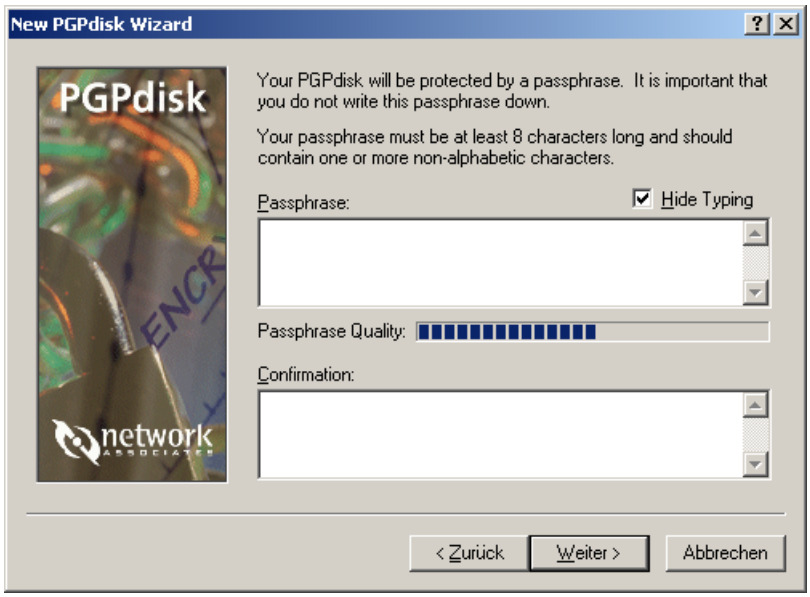
Sinnlos ist jedoch, deine Programme wie z.B. Microsoft Office verschlüsselt zu speichern (die sind meist unter C:\Programme oder C:\Program Files zu finden).

Wähle also den gewünschten Speicherplatz, der in KB (Kilobytes), MB (Megabytes) oder GB (Gigabytes) angegeben werden kann. Wähle weiters den Laufwerksbuchstaben, der dieser Partition zugeteilt werden soll, du kannst aus der Liste einen beliebigen Buchstaben auswählen.

Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Nun musst du wieder eine Passphrase angeben. Je nach Belieben kannst du die gleiche wie für dein Schlüsselpaar bei PGPkeys nehmen oder auch eine neue Passphrase erfinden.



Ohne diese Passphrase kannst du aber die Daten, die auf dieser Partition gespeichert wurden, nicht lesen. Also die Passphrase nie vergessen, sonst sind die Daten nicht mehr entschlüssel- und lesbar.

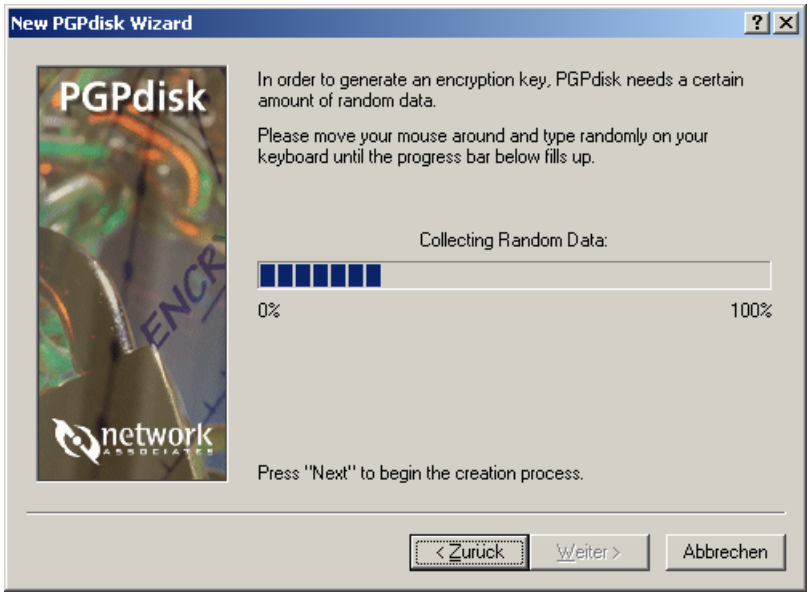
Ein paar Tipps zu guten Passwörtern oder Passphrases findest du im Kapitel Tipps für Passwörter/Passphrases.

Zurück zum Inhalt dieses Kapitels

Nun errechnet PGP deinen Schlüssel für die Verschlüsselung der Festplatte. Dazu benötigt das Programm einige Zufallsdaten, die durch Bewegen deines Mauszeigers oder durch Tippen auf der Tastatur errechnet werden.

Diese Berechnungsgrundlagen sind nie wieder wiederholbar, daher auch die Sicherheit des Schlüssels, daher auch nie deine Passphrase vergessen.

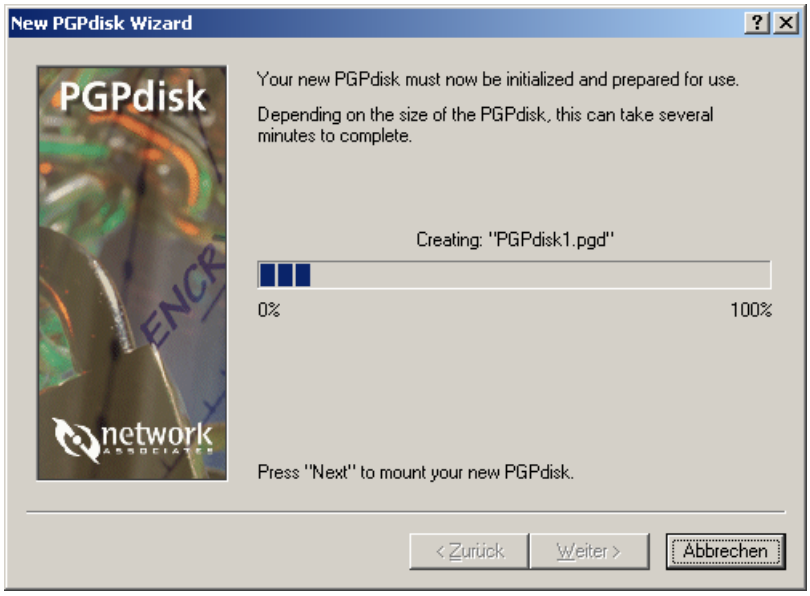
Bewege ein wenig die Maus oder tippe ein wenig auf deiner Tastatur herum.



Wenn der blaue Balken voll ist, kannst du den Button „Weiter“ drücken.

Zurück zum Inhalt dieses Kapitels

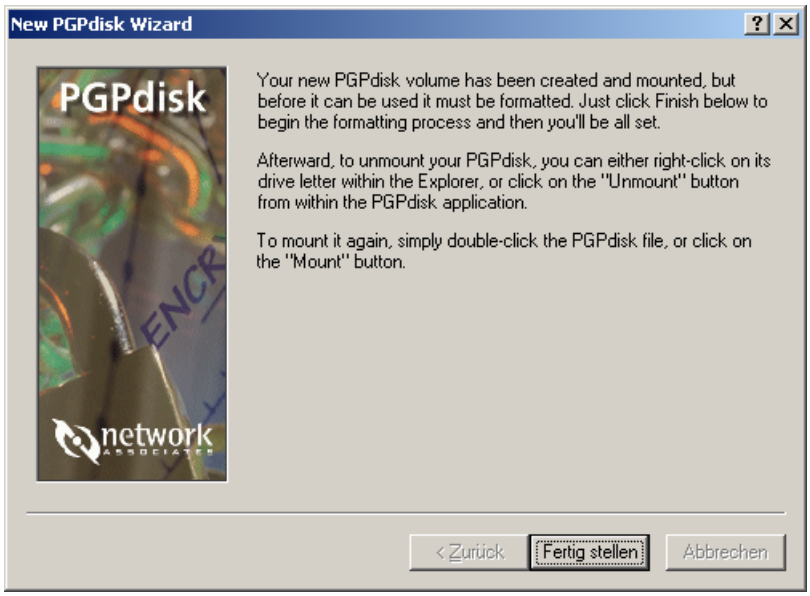
Nun wird die Datei für deine Partition erstellt und vorbereitet:



Ein bisschen Geduld, es dauert aber nicht allzu lange. Wenn die Datei erstellt wurde, kannst du den Button „Weiter“ drücken.

Zurück zum Inhalt dieses Kapitels

Dann erscheint das Fenster zum Fertigstellen der Partition, drücke den Button „Fertig stellen“.

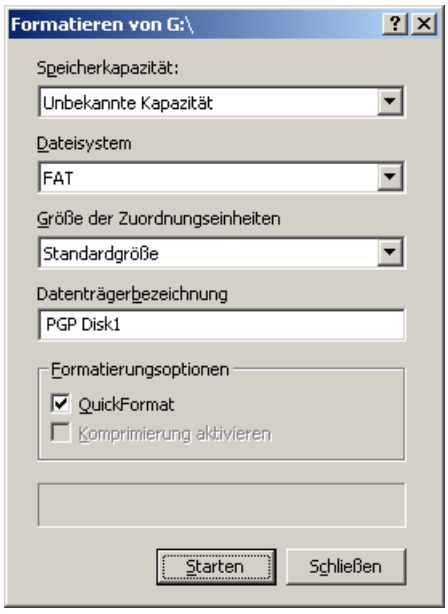


Zurück zum Inhalt dieses Kapitels

Deine neue Partition muss nun für die Verschlüsselung formatiert werden.

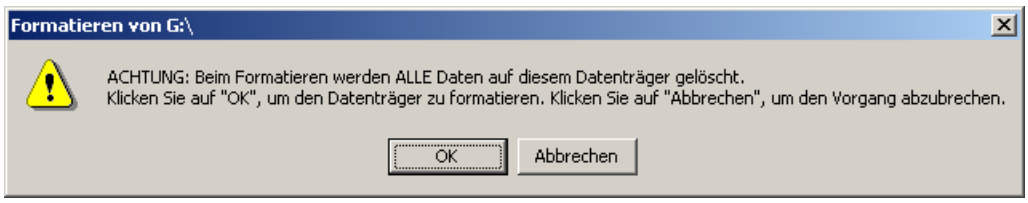
Keine Angst, es wird wirklich nur die Datei für deine verschlüsselten Daten formatiert und nicht deine ganze Festplatte.

Wenn du willst, kannst du der Partition auch einen Namen geben, dieser Name scheint dann z.B. im Windows Explorer neben dem Laufwerksbuchstaben auf.



Zurück zum Inhalt dieses Kapitels

Drücke dann den Button „Starten“, es erscheint dann noch eine Warnung, dass deine Daten auf der neuen Partition gelöscht werden. Aber wie gesagt, keine Angst, es wird nur diese eine Datei für die Verschlüsselung formatiert, alle deine bisherigen Daten und Programme bleiben erhalten.



Drücke den Button „OK“.

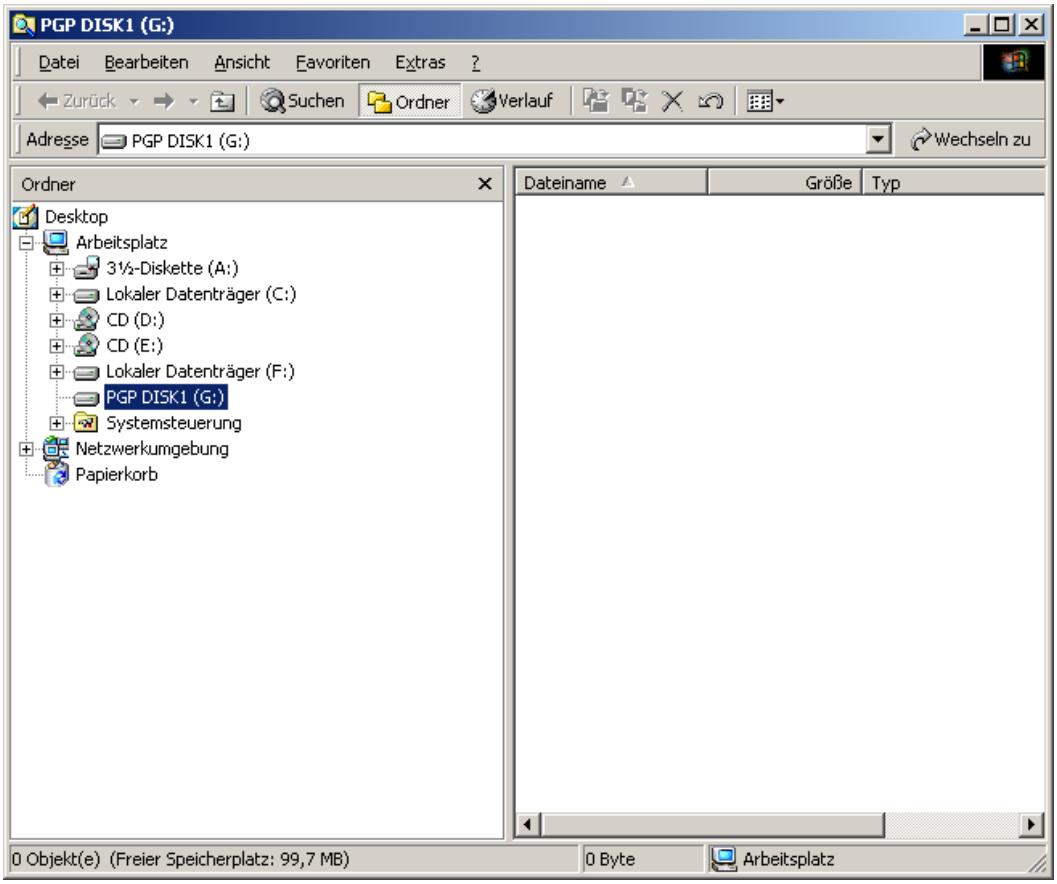
Zurück zum Inhalt dieses Kapitels

Nach der Beendigung der Formatierung erscheint folgende Nachricht:

Drücke den Button „OK“ und im Formatierungsfenster den Button „Schließen“, die Erstellung deiner verschlüsselten Partition ist nun abgeschlossen und das Laufwerk wurde gleich an dein Dateisystem dazugehängt (gemountet).

Zurück zum Inhalt dieses Kapitels

Das erkennst du in Windows im Windows Explorer, der nach dem Abschluss der Einrichtung geöffnet wird, in unserem Beispiel siehst du unter dem Laufwerksbuchstaben G: die neue Partition:

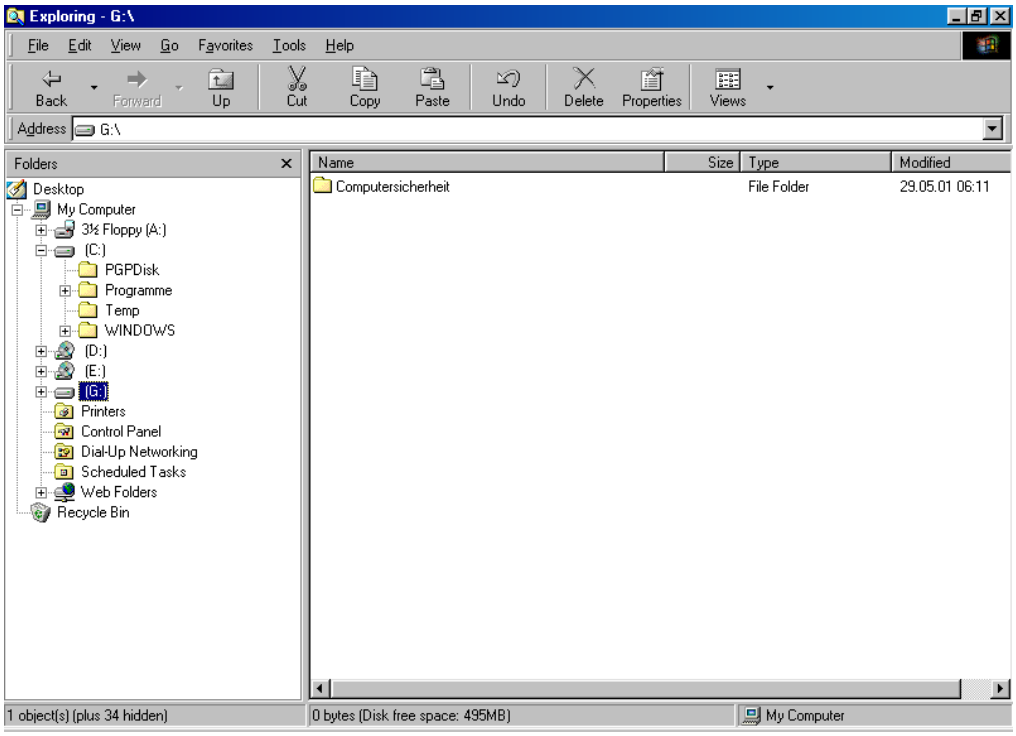


Alles, was du ab sofort auf Laufwerk G: speicherst, wird in verschlüsselter Form gespeichert. Die dort gespeicherten Dateien sind erst nach dem Mounten des Laufwerks mit der Eingabe der Passphrase sicht- und lesbar.

Nach der Erstellung des Laufwerks ist es natürlich zunächst leer, du kannst aber gleich beginnen, deine Dateien auf dieses Laufwerk zu übersiedeln (mit „Ausschneiden“ und „Einfügen“ bzw. „Cut“ und „Paste“).

Zurück zum Inhalt dieses Kapitels

Das machst du im Windows Explorer durch Markieren der Ordner, in denen sich deine Dateien befinden und durch Wählen des Menüpunkts „Bearbeiten Ausschneiden“ bzw. „Edit ⇨ Cut“. Klicke dann auf dein neues Laufwerk und wähle im Menü „Bearbeiten ⇨ Einfügen“ bzw. „Edit ⇨ Paste“. Im Beispiel wurde der Ordner „Computersicherheit“ erstellt, in dem sich alle Dokumente zu diesem Handbuch befinden:



Mehr zum Mounten und Unmounten von PGP Laufwerken erfährst du im nächsten Kapitel.

Zurück zum Inhalt dieses Kapitels

7.4 Das Mounten und Unmounten von PGP Disks (An- und Abhängen an dein bzw. von deinem Dateisystem)

Wie schon erwähnt, musst du deine verschlüsselte(n) Partition(en) (deine PGP Disks) nach jedem Start des Betriebssystems (also z.B. von Windows) an dein Dateisystem anhängen, um den Inhalt öffnen und lesen zu können. Dieser Vorgang des Anhängens wird „mount“ genannt.

Nach dem mounten einer PGP Disk kannst du sie wie ein ganz normales Laufwerk behandeln, also z.B. wie gewohnt Ordner erstellen und deine Dateien darauf speichern.

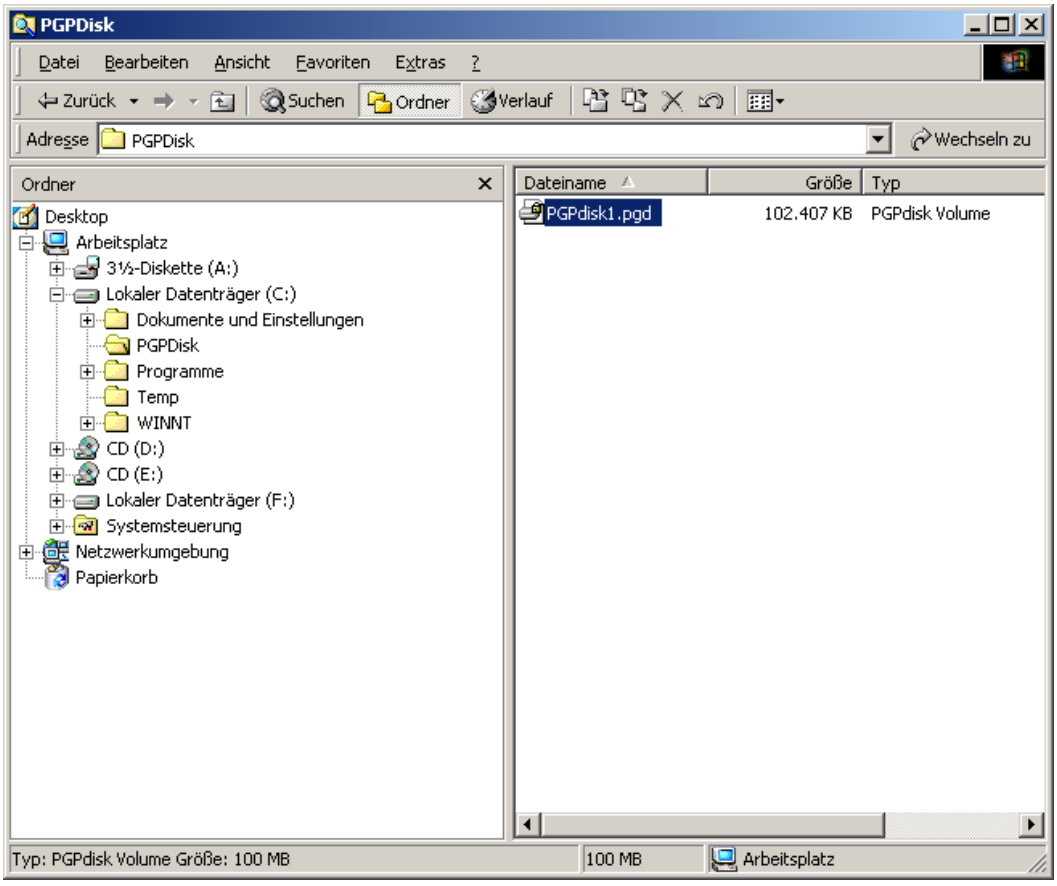
Das Mounten lässt sich auch ein wenig automatisieren, um sich den nachfolgend beschriebenen Vorgang zu erleichtern. mehr dazu erfährst du am Ende des Kapitels.

Zurück zum Inhalt dieses Kapitels

Das PGP Disk Menü

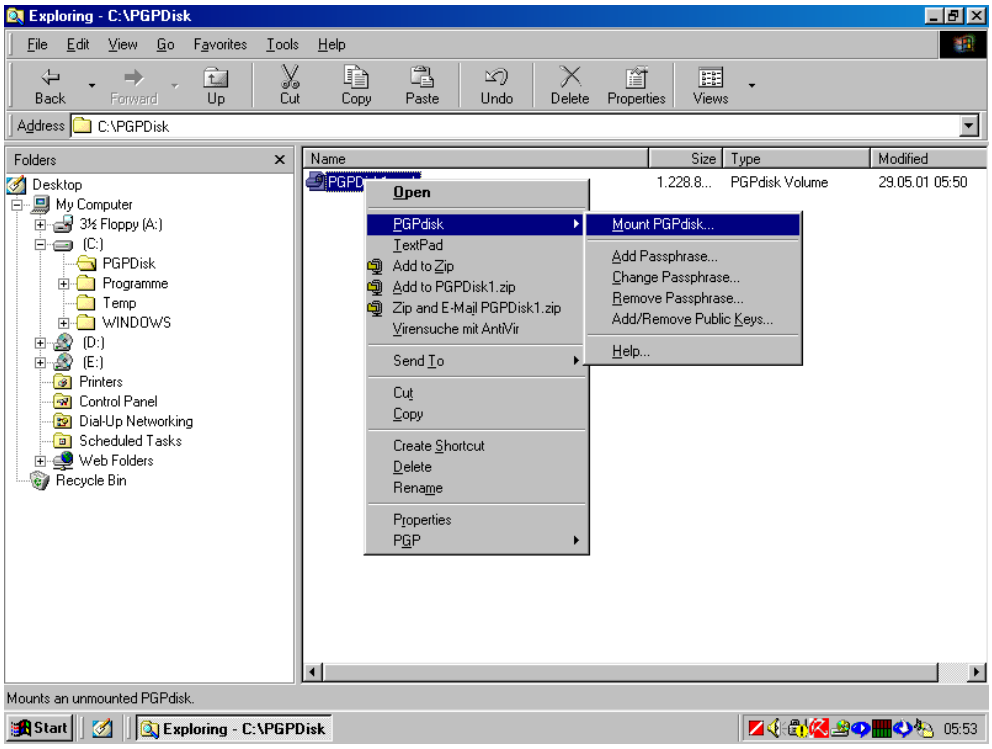
Deine verschlüsselte PGP Disk ist eine einfache Datei auf deinem Computer auf einem unverschlüsselten Festplattenbereich (also z.B. auf C). Du hast bei der Erstellung der Partition im vorigen Kapitel angegeben, wo sie mit welchem Namen gespeichert werden soll. In unserem Beispiel war das der Ordner „PGPDisk“, der Dateiname war „PGPDisk1.pgd“.

Öffne nach dem Starten des Betriebssystems (also z.B. von Windows) den Ordner, in dem sich diese Datei befindet.



Zurück zum Inhalt dieses Kapitels

Zeige mit dem Mauszeiger auf die Datei und drücke die rechte Maustaste.



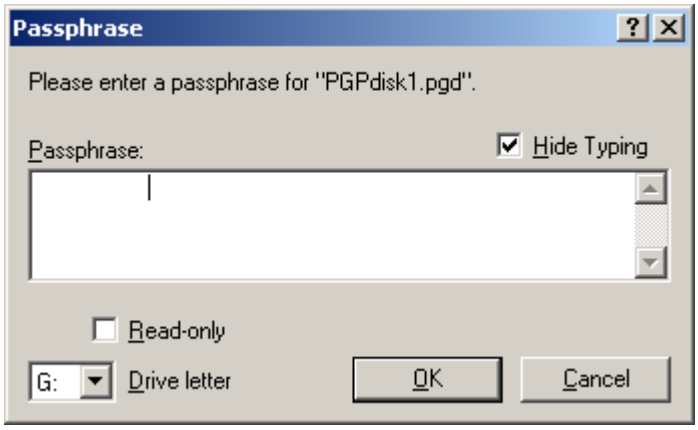
Ein Kontextmenü erscheint, folgende Menüpunkte stehen zur Auswahl:

- Mount PGPdisk... zum Dazuhängen einer PGP Disk
- Add Passphrase... zum Hinzufügen einer zusätzlichen Passphrase
- Change Passphrase… zum Ändern einer Passphrase
- Remove Passphrase… zum Löschen einer Passphrase
- Add/Remove Public Keys zum Aufruf der Schlüsselverwaltung
- Help… ruft die PGPdisk Hilfe auf

Zurück zum Inhalt dieses Kapitels

Das Mounten der PGP Disk

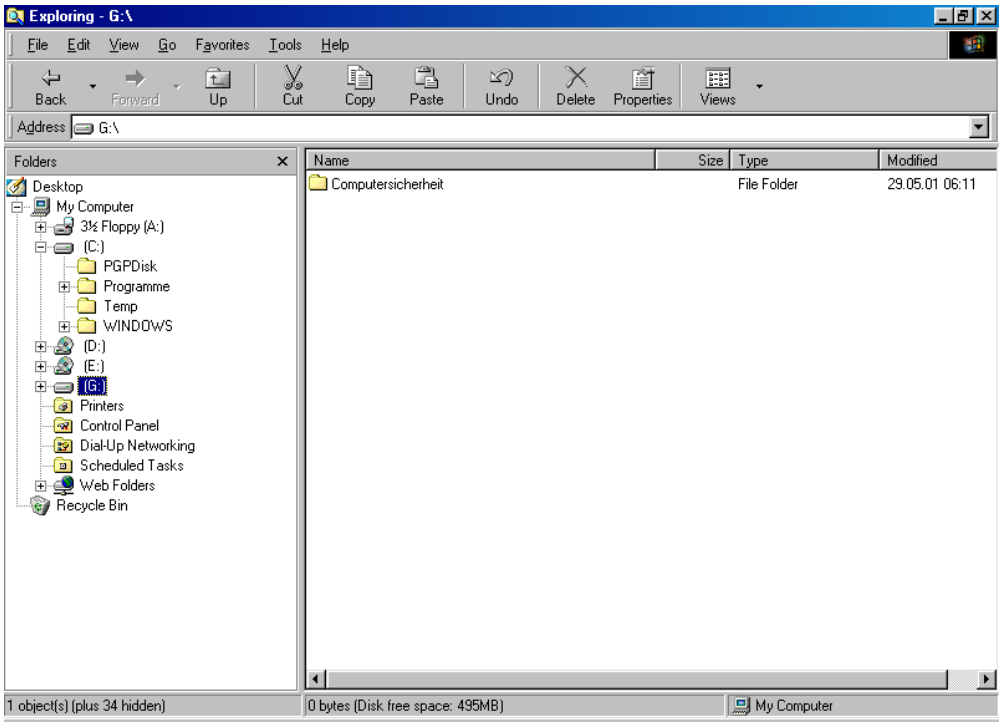
Wähle den Menüpunkt „Mount PGPdisk“. Nun wirst du zur Eingabe deiner Passphrase aufgefordert. Gib die Passphrase an, die du bei der Erstellung deiner PGP Disk angegeben hast.



Drücke nach Eingabe deiner Passphrase den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Wenn du die Passphrase richtig angegeben hast, erscheint im Windows Explorer das Laufwerk. Du kannst nun auf alle Dateien ganz normal zugreifen.

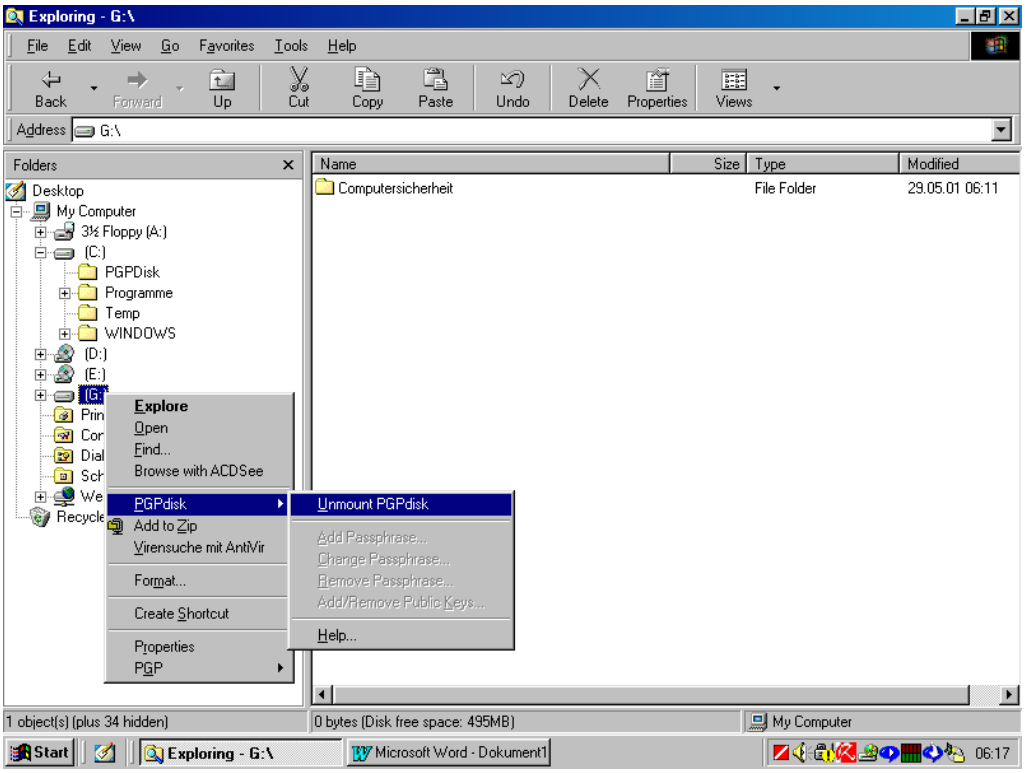


Zurück zum Inhalt dieses Kapitels

Das Unmounten der PGP Disk

So wie du PGP Disks an dein Dateisystem anhängen (mounten) kannst, kannst du sie natürlich auch wieder abhängen (unmounten). Das geschieht automatisch beim Herunterfahren des Betriebssystems (also z.B. bei Beenden von Windows). Du solltest das aber auch jedes Mal tun, wenn der Computer unbeaufsichtigt bleibt.

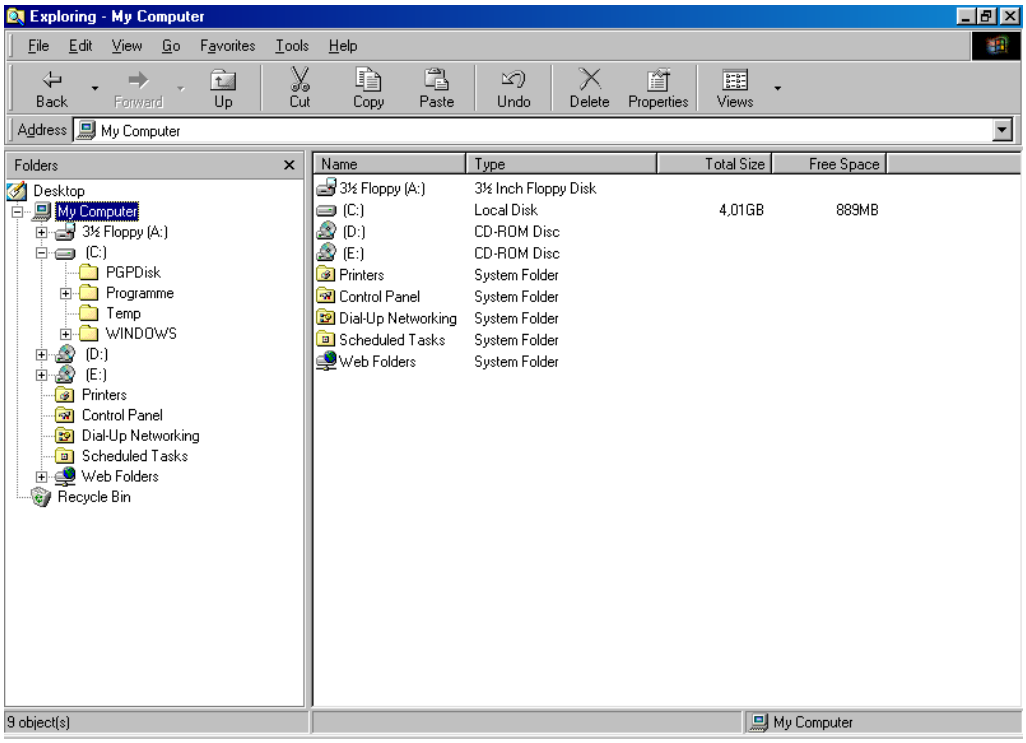
Zum Unmounten zeige im Windows Explorer mit dem Mauszeiger auf den Laufwerksbuchstaben der PGP Disk und drücke die rechte Maustaste. Folgendes Kontextmenü erscheint:



Wähle im Kontextmenü „PGPdisk ⇨ Unmount PGPdisk“.

Zurück zum Inhalt dieses Kapitels

Nach dem Unmounten der PGP Disk verschwindet der Laufwerksbuchstabe im Explorer. Erst nach dem Mounten der PGP Disk mit Eingabe der Passphrase ist der Inhalt wieder sicht- und verwendbar.



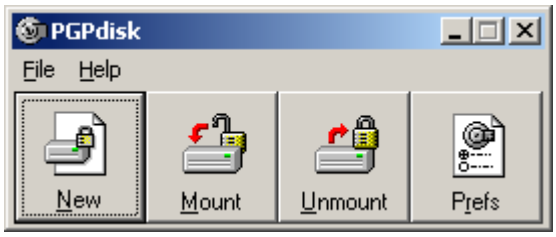
Zurück zum Inhalt dieses Kapitels

Das automatische Unmounten von PGP Disks

Du kannst auch einstellen, dass sich die PGP Disk nach einer gewissen Zeit des Nichtstuns auf dem Computer automatisch selbst abhängt. Das gibt zusätzliche Sicherheit, falls du mal vergisst, den Computer abzudrehen oder den Computer aus irgendwelchen Gründen unbeaufsichtigt lässt.

Allerdings kann das auch ein wenig lästig sein, wenn du z.B. mal auf die Toilette gehst und danach die PGP Disk wieder mounten musst. Du musst selbst entscheiden, ob du diese Möglichkeit nutzt oder nicht, empfohlen ist sie auf jeden Fall.

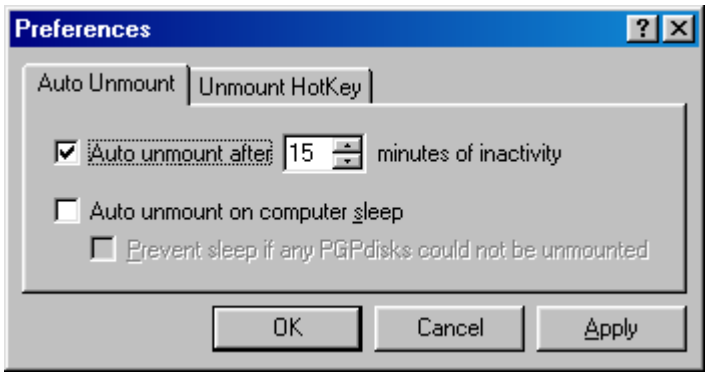
Starte die Toolleiste von PGP, zeige dazu mit dem Mauszeiger auf das Schloss-Symbol am rechten unteren Rand deines Bildschirms und drücke die rechte Maustaste. Wähle aus dem Menü PGPdisk. Folgende Leiste erscheint am Bildschirm:



Drücke nun den Button „Prefs“ zur Eingabe deiner persönlichen Einstellungen (Preferences).

Zurück zum Inhalt dieses Kapitels

Im folgenden Fenster kannst du dann wählen, nach wie vielen Minuten des Nichtstuns sich das Laufwerk oder die Laufwerke selbst unmounten sollen.



Drücke nach Eingabe der Minutenanzahl den Button „OK“. Du kannst diese Einstellung natürlich jederzeit wieder ändern.

Zurück zum Inhalt dieses Kapitels

Schnelles Unmounten mit einem HotKey

Du kannst auch einen sogenannten „HotKey“ (eine Tastenkombination) angeben, nach deren Eingabe sich alle PGP Disks unmounten.

Merke dir diese Tastenkombination aber gut, damit du nicht lange nachdenken musst.

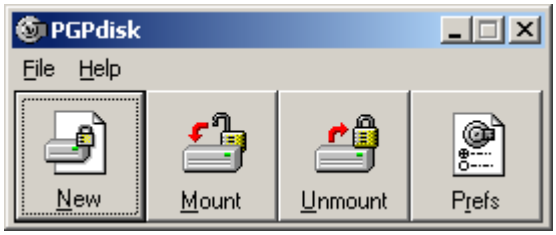
Ein kleiner Tipp ist, die Kombination jedes Mal vor Beenden von Windows einzugeben, auch wenn das nicht notwendig ist, aber so vergisst du die Tastenkombination nicht (siehe aber auch Tipp unten).

Diese Möglichkeit dient vor allem für den Fall, dass du deinen Computer kurz unbeaufsichtigt lässt, aber für diese Zeit nicht abdrehen willst. In Notfällen gibt es viel bessere Vorgangsweisen:

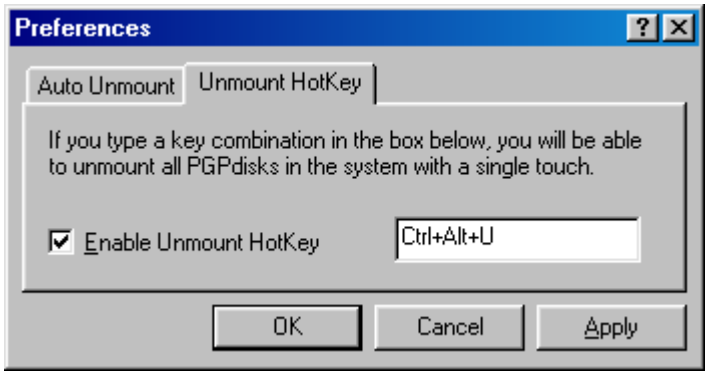
In Notfällen, wenn z.B. neugierige Menschen in deine Wohnung stürmen und du wirklich andere Sorgen hast, als den Windows Explorer zu starten und deine PGP Disk zu suchen, um sie unmounten zu können, einfach den Computer abdrehen oder den Stecker rausziehen, das ist einfach, geht schnell und ist gründlich.

Zurück zum Inhalt dieses Kapitels

Zur Angabe des HotKeys starte die Toolleiste von PGP, zeige dazu mit dem Mauszeiger auf das Schloss-Symbol am rechten unteren Rand deines Bildschirms und drücke die rechte Maustaste. Wähle aus dem Menü PGPdisk. Folgende Leiste erscheint am Bildschirm:



Drücke den Button „Prefs“. Das Fenster zur Angabe deiner Präferenzen erscheint:



Nun kannst du den „HotKey“ (die Tastenkombination) wählen.

Markiere das Kästchen bei „Enable Unmount HotKey“ und drücke einfach die Tastenkombination, die du als HotKey verwenden willst, im Beispiel die Tasten Strg+Alt+U. Drücke dann den Button „OK“ zum Aktivieren des HotKeys. Du kannst diesen HotKey natürlich jederzeit wieder ändern.

Zurück zum Inhalt dieses Kapitels

7.5 Das Sichern von verschlüsselten Daten

Wie schon erwähnt, ist deine verschlüsselte PGP Disk eine einfache Datei auf deinem Computer. Das Schöne daran ist, dass du diese Datei als Sicherung einfach irgendwo hinkopieren kannst, sie bleibt verschlüsselt und lässt sich nur nach dem Mounten mit Eingabe der Passphrase entschlüsseln.

Auf keinen Fall Dateien von deinem verschlüsselten Laufwerk auf ein nicht verschlüsseltes kopieren. Die Dateien bleiben nur verschlüsselt, solange sie sich auf einem deiner verschlüsselten PGP-Disks befinden.

Daher muss zum Sichern auch eine ganze solche PGP-Disk z.B. auf CD gebrannt werden.

Das Sichern auf CD mit einem CD Brenner

Folgende Angaben sind nur Tipps, du kannst dir natürlich auch andere Vorgangsweisen einfallen lassen.

Falls deine Haupt-PGP Disk größer als 600 MB ist, lege dir neben deiner PGP Hauptdisk, auf die du alle deine Dateien speicherst, noch eine zweite PGP Disk mit einer Größe von ca. 600 MB zum Sichern an (bzw. etwas kleiner als auf deinen CDs Platz hat).

Dann kannst du die zu sichernden verschlüsselten Dateien auf deiner Festplatte einfach auf diese zweite Sicherungs-PGP Disk kopieren und die ganze PGP Disk Datei auf eine CD kopieren. Die Daten sind dann verschlüsselt auf der CD, du kannst sie zum Ansehen wieder zurück auf deine Festplatte kopieren und wie jede deiner PGP Disks mounten.

Leider kann mensch eine PGP Disk nicht direkt von einer einmal beschreibbaren CD mounten, da PGP beim Öffnen irgendetwas in diese Datei schreiben will - und das geht natürlich auf einer nur ein Mal beschreibbaren CD nicht.

Daher PGP Disks auf solchen CDs vor dem Öffnen auf die Festplatte kopieren.

Zurück zum Inhalt dieses Kapitels

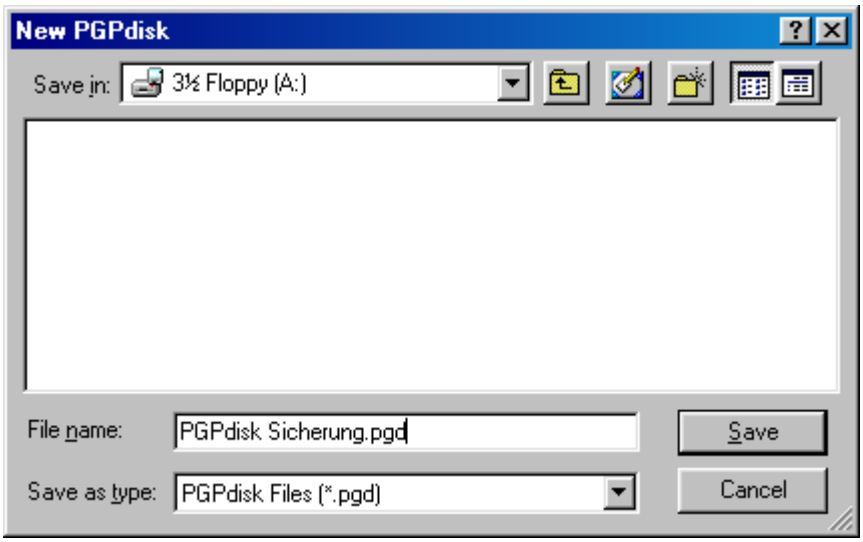
Das Sichern auf Diskette

Bei Disketten ist die Vorbereitung leider nicht ganz so einfach wie beim Sichern auf CD, hier musst du das Ganze ein wenig anders angehen, die Handhabung selbst ist dann aber genauso einfach wie bei einer CD.

Du musst die zweite PGP Disk zum Sichern auf Diskette direkt auf einer Diskette anlegen.

Lege dazu eine leere Diskette ein und mache das Anlegen der PGP Disk genauso, wie in Kapitel Das Erstellen eines verschlüsselten Bereichs auf der Festplatte (einer Partition) beschrieben (siehe auch nächste Seite).

Wenn du Ordner und Namen der Datei angibst, gib einfach einen Dateinamen auf der Diskette an.



Zurück zum Inhalt dieses Kapitels

Bei der Größe der Datei gib 1.400 KB an, das geht sich auf der Diskette aus.

Zurück zum Inhalt dieses Kapitels

Gehe sonst wie gewohnt vor (mit Angabe der Passphrase, dem Formatieren etc., siehe dazu das Kapitel Das Erstellen eines verschlüsselten Bereichs (Partition) auf der Festplatte).

Nachdem du diese PGP Disk direkt auf der Diskette erstellt und formatiert hast, kopiere die Datei mit der neuen PGP Disk in dein Verzeichnis auf der Festplatte, wo du auch deine PGP Hauptdisk hast. Diese Sicherungsdisk muss natürlich einen anderen Dateinamen als deine Hauptdisk haben.

Nun kannst du diese PGP Disk auch ganz normal mounten (siehe Das Mounten der PGP Disk). Dann kannst du Dateien, die du verschlüsselt sichern willst, auf das Laufwerk der Sicherungsdisk kopieren und dann die Datei mit der PGP Disk auf eine beliebige leere Diskette kopieren. Diese Disketten müssen dann nicht mehr extra für PGP Disk präpariert werden.

Zurück zum Inhalt dieses Kapitels

Zusammenfassung CD

Wenn du einen CD Brenner hast und deine Haupt-PGP Disk größer als 600 MB ist, lege auf deiner Festplatte eine zweite PGPDisk mit der Größe an, die sich auf einer CD ausgeht, nämlich ca. 600 MB. Hat sie jedoch eine Größe von 600 MB oder weniger, musst du keine neue PGP Disk anlegen.

Kopiere für die Sicherung deine verschlüsselten Dateien in dieses neue Laufwerk.

Kopiere einfach die Datei mit der Sicherungs-PGP Disk (in unserem Beispiel die Datei „PGPDisk Sicherung.pgd“ im Ordner „PGPDisk“) auf eine CD. Die Daten befinden sich dann verschlüsselt auf der CD, du kannst die PGP Disk auf der CD nach dem Kopieren auf deine Festplatte wie alle deine PGP Disks mounten.

Wenn du einzelne verschlüsselte Ordner und/oder Dateien von einer verschlüsselten Partition auf eine CD oder Diskette kopierst, wird sie dort unverschlüsselt gespeichert. Daher ist die Vorgangsweise mit dem Kopieren der gesamten Datei mit der PGP Disk notwendig.

Zurück zum Inhalt dieses Kapitels

Zusammenfassung Disketten

Wenn du auf Disketten sicherst, lege eine neue PGP Disk direkt auf einer leeren Diskette an (Größe ist 1400 KB).

Kopiere die entstandene Datei auf deine Festplatte dorthin, wo sich auch die andere Datei mit deiner Haupt-PGP Disk befindet (in unserem Beispiel in den Ordner „PGPDisk“, die Sicherungs-PGP Disk hat den Namen „PGPDisk Sicherung.pgd“).

Kopiere deine verschlüsselten Daten in dieses neue Laufwerk, das geht natürlich nur bis zur maximalen Größe von 1,4 MB, mehr hat ja auch sonst auf einer Diskette nicht Platz.

Kopiere einfach die Datei mit der Sicherungs-PGP Disk (in unserem Beispiel die Datei „PGPDisk Sicherung.pgd“ im Ordner „PGPDisk“) auf eine Diskette. Die Daten befinden sich dann verschlüsselt auf der Diskette, du kannst das Laufwerk auf der Diskette genauso wie von der Festplatte mounten.

Wenn du einzelne verschlüsselte Ordner und/oder Dateien von einer verschlüsselten Partition auf eine CD oder Diskette kopierst, wird sie dort unverschlüsselt gespeichert. Daher ist die Vorgangsweise mit dem Kopieren der gesamten Datei mit der PGP Disk notwendig.

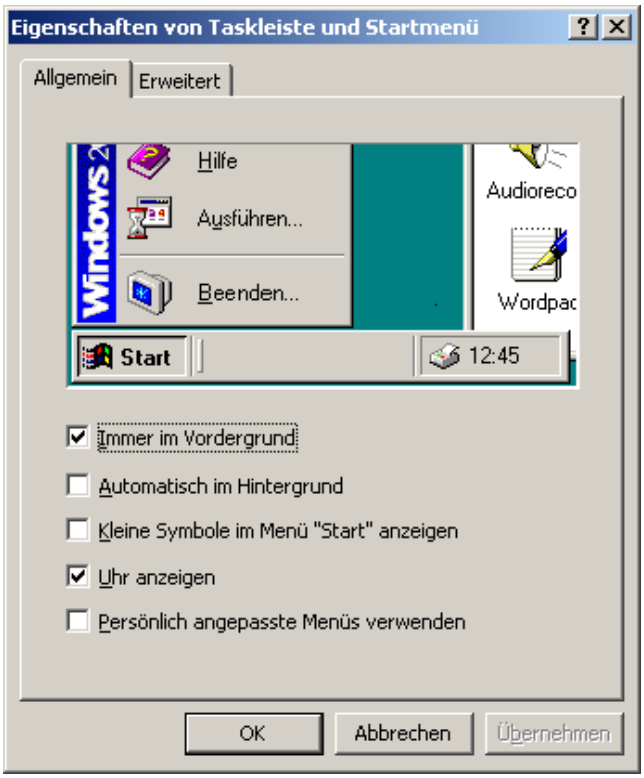
Zurück zum Inhalt dieses Kapitels

Das automatische Mounten von PGP Disks nach dem Starten von Windows

Es ist natürlich etwas mühsam, nach jedem Windows-Start im Explorer auf die Suche nach der Datei mit der PGP Disk zu gehen und dann diese Disk wie beschrieben zu mounten.

Mensch kann sich diesen Schritt etwas erleichtern und angeben, dass dieses Mounten automatisch bei jedem Start von Windows geschehen soll, deine Passphrase musst du natürlich trotzdem angeben, alles andere wäre ja irgendwie tragisch (siehe neugierige Menschen an deinem Computer und so).

Wähle dazu im Start-Menü den Menüpunkt „Start ⇨ Einstellungen ⇨ Taskleiste und Startmenü“ bzw. „Start ⇨ Settings ⇨ Taskbar & Start Menu“. Folgendes Fenster erscheint (oder zumindest ein ähnliches Fenster):



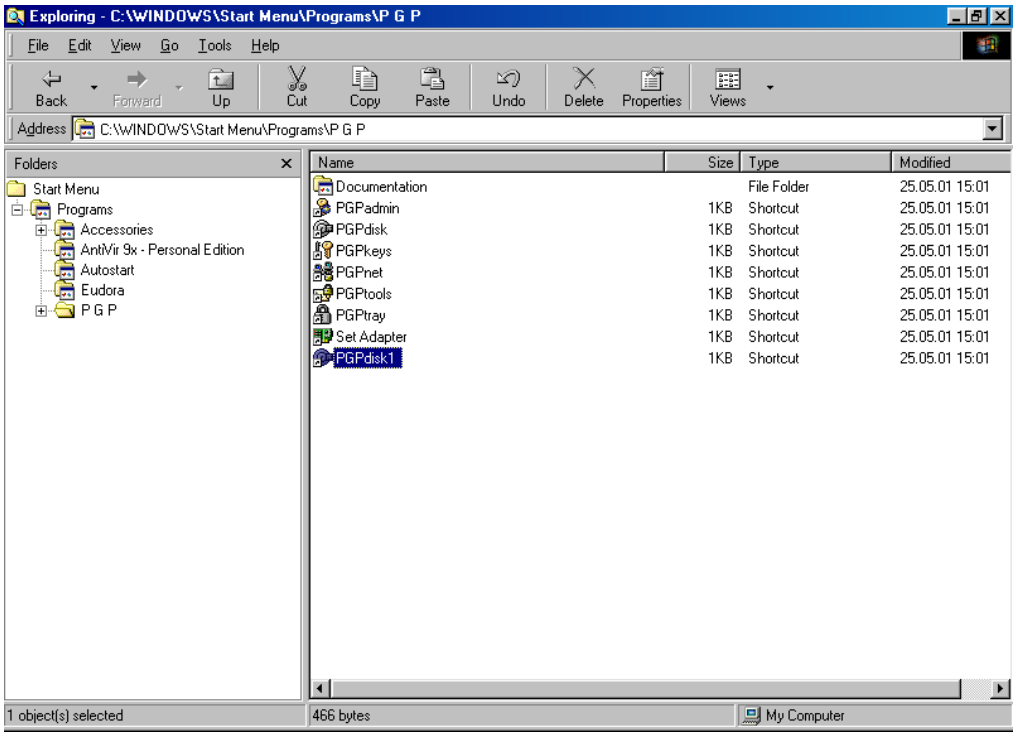
Zurück zum Inhalt dieses Kapitels

Wähle die Karteikarte „Erweitert“ oder „Start Menu Programs“ oder ähnliches, jedenfalls die zweite auf der rechten Seite. Abhängig vom Betriebssystem erscheint eines der unten angezeigten Fenster oder ein ähnliches.

Drücke den Button „Advanced“ oder „Erweitert“.

Zurück zum Inhalt dieses Kapitels

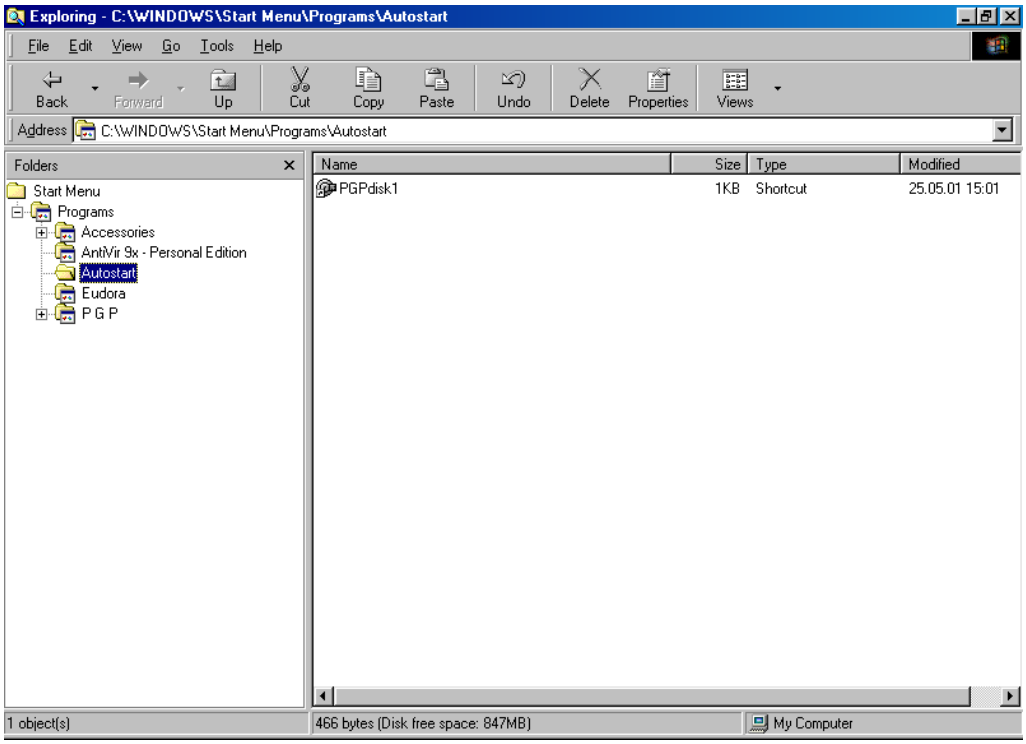
Wiederum abhängig vom Betriebssystem schaut das daraufhin aufgehende Fenster ungefähr so aus:



Zeite mit dem Mauszeiger auf den Eintrag in „Start Menu ⇨ Programme ⇨ PGP ⇨ PGPdisk“, drücke die rechte Maustaste und wähle im Kontextmenü „Verknüpfung erstellen“. Es wird dann eine Verknüpfung zum Programm PGPdisk erzeugt.

Zurück zum Inhalt dieses Kapitels

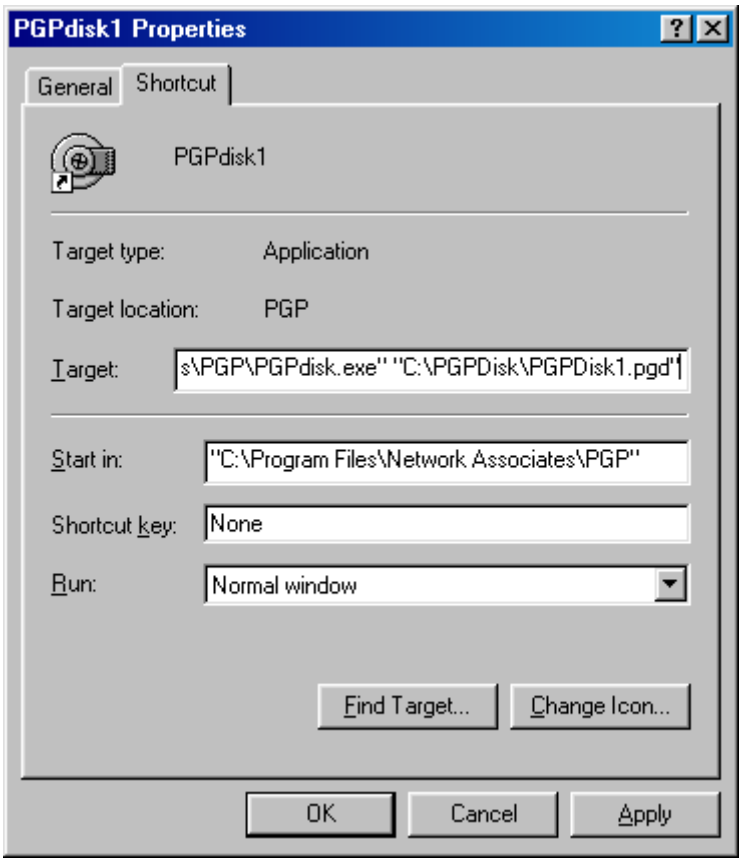
Verschiebe diesen neuen Eintrag in den Ordner „Autostart“. Das machst du mit „Ausschneiden“ und „Einfügen“ bzw. mit „Cut“ und „Paste“.



Zurück zum Inhalt dieses Kapitels

Zeige mit dem Mauszeiger auf die Verknüpfung und drücke die rechte Maustaste. Wähle aus dem Kontextmenü den Eintrag „Eigenschaften“ bzw. „Properties“. Wähle die Karteikarte „Verknüpfung“ bzw. „Shortcut“.

Trage dann im Feld „Ziel“ oder „Target“ ganz hinten unter doppeltem Hochkomma den Pfad und den Dateinamen deiner PGP Disk ein.



Drücke anschließend den Button „OK“. Das Programm PGP Disk wird ab sofort bei jedem Hochfahren von Windows automatisch gestartet, das Programm bekommt außerdem den Namen deiner PGP Disk übergeben und mountet es nach Eingabe der Passphrase automatisch an dein Dateisystem.

Zurück zum Inhalt dieses Kapitels

7.6 Das Speichern von Eudora-Daten auf einem verschlüsselten Laufwerk

Wenn du deine Mails unverschlüsselt auf der Festplatte speicherst, haben natürlich auch neugierige Menschen Zugriff auf deine Mails, wenn sie an deinen Computer kommen. Und das will mensch natürlich nicht.

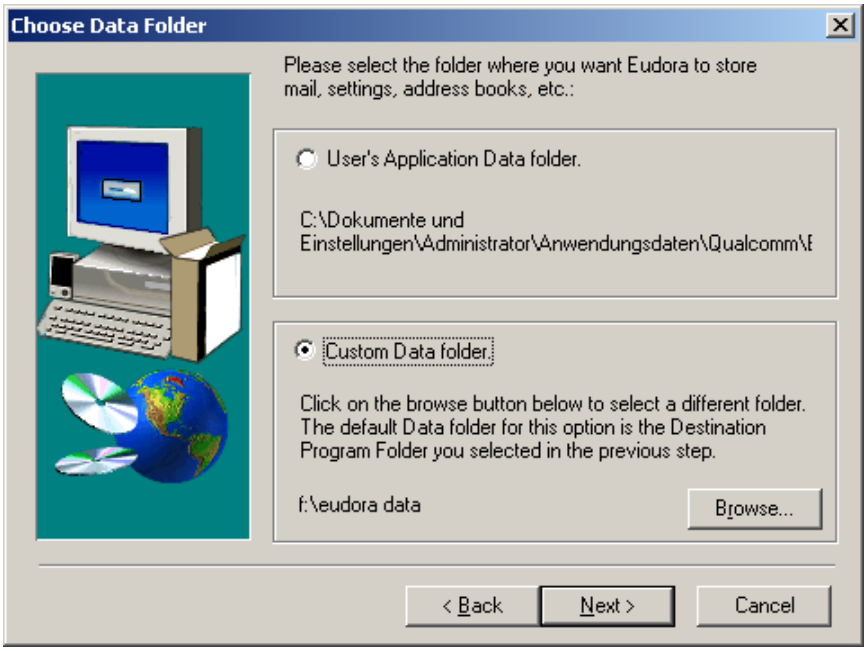
Abhilfe schafft da die Verwendung von PGP Disk und das Speichern der Maildaten auf einem verschlüsselten Laufwerk. Alle deine persönlichen Daten und Einstellungen werden dann auf einem verschlüsselten Bereich gespeichert und können nur nach Mounten dieses Bereichs gelesen werden. Eudora lässt sich ohne Zugriff auf diese Daten nicht einmal starten.

Wie mensch das einrichtet, erfährst du auf den nächsten Seiten.

Zurück zum Inhalt dieses Kapitels

Eudora Daten

Die beste Möglichkeit zur Wahl des Verzeichnisses, in dem deine ganzen Eudora Daten gespeichert werden sollen, hast du bei der Installation von Eudora. Bei der Installation von Eudora wirst du nach ein paar anderen Abfragen nach dem Verzeichnis gefragt, in dem deine Daten gespeichert werden sollen:



Wähle „Custom Data folder" (selbstgewähltes Verzeichnis) und gib das gewünschte Verzeichnis an. Mit „Browse" kannst du es in deinem Dateisystem suchen. Nun gibst du natürlich ein Verzeichnis auf deinem verschlüsselten Laufwerk an (das du vorher mounten musst, sonst siehst du es im Dateisystem nicht), im Beispiel hat es den Laufwerksbuchstaben F.

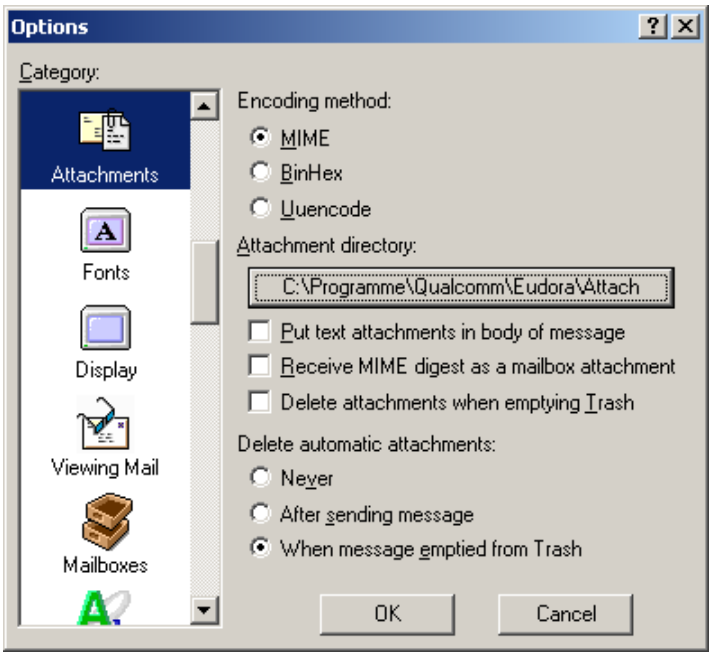
Alle deine persönlichen Maildaten werden dann in diesem Verzeichnis gespeichert, d.h. sie sind bei Wahl eines verschlüsselten Laufwerks verschlüsselt. Ohne vorheriges Mounten dieses Laufwerks kann Eudora dann nicht mehr gestartet werden, und das ist ja gut so.

Zurück zum Inhalt dieses Kapitels

Attachments

Du musst nach der Installation von Eudora extra angeben, wo die Anhänge (Attachments) deiner Mails gespeichert werden sollen.

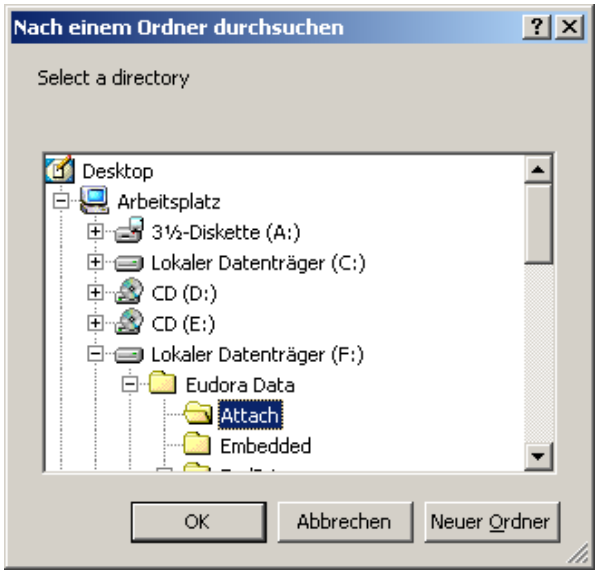
Starte Eudora und wähle im Menü den Punkt „Tools ⇨ Options“. Wähle dann im Fenster die Kategorie „Attachments“.



Drücke den Button bei „Attachment directory“.

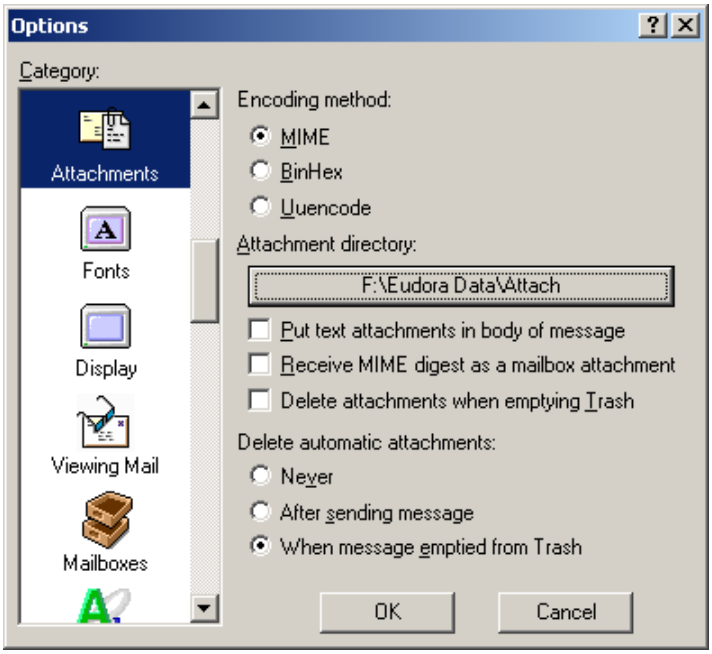
Zurück zum Inhalt dieses Kapitels

Gib dann ein Verzeichnis auf deinem verschlüsselten Laufwerk an (hier im Beispiel ist es Laufwerk F). Du kannst mit „Neuer Ordner“ auch ein neues Verzeichnis erstellen, drücke dann nach Markieren des Verzeichnisses den Button „OK“



Zurück zum Inhalt dieses Kapitels

Das von dir gewählte Verzeichnis erscheint nun auf dem Button.



Drücke den Button „OK“, die Anhänge (Attachments) deiner Mails werden ab sofort in diesem Verzeichnis gespeichert, d.h. sie sind verschlüsselt gespeichert.

Zurück zum Inhalt dieses Kapitels

7.7 Das Speichern von Outlook-Daten auf einem verschlüsselten Laufwerk

Auch bei Verwendung von Outlook als Mailprogramm kannst du deine Mails auf einer verschlüsselten Partition ablegen.

Die verschiedenen Versionen von Outlook haben leider auch völlig verschiedene diesbezügliche Einstellungsmöglichkeiten.

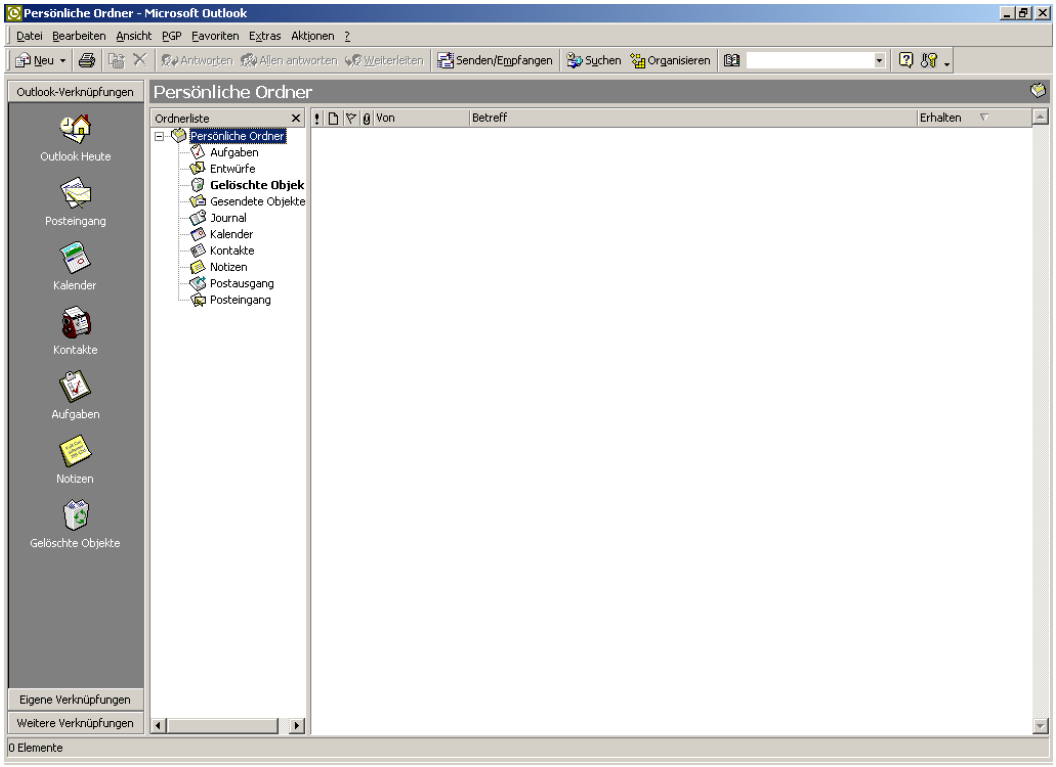
Eine Möglichkeit, die Mails verschlüsselt abzulegen, sollte aber immer funktionieren, und diese Vorgangsweise wird nachfolgend beschrieben.

Zurück zum Inhalt dieses Kapitels

Die Outlook-Ordner

Bei Outlook werden deine Mails in eigenen Ordnern abgelegt. Starte zur Prüfung deiner Ordner Outlook. Nach dem Starten von Outlook siehst du die Liste deiner Ordner im Fenster mit der Überschrift „Ordnerliste“.

Bei Office 2000 sieht das so aus:

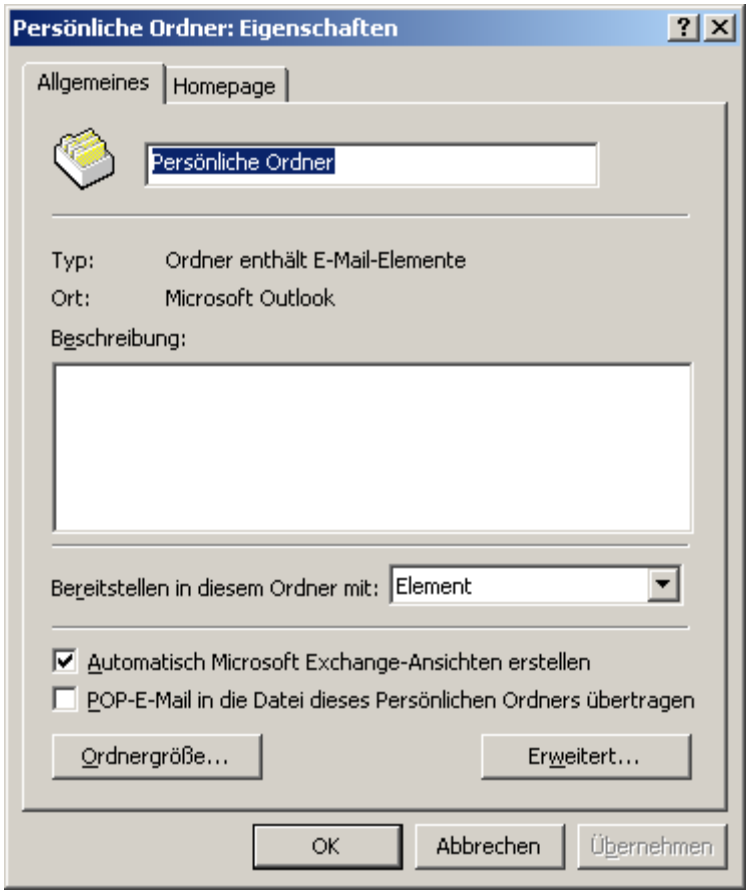


Nach der Installation von Outlook ist der Ordner „Persönliche Ordner“ bereits vorgegeben. Im Normalfall ist das auch bei dir der einzige Ordner, hast du weitere Ordner angelegt, verfahre mit diesen zusätzlichen Ordnern genau so wie bei „Persönlicher Ordner“.

Zurück zum Inhalt dieses Kapitels

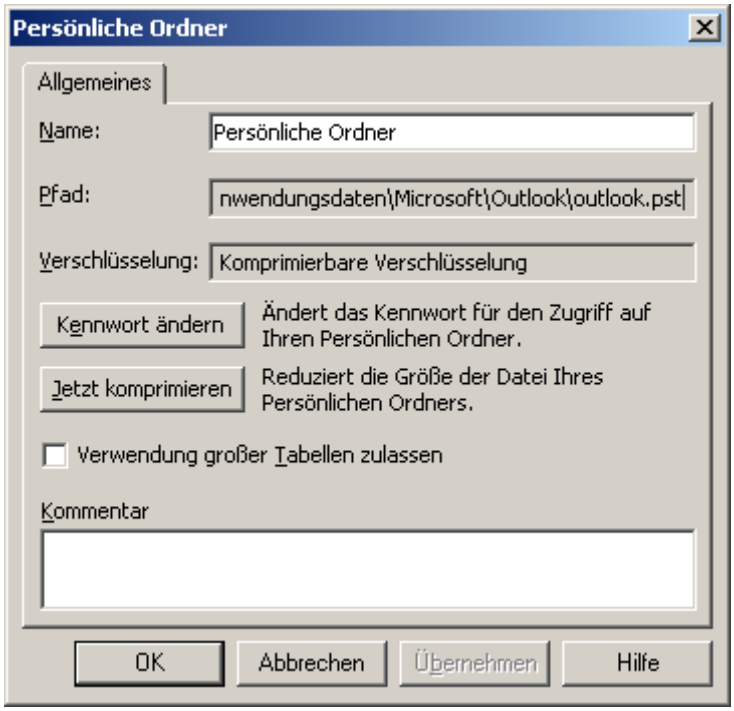
Markiere den Eintrag „Persönliche Ordner“ und drücke die rechte Maustaste. Im aufgehenden Kontextmenü wähle „Eigenschaften“.

Folgendes (oder ein ähnliches) Fenster wird geöffnet:



Zurück zum Inhalt dieses Kapitels

Drücke den Button „Erweitert“. In der Zeile „Pfad“ siehst du den Speicherort, an dem dein „Persönlicher Ordner“ gespeichert wird.

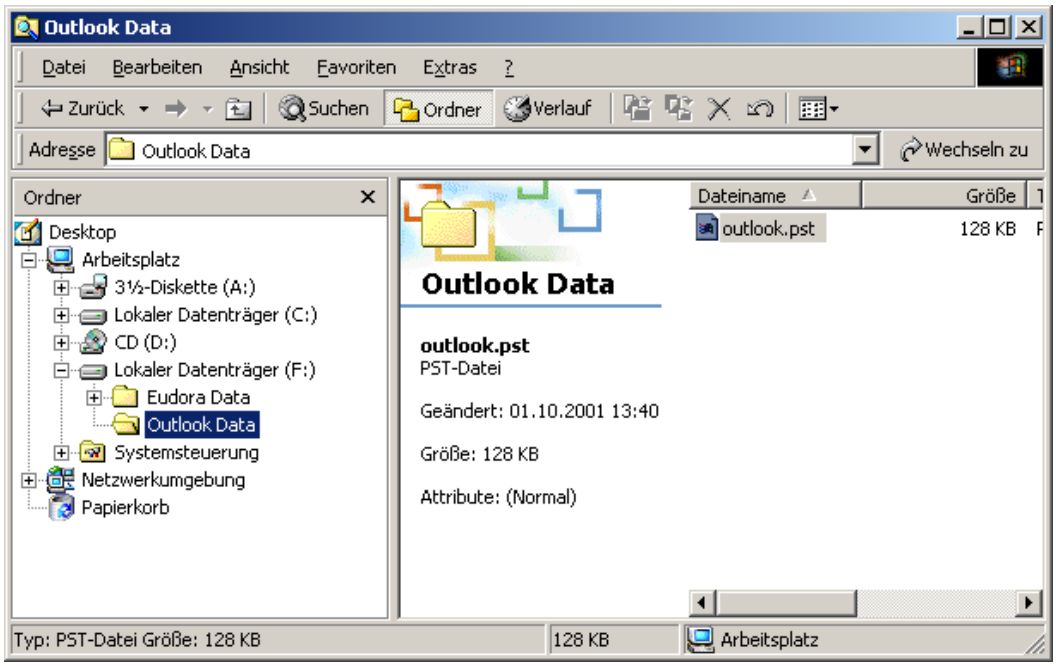


In diesem Beispiel lautet der Dateiname „outlook.pst“, links davon ist der gesamte Pfad angegeben.

Merke dir den Pfad und den Dateinamen (oder schreib sie dir auf) und drücke „Abbrechen“. Beende dann Outlook.

Zurück zum Inhalt dieses Kapitels

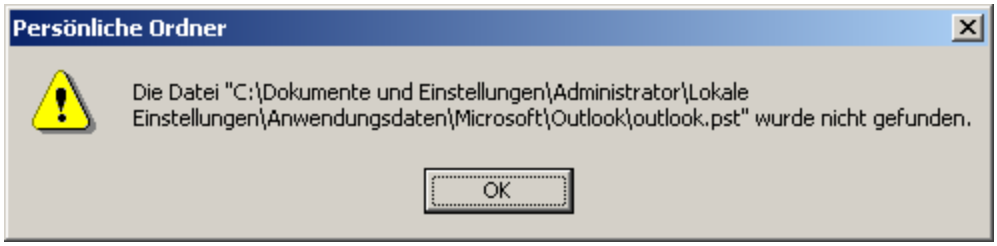
Starte nun den Windows Explorer und verschiebe die Datei mit deinem Ordner (im Beispiel die Datei „outlook.pst“ auf dein verschlüsseltes Laufwerk (durch „Ausschneiden“ und „Einfügen“ bzw. „Cut“ und „Paste“). Lege dazu wie im Beispiel einen eigenen Ordner dafür an.



Du siehst nun die Datei „outlook.pst“ auf dem verschlüsselten Laufwerk F im Ordner „Outlook Data“.

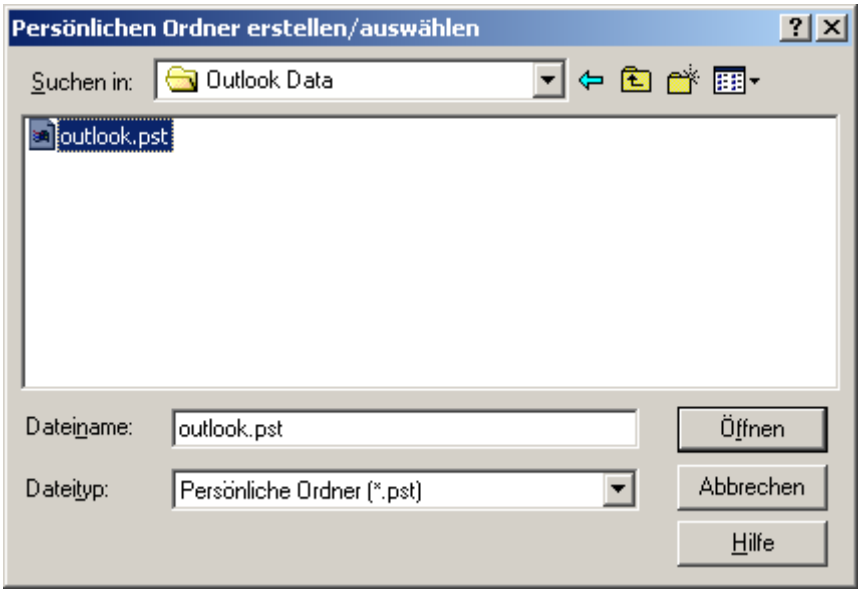
Zurück zum Inhalt dieses Kapitels

Starte nun wieder Outlook. Du erhältst gleich nach dem Start die Fehlermeldung, dass Outlook den Ordner nicht findet. Ist ja kein Wunder, wir haben ihn ja auch an einen anderen Ort verschoben.



Bestätige die Fehlermeldung durch Drücken von OK.

Anschließend musst du angeben, wo sich der Ordner jetzt befindet. Gib den Ordner auf dem verschlüsselten Laufwerk an, zu dem du die Datei „outlook.pst“ verschoben hast und markiere die Datei.



Drücke dann den Button „Öffnen“.

Zurück zum Inhalt dieses Kapitels

So, nun befinden sich deine Mails des „Persönlichen Ordners“ auf dem verschlüsselten Laufwerk. Überprüfen kannst du dies durch Wiederholen des zu Beginn beschriebenen Vorgangs.

Markiere den Eintrag „Persönliche Ordner“ in der Ordnerliste, zeige mit dem Mauszeiger darauf und drücke die rechte Maustaste. Wähle im sich öffnenden Kontextmenü den Eintrag „Eigenschaften“.

Im folgenden Fenster drücke den Button „Erweitert“. Du siehst nun bei der Pfadangabe dein verschlüsseltes Laufwerk mit dem von dir angelegten Ordner, in den du die Datei „outlook.pst“ verschoben hast.

Diesen Vorgang der Angabe des Speicherorts der Maildatei musst du aber nur 1 Mal durchführen, ab der nächsten Verwendung von Outlook funktioniert alles wieder von selbst, die Mails bleiben verschlüsselt, da sie sich weiterhin auf deiner verschlüsselten Partition befinden.

Zurück zum Inhalt dieses Kapitels

8 Zone Alarm (Firewall)

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Zone Alarm, einer Gratis-Firewall für Windows.

Sobald du mit dem Internet verbunden bist, können neugierige Menschen unter Umständen mit ein paar Tricks auf die Daten auf deinem Computer zugreifen, wenn er nicht dagegen abgesichert ist. Genauso könnten Programme, die auf deinem Computer installiert sind, unauffällig Informationen irgendwohin schicken.

Einen gewissen Schutz davor (aber wie immer keinen absolut unüberwindlichen) bieten sogenannte Firewalls, eine Gratis-Firewall für Windows ist Zone Alarm. Ganz besonders empfehlenswert ist so eine Firewall für alle BenutzerInnen von permanenten Inernetverbindungen (wie z.B. Chello u.a.), da sie meist über längere Zeiträume mit dem Internet verbunden sind.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Zone Alarm
- Die Verwendung von Zone Alarm

8.1 Die Installation von Zone Alarm

Du findest das Installationsprogramm von Zone Alarm auf der zugehörigen CD im Verzeichnis „Zone Alarm\Windows“. Leider gibt es dieses Programm nur für Windows.

Doppelklicke auf der CD auf die Datei zonalm26.exe, dann erscheint der Willkommenstext.

Zone Alarm\Windows\

zonalm26.exe

Drücke den Button „Next“.

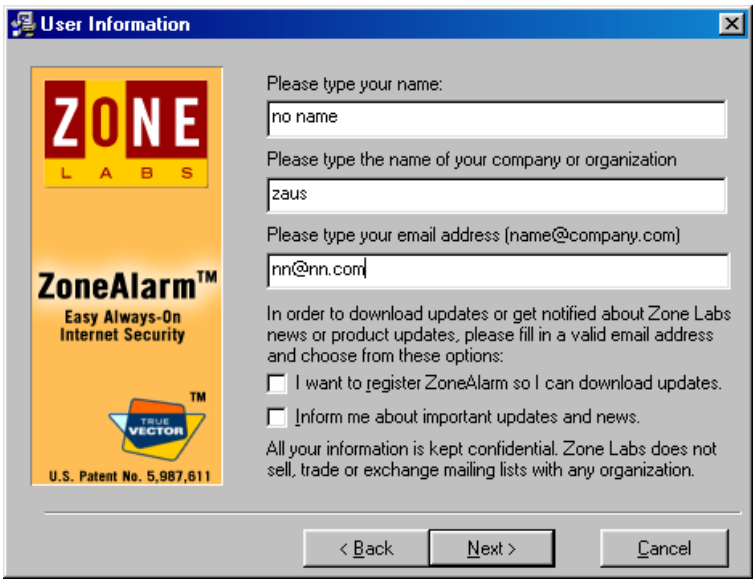
Zurück zum Inhalt dieses Kapitels

Dann folgen einige Informationen über die Systemvoraussetzungen, wo und wie du Hilfe bekommst und einiges mehr.

Drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Dann musst du deinen Namen, den Namen deiner Firma und deine E-Mail Adresse angeben.



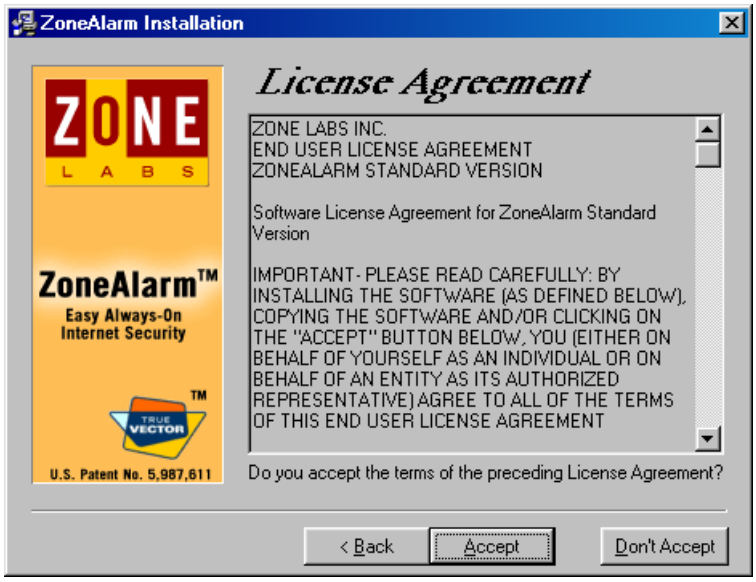
Hier antwortest du natürlich absolut wahrheitsgetreu ;-) mit einem Phantasienamen, einer Firma und einer Phantasieadresse, geht ja alles niemanden etwas an.

Auch das Kästchen mit „I want to register ZoneAlarm“ kannst du ruhig entmarkieren. Da ZoneAlarm ein Gratisprogramm ist, kannst du dir sowieso immer eventuell neuere Versionen aus dem Internet herunterladen.

Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

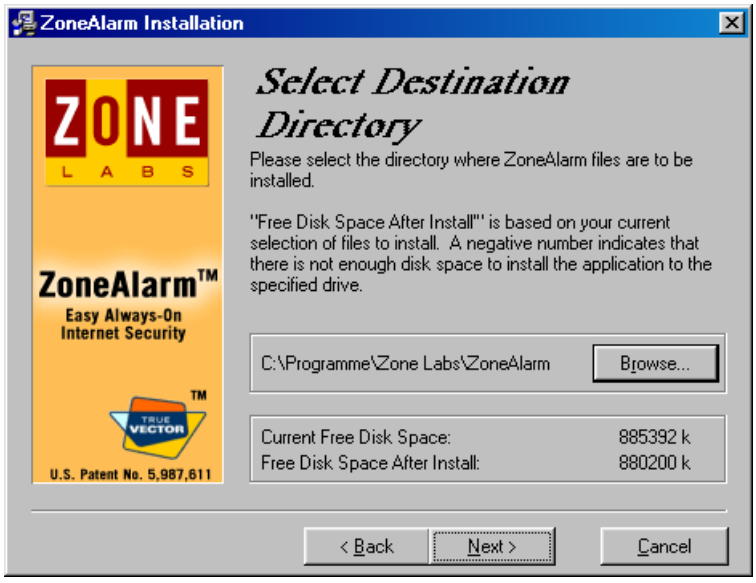
Dann erscheint die Lizenzvereinbarung.



Bestätige sie durch Drücken des Buttons „Accept“.

Zurück zum Inhalt dieses Kapitels

Dann kannst du dir das Installationsverzeichnis aussuchen, in das Zone Alarm installiert werden soll.



Nimm einfach das vorgeschlagenen Ordner oder gib einen anderen an. Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

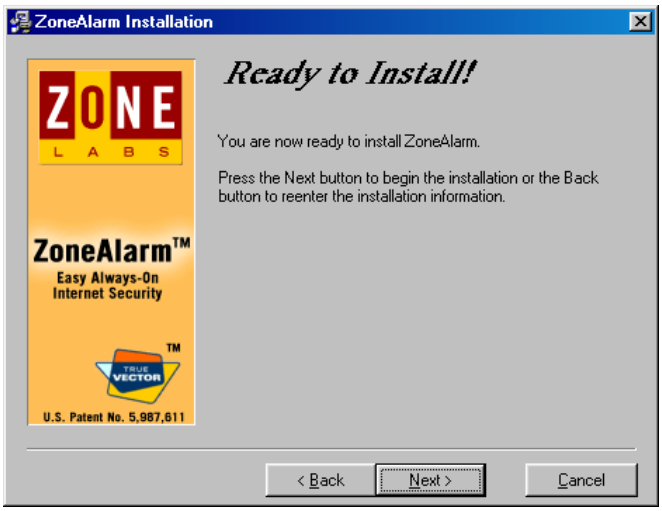
Dann wirst du gefragt, ob dein Webbrowser (also z.B. Microsoft Internet Explorer oder Netscape) die Erlaubnis erhalten sollen, sich ins Internet zu verbinden.

Da du natürlich auch weiterhin im Internet surfen willst, kannst du die vorgeschlagene Erlaubnis angekreuzt lassen. Drücke dann den Button „Next“.

Nach der Installation von ZoneAlarm musst du jedem anderen Programm, das mit dem Internet Verbindung aufnehmen will, ebenfalls die Erlaubnis geben, sich ins Internet zu verbinden, wenn du das beim jeweiligen Programm willst.

Zurück zum Inhalt dieses Kapitels

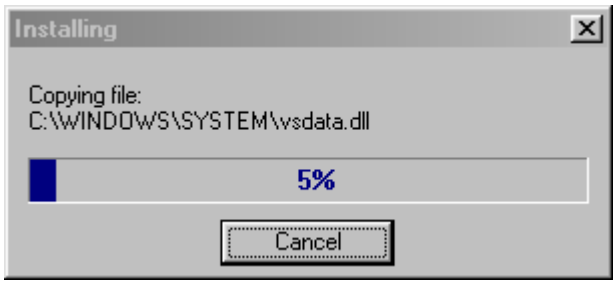
Nun wirst du noch informiert, dass das Installationsprogramm bereit zur Installation ist.



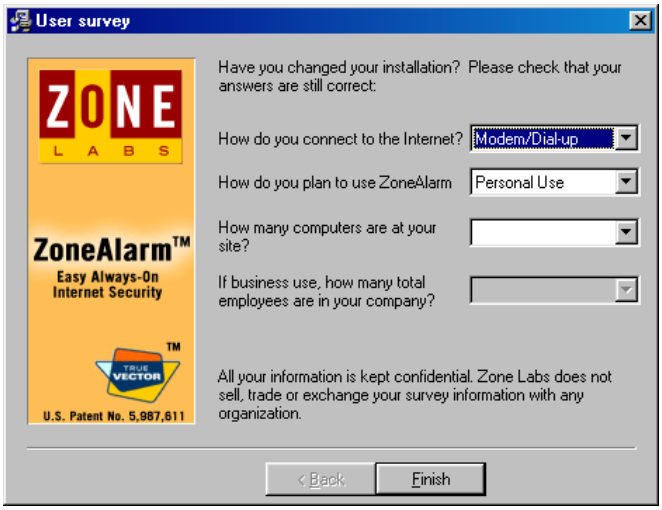
Bestätige durch Drücken des Buttons „Next“.

Zurück zum Inhalt dieses Kapitels

Während der Installation wird dir der Fortschritt der Installation angezeigt:



Nun wird von dir erbeten, noch einige Informationen anzugeben, wie z.B. wie du dich ins Internet verbindest, wie viele Computer du hast etc.

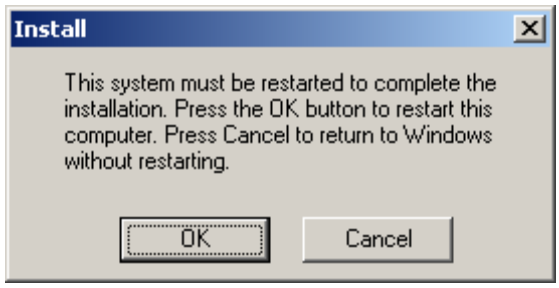


Da du vorher angegeben hast, lieber keine Informationen an die Fa. Zone Labs zu schicken, ist hier völlig egal, was angegeben ist. Auch wenn du die Version registrieren willst, kannst du einfach irgendwas angeben.

Drücke den Button „Finish“.

Zurück zum Inhalt dieses Kapitels

Meist musst du zum Abschluss der Installation deinen Computer neu starten. Wird das verlangt, mache das auch.

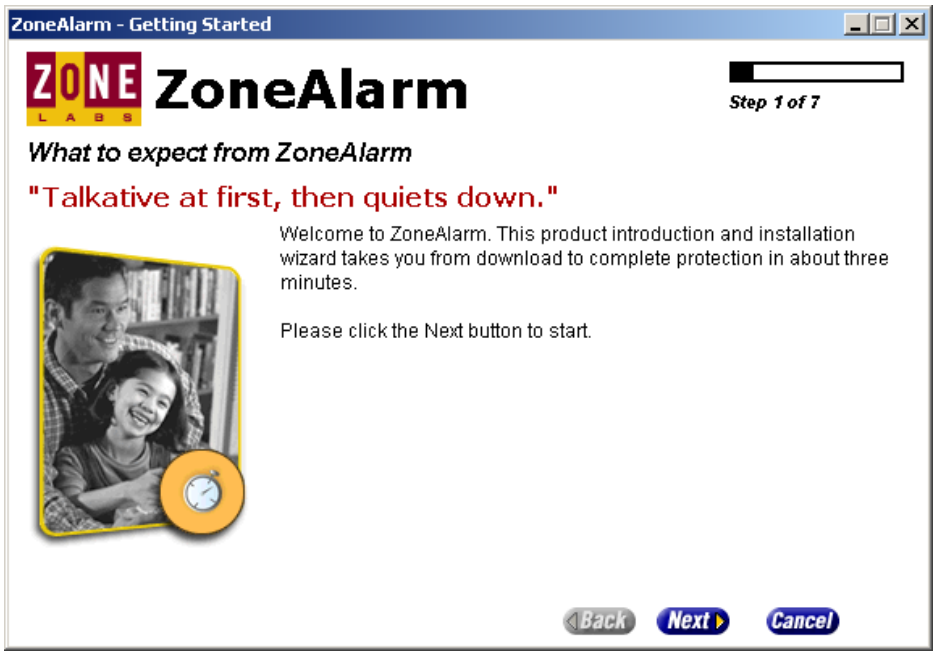


Drücke den Button OK. Der Computer wird neu gestartet.

Zurück zum Inhalt dieses Kapitels

Nach dem Neustart des Computers wird Zone Alarm automatisch gestartet.

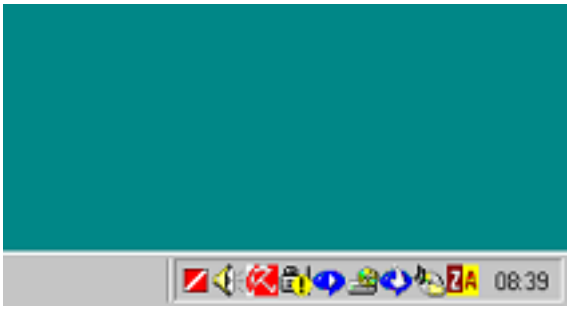
Beim Erststart erscheinen ein paar Einleitungsinformationen zu ZoneAlarm. Wenn du dich noch nie mit Firewalls beschäftigt hast, ist es vielleicht ganz interessant, die paar grundsätzlichen Infos zu lesen, du bekommst auch Hinweise zum Gebrauch von ZoneAlarm.



Drücke dich mit „Next“ durch die 7 Fenster. Beim 7. Fenster (Step 7) drücke den Button „Finish“.

Zurück zum Inhalt dieses Kapitels

Nach dem letzten Fenster schließt das Installationsprogramm. Du siehst nun am rechten unteren Rand deines Bildschirms das Symbol für das Programm, nämlich „ZA“ auf rot/gelbem Hintergrund.



Das bedeutet, dass nun ZoneAlarm im Hintergrund darauf achtet, dass niemand über das Internet in deinen Computer einbricht. Weiters achtet es darauf, dass sich nur Programme, denen du die Erlaubnis dazu gegeben hast, ins Internet verbinden.

Sendest du Daten ins Internet oder erhältst du Daten aus dem Internet (z.B. beim Surfen), ändert das Symbol während des Datenaustauschs sein Erscheinungsbild und wird ein Kästchen mit ein paar Strichen, die den Status des Datenverkehrs anzeigen (es ist das Kästchen rechts neben dem Regenschirm).

So siehst du auch optisch, wann ein Datenaustausch stattfindet.

Zurück zum Inhalt dieses Kapitels

8.2 Die Verwendung von Zone Alarm

ZoneAlarm wird nach der Installation automatisch bei jedem Start von Windows gestartet und wacht im Hintergrund auf den Datenverkehr zum und vom Internet.

Falls du einen lokalen Webserver auf deinem Computer installiert hast (z.B. den Personal Webserver von Microsoft), interpretiert ZoneAlarm auch die Verbindung zu diesem Webserver auf deinem eigenen Computer als Verbindung zum Internet und verhält sich auch genauso, also wäre es ein Webserver auf einem anderen Computer.

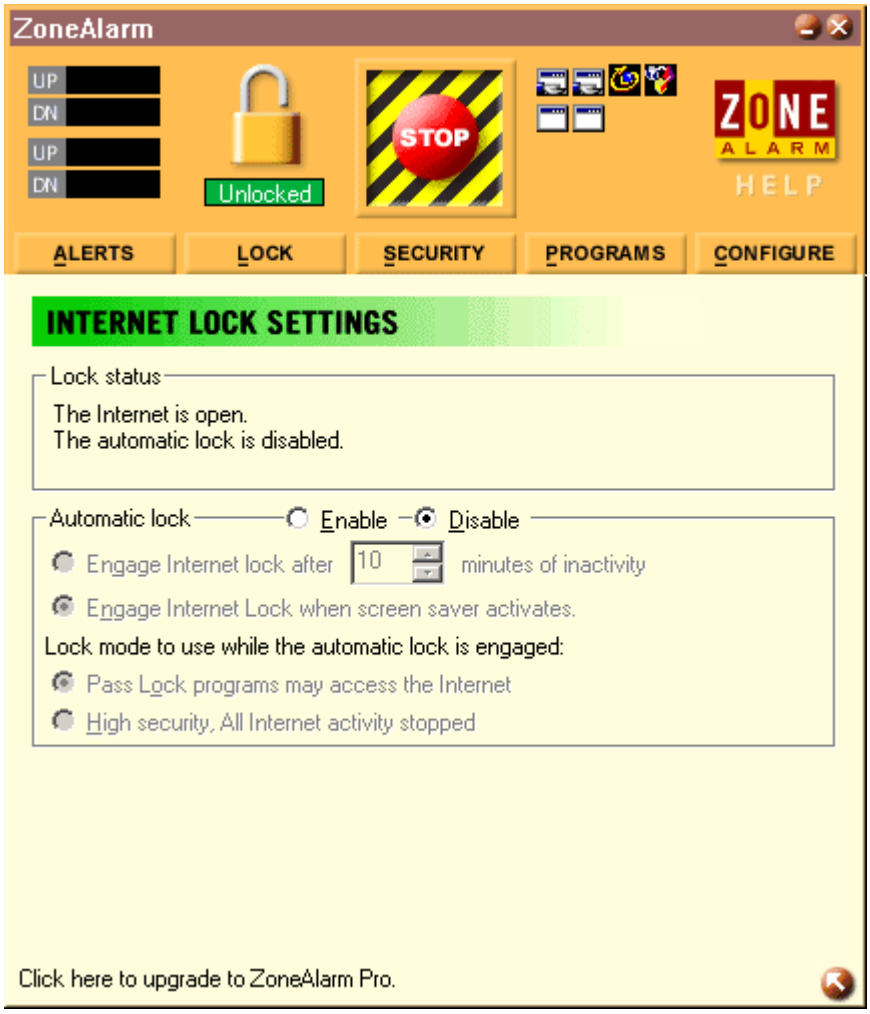
Auch diesen Verbindungen musst du deine Erlaubnis erteilen.

Du kannst, musst aber nicht, einige Einstellungen vornehmen. Wie das geht, erfährst du nachfolgend.

Zurück zum Inhalt dieses Kapitels

Einstellungen/Konfiguration

Starte das Programm im Start-Menü durch Wählen des Menüpunktes „Start ⇨ Programme ⇨ Zone Labs ⇨ ZoneAlarm“ oder doppelklicke auf das ZoneAlarm-Symbol am rechten unteren Rand deines Bildschirms. Folgendes Konfigurationsfenster erscheint.



Mit dem kleinen Pfeil rechts unten kannst du die Art der Anzeige bestimmen.

Zurück zum Inhalt dieses Kapitels

Du kannst hier verschiedene Dinge einstellen.

Alerts: z.B., ob du eine Warnmeldung erhalten willst, falls jemand versucht, deinen Computer übers Internet zu erreichen

Lock: z.B. ob die Verbindung zum Internet automatisch blockiert werden soll, wenn du eine Weile nichts am Computer gemacht hast

Security: die Höhe der Sicherheitsstufe

Programs: welche Programme in welcher Form Zugriff aufs Internet haben sollen etc. Hier kannst du auch zwischendurch mal Aufräumen und Programme entfernen, denen du mal die Erlaubnis gegeben hast.

Configure: z.B. ob ZoneAlarm automatisch beim Starten von Windows gestartet werden soll.

In Normalfall reichen aber die voreingestellten Standardeinstellungen.

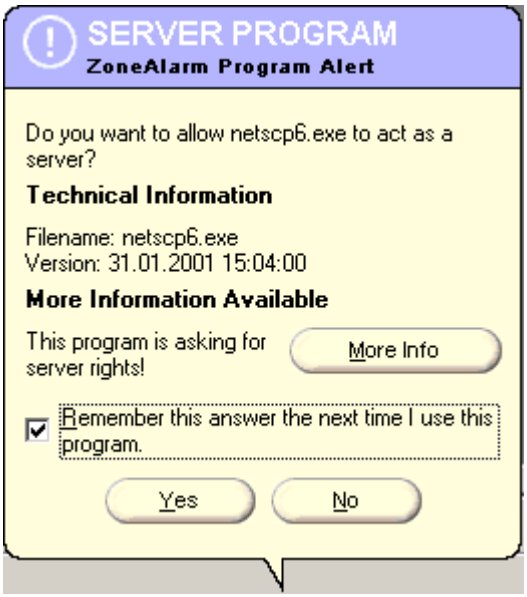
Zurück zum Inhalt dieses Kapitels

Erlaubnis für Programme, sich mit dem Internet zu verbinden

Startest du nach der Installation von ZoneAlarm zum ersten Mal ein Programm, dass sich mit dem Internet verbinden will, erhältst du automatisch eine Abfrage, ob du das zulässt oder nicht.

Es kann eine Abfrage sein, ob das Programm selbst Daten ins Internet schicken darf (als Server fungiert), oder Daten aus dem Internet laden darf.

Server: beim Starten von Netscape sieht das z.B. so aus:



Wenn du einfach „Yes“ drückst, wirst du bei der nächsten Verbindung wieder um Erlaubnis gefragt.

Wenn du vorher das Kästchen bei „Remember this answer the next time I use this program“ anhakst, erlaubst du diesem Programm ohne zukünftige Abfrage, sich mit dem Internet zu verbinden. Dieses Recht kannst du natürlich über die Konfiguration in „Programs“ jederzeit wieder entziehen.

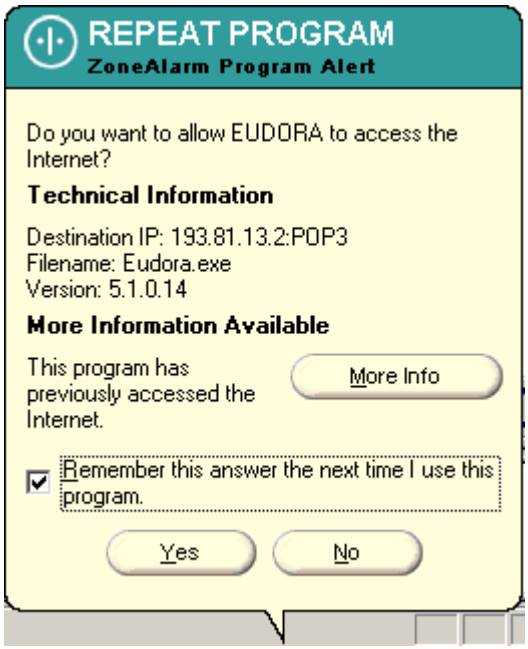
Du willst wahrscheinlich nicht jedes Mal, wenn du deinen Webbrowser startest, die Erlaubnis zur Verbindung geben, ein Webbrowser ist ja schließlich zum Surfen da. In diesem Fall ist es wesentlich bequemer, die Erlaubnis ohne dauernde Abfragen zu geben und das Kästchen anzuhaken.

Wenn mal ein Programm eine Verbindung ins Internet verlangt und du bist dir nicht sicher, was dieses Programm eigentlich tut, probier's einfach mal mit einem „No".

Wenn dann irgendetwas nicht funktioniert, was du brauchst, kannst du beim nächsten Verbindungsversuch noch immer mit einem „Yes" zustimmen.

Zurück zum Inhalt dieses Kapitels

Beim Starten von Eudora sieht es sehr ähnlich aus:



Auch hier gilt: mit Eudora willst du ja immer deine Mails erhalten und Mails verschicken. Es wäre daher etwas mühsam, jedes Mal extra die Erlaubnis geben zu müssen.

Kreuze also hier auch das Kästchen bei „Remember this answer the next time I use this program“ an und bestätige mit „Yes“ die Erlaubnis.

Bei anderen Programmen kannst du von Fall zu Fall entscheiden, ob du überhaupt die Erlaubnis gibt’s, eine einmalige oder grundsätzliche Erlaubnis gibst oder einem Programm verbietest, sich mit dem Internet zu verbinden.

Im Zweifelsfall die Erlaubnis verweigern („No“ drücken) und mal sehen, was passiert.

Wenn dann irgendetwas nicht funktioniert, was du brauchst, kannst du beim nächsten Verbindungsversuch noch immer mit einem „Yes“ zustimmen.

Zurück zum Inhalt dieses Kapitels

Versucht ein anderer Computer, mit deinem Computer Verbindung aufzunehmen, erhältst du eine Warnung mit der weltweit eindeutigen IP-Adresse des kontaktsuchenden Computers. Diese Verbindungen werden natürlich von ZoneAlarm verhindert, dein Computer verhält sich bei Verwendung von ZoneAlarm oder einer anderen Firewall in so einem Fall ganz still, er meldet sich auf die Anfrage einfach nicht.

Und keine Panik, erstens bist du durch die Firewall geschützt, und außerdem bedeutet die Meldung höchstwahrscheinlich nicht, dass jemand versucht hat, in deinen Computer einzubrechen. Aber auch das könnte natürlich mal passieren. Es könnte aber z.B. ein Programm deines Providers sein, das die Information benötigt und sonst nichts Böses im Sinn hat.

Wenn du bei dieser Warnung den Button „More Info“ drückst, bekommst du ausführliche Infos z.B. darüber, dass du dir auch in diesem Fall keine Sorgen machen musst, wenn du ZoneAlarm verwendest, und was hinter so einem Kontaktaufnahmeversuch stehen könnte.

Wenn dich diese Warnhinweise nicht interessieren bzw. nerven, kannst du sie durch Markieren von „Don’t show this dialog again“ ausschalten. Im Logfile von ZoneAlarm, dessen Namen im Konfigurationsfenster unter „Alerts“ angegeben ist, wird in jedem Fall so ein Kontaktaufnahmeversuch vermerkt.

Bestätige die Warnung durch Drücken von „OK“.

Zurück zum Inhalt dieses Kapitels

9 Window Washer

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Window Washer, einem kostenpflichtigen Programm zum Aufräumen von Datenschrott (die Version für MacOS heisst MacWasher).

Vor allem Windows-Programme haben die Angewohnheit, eine Vielzahl von temporären Dateien anzulegen, die teilweise nach Beenden des Programms wieder „gelöscht“ werden (siehe aber dazu Kapitel Gelöschte Daten).

Im gesamten System des Computers werden von Programmen Informationen abgelegt. Z.B. welche Internetseiten du geladen hast, welche Bilder du angezeigt bekommen hast, welche Dateien du zuletzt geöffnet hast, wo du im Internet herumgesurft bist etc.

Im Fall einer Internetverbindung dienen diese Informationen auch dazu, dir das nächste Mal eine Internetseite schneller auf den Bildschirm zaubern zu können. Der Nachteil daran ist, dass auch neugierige Menschen begierig darauf sind zu erfahren, was du mit deinem Computer so treibst.

Abhilfe bietet das Programm „Window Washer“, das diesen Datenschrott aufräumt. Nachfolgend findest du eine Anleitung zur Installation und einen kurzen Überblick, wie mensch das Programm verwendet.

Dieses Programm gibt es für die Betriebssysteme Windows und MacOS, nachfolgend wird das Programm Window Washer für Windows beschrieben.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Window Washer
- Die Verwendung von Window Washer
- Custom Items/Plugins – Gratis-Zusatzprogrämmchen zu Window Washer

9.1 Die Installation von Window Washer

Du findest das Installationsprogramm einer 30-Tage-Testversion von Window Washer (und von MacWasher für MacOS) auf der zugehörigen CD im Verzeichnis „Window Washer\Windows“. Dieses Programm gibt’s nur für Windows und MacOS.

In diesem Kapitel ist die Installation mit der älteren Version 4.0 beschrieben, bei der Version 4.1 funktioniert die Installation aber ganz genauso.

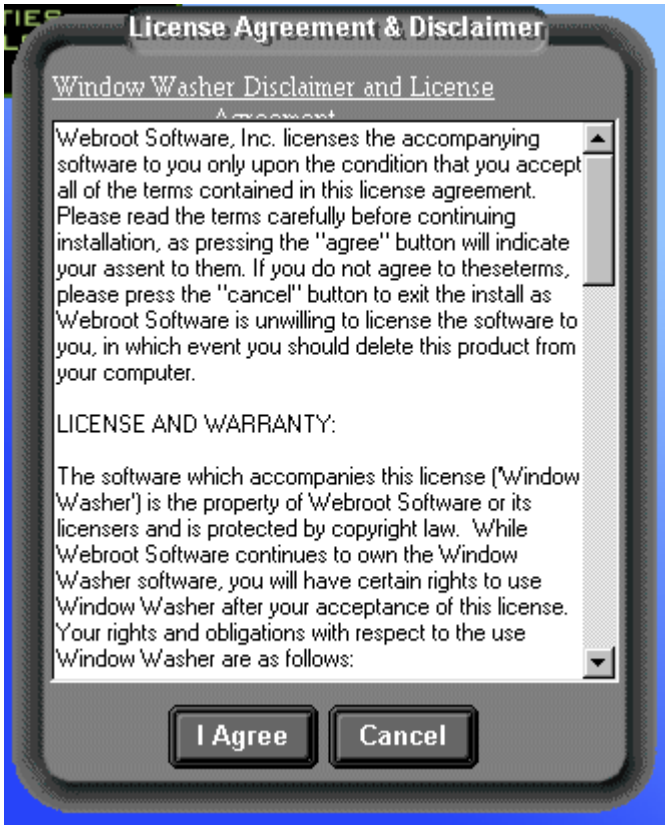
Window Washer\Windows\4.1

wwinstall.exe

Auf der CD befindet sich nur eine 30-Tage-Testversion. Nach Ablauf der 30 Tage müsstest du das Programm bezahlen. Window Washer und MacWasher kosten jeweils ca. USD 30. Und ich meine, dass dieses Programm das verlangte Geld Wert ist.

Zurück zum Inhalt dieses Kapitels

Doppelklicke auf der CD auf die Datei reg3ww.exe. dann erscheint gleich mal das Lizenzvereinbarungsfenster:



Drücke den Button „I Agree“.

Zurück zum Inhalt dieses Kapitels

Dann kannst du dir das Verzeichnis aussuchen, in welches das Programm installiert wird.

Nimm einfach das vorgeschlagene Verzeichnis und drücke nur den Button „Install“, du kannst aber natürlich auch ein anderes Verzeichnis wählen.

Zurück zum Inhalt dieses Kapitels

Nun startet die Installation, die nach kurzer Zeit beendet ist.

Wenn du Window Washer gleich starten willst, lasse den Punkt „Run Window Washer Now“ gleich markiert, die „Release Notes“ beinhalten bei allen Programmen immer die neuesten Infos, die in der Hilfe nicht zu finden sind. Wenn’s dich interessiert, lasse auch diesen Punkt angehakt.

Bestätige die Meldung durch Drücken des Buttons „Exit“. Du findest dann auf deinem Desktop ein Wischer-Symbol, das ist das Symbol des Programms Window Washer. Auch im Startmenü ist das Programm natürlich zu finden.

Zurück zum Inhalt dieses Kapitels

9.2 Die Verwendung von Window Washer

Starte das Programm durch Doppelklick auf das Wascher-Symbol auf deinem Desktop.

Du siehst im rechten Teil des Fensters die aktuellen Einstellungen, was alles gelöscht wird.

Wenn du z.B. nicht willst, dass dein Papierkorb jedes Mal ausgeräumt und gelöscht wird, entmarkiere das entsprechende Feld bei „Recycle Bin“.

Wenn du nicht willst, dass die Listen der zuletzt verwendeten Dateien im Dateimenü z.B. aus Microsoft Word verschwinden, entmarkiere den Punkt „MS-Office Tracks“, usw.

Zurück zum Inhalt dieses Kapitels

Es kann passieren, dass du nach dem Starten von Window Washer eine Fehlermeldung siehst, z.B. bei Verwendung von Mozilla (Netscape etc.) „Failed to open the Mozilla registry file...“. Ist aber nicht weiter allzu tragisch, einfach mit „OK“ bestätigen. Das sind kleine Schwächen von Window Washer, er funktioniert für manche Browser einfach noch nicht.

Wähle dann auf der linken Seite den Menüpunkt „Wash Options“.

Wenn du z.B. nicht willst, dass Window Washer nach jedem Start von Windows geladen wird, entmarkiere den Punkt „Load at Windows Startup“. Das automatische Laden des Programms macht nur Sinn, wenn du einstellst, dass du z.B. jeden Tag aufräumen willst oder ähnliches.

Wirst du das Programm sowieso immer manuell starten und dann aufräumen, brauchst du das automatische Laden nicht.

Zurück zum Inhalt dieses Kapitels

Eine wichtige Einstellung ist, was mit den gelöschten Informationen passieren soll. Was in PGP „Wipe“ heißt, heißt hier „Bleach“, nämlich das mehrmalige Überschreiben der gelöschten Bereiche, damit sie auch mit dem vorhandenen Restmagnetismus auf der Festplatte nicht mehr wiederhergestellt werden können.

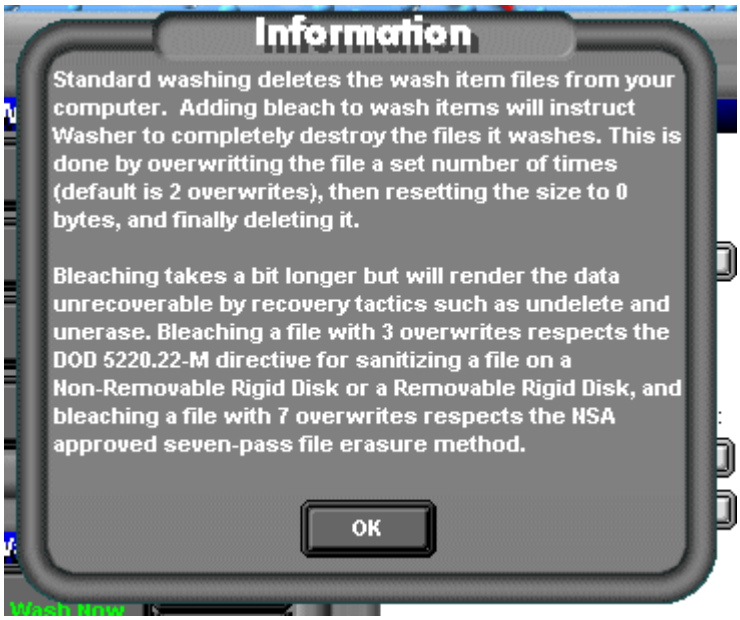
Das Waschen dauert zwar dann länger, dafür sind die Informationen wirklich unwiederherstellbar gelöscht. Entscheide selbst, ob du diese Möglichkeit in Anspruch nimmst oder nicht, empfohlen ist sie auf jeden Fall.

Im Menü „Wash Options“ siehst du auf der rechten Seite den Punkt „Add Bleach to Wash“. Wenn du ein sicheres Löschen willst, markiere das Kästchen daneben.

Zurück zum Inhalt dieses Kapitels

Drücke dann den kleinen Button „Info“ neben „Add Bleach to Wash“. Du kannst dann einstellen, wie oft die gelöschten Bereiche überschrieben werden sollen.

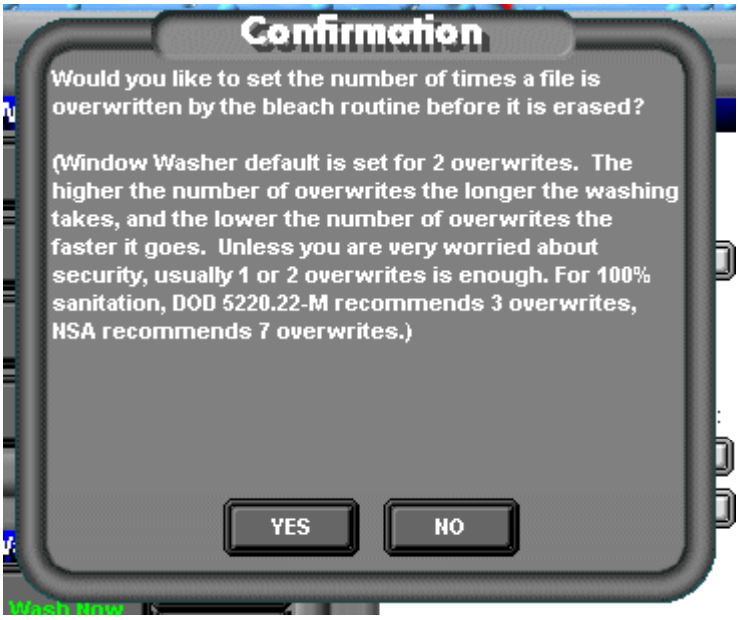
Zuerst erhältst du eine kleine Info zum Löschen mit „Bleach“:



Drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Dann musst du nochmals bestätigen. Der Text klärt dich über diverse Empfehlungen auf, wie oft die gelöschten Bereiche überschrieben werden sollen.



Drücke den Button „YES“.

Zurück zum Inhalt dieses Kapitels

Dann kannst du angeben, wie oft die gelöschten Bereiche überschrieben werden sollen, standardmäßig ist hier zweimaliges Überschreiben eingestellt, du kannst einen höheren Wert angeben (3 ist sicher, 7 ist ganz sicher).

Wie du aber vorher informiert wurdest, dauert das Waschen umso länger, je höher dieser Wert ist. Entscheide selbst und probier's einfach aus. Hier im Beispiel wählen wir dreimaliges Überschreiben.

Drücke nach der Eingabe des Wertes den Button „OK".

Zurück zum Inhalt dieses Kapitels

Starte dann den Waschvorgang durch Drücken des Buttons „Wash Now“. Und schon geht’s los, das Saubermachen deiner Festplatte. Wenn du den Wasch-Vorgang beobachtest, wirst dich wundern, was da alles angelegt worden ist und jetzt gelöscht wird.

Du kannst den Waschvorgang durch Drücken von „Stop“ unterbrechen, z.B. wenn es dir zu lange dauert.

Zurück zum Inhalt dieses Kapitels

Nach dem Ende des Waschvorgangs drücke „Close“ am rechten oberen Rand des Fensters.

Zurück zum Inhalt dieses Kapitels

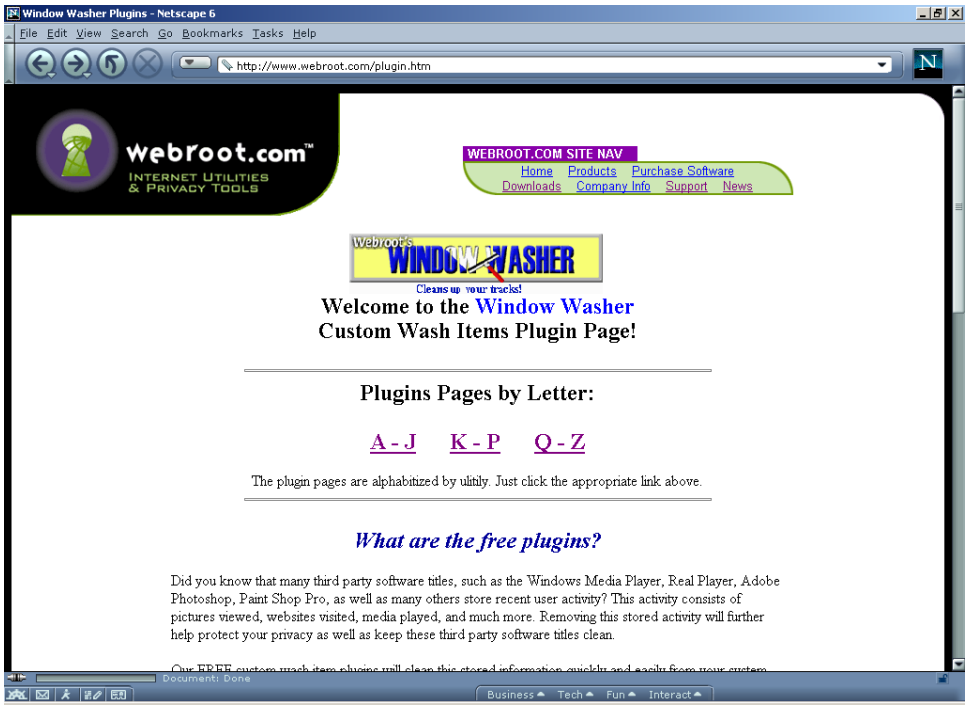
9.3 Custom Items/Plugins

Auf der Webseite der Fa. Webroot kannst du dir gratis kleine Prográmmchen herunterladen, die den Datenmüll anderer Programme als die ohnehin im Programm beinhalteten aufräumen.

Du findest diese Zusatzprogramme unter

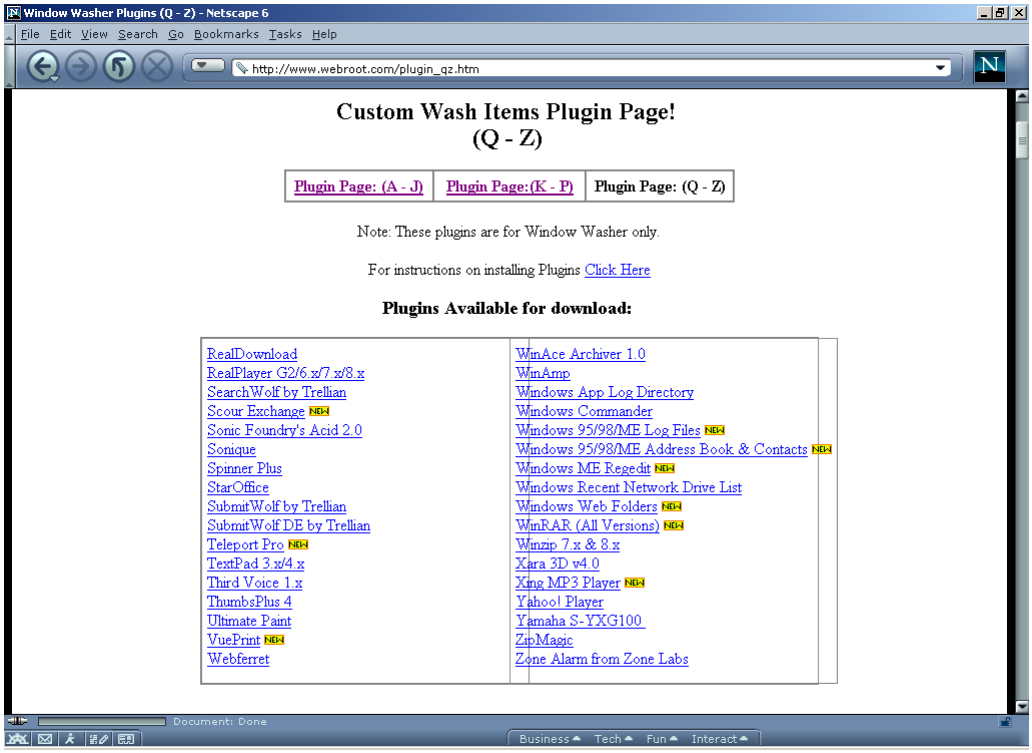
http://www.webroot.com/plugin.htm

in alphabetischer Reihenfolge.



Zurück zum Inhalt dieses Kapitels

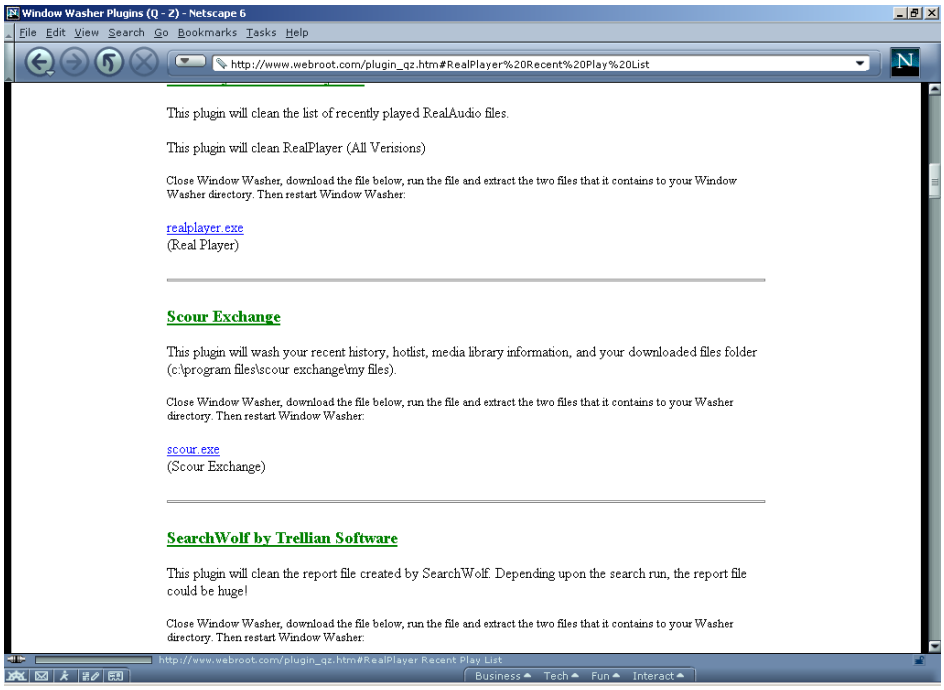
Als Beispiel wird hier das Plugin (Zusatzprogramm) für den Real Player heruntergeladen und installiert. Du findest dieses Plugin auf der Plugin Page Q-Z. Wähle den Link Q-Z.



Wähle den Link RealPlayer G2/6.x/7.x/8.x, du landest dann bei einer Kurzbeschreibung und der Datei zum Herunterladen.

Zurück zum Inhalt dieses Kapitels

Klicke auf die Datei realplayer.exe und lade die Datei auf deine Festplatte.



Zurück zum Inhalt dieses Kapitels

Starte dann das heruntergeladene Programm durch Doppelklick im Windows Explorer.

Bestätige im Fenster, das dir mitteilt, dass das Plugin installiert wird, durch Drücken des Button „Next“

Zurück zum Inhalt dieses Kapitels

Nun musst du angeben, in welchem Ordner sich das Programm Window Washer befindet.

Der richtige Ordner ist meist schon vorgeschlagen, wenn du eine englische Windows Version hast. Hast du das Programm in einen anderen Ordner installiert, gib hier den richtigen Ordner an (bei der deutschen Windows Version ist das dann meist c:\programme\washer).

Drücke nach Eingabe des Ordners den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Gleich darauf erscheint die Erfolgsmeldung der Installation.

Bestätige das Fenster durch Drücken des Buttons „Finish“.

Es erscheint dann noch eine Information zum gerade installierten Plugin mit einer Beschreibung und Tipps zur Handhabung. Empfehlenswert ist, diese Hinweise zu lesen, sie ersparen späteren Ärger.

Die Fa. Webroot übernimmt übrigens keinerlei Garantie, dass diese Plugins auch funktionieren, sie tun das aber fast immer. Schließe nun das Info-Fenster.

Zurück zum Inhalt dieses Kapitels

Starte dann nochmals den Window Washer. Du siehst nun beim Menüpunkt „Custom Wash Items“ auch „RealPlayer“ in der Liste, einige Plugins wurden im Beispiel schon vorher installiert:

Nun wird auch der Datenschrott, den das Programm RealPlayer produziert, beim Waschen aufgeräumt. Das Kästchen muss dazu angehakt sein.

Zurück zum Inhalt dieses Kapitels

10 JAP (Java Anon Proxy)

Überblick

In diesem Kapitel erfährst du Näheres zum Programm JAP, einem derzeit noch kostenlosen Programm zum anonymen Surfen.

Das Problem bei einer Verbindung zum Internet ist, dass jederzeit rückverfolgbar ist, welcher Computer was wann getan hat (z.B. welche Webseiten du aufgerufen hast). Es wird also eine Anonymität vorgegaukelt, die in der Realität nicht existiert.

Du findest Beschreibungen zu folgenden Bereichen:

10.1 Was ist JAP?

Hier ein Text aus der offiziellen Beschreibung von JAP von der JAP-Homepage, die im Internet unter http://anon.inf.tu-dresden.de/ zu finden ist:

„Mit dem Java Anon Proxy (JAP) ist es möglich, Webseiten unbeobachtbar aufzurufen. Das bedeutet, dass weder der angefragte Server noch ein Lauscher auf den Verbindungen mitbekommt, welcher Benutzer welche Webseite aufgerufen hat.

Diese Funktion wird dadurch erreicht, dass die Kommunikationsverbindung nicht direkt an den Webserver geschickt wird, sondern über eine sogenannte Mix Proxy Kaskade geschickt wird.

Da viele Benutzer gleichzeitig den Anonymitätsdienst nutzen, werden die Internetverbindungen jedes Benutzers unter denen aller anderer Benutzer versteckt: Jeder Benutzer könnte der Urheber einer Verbindung gewesen sein. Niemand, kein Außenstehender, kein anderer Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen ein bestimmter Benutzer hat.

Im Regelfall werden in einer Kaskade mindestens drei Mix Proxies arbeiten, die von unabhängigen Institutionen betrieben werden und die in einer Selbstverpflichtung erklären, dass sie weder Log-Files über die transportierten Verbindungen speichern, noch mit den anderen Mix Proxy Betreibern Daten austauschen, die dazu führen könnten, dass ein Benutzer von JAP enttarnt wird.

Unabhängige Prüfstellen überzeugen sich im Namen der JAP-Benutzer davon, dass die Selbstverpflichtung tatsächlich eingehalten wird.“

Kurz gesagt, deine Internetverbindung muss über diese eigenen Server gehen, diese Computer mixen alle IP-Adressen unter den aktuellen BenutzerInnen durcheinander, so ist nicht mehr nachvollziehbar, wer was getan hat.

Der Nachteil daran ist, dass die Schnelligkeit der Internet-Verbindung von diesen Servern abhängt, was die Verbindung derzeit ziemlich langsam macht.

Zurück zum Inhalt dieses Kapitels

10.2 Die Installation von JAP

JAP benötigt als Java-Programm eine aktuelle Version der Java-Umgebung (des Java Runtime Environments – JRE).

Um in Windows eine aktuelle Version der JAVA-Umgebung zu installieren, doppelklicke auf das Installationsprogramm, es befindet sich auf der CD im Ordner „JAP\Windows\Java JRE“. Doppelklicke auf die Datei „jre.exe“. Die Java-Umgebung wird dann fast ohne weitere Abfrage installiert.

JAP\Windows\Java JRE

jre.exe

JAP ist ein Java-Programm. Es benötigt daher die richtige Java-Installation, um normal arbeiten zu können. Beachte die Hinweise auf der JAP-Webseite unter: http://anon.inf.tu-dresden.de/

Von dort kannst du dir auch die jeweils neuesten Versionen von JAP herunterladen. Da auf der angegebenen Webseite eine Vielzahl von Versionen und Hilfestellungen angeboten werden, haben wir nicht alle Installationsprogramm-Versionen auf der CD gespeichert, einfach auf http://anon.inf.tu-dresden.de/ nachsehen und das Gewünschte/Erforderliche runterladen.

Zurück zum Inhalt dieses Kapitels

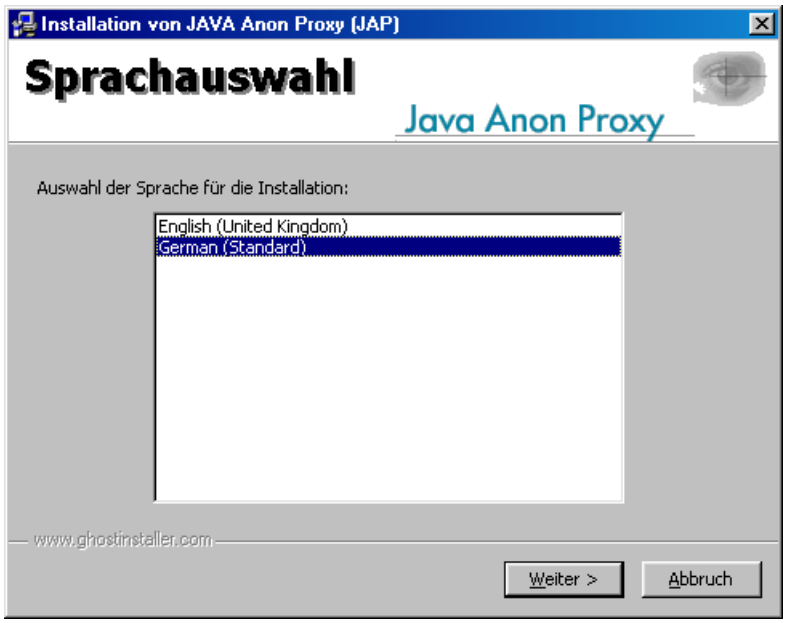
Das Installationsprogramm von JAP selbst findest du auf der CD im Verzeichnis „JAP“ in den Unterordnern für die Betriebssysteme Windows, MacOS, OS/2 und Unix (z.B. für Linux).

Doppelklicke auf der CD auf jeweilige Installationsprogramm, für Windows ist das die Datei setup.exe. Es erscheint dann zuerst mal die Sprachauswahl.


JAP\Windows (MacOS, Unix)

setup.exe

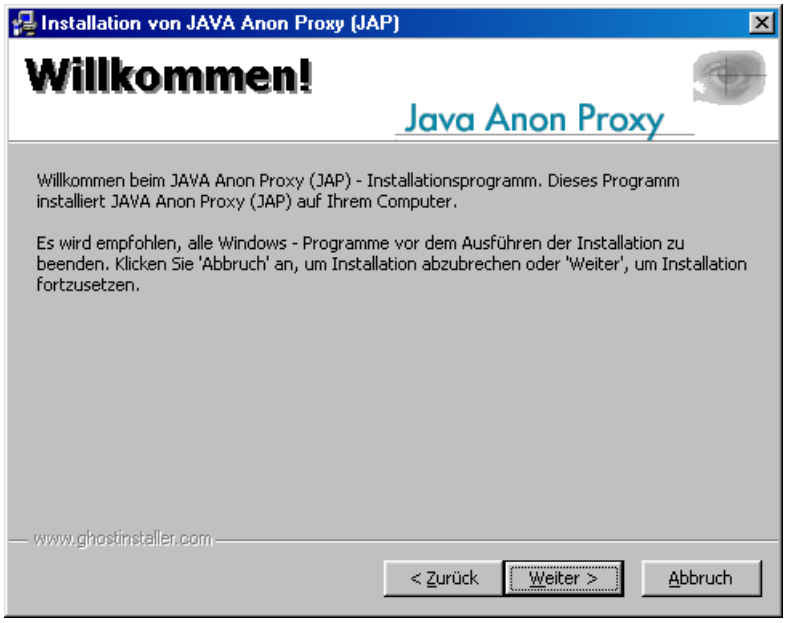
Zu Beginn kannst du dir die Installationssprache auswählen:



Such dir eine Sprache aus (hier im Beispiel wählen wir German) und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

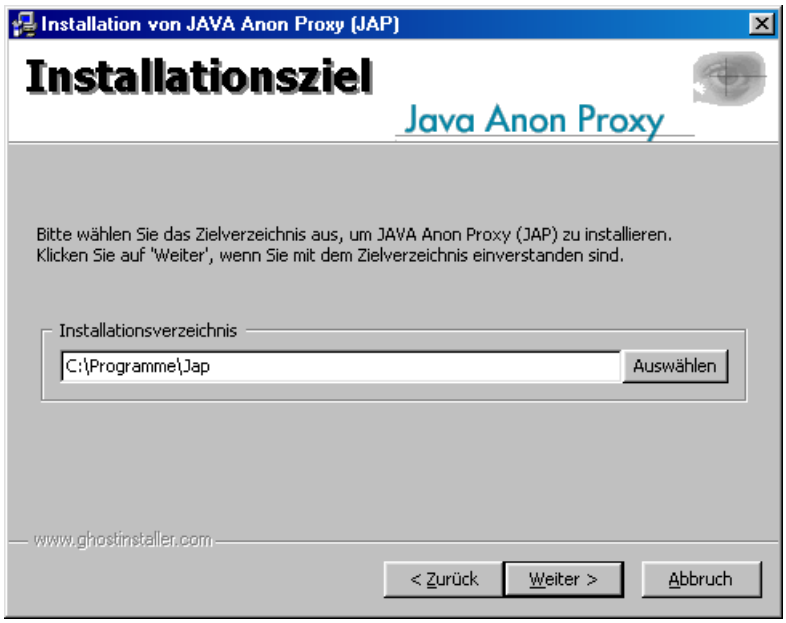
Dann siehst du ein Willkommensfenster.



Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann kannst du das Installationsverzeichnis (hier Installationsziel genannt) angeben, in welches das Programm installiert werden soll:



Nimm einfach das vorgeschlagene Verzeichnis oder gib ein anderes an. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du noch angeben, unter welchem Namen das Programm im Start-Menü eingetragen werden soll.

Nimm einfach den vorgeschlagenen Namen oder wähle einen anderen. Drücke dann den Button „Weiter“.

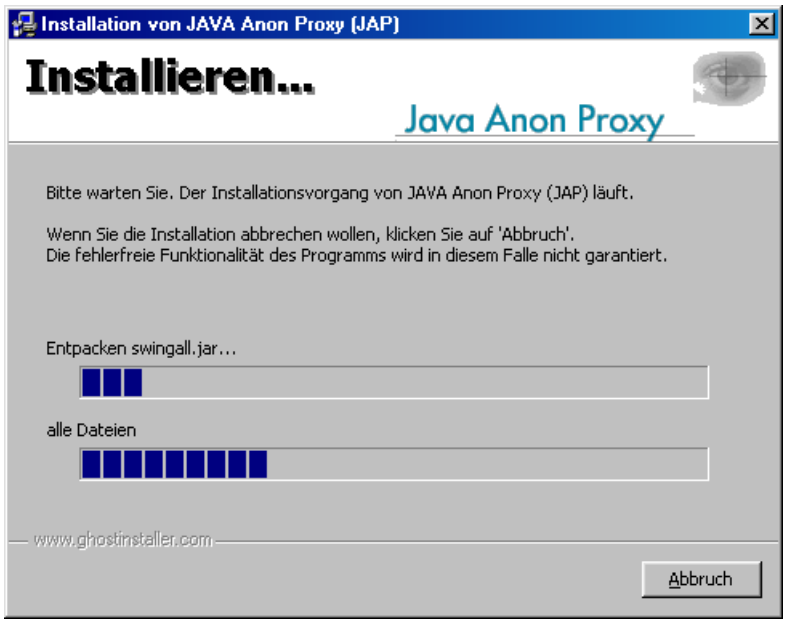
Zurück zum Inhalt dieses Kapitels

Dann wirst du noch informiert, dass das Programm bereit für die eigentliche Installation ist.

Bestätige durch Drücken des Buttons „Weiter“.

Zurück zum Inhalt dieses Kapitels

Während der Installation wirst du über den Status der Installation informiert:



Zurück zum Inhalt dieses Kapitels

Nach dem Ende des Installationsvorgangs wirst du auch darüber informiert:

Bestätige die Meldung durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

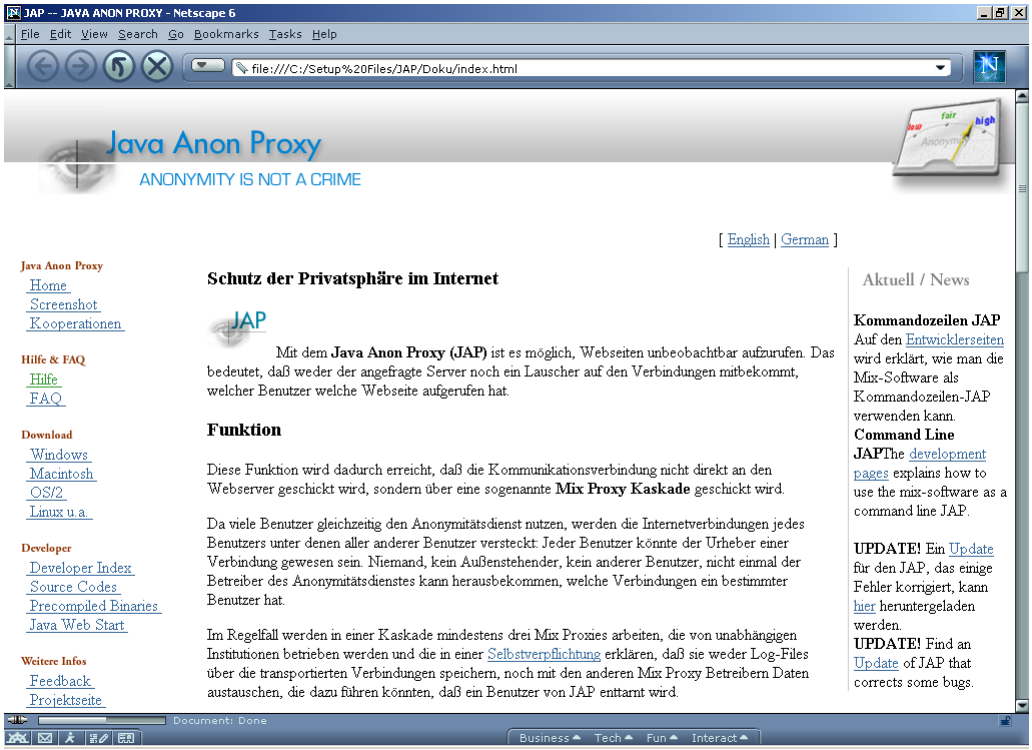
Wenn du nun das Programm JAP startest, musst du noch einige Einstellungen vornehmen. Mehr dazu findest du in der Dokumentation, die sich ebenfalls auf der CD befindet.

Starte deinen Webbrowser (also z.B. Microsoft Internet Explorer oder Netscape) und wähle den Menüpunkt „Datei ⇨ Öffnen“ und gib die Datei „index_de.html“ im Verzeichnis „Jap\Doku“ auf der CD an.


JAP\Doku

index_de.html

Dort findest du wichtige Informationen zum Programm selbst und was du zum Betrieb des Ganzen tun musst.



Bei Verwendung von Netscape 4.7 sieht die Ausgabe unter Umständen nicht ganz so hübsch aus, sie sollte aber doch irgendwie leserlich sein. Du findest diese und mehr Infos aber auch im Internet unter http://anon.inf.tu-dresden.de/

Zurück zum Inhalt dieses Kapitels

10.3 Die Verwendung von JAP

Bei der Installation von JAP hast du auch einen kleinen lokalen sogenannten Proxy-Server installiert, der mit einem der JAP Server kommuniziert. Wenn du JAP verwenden und anonym surfen willst, musst du eine Einstellung von deinem jeweiligen Internet-Browser ändern.

Da mensch wahrscheinlich nicht immer anonym Surfen will, müsste mensch nun immer diese Einstellung immer setzen, dann zurücksetzen, wieder setzen... Und das ist auf die Dauer doch etwas lästig.

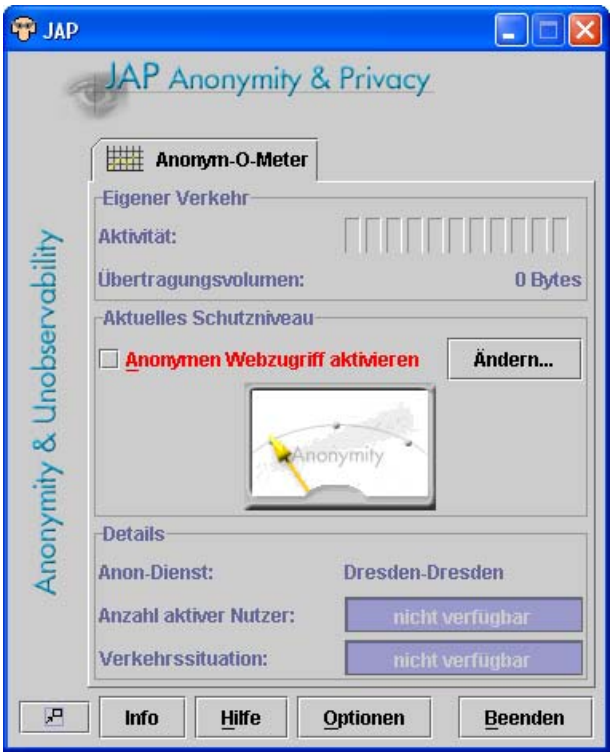
Eine Möglichkeit ist, Opera als Browser zu verwenden, bei Opera kannst du ganz einfach im Menü zwischen der Verwendung dieses Proxy Servers von JAP und dem normalen Internetzugang ohne Proxy Server hin- und herwechseln.

Wenn du andere Browser als Opera verwendest, kannst du einen Browser zum normalen Surfen ohne Anonymisierung und einen anderen Browser zum anonymen Surfen verwenden. So brauchst du auch nicht immer hin- und herschalten.

Zurück zum Inhalt dieses Kapitels

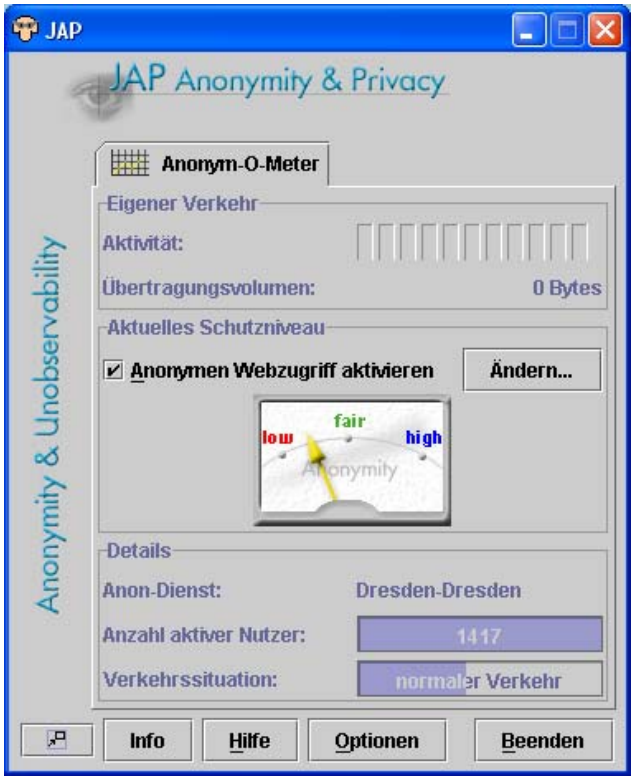
Starten von JAP

Nachdem du das bereits installierte Programm JAP gestartet hast (z.B. durch Doppelklick auf das JAP-Symbol auf deinem Desktop), erscheint folgendes Fenster:



In diesem Fall ist das Programm zwar gestartet, der anonyme Webzugriff ist jedoch noch nicht aktiviert (Kreuzchen in der Mitte). Klicke auf das Kästchen links neben Anonymen Webzugriff aktivieren und warte ein bisschen.

Zurück zum Inhalt dieses Kapitels



Wenn eine Verbindung zum JAP-Server aufgenommen wurde, ist das Kästchen nun angekreuzt und du siehst im unteren Teil des Fensters ein paar Informationen. Nun ist alles klar zum anonymen Surfen, wenn du die in den nächsten Kapiteln beschriebenen Einstellungen des Proxy Servers vorgenommen hast (siehe Kapitel Einstellungen im Browser).

In den Optionen (Button) kannst du angeben, dass sofort nach Start des Programms das Anonymitätsservice gestartet werden soll, mit dieser Option ersparst du dir ab dem nächsten Mal das Ankreuzen von Anonymen Webzugriff aktivieren.

Zurück zum Inhalt dieses Kapitels

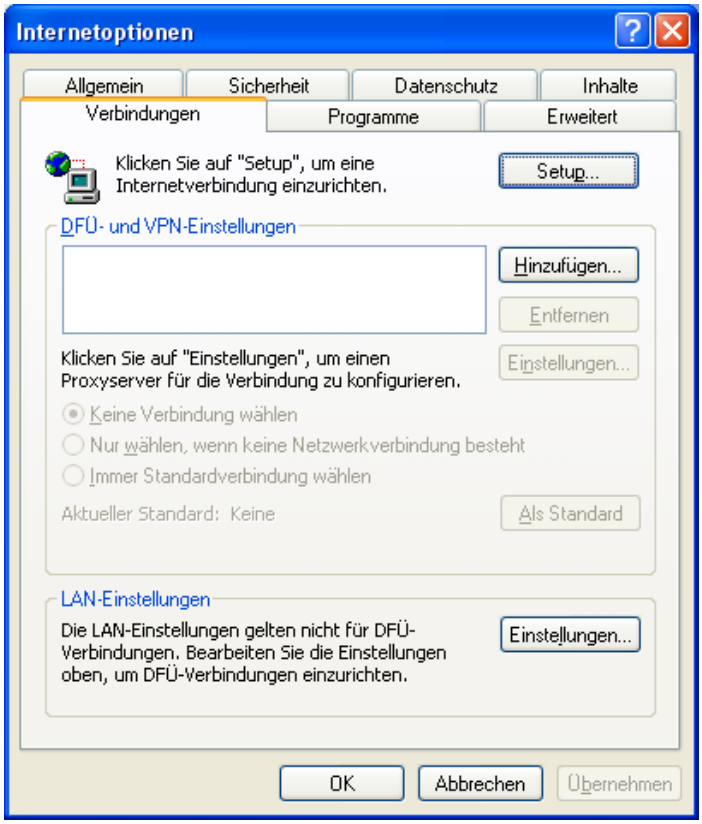
Einstellungen im Browser

Wie schon vorher erwähnt, musst du die Proxy-Server Einstellungen in deinem Browser ändern. Diese Änderung funktioniert bei allen Browsern sehr ähnlich, einziger Unterschied ist der jeweilige Menüpunkt, nachfolgend findest du eine Liste mit einigen Browsern und den zugehörigen Menüpunkten zum Setzen des Proxy-Servers.

Nachdem du das Programm JAP gestartet hast, dich mit einem JAP-Server verbunden hast und die nachfolgend beschriebenen Einstellungen in deinem Browser vorgenommen hast, kannst du wirklich anonym surfen.

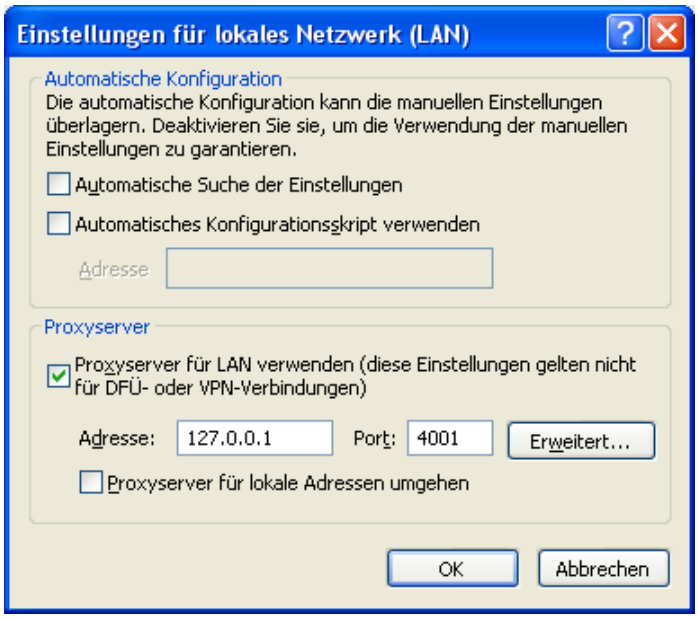
Microsoft Internet Explorer 6

Menü: Extras ⇨ Internetoptionen findest du in der Karteikarte Verbindungen Einstellungsmöglichkeiten für Modem- und für Kabel(LAN)-Verbindungen.



Zurück zum Inhalt dieses Kapitels

Wenn du z.B. bei LAN-Einstellungen auf den Button Einstellungen... drückst, erscheint ein Fenster, in dem du die IP-Adresse und das Port einstellen kannst:



Trage als Adresse 127.0.0.1 und als Port 4001 ein, drücke dann den Button OK.

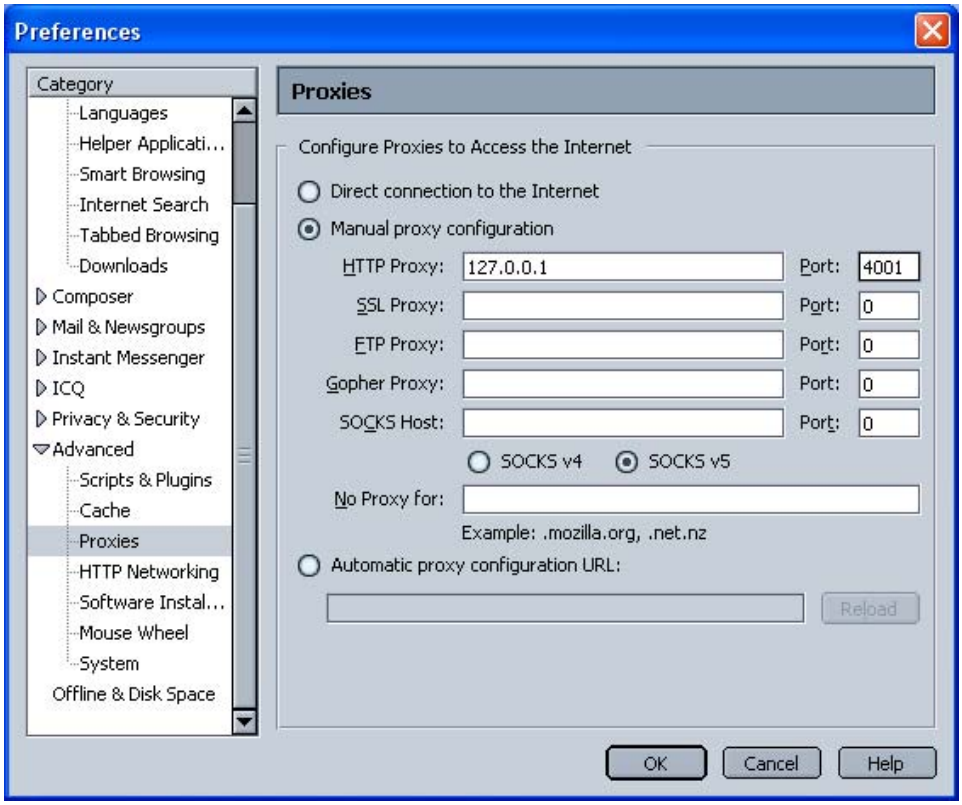
Mit dieser Einstellung kannst du nur mehr mit dem Programm JAP surfen. Wenn JAP nicht gestartet wurde, bekommst du mit dieser Einstellung keine Verbindung mehr zum Internet.

Wenn du ohne Verwendung von JAP surfen willst, musst du im gleichen oben abgebildeten Fenster das Kreuzchen bei Proxyserver wegklicken. Dann kannst du wieder normal ohne JAP surfen.

Zurück zum Inhalt dieses Kapitels

Netscape 7

Menü: Edit ⇨ Preferences findest du in der Category Advanced ⇨ Proxies die benötigten Einstellungen.



Trage als HTTP Proxy 127.0.0.1 und als Port 4001 ein, drücke dann den Button OK.

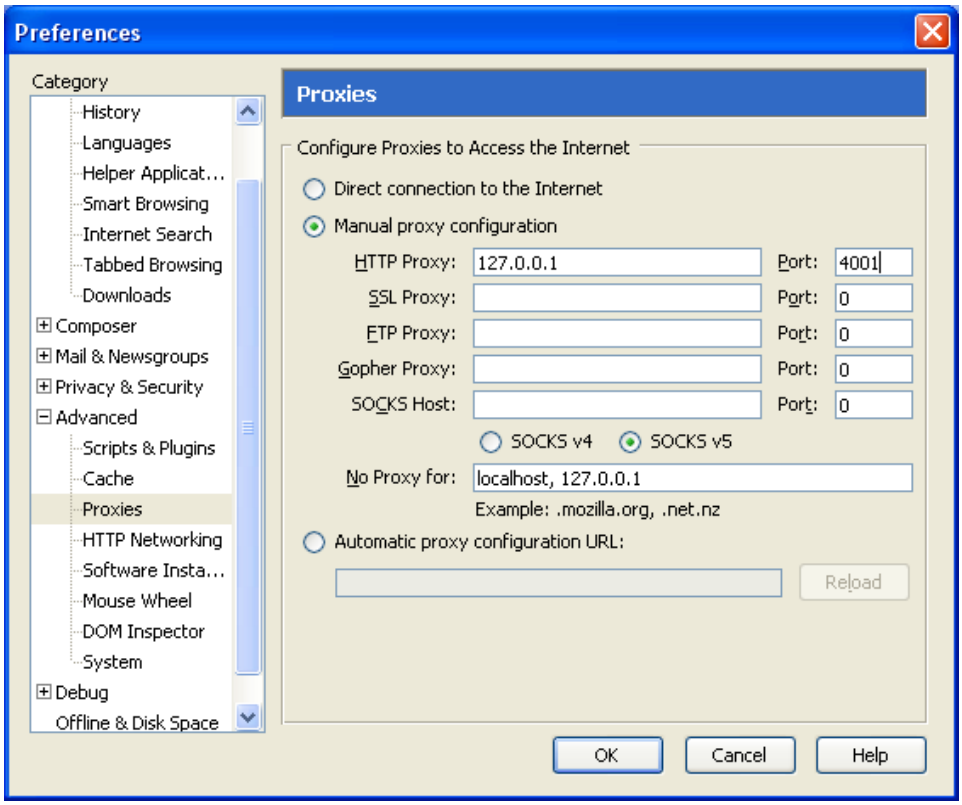
Mit dieser Einstellung kannst du nur mehr mit dem Programm JAP surfen. Wenn JAP nicht gestartet wurde, bekommst du mit dieser Einstellung keine Verbindung mehr zum Internet.

Wenn du ohne Verwendung von JAP surfen willst, musst du im gleichen oben abgebildeten Fenster das Kreuzchen bei Proxyserver wegklicken. Dann kannst du wieder normal ohne JAP surfen.

Zurück zum Inhalt dieses Kapitels

Mozilla 1

In Mozilla ist die Einstellung genauso wie bei Netscape zu setzen: Im Menü: Edit ⇨ Preferences findest du in der Category Advanced ⇨ Proxies die benötigten Einstellungen.



Trage als HTTP Proxy 127.0.0.1 und als Port 4001 ein, drücke dann den Button OK.

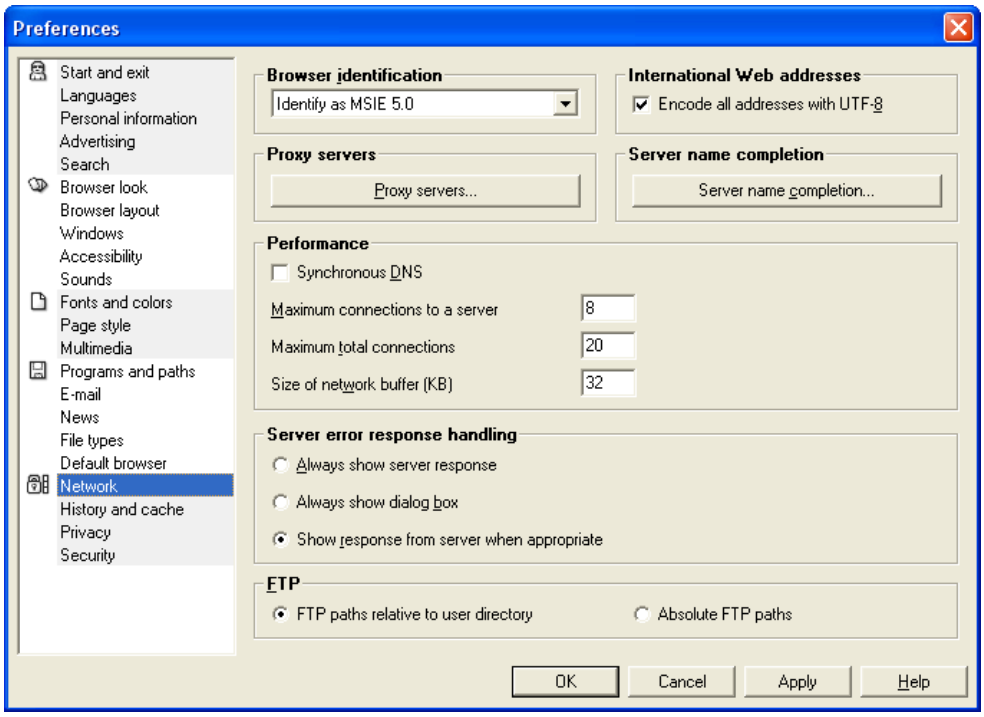
Mit dieser Einstellung kannst du nur mehr mit dem Programm JAP surfen. Wenn JAP nicht gestartet wurde, bekommst du mit dieser Einstellung keine Verbindung mehr zum Internet.

Wenn du ohne Verwendung von JAP surfen willst, musst du im gleichen oben abgebildeten Fenster das Kreuzchen bei Proxyserver wegklicken. Dann kannst du wieder normal ohne JAP surfen.

Zurück zum Inhalt dieses Kapitels

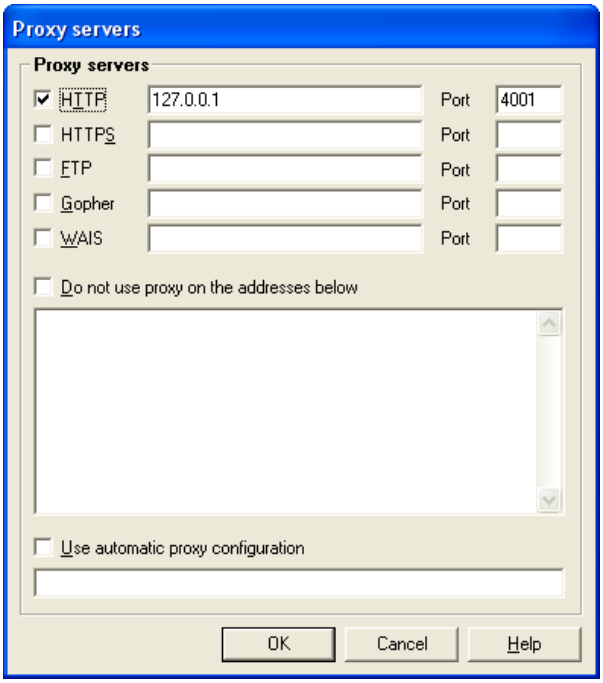
Opera 6

Menü: File ⇨ Preferences geht folgendes Fenster auf:



Wähle den Punkt Network auf der linken Seite und drücke den Button Proxy servers... Dann erscheint ein weiteres Fenster, in dem du die Einstellungen eingeben kannst:

Zurück zum Inhalt dieses Kapitels



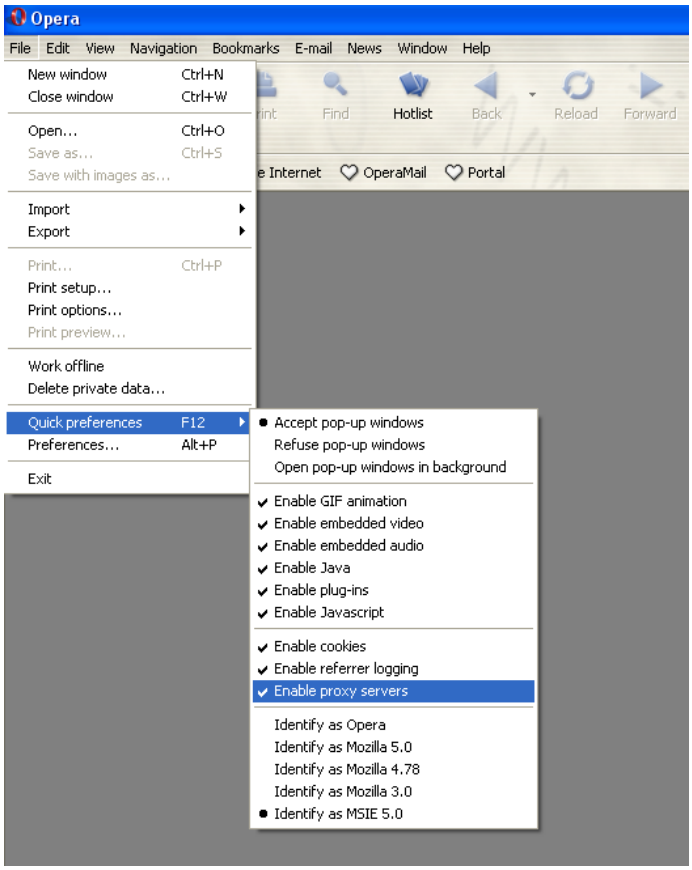
Trage unter HTTP 127.0.0.1 und als Port 4001 ein, drücke dann den Button OK.

Mit dieser Einstellung kannst du nur mehr mit dem Programm JAP surfen. Wenn JAP nicht gestartet wurde, bekommst du mit dieser Einstellung keine Verbindung mehr zum Internet.

Wenn du ohne Verwendung von JAP surfen willst, führe nachfolgend beschriebenen Schritt durch.

Zurück zum Inhalt dieses Kapitels

Das Feine bei Opera ist in diesem Zusammenhang, dass mensch ganz einfach über das Menü des Browsers zwischen der Verwendung dieses Proxyservers für JAP und der Nichtverwendung hin- und herschalten kann.



Jedes Mal, wenn du den Menüpunkt File ⇨ Quick preferences ⇨ Enable proxy servers wählt, wird die Verwendung des Proxy Serves aus- bzw. eingeschalten.

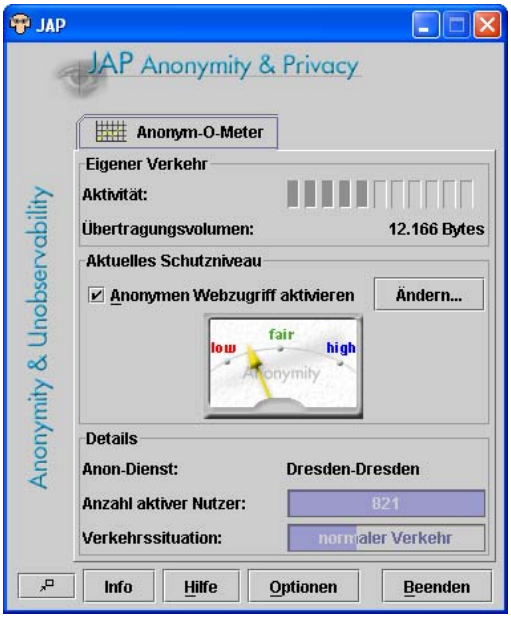
Wenn du JAP verwendest, also darauf achten, dass das Hakerl neben dem Menüpunkt Enable proxy servers aufscheint, wenn du ohne Verwendung von JAP surfen willst, darf kein Hakerl neben dem Menüpunkt sein.

Zurück zum Inhalt dieses Kapitels

Kontrolle der anonymen Verbindung

Wenn du nun alles richtig gemacht hast (so viel war's ja nicht, oder?), kannst du nach dem Aufruf einer Webseite kontrollieren, ob du jetzt wirklich anonym surfst.

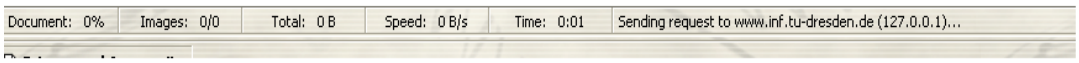
Am besten kontrollierst du die Informationen im JAP Fenster selbst:



Wenn du eine Webseite aufrust, sollte sich rechts nebem der Beschriftung „Aktivität" etwas tun, das Übertragungsvolumen wird größer bzw. behält nach dem fertigen Laden einer Seite einen bestimmten Wert. Das zeigt, dass du über den Anonymisierungsdienst surfst.

Eine andere Möglichkeit ist, nach dem Aufruf einer Seite im jeweiligen Browserfenster die Statusleiste zu beobachten, sie befindet sich meist unten. Sie zeigt an, was der Browser gerade tut. Während die Seite geladen wird, scheint dort irgendetwas mit 127.0.0.1 auf, das bedeutet, dass die Seite über deinen lokalen Proxy Server geladen wird, es funktioniert also alles.

In Opera sieht das z.B. so aus:



Tipp: Schließe deinen Browser nach der Änderung der Einstellung und starte ihn neu bzw. starte den Browser erst nach dem Start von JAP und der Aktivierung des Anonymisierungsdienstes.

Zurück zum Inhalt dieses Kapitels

11 Ad-Aware

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Ad-Aware, einem kostenlosen Programm zum Auffinden und Entfernen von Programmen, die deinen Computer ausspionieren (Spyware)

Solche Spyware ist in Programmen beinhaltet, die du installierst. Meist weißt du gar nicht, dass dieses Programm Spyware beinhaltet. Diese Programmteile schicken dann die gesammelten Information unbemerkt nach außen.

Gründe, die von ProgrammherstellerInnen von Spyware angegeben werden, gehen von Auffinden illegal installierter Software bis zu Marktforschungszwecken. In jedem Fall ist dies eine der übelsten Arten, in die Privatsphäre einer BenutzerIn einzudringen, es wäre wohl niemand freiwillig damit einverstanden, dass solche Informationen einfach an irgendwen geschickt werden.

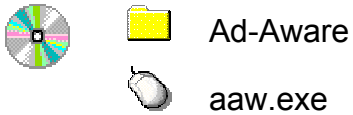
Ad-Aware sucht nach solchen Programmen, du kannst dir bei Auffinden eines solchen Programms aussuchen, ob es gelöscht werden soll oder nicht.

Du solltest das Programm hin und wieder laufen lassen, zumindest dann, wenn du ein neues Programm installiert hast.

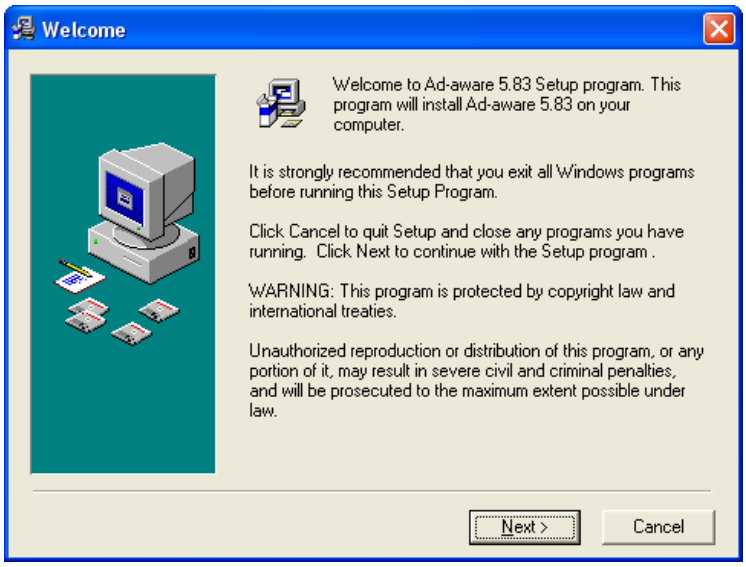
Du findest Beschreibungen zu folgenden Bereichen:

11.1 Die Installation von Ad-Aware

Die Installation von Ad-Aware ist denkbar einfach. Starte das Installationsprogramm durch Doppelklick auf das Programm aaw.exe im Ordner Ad-Aware auf der CD.

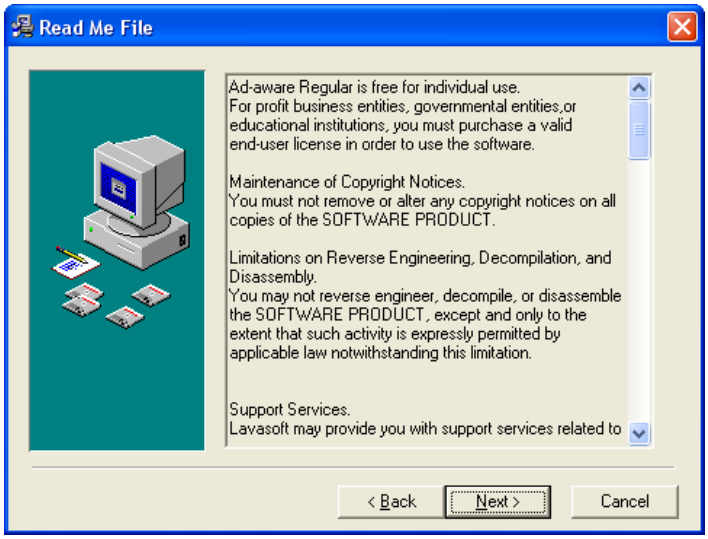


Nach dem Start des Installationsprogramms erscheint ein Begrüßungsfenster.

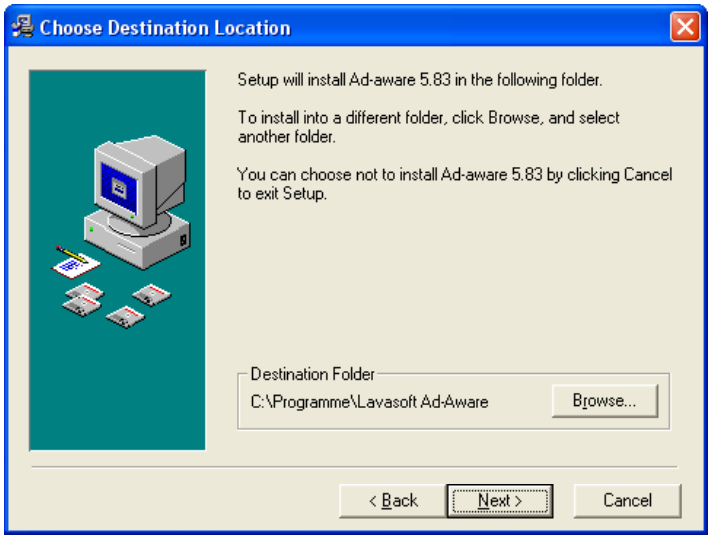


Drücke auf den Button Next, es folgt eine Information über das Programm:

Zurück zum Inhalt dieses Kapitels



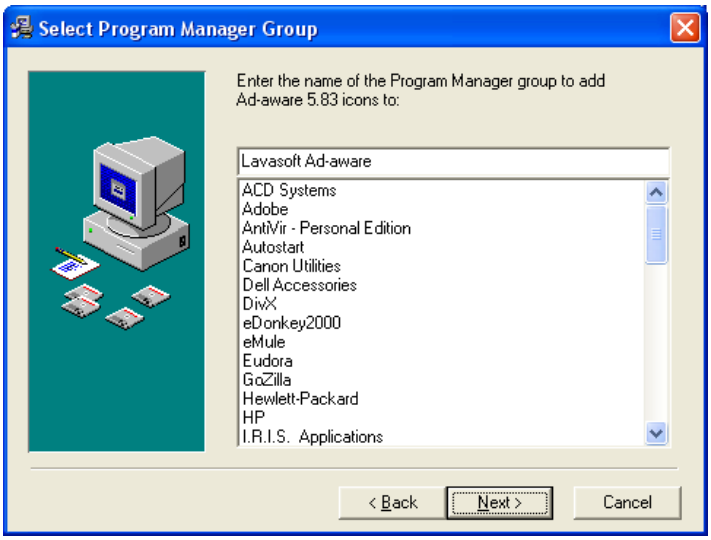
Drücke nochmals den Button Next. Dann kannst du dir den Ordner aussuchen, in dem das Programm installiert werden soll.



Zurück zum Inhalt dieses Kapitels

Nimm einfach den vorgeschlagenen oder wähle bei Bedarf einen anderen Ordner und bestätige die Angabe durch Drücken des Buttons Next.

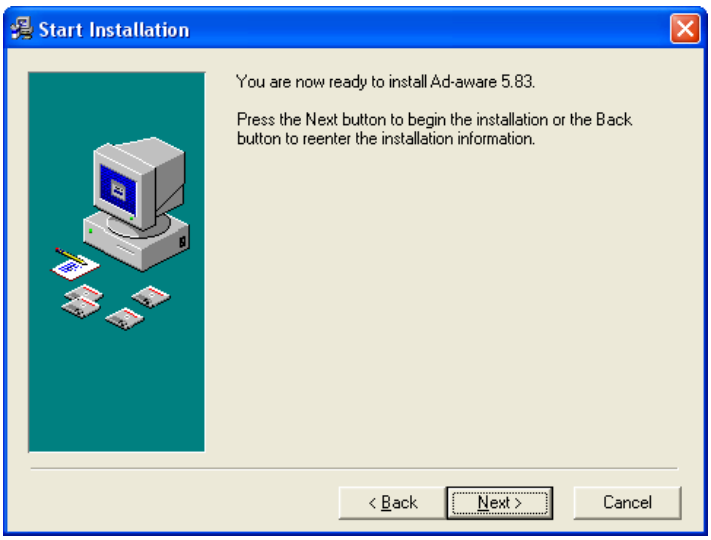
Nun kannst du dir aussuchen, unter welchem Namen das Programm im Startmenü aufscheint:



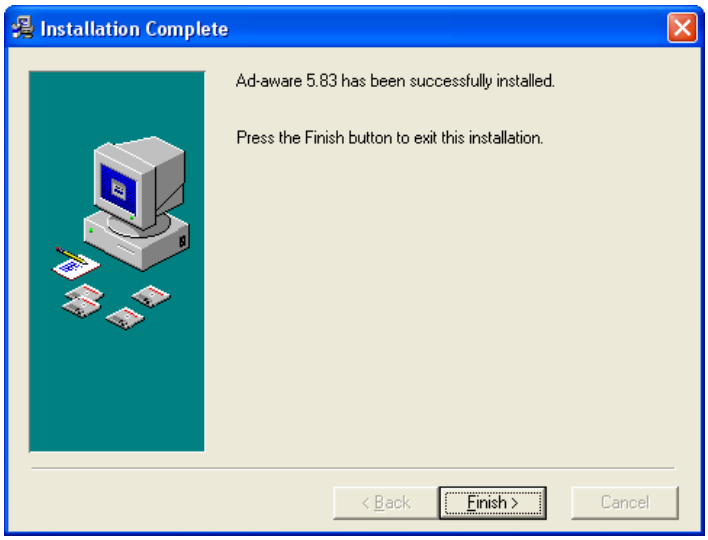
Nimm einfach den vorgeschlagenen Namen Lavasoft Ad-aware oder tippe einen anderen Namen ein. Bestätige die Angabe durch Drücken des Buttons Next.

Zurück zum Inhalt dieses Kapitels

Vor der wirklichen Installation erscheint noch ein Hinweis, dass alles für die Installation bereit ist:



Drücke einfach den Button Next und schon geht's los mit der Installtion. Nach ein paar Sekunden ist die Installation abgeschlossen:

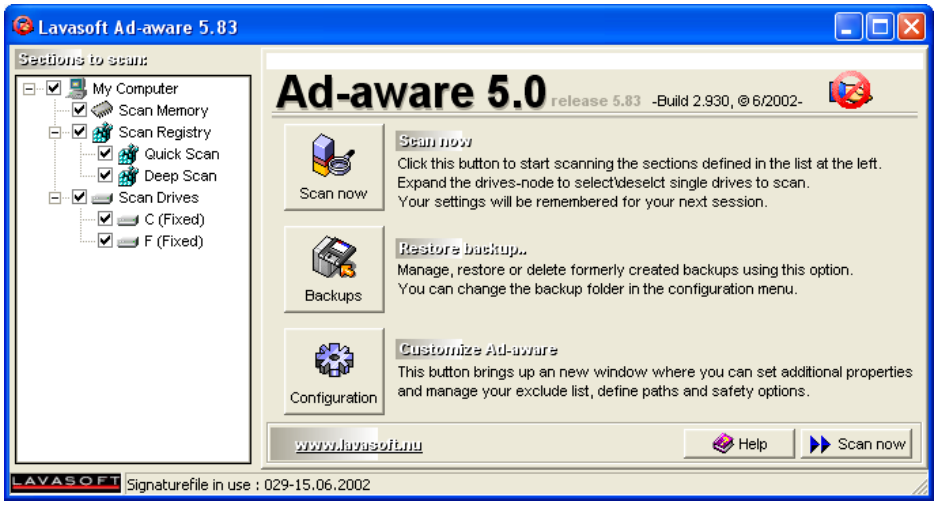


Drücke den Button Finish. Fertig.

Zurück zum Inhalt dieses Kapitels

11.2 Die Verwendung von Ad-Aware

Nach dem Start von Lavasoft Ad-aware erscheint folgendes Fenster:



Im linken Teil des Fensters kannst du angeben, welche Teile des Computers nach Spyware durchsucht werden sollen. Im Beispiel oben ist einfach alles angekreuzt, was zumindest beim erstmaligen Suchen nach Spyware empfehlenswert ist.

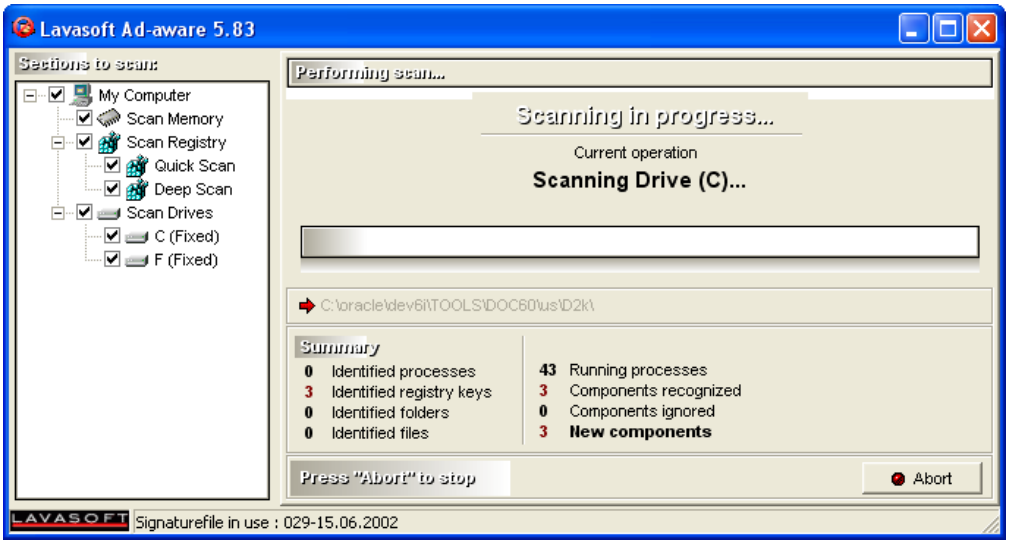
Im rechten Teil des Fensters siehst du 3 Buttons:

- Scan now
- Backups
- Configuration

Mit “Backups” kannst du Einstellungen, die du vorher gesichert hast, zurücksichern (mehr dazu später). Mit „Configuration“ kannst du spezielle Einstellungen vornehmen.

Mit dem Button „Scan now“ startet die Suche nach Spyware:

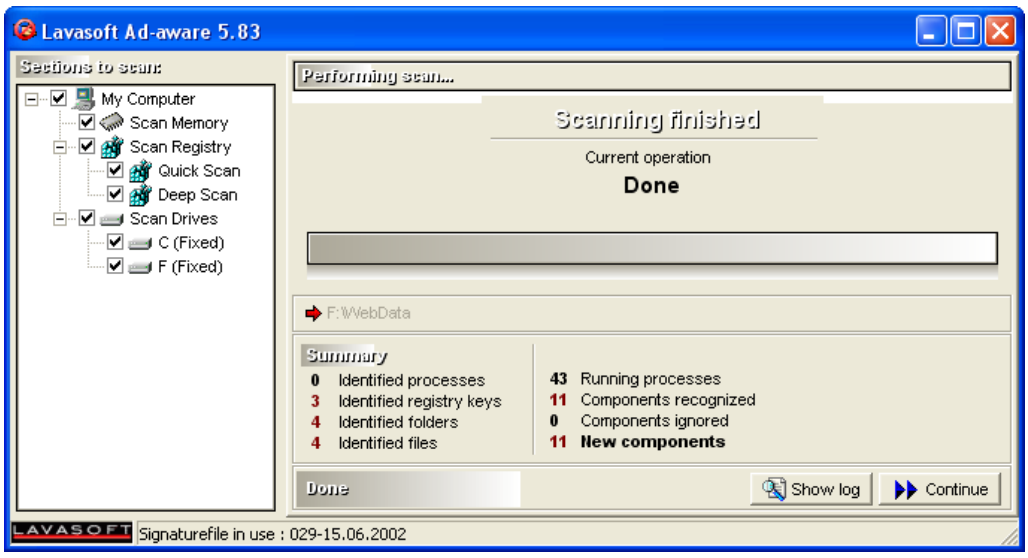
Zurück zum Inhalt dieses Kapitels



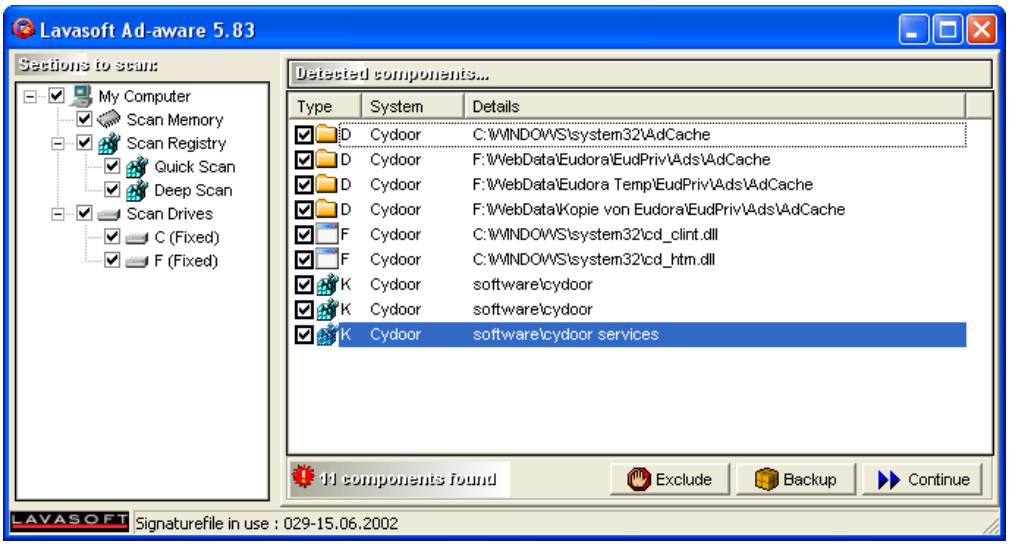
Aber keine Angst, noch passiert nichts mit deinem Computer, nichts wird deinstalliert oder geändert. Es wird nur eine Liste von Spyware-Programmen und Einstellungen erstellt.

Diese Suche dauert eine Weile, abhängig von der Menge an Programmen, die du installiert hast. Im Fenster siehst du immer, was das Programm gerade durchsucht, im Beispiel oben wird gerade das Laufwerk C durchsucht.

Zurück zum Inhalt dieses Kapitels



Nach dem Ende der Suche erscheint im Fenster die Information „Scanning finished, Current operation done“. Drücke den Buton „Continue“. Nun erscheint eine Liste von allen Programmen und Einstellungen, die Spyware betreffen:



Du kannst jetzt alle Programme/Einstellungen ankreuzen, die Spyware beinhalten und die du loswerden willst (z.B. alle wie im Beispiel oben).

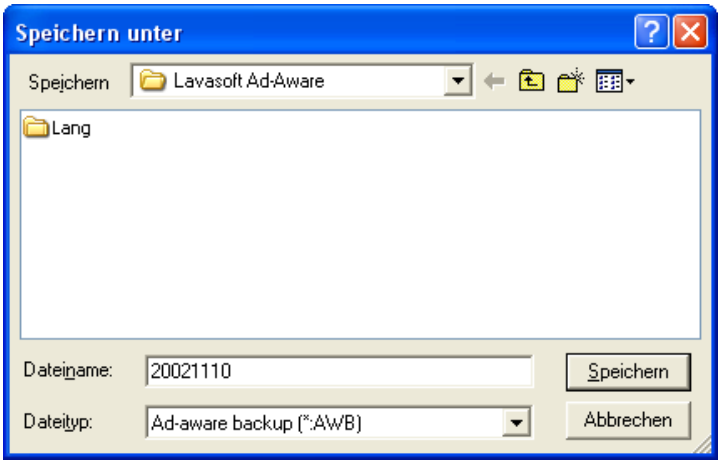
Wenn du wissen willst, ob ein bestimmtes Programm nach dem Entfernen der Spyware noch funktioniert, musst du im Forum von Ad-Aware nachsehen. Dieses Forum findest du im Internet unter der Adresse http://www.lavasoftsupport.com, dort findest du unter Umständen auch eine Alternativen zu Programmen, die Spyware beinhalten.

Selbst wenn nicht sicher ist, ob die Programme, die Spyware beinhalten, nach dem Reinigen mit Ad-Aware noch funktionieren, bleibt die Frage, ob du unbedingt Programme behalten willst, die Spyware beinhalten.

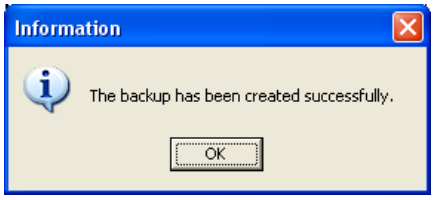
Am besten ist wohl, die Programme zu entfernen und dann Alternativen suchen – nämlich Programme, die keine Spyware beinhalten.

Mit dem Button „Backup“ kannst du eine Sicherung deiner Programme und Einstellungen vornehmen:

Zurück zum Inhalt dieses Kapitels

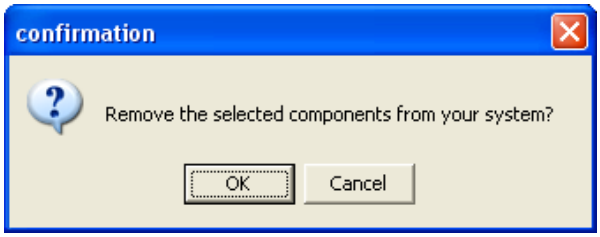


Gib einen Dateinamen für die Sicherung an und drücke den Button „Speichern“. Das Backup wird dann durchgeführt.



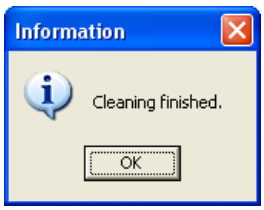
Nach erfolgter Sicherung, die sehr kurz dauert, erscheint der Erfolgshinweis. Bestätige ihn mit dem Button „OK“. Du kehrst dann zum Hauptfenster zurück.

Drücke nach der Auswahl der zu entfernenden Programme/Programmteile und Einstellungen den Button „Continue“. Es erscheint noch eine Sicherheitsabfrage, ob du die Programme/Programmteile wirklich entfernen willst.



Drücke den Button „OK“. Die Programme/Programmteile werden entfernt. Nach Abschluss erscheint ein Hinweisfenster:

Zurück zum Inhalt dieses Kapitels



So, und jetzt kannst du ausprobieren, ob die betroffenen Programme noch funktionieren.

Zurück zum Inhalt dieses Kapitels

12 XP Antispy

Überblick

In diesem Kapitel erfährst du Näheres zum Programm XP Antispy, einem kostenlosen Programm zum Auffinden und Entfernen von Einstellungen und Programmteilen von Windows XP, die Spyware beinhalten.

Näheres zum Thema „Spyware“ findest du im Kapitel Ad-Aware

Du findest Beschreibungen zu folgenden Bereichen:

- Die Verwendung von XP Antispy

12.1 Die Verwendung von XP Antispy

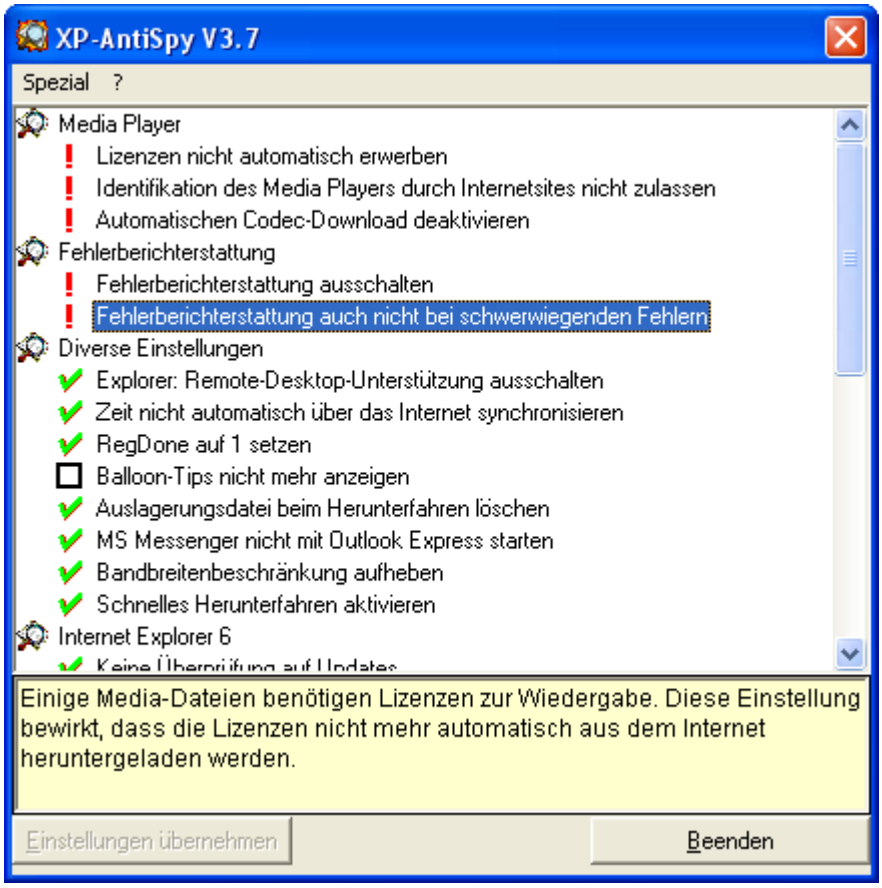
XP Antispy muss nicht extra installiert werden. Einfach das Programm auf der CD aufrufen und los geht’s.

XP Antispy

xp-AntiSpy3D

Zurück zum Inhalt dieses Kapitels

Nach dem Start des Installationsprogramms erscheint eine Liste von Einstellungen und eventuell empfohlene Änderungen:



Wenn du mit dem Mauszeiger über die einzelnen Einstellungen fährst, erscheint im unteren Teil des Fensters eine Beschreibung des Problems.

Die Bedeutung der einzelnen Zeichen neben den Einstellungen findest du in der Hilfe, die du unter „? ⇨ Über xp-AntiSpy...“ aufrufen kannst.

- Grüne Hakerln neben der Einstellung bedeutet natürlich, dass alles ok ist (d.h. die Einstellung deaktiviert ist).
- Bei Rechtecken kannst du wählen, ob du die Einstellung deaktivieren willst oder nicht. Wenn du sie ankreuzt, wird die Einstellung deaktiviert.
- Rote Rufzeichen bedeuten, dass die Einstellung derzeit aktiv ist und anschließend deaktiviert wird. Durch Anklicken des Rufzeichens wird es aber zum schwarzen Rechteck, mit dem du dir aussuchen kannst, ob du die Einstellung aktiviert belassen oder sie deaktivieren willst.

Zurück zum Inhalt dieses Kapitels

Drücke nach der Auswahl der zu deaktivierenden Punkte den Button „Einstellungen übernehmen“. Jetzt siehst du hoffentlich viel mehr grüne Hakerln als vorher. Durch Drücken des Buttons „Beenden“ schließt du das Programm.

Rückgängigmachen von Änderungen

Wenn du das Programm startest und danach mit der Maus auf eine Einstellung zeigst, die du wieder in ihren ursprünglichen Wert zurücksetzen willst, drücke die rechte Maustaste.

Es öffnet sich ein Kontextmenü mit dem einzigen Menüpunkt „Funktion auf ihren ursprünglichen Wert zurücksetzen“. Stamm dem grünen Hakerl ist jetzt wieder ein rotes Rufzeichen sichtbar. Doppelklicke in die Zeile, aus dem roten Rufzeichen wird jetzt wieder ein schwarzes Kästchen. Du kannst jetzt angeben, dass die Funktion nicht deaktiviert werden soll (also wieder aktiviert wird, leeres Kästchen).

Durch Drücken des Buttons „Einstellungen übernehmen“ wird die Änderung durchgeführt.

Zurück zum Inhalt dieses Kapitels

13 Webwasher

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Webwasher, einem kostenlosen Programm zum Schutz der Privatsphäre beim Surfen.

Trotz „Anonymen Surfen“ - siehe Kapitel JAP (Java Anon Proxy) – kann beim Surfen eine Vielzahl von Informationen ausspioniert werden.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Funktionalität von Webwasher
- Die Schnelligkeit von Webwasher
- Die Installation von Webwasher
- Die Verwendung von Webwasher

13.1 Die Funktionalität von Webwasher

Webwasher bietet eine Vielzahl von Funktionalitäten zum Schutz der Privatsphäre beim Surfen im Internet. Die nachfolgende Liste dieser Funktionalitäten ist der deutschen Webseite von Webwasher http://www.webwasher.com/de/products/wwash/functions.htm entnommen:

Filtern von Inhalten

Die Standardfilter des WebWasher verhindern das Laden und Anzeigen von unerwünschten Datenobjekten auf Webseiten. Folgende konfigurierbare Funktionen stehen zur Verfügung:

Größen-Filter

Filtert unerwünschte Werbebanner. Neue Formate können jederzeit aufgenommen werden.

URL-Filter

Filtert mittels einer Filterliste unerwünschte Datenobjekte aus Webseiten. Beispielsweise können Grafiken einfach durch einen rechten Mausklick auf das betreffende Bild der Liste hinzu gefügt werden und erscheinen dann bei einem erneuten Aufruf der Seite nicht mehr.

Pop-Up-Fenster

Alle Pop-Up-Fenster auf Webseiten werden eliminiert.

Skripte

Beim Laden oder Schließen von Webseiten auszuführende Skripte werden verhindert.

Animationen

Animierte Grafiken können vollständig verhindert werden. Alternativ ist die Festlegung der Wiederholungen oder die Anzeige des ersten Bildes möglich.

Optionen

Die entfernten Bilder können durch ein selbst definiertes Bild ersetzt werden.

Zurück zum Inhalt dieses Kapitels

Schutz der Privatsphäre

Die Filter des WebWasher verhindert zum Schutz der Privatsphäre, dass ohne Wissen des Anwenders Informationen über ihn an Dritte weitergegeben werden.

Web Bugs-Filter

Filtert kleine, unsichtbare Grafiken, die in Dokumenten versteckt sind und Rückmeldungen an Dritte auslösen. Web Bugs werden von Datensammlern benutzt, um aus dem Surfverhalten des Anwenders Profile zu erstellen.

Referer-Filter

Verhindert die Nachverfolgung der durch die Internet-Nutzung verursachten Datenspuren durch Dritte. Zum Beispiel von welcher Seite Sie zu einer anderen gelangen, oder welche Suchbegriffe Sie vorher in eine Suchmaschine eingegeben haben.

Cookie-Filter

Verhindert das unerwünschte Senden oder Empfangen von Cookies durch Ihren Browser aus dem Internet. Mit Cookies kann der Anwender im Internet eindeutig identifiziert werden. Der Cookie- Filter ermöglicht die Einteilung in "gut", "schlecht" und "neutral". So können Sie beispielsweise die "guten" Cookies weiterhin für elektronischen Einkauf nutzen, während Cookies, die den Anwender ausspionieren, unschädlich gemacht bzw. ganz ausgefiltert werden.

Zurück zum Inhalt dieses Kapitels

Zugriffskontrolle

Der WebWasher erlaubt dem Anwender einen kontrollierten Zugriff auf das Internet. Gewünschtes kommt durch. Unerwünschte Webseiten oder Daten werden blockiert.

Negativ-Liste

Erlaubt eine Sperrung des Zugriffs auf unerwünschte Webadressen. Damit können beispielsweise Seiten mit rechtswidrigen Inhalten vom Anwender fern gehalten werden. Außerdem kann das Herunterladen von bestimmten Datentypen, wie z. B. Programme oder Musikdateien, blockiert werden.

Positiv-Liste

Sperrt den gesamten Zugriff auf das Web. Nur bestimmte Webadressen werden frei geschaltet. Beispielsweise kann die Internetnutzung von Mitarbeitern in einer Firma auf die tatsächlich arbeitsrelevanten Inhalte, wie z. B. einen Lieferantenkatalog, beschränkt werden.

Optionen

Der Zugriff auf eine gesperrte Seiten kann auf eine frei definierbare Webadresse umgelenkt werden. Diese Option ermöglicht das Einblenden einer eigenen Infoseite oder das automatische Wechseln zu Alternativangeboten.

Zurück zum Inhalt dieses Kapitels

13.2 Die Schnelligkeit von Webwasher

Zum Herausfiltern von Werbebanner aus Internetseiten benötigt Webwasher natürlich ein wenig Zeit, mit Webwasher ist das Surfen daher etwas langsamer als ohne die Verwendung von Webwasher.

Die Verzögerung liegt aber unserer Meinung nach absolut im akzeptablen Bereich. Probiere es einfach selbst aus, wenn dich diese kleinen Verzögerungen nicht stören, verwende ihn immer. Wenn es für dich doch störend ist, verwende ihn bei Bedarf.

Zurück zum Inhalt dieses Kapitels

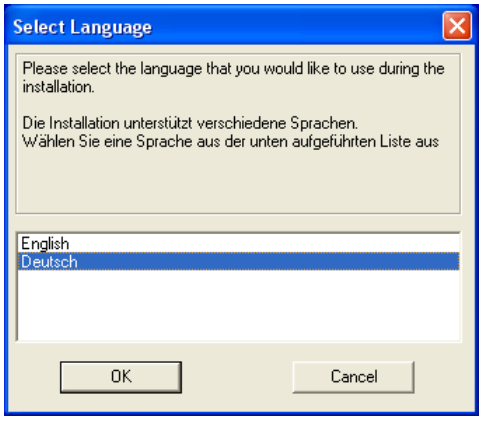
13.3 Die Installation von Webwasher

Die Installation von Webwasher startest du durch Doppelklick auf das Programm wash32b4 im Ordner Webwasher auf der CD.


Webwasher

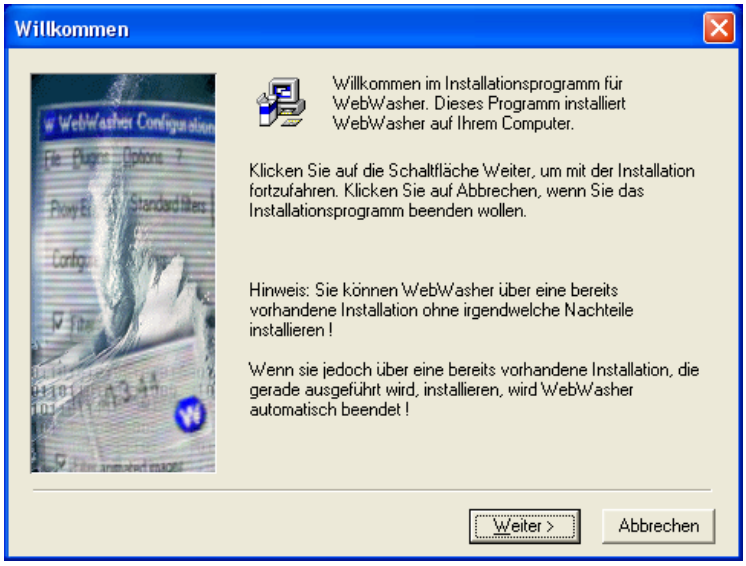
wash32b4.exe

Nach dem Start des Installationsprogramm kannst du dir die gewünschte Sprache auswählen:

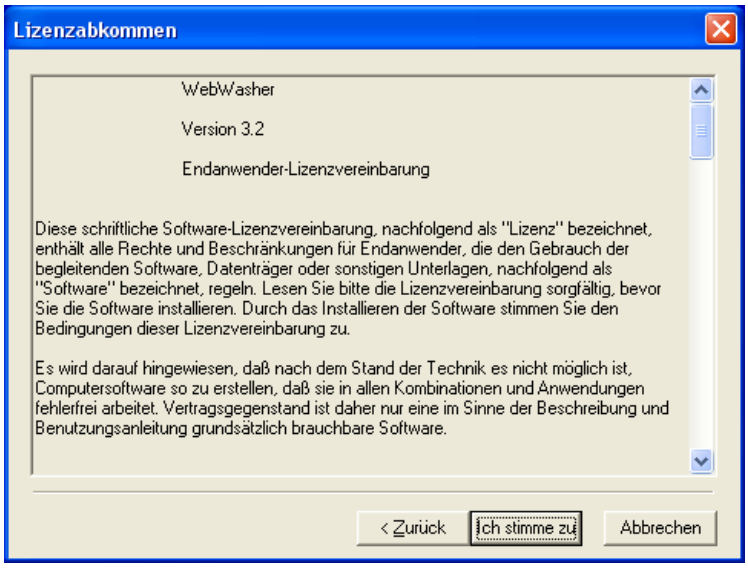


Im Beispiel oben wird „Deutsch“ gewählt, drücke dann den Button „OK“. Natürlich gibt’s dann wieder ein freundliches Begrüßungsfenster mit ein paar Hinweisen:

Zurück zum Inhalt dieses Kapitels



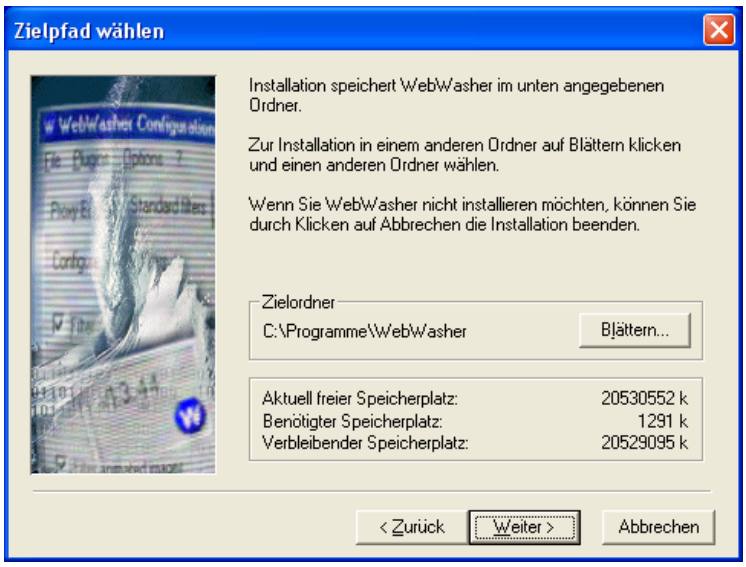
Bestätige das Fenster mit dem Button „Weiter“. Dann erscheint das Lizenzabkommen:



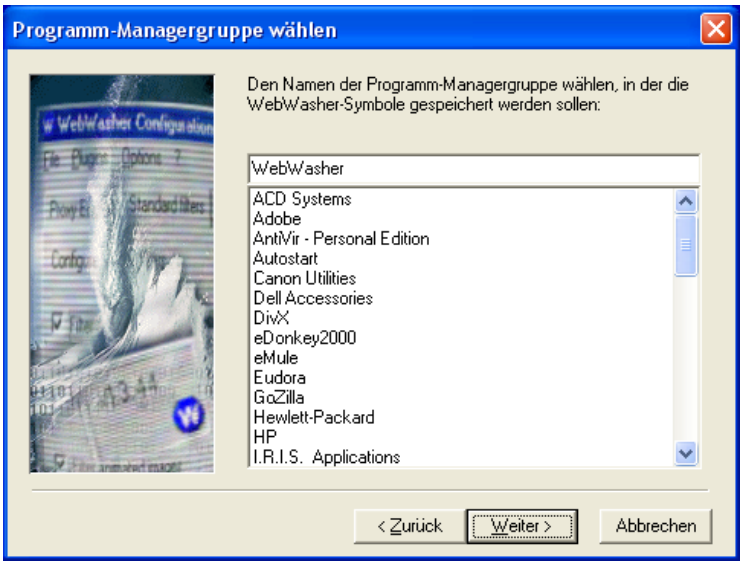
Falls du mit allem einverstanden bist, drücke den Button „Ich stimme zu“.

Zurück zum Inhalt dieses Kapitels

Danach kannst du dir den Ordner aussuchen, in dem du Webwasher installieren willst:



Nimm einfach den vorgeschlagenen Ordner oder ändere ihn bei Bedarf. Drücke dann den Button „Weiter“. Dann kannst du dir noch den Namen im Programm-Menü aussuchen:



Nimm ebenfalls einfach den vorgeschlagenen Namen oder tippe einen anderen ein. Bestätige das Fenster mit „Weiter“.

Zurück zum Inhalt dieses Kapitels

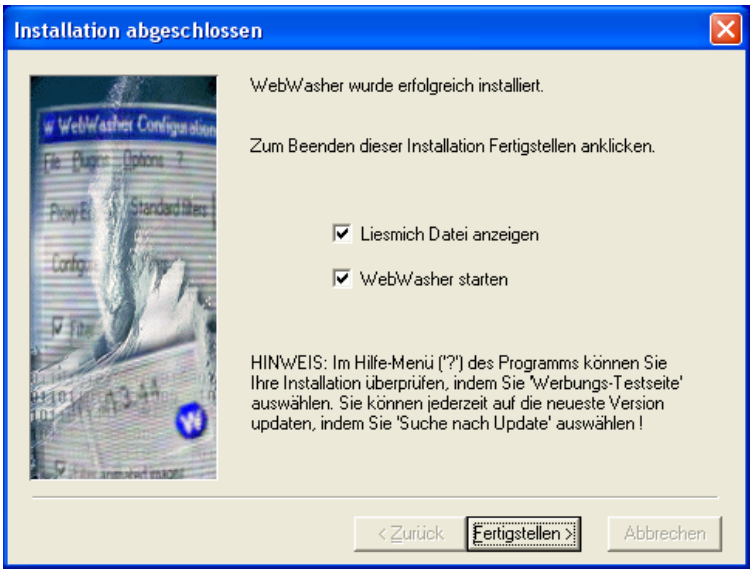
Dann kannst du noch ein paar Optionen angeben:

Wenn du den Punkt „Beim Windows Start WebWasher starten“ ankreuzt, wird er automatisch gestartet.

Durch Drücken des Buttons „Weiter“ wird die Installation gestartet, sie dauert nur ein paar Sekunden.

Zurück zum Inhalt dieses Kapitels

Nach dem Abschluss der Installation erscheint das übliche Erfolgsfenster:

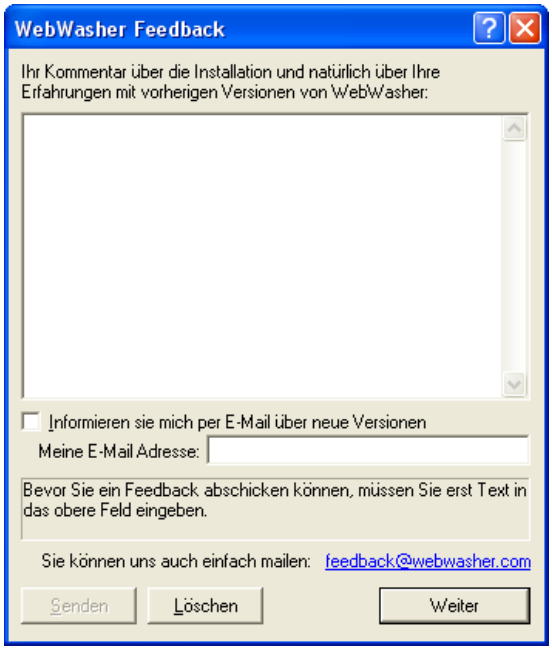


Du kannst zum Abschluss noch angeben, ob du Webwasher gleich starten willst und ob du die Liesmich-Datei angezeigt haben willst. Wenn du nähere Informationen zu dieser Version von Webwasher lesen willst, kreuze das ensprechende Kästchen an. Bestätige deine Wahl durch Drücken des Buttons „Fertigstellen“.

Zurück zum Inhalt dieses Kapitels

13.4 Die Verwendung von Webwasher

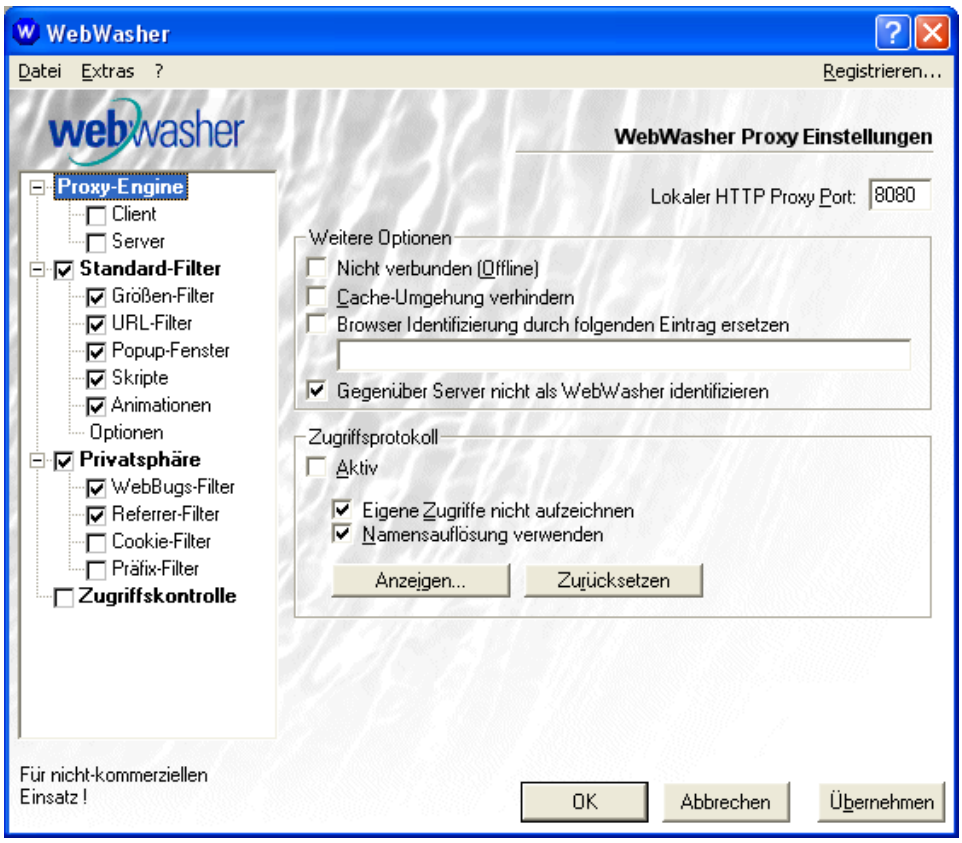
Beim ersten Start von Webwasher erscheint ein Feedback-Fenster:



Drücke einfach den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Im Webwasher-Fenster kannst du einstellen, was beim Browsen gefiltert werden soll:



Neben dem Ankreuzen der Filter, die du einsetzen möchtest (beim Anklicken eines Filters erscheint eine kurze Erklärung im Fenster) ist die Einstellung „Lokaler http Proxy Port“ (hier 8080) wichtig.

Zurück zum Inhalt dieses Kapitels

Diese Portnummer musst du auch bei deinem Browser angeben. Wie mensch die Proxy-Adresse und das Port angibt, ist im Kapitel Einstellungen im Browser beschrieben. Es ist der gleiche Vorgang wie dort angegeben, es wird genauso die Proxy-Adresse 127.0.0.1 angegeben, statt Port 4001 aber der im Webwasher Fenster angezeigte, im Beispiel oben also 8080.

Du kannst durch Aufruf der Webwasher-Internetseite

http://www.webwasher.com/de/products/wwash/testpag1.htm

prüfen, ob der Webwasher bei dir funktioniert. Wenn 2 zusätzliche kleine Browserfenster aufgehen und du Werbung auf der Seite siehst, dann ist Webwasher nicht aktiv.

Siehst du keine Werbung und gehen keine zusätzlichen Fenster auf – super, alles ok.

Zurück zum Inhalt dieses Kapitels

14 AntiVir (Anti-Virenprogramm)

Überblick

Dieses Kapitel enthält eine Beschreibung, wie mensch AntiVir, ein Viren-Schutzprogramm für Windows installiert und verwendet.

Es gibt zahlreiche kostenpflichtige und kostenlose Viren-Schutzprogramme, AntiVir für Windows ist nur eines davon. Wichtig ist aber vor allem, überhaupt einen sogenannten Viren-Scanner auf dem Computer zu installieren und diesen immer auf aktuellem Stand zu halten, denn es tauchen ständig neue Computerviren auf.

Noch kurz zu Word-Dokumenten, die per Mail verschickt werden. Da Word-Dokumente aufgrund einer integrierten Programmiersprache Viren enthalten können (Makroviren), sollten sie nur per Mail verschickt werden, wenn dies wirklich notwendig ist.

Am besten ist, diese Word-Dokumente vor dem Abschicken ins Rich Text Format (RTF) umzuwandeln, RTF-Dokumente können nämlich keine Viren enthalten (das machst du mit Datei ⇨ Speichern unter ⇨ Rich Text Format *.rtf).

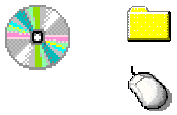
Auch wissen das Menschen zu schätzen, die keinen Kabel- oder ADSL-Anschluss zu Hause haben und mit einem Modem zum Internet verbunden sind. Word-Dokumente sind ja meist aufgrund der vielen Formatierungen sehr groß, reine Texte, wie du sie mit deinem E-Mail Programm eintippst, sind jedoch für alle blitzschnell auf den Bildschirm zu zaubern und garantiert virenfrei.

Du findest Beschreibungen zu folgenden Bereichen:

14.1 Die Installation von AntiVir

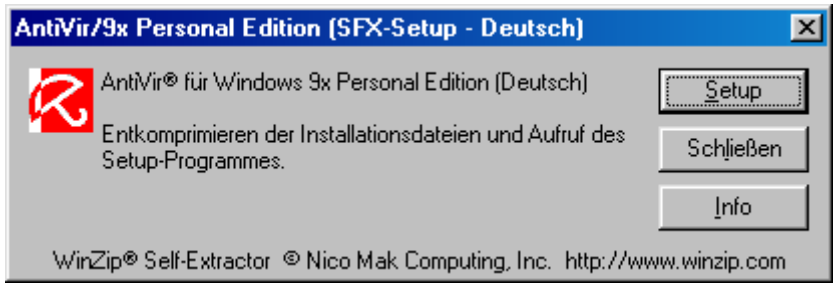
Du findest das Installationsprogramm von AntiVir für Windows auf der zugehörigen CD im Verzeichnis „AntiVir\Windows“ im jeweiligen Ordner für Windows NT/2000 oder im Ordner für Windows 9x (Windows 95/98/ME). Leider gibt es dieses Programm nur für Windows. Du findest aber sicherlich im Internet auch Gratis-Virenscanner für das von dir verwendete Betriebssystem.

Doppelklicke auf der CD bei Verwendung von Windows 9x auf die Datei avwin9xp.exe, bei Verwendung von Windows NT/2000 auf die Datei avwinntp.exe. Dann erscheint gleich mal folgende Information



AntiVir\Windows\Windows NT/2000 (Windows 9x)

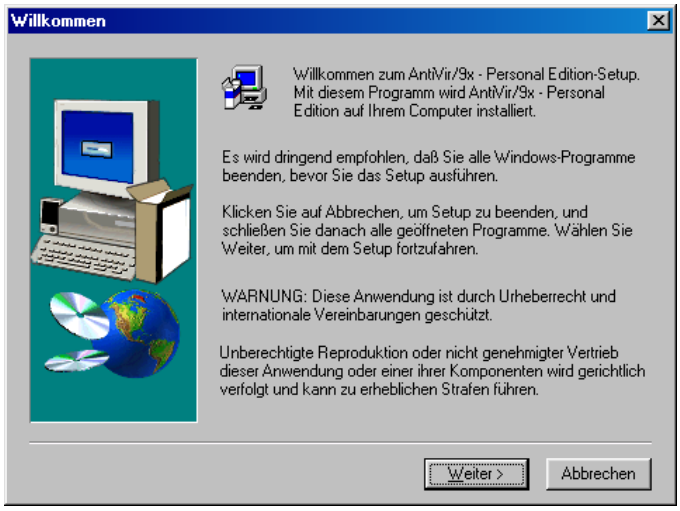
avwinntp.exe (avwin9xp.exe)



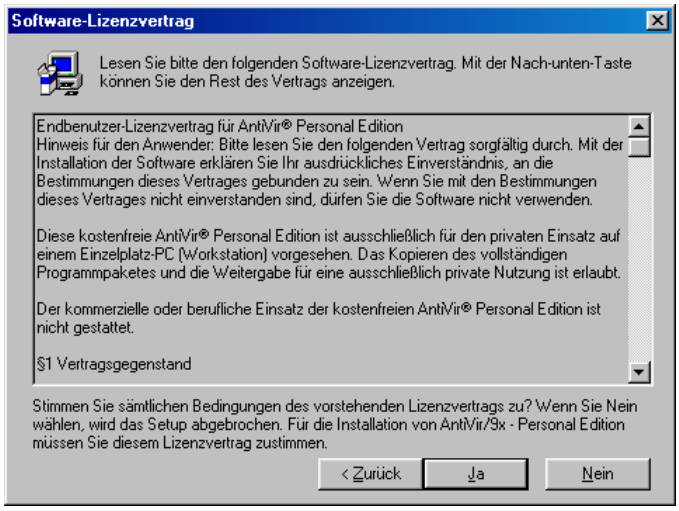
Der Installationsvorgang beginnt nach Drücken des Buttons „Setup“.

Zurück zum Inhalt dieses Kapitels

Dann erscheint das übliche Willkommensfenster:



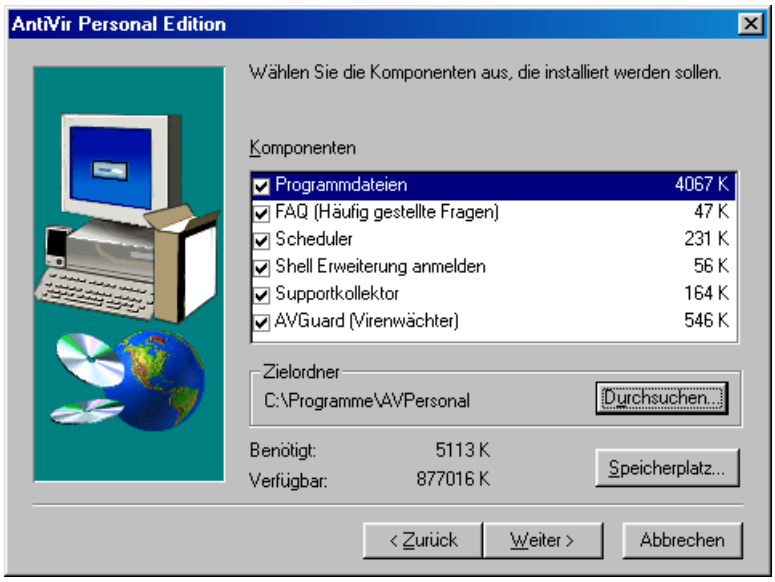
Bestätige das Fenster durch Drücken des Buttons „Weiter“. Dann kommt natürlich der Lizenzvertrag:



Bestätige das Fenster mit „Ja“.

Zurück zum Inhalt dieses Kapitels

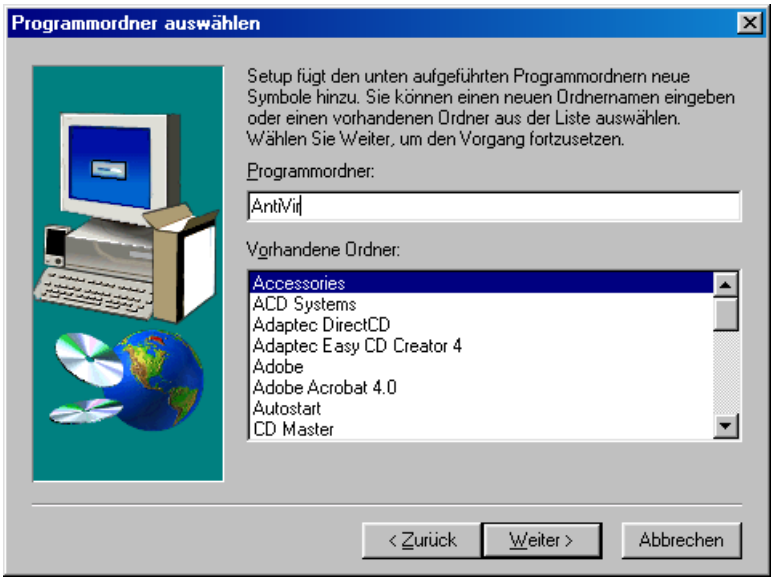
Nun kannst du dir die zu installierenden Komponenten und das Installationsverzeichnis (Zielordner) aussuchen:



Du willst natürlich wie vorgeschlagen alles installieren. Nimm den vorgeschlagenen Installationsordner (Zielordner) oder gib einen dir genehmeren an. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

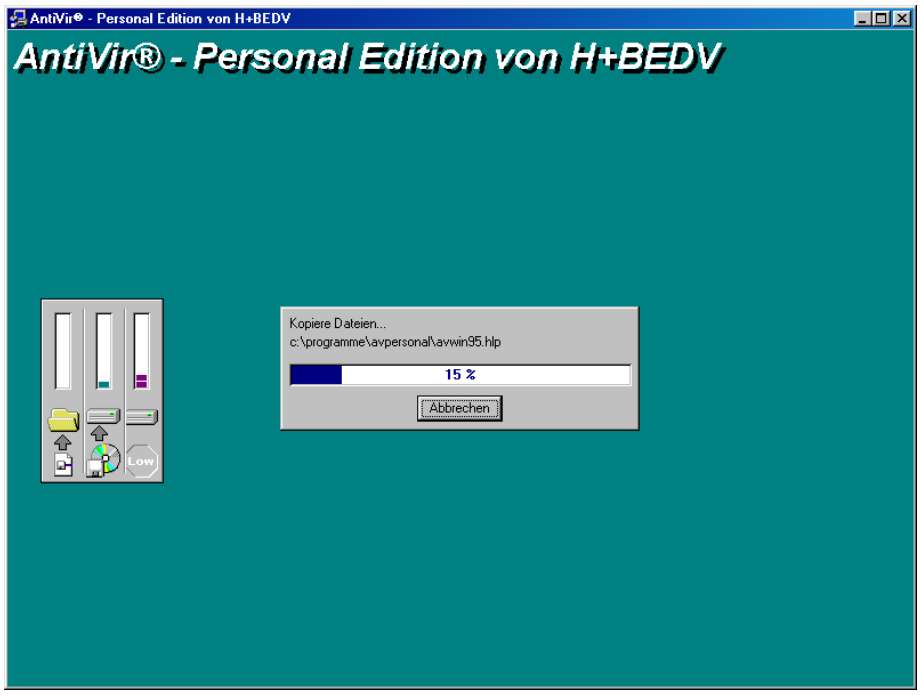
Jetzt kannst du dir den Programmordner aussuchen, unter dem das Programm im Start-Menü erscheint.



Nimm einfach den vorgeschlagenen Namen oder gib einen anderen an, unter dem du das Programm dann im Start-Menü wiederfindest (z.B. reicht „AntiVir“ hier im Beispiel). Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann beginnt die eigentliche Installation des Programms.



Zurück zum Inhalt dieses Kapitels

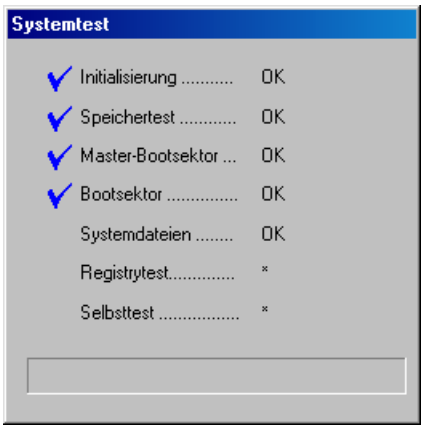
Nach dem Beenden der Installation wirst du gefragt, ob du gleich deinen Computer nach Viren durchsuchen willst.

Es ist sicherlich eine gute Idee, diese Suche jetzt gleich mal durchzuführen. Danach kannst du ziemlich sicher sein, keinen Virus (mehr) auf dem Computer zu haben. Wähle also wie vorgeschlagen „Ja, jetzt nach Viren suchen“ und drücke den Button „ Weiter“.

Falls du aber gerade keine Zeit dafür hast, den doch etwas zeitraubenden Virensuchvorgang abzuwarten, kannst du natürlich auch zu einem späteren Zeitpunkt jederzeit deinen Computer nach Viren durchsuchen lassen.

Zurück zum Inhalt dieses Kapitels

Beim Normalbetrieb kannst du dir aussuchen, welche Festplatten bzw. Disketten nach Viren durchsucht werden. Hier wird gleich mal ohne viel zu fragen alles durchsucht. Zuerst wird ein Systemtest durchgeführt:



Bei diesem Systemtest wird z.B. dein Arbeitsspeicher nach Viren durchsucht, außerdem beinhaltet so ein Test auch immer den Selbsttest, bei dem das Programm prüft, ob es nicht selbst von einem Virus befallen ist.

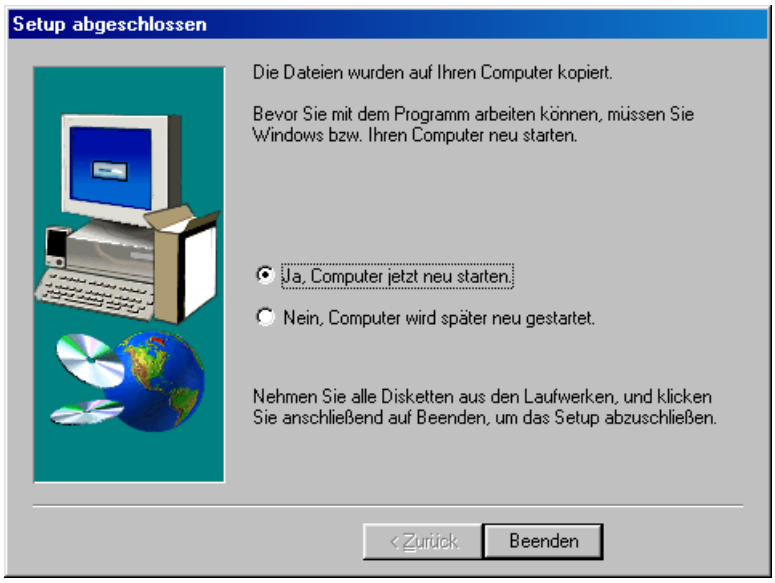
Zurück zum Inhalt dieses Kapitels

Dann werden alle anderen Dateien auf deinem Computer nach Viren durchsucht:

Du kannst den Suchvorgang jederzeit durch Drücken des Buttons „Stop“ abbrechen.

Zurück zum Inhalt dieses Kapitels

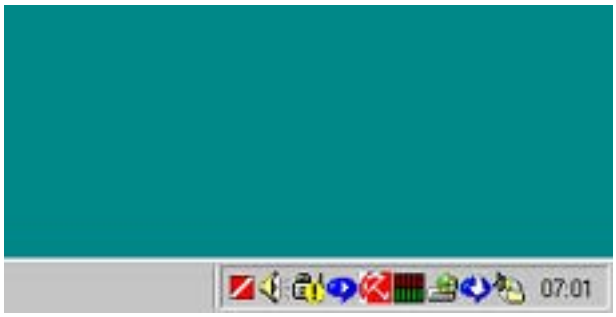
Falls ein Virus gefunden wurde, wirst du immer gefragt, ob die befallene Datei repariert werden soll, was du natürlich immer willst. Nach dem Ende der Installation musst du den Computer neu starten.



Drücke den Button „Beenden“, Windows wird dann beendet und der Computer neu gestartet.

Zurück zum Inhalt dieses Kapitels

Nach dem Neustart findest du das Regenschirm-Symbol am rechten unteren Rand deines Bildschirms.



Das bedeutet, dass der Virenwächter nun im Hintergrund darauf aufpasst, dass kein Virus auf deinen Computer kommt.

Zurück zum Inhalt dieses Kapitels

14.2 Die Verwendung von AntiVir

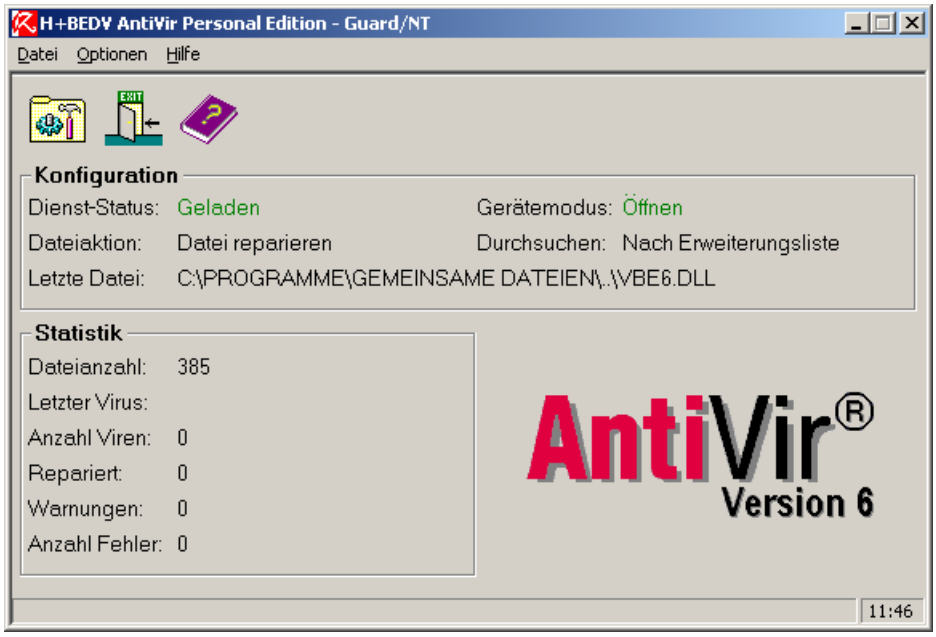
Der AntiVir Guard

Nach der Installation von AntiVir ist der AntiVir Guard automatisch aktiviert und wird bei jedem Start von Windows automatisch gestartet.

Dieser Guard wacht die ganze Zeit im Hintergrund darauf, dass dir kein Computervirus auf den Computer kommt. Alle Dateien, die einen Virus enthalten könnten, werden vor dem Starten schnell auf Viren geprüft. Beinhaltet eine Datei einen Virus, wirst du sofort informiert und kannst den Virus entfernen lassen.

Dass dieser Guard läuft, erkennst du am weißen Regenschirm auf rotem Hintergrund am rechten unteren Rand deines Bildschirms.

Für Neugierige: wenn du auf dieses kleine Regenschirm-Symbol am rechten unteren Rand deines Bildschirms doppelklickst, erhältst du ein Fenster mit einer Statistik, was der Guard so geprüft hat:

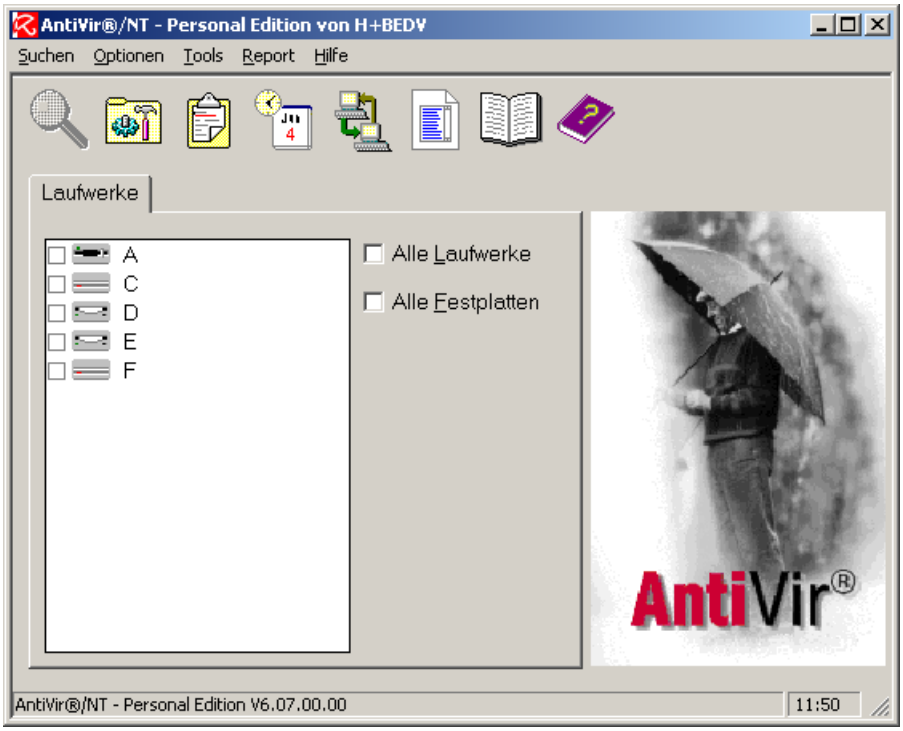


Zurück zum Inhalt dieses Kapitels

Das Durchsuchen nach Computerviren

Wenn du z.B. eine Diskette von einer anderen Person erhältst, willst du möglicherweise sichergehen, dass diese Diskette keinen Virus enthält. Dazu dient das „Hauptprogramm“ von AntiVir. Mit diesem Programm kannst du angeben, was du gezielt nach Viren durchsuchen willst.

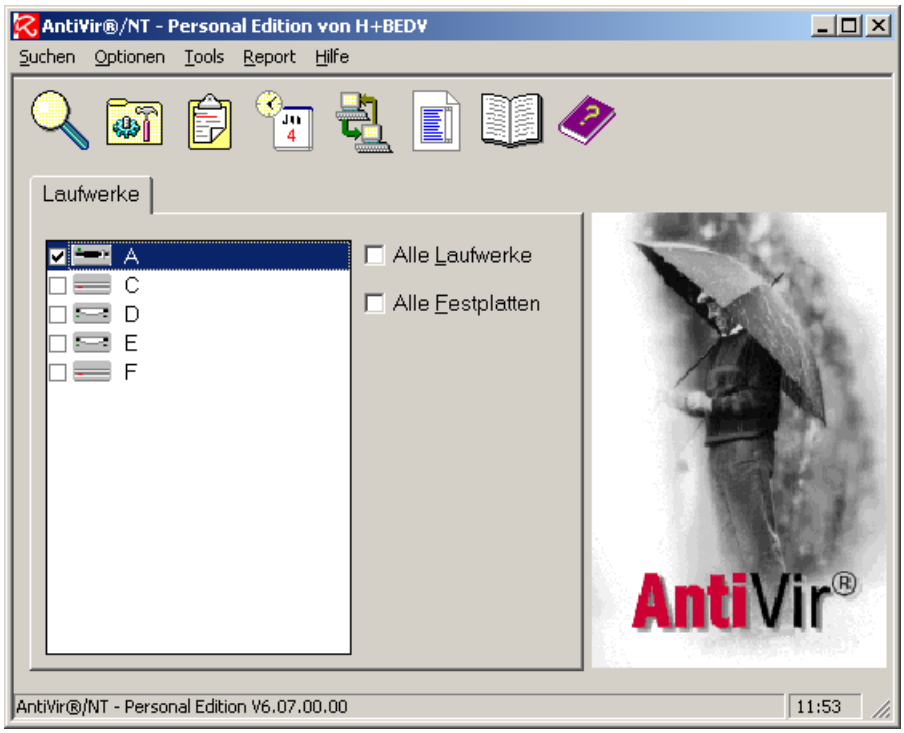
Du findest es im Startmenü unter „Start ⇨ Programme ⇨ AntiVir (Personal Edition...) ⇨ AntiVir 9x oder AntiVir NT“ - je nach installierter Betriebssystemversion.



Du kannst dir nun aussuchen, welche Bereiche du nach Viren durchsuchen willst. Du findest in der Liste übrigens auch eine eventuell eingerichtete PGP Disk-Partition, die wie eine eigene Festplatte angezeigt und behandelt wird.

Zurück zum Inhalt dieses Kapitels

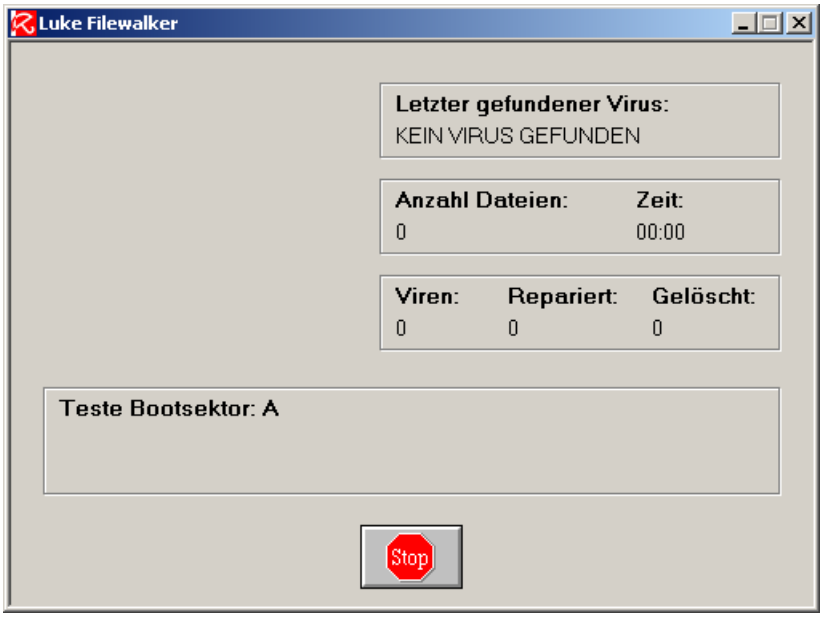
Für das Durchsuchen einer Diskette kreuze das Feld neben A (als Standard-Laufwerksbuchstaben für Diskettenlaufwerke) an.



Drücke dann den Button mit der Lupe für „Suchen“.

Zurück zum Inhalt dieses Kapitels

Dann beginnt das Durchsuchen der Diskette, was bei einer Diskette sehr schnell geht.



In diesem Beispiel wird gerade angezeigt, dass noch kein Virus gefunden wurde.

Zurück zum Inhalt dieses Kapitels

Nach dem Durchsuchen erhältst du einen Report über die Suche.

In diesem Beispiel wurden 2 Dateien durchsucht, dabei keine Viren gefunden und daher auch keine Viren entfernt.

Nach Drücken des Buttons „OK“ kehrst du zum Hauptprogramm-Fenster zurück.

Zurück zum Inhalt dieses Kapitels

15 Tipps für Passwörter/Passphrases

Überblick

Der wichtigste Schutz vor unbefugtem Zugriff auf deinen Computer bzw. die Daten darauf sind immer die zugehörigen Passwörter (oder z.B. bei PGP ganze Passwort-Sätze - Passphrases).

Es ist also ungemein wichtig, dass deine Passwörter nicht geknackt werden. Dazu ist es wichtig zu wissen, wie Programme versuchen, deine Passwörter herauszufinden. Sie machen es einfach durch Ausprobieren.

Es ist völlig sinnlos, ganz tolle Programme zur Computersicherheit zu installieren und sie nur mit schlechten Passwörtern zu schützen. Nach Herausfinden des Passworts können natürlich so wie du auch neugierige Menschen auf deine Daten problemlos zugreifen.

Du findest Beschreibungen zu folgenden Bereichen:

- Wie werden Passwörter geknackt?
- Tipps für Passwörter

15.1 Die Tipps

Wie werden Passwörter geknackt?

An erster Stelle steht immer die lexikalische Suche. Das heißt, dass alle Wörter von verschiedenen Sprachen ausprobiert werden, die in Lexikona zu finden sind.

Nimmst du also z.B. „Haus“, „Dach“ oder „Maxi“ als Passwort, haben diese Programme kein großes Problem es herauszufinden.

Der nächste Schritt ist dann die Kombination von Wörtern. Wenn dein Passwort also z.B. „Hausdach“ ist, werden es diese Programme ebenfalls schnell knacken können.

Sehr beliebt bei Computer-EinbrecherInnen sind auch Standardpasswörter, die bei der Installation vergeben werden. Es wird zwar so gut wie immer bei der Installation darauf hingewiesen, dass mensch diese Erst-Passwörter nach der Installation sofort ändern soll, viele vergessen aber dann darauf.

Zurück zum Inhalt dieses Kapitels

Tipps für Passwörter

Was mensch dagegen tun kann, ist Passwörter zu wählen, die in der Realität (im Lexikon) nicht vorkommen. Außerdem sollte mensch Ziffern, Sonderzeichen wie Strich- oder Doppelpunkte oder ähnliches daruntermischen.

Aber irgendwie muss mensch sich ja ihr/sein ausgeklügeltes Passwort auch merken. Dazu gibt es mehrere mögliche Vorgangsweisen, hier ein paar Vorschläge dazu:

- Denke dir einen Satz aus, nimm die jeweils ersten Buchstaben des Satzes und stelle so dein Passwort zusammen. Beispiel: der Satz lautet „Heute ist ein schöner Tag; ich fahre in die Lobau!“, das würde z.B. das Passwort „Hi1sT;ifidL!“ ergeben.
- Nimm statt der ersten die letzten Buchstaben eines Satzes, das ergäbe beim obigen Beispiel „!Ldifi;Ts1iH“. Das ist aber dann ein wenig schwieriger zu merken bzw. einzutippen.
- Wenn du wie z.B. bei PGP die Möglichkeit hast, ganze Sätze anzugeben, nutze diese Möglichkeit, mische aber trotzdem zumindest ein Wort wie im ersten Beispiel darunter.
- Je länger und (lexikalisch gesehen) wirrer ein Passwort ist, desto schwieriger ist es zu knacken.

Das sind nur einige Möglichkeiten, wenn du diese Grundregeln beachtest, sind deiner Phantasie keine Grenzen gesetzt.

Und dass Passwörter nicht gerade auf einem Zettel neben dem Computer oder im Adressbuch notiert werden sollten (auch nicht im Geheimtresor hinter dem Van Gogh-Gemälde), versteht sich wohl von selbst, wird aber erfahrungsgemäß oft missachtet.

Eine Empfehlung ist auch, für den Systemstart (Windows oder andere), für PGP und andere Dinge nicht das gleiche Passwort zu verwenden. Der Sinn dahinter ist, dass ein neugieriger Mensch, der dein Systempasswort herausfindet, damit nicht auch gleich z.B. in deine verschlüsselten Daten Einsicht nehmen kann.

Auch sollte mensch die Passwörter unbedingt von Zeit zu Zeit wechseln, muss ja nicht jeden Tag sein.

Zurück zum Inhalt dieses Kapitels

16 Lexikon

Client

Wird für Computer und für Programme verwendet. Ist das Programm, das die Dienste eines Serverprogramms in Anspruch nimmt.

Beispiel Internet: an deinem Computer (Client) möchtest du eine Internetseite sehen. Dazu wird von deinem Computer bzw. dem Programm (dem Browser, ist ein Client-Programm) eine Anfrage an einen Server mit einem Serverprogramm gestellt und von diesem die Internetseite an deinen Computer und dein Clientprogramm (an deinen Browser) geschickt.

Computerdaten

Als Daten werden normalerweise alle Dateien, die keine Programme sind bzw. nicht direkt zu einem Programm gehören, bezeichnet. Das sind also z.B. deine Mails, deine Word-Dokumente etc.

Dateien allerdings können sowohl Programme (Programmdateien) oder normale Daten, wie oben beschrieben, sein.

Daten

Siehe Computerdaten

Decrypt

Entschlüsseln, einen verschlüsselten Text wieder lesbar machen.

Encrypt

Verschlüsseln, einen normalen Text (oder eine ganze Datei) für nicht Berechtigte unlesbar machen.

Export Key

Exportieren eines Schlüssels, bei PGP das Speichern eines Schlüssels des Schlüsselbunds in einer normalen Textdatei.

Firewall

Programm, das zwischen den Programmen deines Computers und dem Internet steht. Es überwacht den Datenverkehr zwischen deinem Computer und dem Internet.

Dabei wird sowohl geprüft, was für Daten von deinem Computer nach aussen gehen und welche Programme aufs Internet zugreifen, als auch, was von aussen zu deinem Computer kommt.

Hoax

"Hoax" ist eine englische Bezeichnung für "schlechter Scherz". Der Begrieff "Hoax" hat sich im Internet als Bezeichnung für die zahlreichen falschen Warnungen vor bösartigen Computerprogrammen eingebürgert, die angeblich Festplatten löschen, Daten ausspionieren oder anderweitig Schaden auf den Rechnern der Betroffenen anrichten sollen.

Nicht nur Neulinge im Netz, sondern auch erfahrene Netzwerk-Administratoren fallen auf die schlechten Scherze oft herein, die via elektronischer Post (E-Mail) wie ein Kettenbrief durch das weltumspannende Computernetzwerk wandern.

Der Chaos Computer Club (CCC) in Hamburg warnt vor Leichtgläubigkeit: "Wer etwas nachdenkt, kommt darauf, dass das Quatsch sein muß. Die Warnungen enthalten zudem oft völlig allgemeine Aussagen, wie jeder, der diese Mail öffne, sei betroffen, alle Computer würden zerstört, obwohl so etwas nicht möglich ist."

Kein Virus sei in der Lage, so der Club, sämtliche Mail-Programme und Computer- Konfigurationen so genau zu kennen, daß er auf allen Rechnern Schaden anrichten könne. "Jede Warnung im Internet per E-Mail ist primär erstmal als Hoax oder Verulkung einzustufen". Insofern sind Hoaxes durch die Ausfälle an Arbeitszeit dann doch oft gefährlich

Im Standard-ASCII-Format erstellte E-Mails (Microsoft Outlook bezeichnet dieses Format als "nur Text"-Format) sind bezüglich des eigentlichen Textes unbedingt als virenfrei anzusehen. Die Warnung vor solchen E-Mails ist der eigentliche Virus und wird als "HOAX" bezeichnet.

Definition aus http://www.glossar.de, siehe auch Virus, Wurm, Trojanisches Pferd (Trojaner)

Import Key

Importieren eines Schlüssels, bei PGP das Aufnehmen eines Schlüssels von einer normalen Textdatei in deinen Schlüsselbund.

Key

Schlüssel, kann bei PGP der private (secret key, private key) oder der öffentliche (public key) sein.

Key File

Datei, die einen Schlüssel enthält. Der Schlüssel wird bei PGP durch Exportieren (export key) in diese Datei gespeichert und durch Importieren (import key) in den Schlüsselbund aufgenommen.

Key Server

Computer, die dazu existieren, um die öffentlichen Schlüssel (public keys) zu speichern und für andere Personen zugänglich zu machen.

Keyring

Schlüsselbund, besteht bei Erstellung zunächst nur aus deinem privaten (secret key, private key) und deinem eigenen öffentlichen Schlüssel (public key).

Danach können öffentliche Schlüssel von anderen Personen in den Schlüsselbund aufgenommen werden, um diesen Personen verschlüsselte Nachrichten zusenden zu können.

Kontextmenü

Durch Zeigen auf ein bestimmtes Element mit dem Mauszeiger und drücken der rechten Maustaste geht ein Menü auf, das auf das Element angepasst ist.

Für LinkshänderInnen kann dafür auch die linke Taste eingestellt sein.

Kryptographie

Verschlüsselungstechniken.

Mount

Logisches Dazuhängen an dein Dateisystem. Logisch deshalb, weil es der BenutzerIn (bzw. einem Programm) völlig gleich ist, wo und wie der dazuzuhängende Teil physikalisch gespeichert wurde.

Bei PGP das Dazuhängen einer PGP Disk an dein Dateisystem. Diese Disk erhält dann einen eigenen Laufwerksbuchstaben und ist in deinem Dateisystem (z.B. im Windows Explorer) wie eine eigene Festplatte zu behandeln.

Netzwerk

Durch irgendeine Verbindung verbundene Computer. Meist sind sie mittels Kabel verbunden, können aber auch z.B. durch eine Satellitenverbindung verbunden sein.

Öffentlicher Schlüssel

Siehe Public Key

Passphrase

Wie ein Passwort, es können aber ganze Sätze statt nur ein einzelnes Passwort angegeben werden.

PGP Disk

Teilprogramm von PGP zur Erstellung von verschlüsselten Partitionen (Teile von Festplatten, Disketten u.a.).

Eine PGP Disk, die einfach eine eigene Datei auf deinem Computer ist, wird dann zu deinem Dateisystem gemounted, die Daten darauf werden erst nach Eingabe des Passworts (der Passphrase) lesbar.

PGP Keys

Teilprogramm von PGP zur Erstellung und Verwaltung der privaten (secret keys, private keys) und öffentlichen Schlüssel (public keys).

PGP Tools

Alle PGP Programme, ist eine Leiste mit Symbolen der Teilprogramme von PGP.

Private Key

Siehe Secret Key

Privater Schlüssel

Siehe Secret Key

Provider

Firma, die dir den Zugang zum Internet ermöglicht.

Public Key

Der Schlüsselteil, der anderen Personen ermöglicht, der BesitzerIn des öffentlichen Schlüssels verschlüsselte Nachrichten zu senden.

Die BesitzerIn des öffentlichen Schlüssels benötigt dann auch ihren privaten Schlüssel (private key, secret key), um die Nachricht entschlüsseln zu können.

Du schickst deinen öffentlichen Schlüssel an andere Personen, diese können dir dann verschlüsselte Nachrichten senden.

Du hast öffentliche Schlüssel von anderen Personen, damit kannst du diesen Personen verschlüsselte Nachrichten senden.

Schlüsselbund

Siehe Keyring

Secret Key

Dieser Schlüssel (privater Sclüssel, secret key, private key) ist Teil des Schlüsselpaars. Er bleibt bei dir und wird nicht wie der öffentliche Schlüssel weitergegeben.

Du benötigst diesen privaten Schlüssel, um für dich verschlüsselte Nachrichten entschlüsseln zu können. Andere Personen benötigen diesen Schlüssel nicht.

Server

Wird für Computer und für Programme verwendet. Ist das Programm, das Anfragen von Clients (Client-Programmen) entgegennimmt und erfüllt.

Beispiel Internet: an deinem Computer (Client) möchtest du eine Internetseite sehen. Dazu wird von deinem Computer bzw. dem Programm (dem Browser, ist ein Client-Programm) eine Anfrage an einen Server mit einem Serverprogramm gestellt (Internetserver) und von diesem dann die Internetseite an deinen Computer und dein Clientprogramm (an deinen Browser) geschickt.

Sign/Signed

Signieren einer Nachricht, bei PGP das Verschlüsseln einer Nachricht mit Eingabe des Passworts (der Passphrase).

Bei PGP können Texte sowohl signed als auch unsigned (ohne Angabe des Passworts) verschlüsselt werden. Es wird jedoch empfohlen, bei der Verschlüsselung immer zu signieren (Encrypt & Sign), da für die EmpfängerIn nur so sichergestellt ist, dass die Nachricht auch von der angenommenen Person geschickt wurde.

Die EmpfängerIn sieht in der Nachricht, ob sie signiert wurde oder nicht.

Trojanisches Pferd, Trojaner

Der wesentliche Unterschied zwischen Viren und Trojaner besteht darin, dass sich Trojaner nicht selbständig fortpflanzen können. Ein Trojan ist nichts anderes, als ein eigenständiges Programmm, das die Daten des Computers für andere freigibt.

Dazu muss es aber bei jedem Systemstart geladen werden. Das geschieht meist über die Windows-Registry mit entsprechenden Autorun-Einträgen.

Ein Trojan ist eine .exe-Datei die sich irgendwo im System versteckt hält, sich aber jedoch im Gegensatz zu Viren auch händisch löschen lässt - vorausgesetzt man weiß wie.

Definition aus http://www.anti-trojan.net/, siehe auch Virus, Wurm, Hoax

Unmount

Abhängen von deinem Dateisystem. Bei PGP das Abhängen einer PGP Disk von deinem Dateisystem. Die Daten auf dieser PGP Disk sind dann bis zum nächsten Mountvorgang nicht lesbar, der zugeteilte Laufwerksbuchstabe verschwindet z.B. aus dem Windows Explorer.

Unsigned

Nicht signiertes Verschlüsseln einer Nachricht (Encrypt im Gegensatz zu Encrypt & Sign), d.h. Verschlüsseln ohne Angabe des Passworts (der Passphrase).

Bei PGP können Texte sowohl signed als auch unsigned (ohne Angabe des Passworts) verschlüsselt werden. Es wird jedoch empfohlen, bei der Verschlüsselung immer zu signieren (Encrypt & Sign), da für die EmpfängerIn nur so sichergestellt ist, dass die Nachricht auch von der angenommenen Person geschickt wurde.

Die EmpfängerIn sieht in der Nachricht, ob sie signiert wurde oder nicht.

Updates

Neuerungen bei Programmen, im Fall von AntiVir z.B. die Aufnahme neuer Viren in das Programm zur Virensuche.

Diese Updates können meist vom Internet auf den Computer geladen werden, wie diese Neuerungen in dein Programm eingespielt werden, beschreibt eine dazugehörige Dokumentation dort, wo du die Neuerungen herunterladest.

Verschlüsselung

Aus einzelnen Texten, irgendwelchen Dateien oder ganzen Festplattenbereichen (auch Bereiche von Disketten etc.) einen unlesbaren Haufen von scheinbar bunt zusammengewürfelten Zeichen machen.

Mit Hilfe eines oder mehrerer Schlüssel werden die Daten wieder entschlüsselt.

Nur die BesitzerIn des Passworts (der Passphrase) oder bei Mails die BesitzerIn des privaten Schlüssels (secret key, private key) kann die Daten wieder lesbar machen.

Virus

Unter Viren versteht man Programme bzw. Programmsequenzen, die sich an andere Dateien anhängen. Sie bilden somit keine eigenständige .exe-Datei die man im Dateisystem sehen, geschweige denn entfernen kann.

Viren haben meist die Eigenschaft, sich selbst fortzupflanzen. D.h. sobald ein Virus ein Programm infiziert hat, verbreitet er sich (meist während des Kopierens von Daten) weiter. Auch über Netzwerke (Internet) können somit Viren verbreitet werden, sobald jemand ein infiziertes Programm weiterschickt.

Viren können dann auf verschiedenste Weise ihr Unheil anrichten, z.B. Daten löschen, verändern, etc. Um Viren effizient löschen zu können, muss man die Bytesequenz des Viruses aus der Programmdatei rausfiltern.

Definition aus http://www.anti-trojan.net/, siehe auch Trojanisches Pferd (Trojaner), Wurm, Hoax

Virtuell

Nicht real existierend, bei PGP Disk verhält sich die verschlüsselte Partition (der verschlüsselte Festplattenbereich) wie eine zusätzliche Festplatte, auch wenn mensch keine neue Festplatte eingebaut hat.

Wurm

Diese neue Klasse von Viren hat sich in der letzten Zeit rasant verbreitet und sich innerhalb kürzester Zeit an die Spitze der Virenhitliste gesetzt. Das bekannteste Beispiel dieser Klasse dürfte der Virus VBS/Loveletter (auch VBS/Love oder VBS/ILoveYou genannt) sein. Technisch gesehen ist Loveletter ein Wurm. Ein Wurm ist ein Programm, das sich selbst zu vervielfältigen vermag, ohne ein Wirtsprogramm zu brauchen.

Diese Viren sind extrem einfach zu programmieren und verbreiten sich - entsprechende Techniken vorausgesetzt - innerhalb weniger Stunden per Email um die ganze Welt. Da durch einfaches Ändern einiger Textzeilen ein "neuer" Virus erzeugt werden kann, tauchen auch immer wieder leicht veränderte Ableger auf, die vielen Antivirenprogrammen Probleme bereiten. Von VBS/Loveletter beispielsweise sind über hundert Varianten bekannt.

Definition aus http://www.antivir.de, siehe auch Virus, Trojanisches Pferd (Trojaner), Hoax

17 Die CD

PGP

Unterverzeichnis	Datei	Beschreibung
Doku		Dokumentationen und Texte zu PGP
PGP Original Dokumentationen Englisch		Original Dokumentationen in Englischer Sprache
	PGPWinUsersGuide.pdf	PGP BenutzerInnenhandbuch
	IntroToCrypto.pdf	Einführung in die Kryptographie
PGP Dokumentation Deutsch		Dokumentation in Deutscher Sprache
	pgp5kurs.htm	Startseite zur Dokumentation
FAQ – Haeufig gestellte Fragen		Listen mit häufig gestellten Fragen zu PGP und deren Antworten
	Pgpfaq.html	Fragen und Antworten zu PGP mit Inhaltsverzeichnis
	Pgp-faq.de.html	Andere Fragen und Antworten zu PGP ohne Inhaltsverzeichnis
	hu-berlin antworten.htm	Noch mehr Fragen und Antworten zu PGP ohne Inhaltsverzeichnis

Unterverzeichnis	Datei	Beschreibung
Warum nicht Version 7		Dokumente, warum nicht die neueste PGP Version 7 verwendet werden sollte
	Warum nicht v7 – erklaerung.html	Erklärung von Kai Raven (siehe auch deutsche Anleitung), warum er die PGP Version 7 nicht unterstützt
Links		Diverse Links zu Verschlüsselung u.a.
	krypto.html	Viele Links zu Kryptographie, Hackerseiten u.a.
Windows		PGP Installationsprogramme für Windows
6.5.1		Version 6.5.1
Deutsch		Installationsprogramm der deutschen Version
	PGP651intFreeware_DE.exe	Installationsprogramm
Diskhack		Hackprogramm für PGP Disk
	pgpdiskhack.exe	Hackprogramm für PGP Disk
	pgpdiskhack.txt	Beschreibung zum Hackprogramm für PGP Disk
Englisch		Installationsprogramm der englischen Version
	PGPfreeware651int.exe	Installationsprogramm
6.5.3		Version 6.5.3
Englisch		Installationsprogramm der englischen Version
	Setup.exe	Installationsprogramm
	Whatsnew.txt	Infos zu Neuerungen dieser Version

Unterverzeichnis	Datei	Beschreibung
	WhatsNew.htm	Gleich wie Whatsnew.txt, aber für Webbrowser
Diskhack		Hackprogramm für PGP Disk
	pgpdiskhack.exe	Hackprogramm für PGP Disk
	pgpdiskhack.txt	Beschreibung zum Hackprogramm für PGP Disk
6.5.8		Version 6.5.8
Englisch		Installationsprogramm der englischen Version
	pgp658ckt02.exe	Installationsprogramm
	pgp658ckt02.txt	Beschreibung der Neuerungen dieser Version
8.0		Installationsprogramm der neuen Version 8
	PGP8.exe	Installationsprogramm der Gratis-Version 8
MacOS		PGP Installationsprogramme für MacOS
6.5.1		Version 6.5.1
	PGP651IntFreeware.hqx	Installationsprogramm
6.5.2		Version 6.5.2
	PGPfreeware652a.sit.hqx	Installationsprogramm
6.5.8		Version 6.5.8
	PGPFW658Mac.sit.bin	Installationsprogramm
7.0.3		Version 7.0.3
	PGPfreeware703.sit.bin	Installationsprogramm

Unterverzeichnis	Datei	Beschreibung
8.0		Version 8
	PGP800-F-X.sit.bin	
Unix		PGP Installationsprogramme für Unix-Derivate
AIX		Installationsprogramme für AIX
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.AIX_FW.tar.gz	Installationsprogramm
HP-UX		Installationsprogramme für HP-UX
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.HPUX_FW.tar.gz	Installationsprogramm
Linux		Installationsprogramme für Linux
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.Lnx_FW.tar.gz	Installationsprogramm
RedHat Linux		Installationsprogramme für RedHat Linux
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.Lnx_FW.rpm.tar	Installationsprogramm
Sun Solaris		Installationsprogramme für Sun Solaris
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.Sol_FW.tar.gz	Installationsprogramm
Sun Solaris – Package		Installationsprogramme für Sun Solaris

Unterverzeichnis	Datei	Beschreibung
6.5.8		Version 6.5.8
	PGPcmdln_6.5.8.SolPkg_FW.tar.gz	Installationsprogramm

ZoneAlarm

Unterverzeichnis	Datei	Beschreibung
Doku		Dokumentationen und Texte zu ZoneAlarm
	Zonealarm.html	Deutsche Anleitung
	Doku.html	Andere deutsche Anleitung
Zone		Bilder zu deutscher Anleitung
FAQ – Haeufig gestellte Fragen		Häufig gestellte Fragen
	support_za_all_faq.htm	Liste mit häufig gestellten Fragen zu ZoneAlarm und deren Antworten
Windows		Installationsprogramme für Windows
	zaSetup_1001.exe	Installationsprogramm

Window Washer (MacWasher)

Unterverzeichnis	Datei	Beschreibung
Windows		Installationsprogramme für Windows
4.1		Aktuelle Version 4.1
	wwinstall.exe	Installationsprogramm
MacOS		Installationsprogramme für MacOS
2.1.2		Aktuelle Version 2.1.2
	mwdemo.sit.hqx	Installationsprogramm
Doku		Dokumentation
	wwhelp.htm	Kurzdokumentation

WebWasher

Unterverzeichnis	Datei	Beschreibung
	betriebssysteme.txt	Liste mit Betriebssystemen, auf denen WebWasher läuft
3.0		Aktuelle Version 3.0
	wash30.exe	Installationsprogramm

JAP

Unterverzeichnis	Datei	Beschreibung
Doku		JAP
	index_de.html	Deutsche Anleitung
Windows		Installationsprogramme für Windows
	setup.exe	Installationsprogramm
Java JRE		Für Installation benötigtes Java Runtime Environment
	jre.exe	Installationsprogramm
MacOS		Installationsprogramm für MacOS
	JAPMacOSX.dmg.sit	Installationsprogramm
OS2		Installationsprogramme für OS2
	jap.jar	Installationsprogramm
	swingall.jar	Installationsprogramm
Unix		Installationsprogramme für Unix
	jap.jar	Installationsprogramm
	swingall.jar	Installationsprogramm

Ad-Aware

Unterverzeichnis	Datei	Beschreibung
	aaw.exe	Installationsprogramm von Ad-Aware

XP AntiSpy

Unterverzeichnis	Datei	Beschreibung
	xp-AntiSpy3D.exe	Programm für Windows XP (ohne Installation, einfach aufrufen)

Webwasher

Unterverzeichnis	Datei	Beschreibung
Windows 95-98-ME-NT-2000 3.0		Installationsprogramm für Windows-Versionen (nicht für Windows XP!)
	wash30.exe	Installationsprogramm
Windows 95-98-ME-NT-2000-XP 3.2 Beta		Installationsprogramme für Windows-Versionen inklusive Windows XP
	wash32b4	Installationsprogramm der Beta-Version
MacOS 2.1.1		Installationsprogramm für MacOS
	ww211rc-ger.sit	Installationsprogramm
Linux 3.0 tar.gz		Installationsprogramm für Linux mit tar.gz
	webwasher-3.0-linux-i386.tar.gz	Installationsprogramm
Linux 3.0 rpm		Installationsprogramme für Linux mit rpm
	webwasher-3.0-linux-i386.rpm	Installationsprogramm

AntiVir

Unterverzeichnis	Datei	Beschreibung
Windows		Installationsprogramm für alle Windows-Versionen
6.16		Verzeichnis mit aktueller Version
	avwinsfx.exe	Installationsprogramm

18 Indexverzeichnis

19 Quellen/Verweise/Weitere Infos

Software

http://www.pgp.com/	PGP
http://www.webroot.com/	Window Washer (MacWasher)
http://www.zonelabs.com	Zone Alarm
http://www.free-av.de/	AntiVir
http://www.webwasher.com/	WebWasher (WebWasher Client)
http://www.eudora.com/	Eudora
http://anon.inf.tu-dresden.de/	JAP
http://www.lavasoft.de/	Ad-Aware
http://www.xpantispy.de	XP AntiSpy
http://www.webwasher.com/	Webwasher
http://www.heise.de/ct/shareware/	Diverse Programme, gratis oder fast gratis
http://www.gulli.com/tools/	Eine Reihe nützlicher Werkzeuge und Anwendungen, die mensch im alltäglichen Onlineleben immer wieder braucht: von der whois-Abfrage bis zum Passwortgenerator.

Computersicherheit

http://www.ccc.de/	Chaos Computer Club e.V. - Kabelsalat ist gesund: genau DER legendäre Computerclub. Informationen zu Netzpolitik, Überwachung, Strategien und Aktionen gegen (Internet)-Zensur.
http://www.datenschutz.de/(de)/	“Virtuelles Datenschutzbüro”, zahlreiche leicht verständliche Infos zu Datenschutz und Überwachung
http://www.it-secure-x.net	Viele Fragen und Antworten zu Computersicherheit, zahlreiche Gratis-Software zum Thema Computersicherheit zum downloaden
http://www.bluemerlin-security.de	Viele Infos zu „Trojanischen Pferden“, zahlreiche Gratis-Software zum Thema Computersicherheit zum downloaden
http://www.anti-trojan.net/	Infos zu „Trojanischen Pferden“, Testversion und kostenpflichtige Software, gratis Online-Check
http://de.trendmicro-europe.com/	Informationen zu aktuellen Viren inklusive Virenkarte und "Topliste" der aktivsten Viren.
http://www.privacy.net/	Infos und Checks zu Sicherheit im Internet und bei der Datenübertragung
http://www.kryptocrew.de	Derzeit „nur“ zahlreiche Links zum Thema Computersicherheit
https://grc.com/x/ne.dll?bh0bkyd2	Gratis-Sicherheitscheck „Shields UP“ für Internetverbindungen
http://www.gulli.com/tools/anoncheck.html	Hier kannst du dir die Informationen ansehen die beim Internetseitenaufruf von deinem Browser mitgesendet werden.

Online-Zeitungen

http://www.heise.de/tp/	Telepolis, sehr nette Online-Zeitung, die viel zu Überwachung und Internet schreibt (große Empfehlung)

Allgemeines

http://www.glossar.de	Alle möglichen Begriffe aus der Computerwelt erklärt, nach Anfangsbuchstaben sortiert
http://www.pc-helpnet.de/board/index.php	Computer Board, allgemeine Fragen und Antworten zu Computern
http://www.gulli.com/lexikon/	Lexikon: von appz bis warez - underground-internet-lexikon. Das gulli:lexikon bietet Erklärungen von Szenebegriffen, die in anderen Online-Lexika meistens vergeblich gesucht werden.

Bücher

http://members.aol.com/InfoWelt/buch.html	„Vom Ende der Anonymität, die Globalisierung der Überwachung“, Buch von Christiane Schulzki-Haddouti
http://members.aol.com/InfoWelt/buch2.html	„Datenjagd im Internet, eine Anleitung zur Selbstverteidigung“, auch sehr gutes Buch von Christiane Schulzki-Haddouti