Handbuch

Computersicherheit 1.2

Ein kleines Handbuch...

Version 1.2

Inhaltsverzeichnis

1 Inhalt

Überblick

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

Du findest folgende Infos:

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, vor allem bei Verwendung des Betriebssystems Windows. 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 Liste Verweise zu Internetseiten, auf denen es detailliertere Informationen gibt.

Den größten Teil des Handbuchs bilden die ausführlichen Installations- und Bedienungsanleitungen der behandelten Programme. Mit diesen Anleitungen solltest du die behandelten Programme problemlos selbst installieren und bedienen können, auch wenn hier nicht die allerletzte aktuellste Version beschrieben ist.

Zurück zum Inhalt dieses Kapitels

Benötigte Kenntnisse

Zum Lesen dieses Handbuchs brauchst du zwar keine „Computer-ExpertIn“ 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 (Arbeitsplatz) u.ä.

Zurück zum Inhalt dieses Kapitels

Was gibt es Neues in dieser Version?

Lange, lange ist es her, dass die letzte Version 1.1 dieses Handbuchs erschienen ist – und natürlich hat sich sehr viel getan in dieser Zeit. Die in den früheren Versionen angeführten Probleme und Programme sind aber noch immer aktuell, neue Bereiche sind hinzugekommen.

Die Programmversionen, die wir auf der zugehörigen CD zur Verfügung gestellt haben, sind großteils längst durch neue Versionen ersetzt worden. Natürlich haben wir auch die Versionen auf der CD und einige Installationsbeschreibungen aktualisiert. Am Besten ist aber, wenn du dir die jeweils aktuellen Version im Internet herunterladest, die zugehörigen Internet-Adressen findest du bei den Links.

Wir wollen in dieser Version neben den aktualisierten und den wenigen neu vorgestellten Programmen vor allem ein paar Themenbereiche ansprechen, die bezüglich Computersicherheit überaus wichtig sind (z.B. Browser, das Zusammenspiel von Computerviren, Spyware und Spam u.a.).

Wenn du die früheren Versionen des Handbuchs kennst (Versionen 1.0 und 1.1), musst du aber nicht alles noch einmal durchackern. Bei folgenden Themen hat sich zur letzten Version 1.1 etwas geändert.

Grundlegendes

- Uns fallen immer neue Themenbereiche und Programme ein, die wir gerne im Rahmen dieses Handbuchs vorstellen würden, z.B. eine Alternative zum kostenlosen Anti-Virenprogramm AntiVir, Anti-Spamprogramme etc.

Allerdings würde das Handbuch dadurch unübersichtlich werden, und das wollen wir unbedingt vermeiden. Wir haben daher z.B. die Anleitung zu Kaspersky Anti-Virus (als kostenpflichtige Alternative zum freien AntiVir) in ein eigenes Dokument auf der CD übersiedelt – wenn du dich dafür interessierst, findest du dort alles Wissenswerte.

Geändert

- Die wichtigste Änderung in diesem Handbuch ist der Umstieg vom in früheren Versionen vorgestellten Programmpaket PGP (Pretty Good Privacy) auf die kostenlosen OpenSource-Programme Windows Privacy Tools (WinPT, zum Verschlüsseln von Texten/Mails und einzelnen Dateien mittels GnuPG) und TrueCrypt (zum Verschlüsseln von Festplattenbereichen).

  Einer der Gründe dafür ist, dass es seit der aktuellen PGP Version 9 keine kostenlose Version mehr gibt.

Neu

- Zum Problem „Spyware“ (Spionage-Programme) stellen wir neben den schon in den früheren Versionen dieses Handbuchs beschriebenen Programmen Ad-Aware und XP-Antispy noch das ebenfalls kostenlos erhältliche Programm Spybot Search & Destroy vor.

  Und dabei haben wir auch einen äußerst peinlichen Fehler bei den Links ausgebessert: Wir haben in der Handbuchversion 1.1 einen falschen Link zu XP Antispy angeführt. Die in Version 1.1 dieses Handbuchs angegebene Webseite versucht, einen Dialer zu installieren. Wie gesagt, peinlich peinlich – wir bitten vielmals um Entschuldigung.

- Im Kapitel über Anti-Virenprogramme stellen wir neben dem kostenlosen Virenscanner AntiVir auch noch einen zweiten, kostenpflichtigen vor: Kaspersky Anti-Virus. Das deshalb, weil AntiVir im Gegensatz zu Kaspersky in Tests wiederholt nicht besonders gut abgeschnitten hat.

  Das Handbuch selbst beinhaltet allerdings keine komplette Installations- und Bedienungsanleitung zu Kaspersky Anti-Virus, die findest du in einer eigenen Anleitung auf der CD.

- Ein Kapitel beschäftigt sich mit Spam (Mails mit absolutem Mist wie Viagra-Sonderangeboten, Geldanlage, Penisverlängerungen, Pornowerbung u.ä.). Das Kapitel gibt auch ein paar Tipps, wie mensch Spam so halbwegs in den Griff bekommen kann.

- Ein weiteres sehr wichtiges neues Kapitel beschäftigt sich mit der Sicherheit von Internet-Browsern (den Programmen, mit denen du im Internet surfst) und gibt Empfehlungen zur Verwendung dieser Browser.

  Du findest auch Links, bei denen du die Sicherheit deines Browsers, Mail-Programms und Anti-Virenprogramms selbst prüfen kannst.

Weggefallen

- Das Programm WebWasher zum Herausfiltern von Werbebannern und Webkäfern (Webbugs) aus Internetseiten haben wir in dieser Ausgabe des Handbuchs gestrichen.

  Gründe sind neben dem bereits in Grundlegendes angesprochenen Problem der Übersichtlichkeit des Handbuchs, dass kaum jemand WebWasher verwendet und dass die meisten Probleme, die WebWasher beseitigt, bereits in den (guten) Internet-Browsern selbst gelöst werden (z.B. Webbugs, Popup-Fenster etc. in Firefox).

- Wie bereits erwähnt, sind alle Beschreibungen in Zusammenhang mit PGP (Pretty Good Privacy) weggefallen. Als Ersatz dafür werden jetzt Windows Privacy Tools (mit GnuPG) und TrueCrypt vorgestellt und beschrieben.

- Weiters weggefallen sind alle Anleitungen für das Mailprogramm Microsoft Outlook. Es ist zwar noch immer weit verbreitet, wir empfehlen aber (nicht nur) aus Sicherheitsgründen dringend einen Umstieg auf ein anderes Mailprogramm.

  Wir beschränken uns in diesem Handbuch auf konkrete Beschreibungen für die kostenlosen Mailprogramme Thunderbird und Eudora (z.B. in Zusammenhang mit Verschlüsselung). Du findest aber auch eine Anleitung, wie du mit jedem beliebigen Mailprogramm oder über Webmail Mails ver- und entschlüsseln kannst.

Aktualisiert

- Alle Programmversionen auf der CD und alle Installations- und Bedienungsbeschreibungen dieser Programme wurden aktualisiert (Stand November 2005).

- Die Beispiel-Installationen in dieser Version des Handbuchs wurden auf Windows XP durchgeführt.

- Natürlich haben wir auch die Internet-Links durchgecheckt und ein bisschen erweitert.

Zurück zum Inhalt dieses Kapitels

In diesem Handbuch behandelte Programme

Du findest in diesem Handbuch Installations- und Bedienungsanleitungen zu folgenden Programmen:

- Windows Privacy Tools: Zum Ver- und Entschlüsseln von Texten, z.B. von Mails mittels GnuPG, Ersatz für Pretty Good Privacy (PGP)
- TrueCrypt: Zum Verschlüsseln von ganzen Festplattenbereichen, Ersatz für PGP Disk
- Zone Alarm: Firewall, zum Schutz vor Zugriffen von außen bei Internetverbindungen, nur für das Betriebssystem Windows
- AntiVir: Anti-Virenprogramm, nur für das Betriebssystem Windows
- JAP: Java Anon Proxy, zum anonymen Surfen
- Ad-Aware: Gegen Spyware (Spionageprogramme) auf deinem Computer
- Spybot Search & Destroy: Wie Ad-Aware gegen Spyware (Spionageprogramme) auf deinem Computer
- XP AntiSpy: Gegen bedenkliche Einstellungen von Windows XP
- Firefox: Internet-Browser zum Surfen im Internet als gute Alternative zu Microsoft Internet Explorer.
- Thunderbird: Mailprogramm als gute Alternative zum unsicheren Microsoft Outlook.
- Window Washer: Zum Aufräumen von Müll auf der Festplatte, nur für das Betriebssystem Windows (kostenpflichtig)

Zurück zum Inhalt dieses Kapitels

In eigenen Dokumenten behandeltes Pogramm

Nicht in diesem Handbuch, aber in eigenen Dokumenten auf der CD findest du Installations- und Bedienungsanleitungen zu folgenden Programmen:

- Kaspersky Anti-Virus: Lizenz(kosten)pflichtiges Anti-Virenprogramm für Windows und Linux

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 mittlerweile weit verbreitete Windows XP verwendet.

In anderen Windows Versionen ist das Ganze aber sehr ähnlich. Auch wenn sich das vorliegende Handbuch derzeit voll und ganz auf den Einsatz unter Windows konzentriert, mit ein wenig Phantasie lassen sich einige der Tipps auch unter anderen Betriebssystemen wie Linux oder Mac OS X zum Einsatz bringen. Andere hingegen nicht, diese Lücken zu schließen wäre eine Aufgabe für eine künftige Version des Handbuchs.

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

Wo bekommst du Hilfe?

Neben den in den Programmen meist enthaltenen Hilfefunktionen und diversen Webseiten gibt es auch noch das äußerst empfehlenswerte politische Diskussionsforum n3tw0rk.org. Falls du mal Hilfe zu einem Programm in diesem Handbuch oder auch zu anderen Programmen/Problemen brauchst, in diesem Forum wird dir rasch und kompetent geholfen.

Dieses Forum ist vor allem als Diskussionsplattform zu politischen Themen gedacht - so gibt es z.B. Themenbereiche zu Sexismus, Sex and Gender, Antifaschismus und Antisemitismus und vieles mehr.

Es gibt aber auch Themenbereiche zu „Computer und Technix“, z.B. zu Software oder speziell zu Computersicherheit (dort gibt’s übrigens auch einen Link zum Herunterladen dieses Handbuchs). In diesen Themenbereichen kannst du jederzeit Fragen stellen (posten), du wirst sehen, in kurzer Zeit bekommst du kompetente Antwort.

Für dieses Forum gilt daher: große Empfehlung! Auch das reichhaltige Angebot an Smilies ist wirklich beeindruckend. Du musst dich bei diesem Forum registrieren – es ist aber natürlich nicht daran gedacht, dass du deinen wirklichen Namen angibst, gib einfach irgendeinen Phantasienamen an und schon geht’s los. Schau einfach mal rein.

Du findest das Forum unter http://www.n3tw0rk.org (Achtung: eine „3“ statt dem „e“ und die Ziffer Null statt dem Buchstaben „O“)

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 und Links zu den jeweiligen Programmen
Allgemeine Informationen	Ein paar Kapitel zu den Themenbereichen Spam, Browser-Problematik, Open Source u.a.
Verschlüsselung	Beinhaltet eine Beschreibung, was Verschlüsselung ist und wie es funktioniert
WinPT (Windows Privacy Tools): Verschlüsselung - Installation und Schlüsselverwaltung	Beinhaltet eine detaillierte Anleitung zur Installation von WinPT, außerdem zur Erstellung und Verwaltung von Schlüsseln, die zur Ver- und Entschlüsselung von Texten (z.B. Mails) benötigt werden
Die Verwendung von WinPT mit Mailprogrammen	Beinhaltet detaillierte Anleitungen, wie WinPT (bzw. eigentlich GnuPG) mit den Mailprogrammen Eudora, Thunderbird und anderen Programmen zu verwenden ist, um Mails zu ver- bzw. entschlüsseln
TrueCrypt	Beinhaltet eine Anleitung, wie Festplattenbereiche mit TrueCrypt verschlüsselt werden können
Zone Alarm (Firewall für Windows)	Beinhaltet eine Installationsanleitung und eine Beschreibung, wie mensch Zone Alarm als Firewall verwendet

AntiVir (Viren-Schutzprogramm für Windows)	Beinhaltet eine Erklärung von AntiVir, eine Installationsanleitung und eine Beschreibung, wie mensch das kostenlose AntiVir verwendet
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)
Spybot Search & Destroy	Sucht und beseitigt wie Ad-Aware Spionageprogramme (Spyware)
XP Antispy	Hilft bei der Beseitigung von kritischen Windows XP Programmen/Einstellungen
Firefox	Internet-Browser zum Surfen im Internet als gute Alternative zu Microsoft Internet Explorer
Thunderbird	Mailprogramm als Alternative zu Microsoft Outlook
Window Washer	Kostenpflichtiges Programm zum Aufräumen von Datenschrott
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
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
- Gelöschte Daten
- Verbindung zum Internet
- Computerviren
- Spionageprogramme (Spyware)
- Browser zum Surfen im Internet
- Webkäfer, Werbebanner etc.
- Anonymes Surfen
- Spam
- Von Programmen verursachter „interessanter“ Datenschrott
- Passwörter

2.1 Die Problembereiche

Datenverkehr im Internet - Mails

Ohne Verschlüsselung reisen Mails völlig ungesichert quer durchs weltweite Netzwerk. Für neugierige Menschen 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, ein bequemes und gutes Programm dazu ist das im Internet kostenlos erhältliche Programm WinPT (Windows Privacy Tools auf Basis von GnuPG).

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.

Weitere Informationen zu Echelon findest du z.B. unter

http://www.heise.de/tp/r4/special/ech.html und
http://de.wikipedia.org/wiki/Echelon

Weiteres zur Lösung dieses Problems findest du im Kapitel WinPT (Windows Privacy Tools).

Zurück zum Inhalt dieses Kapitels

Gespeicherte Daten auf dem Computer

Es ist sicher nachvollziehbar, dass die auf deinem Computer gespeicherten Daten für neugierige Menschen furchtbar interessant sind. Schutz vor unberechtigtem Zugriff auf diese Daten bietet das Programm TrueCrypt. Damit werden ganze Festplattenbereiche verschlüsselt.

Weiteres zur Lösung dieses Problems findest du im Kapitel TrueCrypt.

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.

Im einfacheren Fall können die Daten ganz einfach wiederhergestellt werden (sie sind in Windows nämlich nicht wirklich gelöscht, sondern als „gelöscht“ markiert). Sind diese „gelöschten“ Daten bereits von anderen Dateien überschrieben worden (darauf hat mensch aber keinen Einfluss), können sie noch immer aufgrund des Restmagnetismus auf den Speichermedien (z.B. auf der Festplatte) oft wiederhergestellt werden.

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

Weiteres zur Lösung dieses Problems findest du im Kapitel WinPT (Windows Privacy Tools).

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 („Feuermauer“ zwischen deinem Computer und dem Internet). Ganz besonders empfehlenswert ist so eine Firewall für alle BenutzerInnen von permanenten Internetverbindungen (wie z.B. bei Chello und ADSL), da sie über lange Zeiträume mit dem Internet verbunden sind. Wir stellen dazu das kostenlose Programm ZoneAlarm vor.

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

Zurück zum Inhalt dieses Kapitels

Computerviren

Ein weiteres leidliches Thema sind 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, siehe z.B. auch das Problem des Zusammenspiels von Computerviren, Spyware und Spam.

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-Breitbandanschluss 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.

Neben dem bereits in früheren Versionen dieses Handbuchs vorgestellten für den privaten Gebrauch kostenlosen Antiviren-Programm AntiVir stellen wir noch ein zweites, kostenpflichtiges Programm vor: Kaspersky Anti-Virus.

Weiteres zur Lösung dieses Problems findest du in den Kapiteln AntiVir – Viren-Schutzprogramm und Kaspersky

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 drei kostenlose Programme vorgestellt:

- Das Programm Ad-Aware durchsucht deinen Computer nach solchen Spionageprogrammen und beseitigt bzw. entschärft sie auf Wunsch
- Das Programm Spybot Search & Destroy, das deinen Computer wie Ad-Aware nach Spionageprogrammen durchsucht und sie beseitigt (im Doppelpack mit Ad-Aware sehr wirkungsvoll)
- Das Programm XP Antispy speziell für Windows XP Systemprogramme und Einstellungen

Weiteres zur Lösung dieses Problems findest du in den Kapiteln Ad-Aware, Spybot Search & Destroy und XP Antispy

Zurück zum Inhalt dieses Kapitels

Browser zum Surfen im Internet

Der marktbeherrschende Browser zum Surfen im Internet ist noch immer der Microsoft Internet Explorer. Das wohl auch deshalb, weil er mit dem Betriebssystem Windows gleich mitgeliefert wird und mensch kein zusätzliches Programm installieren muss.

Da aber seit Jahren bis heute fast wöchentlich neue Sicherheitslücken in diesem Browser bekannt werden, über die sich Viren auf deinen Computer schleichen können, Spyware installiert werden kann, das Ganze bis zur Kontrolle deines Computers von außen gehen kann, raten wir dringend davon ab, diesen Browser zu verwenden.

Glücklicherweise gibt es ausgezeichnete Alternativen zum Microsoft-Produkt, als Beispiel stellen wir den kostenlosen Open-Source Browser Firefox vor.

Natürlich ist auch Firefox kein Allheilmittel vor allen Gefahren des Internets - regelmäßige Updates sollten auch beim Firefox zur Routine werden. Trotzdem: alles in allem seid ihr mit Firefox derzeit sicherer im Netz unterwegs.

Weiteres zur Lösung dieses Problems findest du im Kapitel Firefox

Zurück zum Inhalt dieses Kapitels

Webkäfer, Popup-Fenster 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 sogenannten „Web Bugs“ (Webkäfer) werden von DatensammlerInnen benutzt, um aus dem Surfverhalten der AnwenderInnen Profile zu erstellen.

Vor den meisten dieser Probleme schützt dich die Verwendung eines guten Internet Browsers, z.B. Firefox.

Weiteres zur Lösung dieses Problems findest du ebenfalls im Kapitel Firefox

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 kostenlose 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

Spam

Mittlerweile ist das Spam-Problem sehr massiv geworden: mensch erhält eine Unzahl von Mails, die verschiedenen Mist anbieten: von Viagra bis Geldanlage, von Pornowerbung bis zu Versuchen, deine Bankdaten auszuspionieren. Und dann muss mensch die wirklichen Mails aus dieser Ansammlung von Mist heraussuchen, übersieht dabei eventuell wichtige Mails.

Das Ganze ist zeitraubend, nervig und gefährlich. Außerdem verstopft es deine Mailordner und sorgt für erheblichen Netzwerk-Verkehr. Obwohl es noch keine wirklich befriedigende Lösung dafür gibt, stellen wir einige Möglichkeiten vor, sich das Leben diesbezüglich ein wenig leichter zu machen.

Wenn du eine Mail an viele Personen schickst (z.B. im selbst erstellten Mailverteiler), trage als EmpfängerIn dich selbst und die eigentlichen EmpfängerInnen unter bcc (blind carbon copy) ein!

So sehen die EmpfängerInnen nicht, an welche Personen du die Mails noch geschickt hast.

Abgesehen davon, dass es den EmpfängerInnen wahrscheinlich nicht recht ist, dass ihre Mailadressen öffentlich verteilt werden, verhindert das auch, dass unter Umständen eine der EmpfängerInnen die Mailadressen unbefugt weitergibt und so das Verschicken von (noch mehr) Spam provoziert.

Weiteres zur Lösung dieses Problems findest du im Kapitel Spam – was tun?

Zurück zum Inhalt dieses Kapitels

Von Programmen verursachter „interessanter“ Datenschrott

Vor allem Windows-Programme haben die unangenehme Eigenschaft, 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 kostenpflichtige Programm „Window Washer“, das diesen Datenschrott aufräumt.

Weiteres zur Lösung dieses Problems findest du im Kapitel Window Washer

Zurück zum Inhalt dieses Kapitels

Passwörter

Diese ganzen tollen hier vorgestellten 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 (hohe) 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 das AntiViren-Programm Kaspersky Anti-Virus als 30-Tage-Testversionen, alle anderen vorgestellten Programme sind kostenlos. Folgende Programme werden beschrieben:

Du findest Infos zu folgenden Programmen:

- WinPT (Windows Privacy Tools) (Ver- und Entschlüsseln von Texten/Mails und einzelnen Dateien auf Basis von GnuPG und nicht wiederherstellbares Löschen von Dateien und ganzen „leeren“ Festplattenbereichen)
- TrueCrypt (Verschlüsseln von ganzen Festplattenbereichen)
- Zone Alarm (Firewall) (Schutz bei Verbindungen ins Internet)
- AntiVir – kostenloses Viren-Schutzprogramm
- Kaspersky Anti-Virus, wie AntiVir ein Viren-Schutzprogramm, aber nicht kostenlos
- Ad-Aware (Gegen diverse Spionageprogramme von Windows)
- Spybot Search & Destroy (wie Ad-Aware gegen Spionageprogramme in Windows)
- XP Antispy (Gegen Spionageprogramme und bedenkliche Einstellungen von Windows XP)
- Firefox (kostenloser Internet-Browser)
- Thunderbird (kostenloses Mailprogramm)
- JAP (Java Anon Proxy) (Anonymes Surfen im Internet)
- Window Washer (Aufräumen von Datenschrott)

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

- Passwörter und Passphrases

3.1 Lösungsansätze

WinPT (Windows Privacy Tools)

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. WinPT ist ein (Open Source) Programm zum Verschlüsseln von Texten (z.B. Mails), das mensch gratis im Internet herunterladen kann.

Es bildet die grafische BenutzerInnenoberfläche für das Programm GnuPG (GPG), das im Programm enthalten ist. Es dient zum

- Ver- und Entschlüsseln von Texten (z.B. Mails)
- Verwalten der zugehörigen Schlüssel
- Nichtwiederherstellbaren Löschen von Dateien bzw. Festplattenbereichen

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 WinPT findest du im Kapitel WinPT (Windows Privacy Tools).

Zurück zum Inhalt dieses Kapitels

TrueCrypt

Bekommen neugierige Menschen Zugang zu deinem Computer, nützen dir auch die besten Windows- oder Linux-Passwörter nichts, deine Daten sind mit ein paar Handgriffen offen zu lesen, wenn sie nicht davor geschützt werden.

Den einzigen Schutz davor bietet die Verschlüsselung deiner Daten auf der Festplatte (Diskette etc.). Ein kostenloses Open Source-Programm dazu ist TrueCrypt. Es dient zum

- Erstellen von verschlüsselten Partitionen (Teilen von Festplatten)
- Verwalten dieser verschlüsselten Partitionen

Und keine Sorge: es geht alles sehr einfach. Du kannst diese verschlüsselten Teile der Festplatte nach Eingabe des richtigen Passworts wie gewohnt benutzen: neue Dokumente erstellen und hinspeichern, löschen, Dateien kopieren bzw. verschieben, Ordner anlegen etc.

Detailliertere Informationen zu TrueCrypt findest du im Kapitel TrueCrypt.

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 oder Programme von dir ungewollt Verbindung mit anderen Computern aufnehmen.

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 kostenlos im Internet erhältlich.

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

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 auch ständig im Hintergrund, damit du dir nicht irgendwie einen Computervirus einfängst. In diesem Handbuch stellen wir zwei Viren-Schutzprogramme vor: AntiVir von der Firma H+BEDV und Kaspersky Anti-Virus. Es gibt aber eine ganze Menge dieser Programme, auf jeden Fall gilt: irgendein aktueller Virenschutz ist viel besser als kein Virenschutz.

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

In den früheren Versionen dieses Handbuchs haben wir nur AntiVir vorgestellt. Da dieses Viren-Schutzprogramm aber bei Tests wiederholt nicht besonders gut abgeschnitten hat, stellen wir jetzt auch ein zweites kostenpflichtiges Programm vor: Kaspersky Anti-Virus (siehe nächstes Kapitel).

Aber bitte keine Panik: so schlecht ist AntiVir auch wieder nicht, wir wollen einfach eine bessere, aber leider auch teurere Alternative zeigen.

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

Zurück zum Inhalt dieses Kapitels

Kaspersky Anti-Virus

Kaspersky Anti-Virus ist ein Viren-Schutzprogramm wie AntiVir. Im Gegensatz zu AntiVir ist dieses Programm jedoch kostenpflichtig, derzeit kostet eine 1jährige Lizenz USD 41,50, eine 2jährige USD 66,40.

Wie schon bei AntiVir erwähnt, haben wir diesen Virenscanner ins Handbuch aufgenommen, weil er bei Tests immer sehr gut abgeschnitten hat. Es gibt aber weitere Anti-Virenprogramme, die ebenfalls so gut oder zumindest fast so gut beurteilt wurden.

Das absolut perfekte Anti-Virenprogramm gibt es leider nicht, jeder Virenscanner hat seine Vor- und Nachteile bzw. Eigenheiten. Wir haben Kaspersky ausgewählt, weil er neben einer ausgezeichneten Erkennungsrate eine sehr große Aktualisierungs-Häufigkeit hat (alle 3 Stunden) – und das bei sehr kurzen Reaktionszeiten bei Auftauchen von neuen Viren.

Detailliertere Informationen dazu findest du auf der CD im Dokument Kaspersky Anti-Virus Testversion\Doku\kav4.5_personalde.pdf

Zurück zum Inhalt dieses Kapitels

Ad-Aware

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

Ad-Aware ist ein sehr einfach zu installierendes und zu bedienendes kostenloses 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

Spybot – Search & Destroy

Das ebenfalls kostenlose Spybot bietet das Gleiche wie Ad-Aware: das Auffinden und Beseitigen von Spyware (Spionage-Programmen).

Warum ein zweites solches Programm? Erfahrungsgemäß ist die gemeinsame Verwendung von beiden Programmen sehr effektiv: „übersieht“ Ad-Aware etwas, findet es Spybot und umgekehrt.

Wie Ad-Aware ist auch Spybot sehr einfach zu installieren und zu bedienen.

Detailliertere Informationen zu Spybot findest du im Kapitel Spybot Search & Destroy

Zurück zum Inhalt dieses Kapitels

XP Antispy

So wie Ad-Aware und Spybot eine Vielzahl von Spionageprogrammen finden und beseitigen können, 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 Einstellungen ein.

XP Antispy ist ebenfalls sehr einfach zu installieren und zu bedienen.

Detailliertere Informationen zu XP Antispy findest du im Kapitel XP Antispy

Zurück zum Inhalt dieses Kapitels

Firefox

Ihr werdet wahrscheinlich auch schon darüber gelesen haben: seit Jahren werden fast wöchentlich neue Sicherheitslücken im weit verbreiteten Microsoft Internet Explorer bekannt – mensch kann sich durch simples Surfen im Internet Viren einhandeln, Spyware natürlich auch usw. usf.

Glücklicherweise gibt es gute Alternativen zu diesem Microsoft Produkt. Wir stellen den kostenlosen Open Source Internet-Browser Firefox vor.

Detailliertere Informationen dazu findest du im Kapitel Firefox

Zurück zum Inhalt dieses Kapitels

Thunderbird

Auch beim weit verbreiteten Mailprogramm Microsoft Outlook gilt das Gleiche wie beim Internet Browser Internet Explorer: Sicherheitslücken, Sicherheitslücken, Sicherheitslücken.

Doch auch hier gibt es gute Alternativen. Wir stellen das kostenlose Open Source-Programm Thunderbird mit integriertem Spamschutz vor.

Wenn du bisher Microsoft Outlook verwendet hast und auf Thunderbird umsteigen willst, gibt es komfortable Möglichkeiten zur Übernahme deiner Einstellungen und Mails.

Detailliertere Informationen dazu findest du im Kapitel Thunderbird

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 (kann also immer eine andere sein). 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 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

Window Washer

Window Washer ist ein kostenpflichtiges Programm für Windows, das den Datenschrott auf der Festplatte aufräumt.

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

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 Allgemeine Informationen

Überblick

Hier findest du einige allgemeine Informationen und Diskussionsbeiträge. Auch wenn's vielleicht auf den ersten Blick schwer erkennbar ist – alle Themen dieses Kapitels haben etwas mit Computersicherheit zu tun.

Du findest Beiträge zu folgenden Themen:

- Problematik bei Internet Browsern / Internet Browser- und E-Mail-Check
- Spam - was tun?
- Das Zusammenspiel von Computerviren, Spyware und Spam
- Open Source

4.1 Problematik bei Internet-Browsern / Browser- und E-Mail-Check

Viele Tricks

Es gibt viele Möglichkeiten, BenutzerInnen von Internet-Browsern und Mailprogrammen auszutricksen. Es können unbemerkt Programme ausgeführt werden, Viren installiert werden, BenutzerInnendaten gesammelt werden usw. usf. Der mittlerweile wohl berühmteste ist „Phishing“ (Passwort fischen), dabei werden Massenmails mit der (gefälschten) AbsenderIn einer Bank verschickt, mit der Bitte um irgendeine Aktualisierung von Daten. Dabei kann mensch in der Mail gleich einen Link anklicken, der vermeintlich auf die Webseite der Bank verweist.

Diese aufgerufene Seite sieht auch aus wie die gewohnte Bank-Seite, ist es aber nicht. Sie wurde nur exakt nachgebildet. Tja, und dann wird’s ernst: es werden BenutzerInnenname und Passwort abgefragt, die gehen direkt zu einem zentralen Computer, wo diese Informationen gesammelt werden. Das Konto kann von den BetreiberInnen dieses Computers dann problemlos ausgeräumt werden.

Ähnliches, nämlich das Herausfinden deiner Daten und deiner Passwörter, wird auch z.B. mit der Aufforderung nach Aktualisierung deines ebay- oder eines Mail-Accounts versucht.

Aber auch etwas gefinkeltere Tricks werden angewendet: auf einer gefälschten Webseite wird eine Zahlen/Buchstabenkombination (TAN-Code) abgefragt, die du bei jedem Vorgang auf deinem Konto eintippen musst und die dann nach diesem Vorgang verfällt (nicht mehr benutzbar ist). Du erhältst dann die Fehlermeldung, dass diese Zahlen/Buchstabenkombination bereits verbraucht wurde. In Wirklichkeit wird dieser TAN-Code sofort dazu benutzt, Geld auf ein fremdes Konto zu überweisen.

Zurück zum Inhalt dieses Kapitels

Microsoft Internet Explorer und andere Browser

Wie so oft, wenn's um Sicherheitsprobleme geht, hat sich auch hier der Internet Explorer von Microsoft im negativen Sinn besonders hervorgetan. Aber auch andere Browser müssen eventuell auf neue Probleme reagieren, und die tun es auch – und meist viel rascher als z.B. Microsoft.

Mittlerweile benutzen immer mehr Menschen alternative Browser, seit dem Bekanntwerden der Sicherheitslücken des Microsoft Internet Explorers im ersten Halbjahr 2004 setzte ein regelrechter Boom auf andere Browser ein (z.B. auf Firefox, der auch in diesem Handbuch vorgestellt wird). Die Dominanz des Internet Explorers ist aber noch immer groß, aber das kann sich ja ändern.

Die Frage „Microsoft Internet Explorer oder nicht" ist keine Geschmacksfrage, sondern wir raten aufgrund der aufgetretenen Probleme hier einfach eindringlich von der Verwendung dieses Browsers ab. Und du wirst sehen – die Alternativen sind in jeder Hinsicht viel besser, nicht nur in Bezug auf Sicherheit.

Zurück zum Inhalt dieses Kapitels

Aktualität von Programmen

Das betrifft nicht nur Internet Browser: es ist sehr wichtig, immer die neuesten Versionen des jeweiligen Betriebssystems (z.B. Windows) und der sicherheitsrelevanten Programme zu haben (z.b. Internet Browser, E-Mail-Programm, Virenscanner, Firewall etc.).

Das ist deshalb wichtig, weil bei neuen Versionen dieser Programme bekannte Sicherheitsprobleme beseitigt werden. Viele Programme bieten auch eigene Menüpunkte zum Laden von neuesten Versionen an (Online Update), das ermöglicht natürlich ein besonders bequemes Aktualisieren der Software (z.B. bei Anti-Viren und Anti-Spyware Programmen und beim Internet Browser Firefox).

Auch automatische Aktualisierungen werden oft angeboten, das ist z.B. bei Virenscannern, die eine Aktualisierungsrate der Virenerkennungsdateien von 3 Stunden haben können (wie bei Kaspersky) fast schon Bedingung für ein Aktuell-Halten dieser Programme.

Zurück zum Inhalt dieses Kapitels

Internet Browser- und E-Mail-Check

Die Webseite der Zeitschrift c't bietet auf ihrer Webseite eine sehr empfehlenswerte kostenlose Prüfung der Versionen und Einstellungen für verschiedene Browser an. Dabei können verschiedene Dinge gefahrlos ausprobiert werden (z.B. das unter „Viele Tricks" beschriebene „Phishing"-Problem).

c't Browsercheck unter
http://www.heise.de/security/dienste/browsercheck/

Auch E-Mails können gecheckt werden, es kann z.B. ausprobiert werden, ob angehängte Dateien etwas vortäuschen bzw. Schaden anrichten können. Mensch lässt sich dazu z.B. Mails mit (natürlich harmlos gemachten) Viren zusenden und beobachtet, was das jeweilige E-Mail-Programm in Zusammenspiel mit dem Anti-Virenprogramm damit tut – das natürlich ohne jede Gefahr eines Schadens.

c't E-Mail-Check unter
http://www.heise.de/security/dienste/emailcheck/

Mensch erhält auch immer entsprechende Hinweise zur Beseitigung der Probleme.

Zurück zum Inhalt dieses Kapitels

4.2 Spam – was tun?

Problematik

Du hast immer gut aufgepasst, dass deine E-Mail-Adresse nur vertrauenswürdigen Personen bekannt ist? Du hast daher geglaubt, dass dich das Problem mit Spam-Mails nicht treffen kann? Seit einiger Zeit bekommst du trotzdem haufenweise Angebote für Viagra, Penis-Verlängerungen, Anlegemöglichkeiten für dein riesiges Vermögen usw. usf…? Wie kann das passieren?

Tja, entweder ist deine E-Mail-Adresse doch irgendwo angeführt gewesen (das lässt sich ja wirklich kaum vermeiden) oder ein eigener Adress-Generator hat zufällig auch deine E-Mail-Adresse ausprobiert – da keine Meldung zurückgekommen ist, dass die Mail nicht zustellbar ist, ist klar, dass sie existiert. Diese Information wird natürlich sofort an andere Spam-VersenderInnen weiterverkauft… Tja, und jetzt ist dein Mail-Briefkasten jeden Tag mit Schrott angefüllt.

Und jetzt geht die Mühsal los: den ganzen Schrott täglich loswerden und dabei keine wichtigen Mails übersehen. Das Netzwerk wird durch den erhöhten Datenverkehr belastet.

Zurück zum Inhalt dieses Kapitels

Abwehr von Spam

Einige AnbieterInnen von E-Mail-Diensten versuchen, zumindest einen Teil dieses Mists schon vor der Zustellung der Mails herauszufiltern (z.B. gmx). Es gibt dabei mehrere mögliche Vorgangsweisen, meist werden auch mehrere Möglichkeiten kombiniert.

Das Problem dabei ist, dass auf gar keinen Fall Nicht-Spam-Mails erwischt werden dürfen, dass „Ham“ und „Spam“ falsch zugeordnet werden. Es wäre ja sehr unangenehm, wenn du eine wichtige Mail nicht zugestellt bekommst, nur weil das Spam-Filterprogramm deiner ProviderIn meint, dass es Spam ist.

Da das automatisierte Auseinanderhalten von Mist (Spam) und Nicht-Mist (Ham) sehr von deiner persönlichen Art und Weise abhängt, wie du E-Mail verwendest, ist es nicht möglich, für alle NutzerInnen eines E-Mail-Services Regeln zusammenzustellen, die für alle gültig sind.

Abhilfe bieten Anti-Spam-Programme, die entweder schon in deinem E-Mail-Programm integriert sind (z.B. bei Eudora in der kostenpflichtigen Version und kostenlos bei Thunderbird) oder extra installiert werden müssen. Solche Anti-Spam-Programme lernen meist mit der Zeit aufgrund deiner (Nicht-)Korrekturen, wie sie Mist und Nicht-Mist auseinanderhalten können.

Fehler können aber trotzdem manchmal passieren – es bleibt dir daher in keinem Fall erspart zu prüfen, ob von diesem Programm alles richtig kategorisiert wurde. Trotzdem ist es eine enorme Hilfe, fast alle Mails mal korrekt vorkategorisiert zu erhalten.

Die Programme, die in den beiden nächsten Kapiteln erwähnt werden, zeichen sich durch eine sehr hohe Trefferquote und eine sehr kleine Fehlerquote aus. Die normalen Mails werden in deinen Eingangsordner geleitet, die als Spam klassifizierten in einen eigenen Mail-Ordner (Junk, Spam o.ä.).

Zurück zum Inhalt dieses Kapitels

Spamfilter in E-Mail-Programmen

Wie schon angesprochen, haben die in diesem Handbuch behandelten E-Mail-Programme Eudora (nur in der kostenpflichtigen Version) und das kostenlose Thunderbird äußerst wirkungsvolle Anti-Spam-Filter integriert. Der große Vorteil ist, dass du keine anderen Programme installieren und verwenden musst, das erspart einiges an Aufwand.

Beide Programme lernen mit: falls eine Spam-Mail nicht erkannt wird, kannst du diese Mail nachträglich als Spam markieren, das Gleiche funktioniert auch umgekehrt. Mit diesen Angaben lernt der Anti-Spam-Filter immer besser, Mist von Nicht-Mist korrekt auseinanderzuhalten.

Falls du z.B. Microsoft Outlook als Mailprogramm verwendest und nicht zu sehr an diesem Programm hängst, denk doch mal über einen Umstieg auf z.B. Thunderbird nach – durch Import-Funktionen kannst du deine bisherigen Mails (z.B. aus Outlook) sehr leicht in das neue Mailprogramm übernehmen und du hast einen der wirkungsvollsten Spam-Filter gleich dabei.

Zurück zum Inhalt dieses Kapitels

Separate Spam-Filterprogramme

Verwendest du ein anderes als die vorher angeführten Mailprogramme, das keinen Spam-Filter integriert hat, kannst du ein separates Anti-Spam-Programm installieren.

Diese Programme stehen zwischen deinem E-Mail-Programm und deiner E-Mail-ServiceanbieterIn. Sie holen deine Mails ab, prüfen sie und reichen Sie dann vorkategorisiert an das entsprechende E-Mail-Programm weiter.

Bei Tests haben folgende kostenlosen Anti-Spam-Programme sehr gute Ergebnisse erzielt:

- K9 (http://keir.net/k9.html)
- SpamBayes (nur für Outlook als Erweiterung) (http://spambayes.sourceforge.net/windows.html)

Zurück zum Inhalt dieses Kapitels

4.3 Das Zusammenspiel von Computerviren, Spyware und Spam

Einleitung

Ein relativ neues Phänomen ist die Zusammemarbeit von EntwicklerInnen von Computerviren und Spyware mit den VersenderInnen von unerwünschten Massenmails (Spam).

Zurück zum Inhalt dieses Kapitels

Beispiel aus der Praxis

Es wurde von der Zeitschrift c't (Ausgabe 05/04) bewiesen, dass EntwicklerInnen von Computerviren mit Spam-VersenderInnen sehr profitabel zusammenarbeiten können.

So installierte z.B. der Virus mit dem Namen "BDS/IRCBot.V" ein Programm, das Kontakt mit einem zentralen Computer (Host) aufnahm. Neben dem Ausspionieren und Versenden der jeweiligen IP-Adresse des befallenen Computers hat der Virus ein Programm aus dem Internet geladen und installiert, das zum Versenden von Spam (Massenmails) dient. So nebenbei durchsuchte der Virus auch noch die Windows-Registry nach einem Lizenzschlüssel eines Spiels, wurde er fündig, schickte er diesen Lizenzschlüssel an besagten zentralen Computer.

Zur Tragweite des Ganzen: zum Zeitpunkt des Nachforschens hatten die BetreiberInnen des Servers (Hosts) Gewalt über mehr als 10.000 PCs, die von diesem Virus befallen und damit bereit waren, Spam zu verschicken. So können massenweise Mails verschickt und/oder DoS-Attacken (Denial of Service) gestartet werden. Natürlich könnte auch jeder andere Mist auf jedem einzelnen der infizierten Computer gemacht werden. Listen mit den befallenen PCs konnten zum Versenden von Massenmails käuflich erworben werden.

Zurück zum Inhalt dieses Kapitels

Was tun?

Ausgangspunkt des Problems ist immer ein Computervirus und/oder Spyware. Das heißt, mensch muss sich einfach sehr gut gegen Viren und gegen Spyware mit entsprechenden Programmen schützen.

Einige Programme und Tipps dazu findest du in dieser Dokumentation.

Zurück zum Inhalt dieses Kapitels

4.4 „Open Source“

Was ist eigentlich “Open Source”?

Programme werden mittels einer Programmiersprache (z.B. Java) programmiert, d.h. in von Menschen lesbarer Textform erstellt. Dann wird dieser von Menschen lesbare „Source-Code“ (Quellcode) meist in Maschinensprache übersetzt (compiliert), dieser „Maschinen-Code“ ist für Menschen nicht mehr lesbar, dafür kann der Computer dann etwas damit anfangen.

Erhält mensch beim Kauf von Software nur den Maschinen-Code, weiss mensch nicht, wie dieses Programm programmiert ist und was es im Hintergrund genau tut.

Erhält mensch jedoch mit diesem nur für den Computer verständlichen Programm auch den von Menschen lesbaren Source(Quell)-Code, können fachkundige Menschen prüfen, wie das Programm gemacht ist und was es genau tut. „Open Source“ bedeutet, dass jeder Mensch mittels Lesen des Source-Codes Einblick in das Programm nehmen kann.

Weiteres zu „Open Source“ findest du z.B. unter

http://de.wikipedia.org/wiki/Open_source
http://de.wikipedia.org/wiki/Open_Source_Definition
http://www.opensource.org/

Zurück zum Inhalt dieses Kapitels

Open Source als „Freie Software“?

Viele Open Source-Programme werden kostenlos angeboten, es gibt aber keinen direkten Zusammenhang zwischen Open Source und kostenlos. Auch Programme, die nicht als Open Source zur Verfügung gestellt werden, sind oft kostenlos, nicht jedes Open Source-Programm ist gratis.

Es gibt das Missverständnis, dass Open Source automatisch heißt, dass engagierte ProgrammiererInnen tolle Programme schreiben, die völlig uneigennützig zur Verfügung gestellt werden.

Das mag zwar zum Teil stimmen – es gibt wirklich unzählige Menschen, die unbezahlt an diesen Projekten mitarbeiten. Es gibt aber auch viele Firmen, die mittlerweile mit Open Source-Programmen viel Geld verdienen, z.B. werden auch von der Firma IBM immer mehr Programme als Open Source-Programme lizenziert.

Ob und wie damit Geld verdient wird, ist ganz unterschiedlich. Manchmal wird das Programm selbst kostenlos zur Verfügung gestellt, die Firmen verdienen über Serviceverträge, manchmal kostet die Software selbst genauso Geld wie andere Programme, anderes ist gänzlich frei.

Zurück zum Inhalt dieses Kapitels

Lizenzbedingungen

Auch bei Open Source sind die Bedingungen, wie Software vertrieben wird, genau geregelt. Firmen, die Open Source-Software vertreiben und sich einem Lizenzierungsvorgang verpflichten, müssen sich genau an diese Richtlinien halten und dementsprechend zertifiziert werden.

Zurück zum Inhalt dieses Kapitels

Kosten von Open Source-Programmen

Auch die Kosten bei der Verwendung von Open Source-Programmen sind nicht zwingenderweise niedriger als bei Verwendung anderer Software. Zumindest längerfristig sind natürlich Kostenersparnisse wahrscheinlich, da mensch nicht von den AnbieterInnen der Software abhängig ist und sich in Zukunft keinen Monopolstrukturen mit entsprechender Preisgestaltung unterwerfen muss.

Die Kostenersparnis ist damit zwar ein wichtiger Faktor zur Entscheidung für Open Source-Programme, aber sicher nicht der einzige.

Zurück zum Inhalt dieses Kapitels

Vorteile von Open Source

Was ist dann eigentlich der Vorteil von Open Source? Dazu einige Punkte:

- Sicherheit: Programme, deren Source Code bekannt ist, können auf Schwachstellen und Sicherheitslücken geprüft werden. Werden solche Probleme gefunden, können sie rasch beseitigt werden.
- Erweiterbarkeit: Programme können erweitert werden. Da die volle Funktionalität eines Programms bekannt ist, können Erweiterungen dazuprogrammiert werden.
- Schnittstellen: Andere Programme können mit einem Programm zusammenarbeiten. Es können Programme geschrieben werden, die mit dem Programm kommunizieren, Teile des Programms können verwendet werden.
- Unabhängigkeit. Es soll ja vorkommen, dass Firmen in Konkurs gehen oder sonstwie vom Markt verschwinden. Ist der Source-Code der Programme dieser Firmen nicht bekannt, können die Programme nicht weiterentwickelt werden, Fehler und Schwächen können nicht beseitigt werden. Die Software wird sehr schnell wertlos (weil veraltet und fehlerhaft), die dafür getätigten Ausgaben sind verloren.
- Weiterentwicklung der Software. Unter Einhaltung der Linzenzbedingungen können oft Firmen, die Open Source-Software verwenden, diese selbst weiterentwickeln. Auch hier wird die Abhängigkeit von Software-HerstellerInnen wesentlich kleiner.

Zurück zum Inhalt dieses Kapitels

Behaupteter Nachteil von Open Source

Es wird z.B. von Microsoft behauptet, ein entscheidender Nachteil von Open Source sei, dass auch Menschen, die Schwachstellen eines Programms ausnutzen wollen, wertvolle Informationen und Ansatzpunkte geliefert bekommen.

Dieses Argument scheint zwar nachvollziehbar, wird aber durch die Tatsache entkräftet, dass Open Source-Programme durch die weltweite Prüfung von fachkundigen Menschen auch wesentlich sicherer sind und solche Sicherheitslücken viel schneller beseitigt werden.

Auch entkräftet wird dieses Argument duch bisherige Erfahrungen: gerade bei nicht quelloffener Software werden ständig Sicherheitslücken bekannt, es entsteht immer wieder großer Schaden. BenutzerInnen von solcher Software müssen oft lange warten, bis diese Sicherheitslücken von den HerstellerInnenfirmen beseitigt werden.

Zurück zum Inhalt dieses Kapitels

Linux und Open Source

Auch hier: es gibt keinen zwingenden Zusammenhang zwischen dem freien und quelloffenen Betriebssystem Linux (z.B. als Alternative zu Windows) und Open Source. Es können auch Windows-Programme als Open Source-Software zur Verfügung gestellt werden.

In der Realität geht aber die treibende Kraft zu Open Source u.a. vom Linux-Umfeld aus. Linux selbst ist ja ein solches Open Source-Projekt und daher wird auch oft (berechtigterweise) der Zusammenhang zwischen Linux und Open Source hergestellt. Auf der anderen Seite bekämpft z.B. Microsoft dieses Konzept massiv und lehnt es strikt ab.

Zurück zum Inhalt dieses Kapitels

Fazit

Open Source ist ein sehr interessanter Ansatz, ist aber sicher nicht das vielleicht erhoffte „Allheilmittel“. „Open Source verwenden und alles in der Softwarewelt wird gut“ – diese Hoffnung wird sich sicher nicht erfüllen. Aber das Open Source-Konzept hat einfach so bestechende Vorteile, dass es wohl eine immer weitere Verbreitung finden wird.

Das Thema wird derzeit sehr intensiv diskutiert, auch ausgelöst durch die immer breitere Verwendung von Open Source-Programmen, z.B. bei der geplanten Umstellung von ganzen Kommunen/Ländern auf Linux und Open Source-Software (z.B. Wien, München, Venezuela).

Zurück zum Inhalt dieses Kapitels

5 Verschlüsselung

Überblick

In diesem Kapitel findest du einiges zum Thema Verschlüsselung, in nachfolgenden Kapiteln werden dann die zugehörigen Programme

- WinPT (Windows Privacy Tools) zum Verschlüsseln von Texten/Mails und einzelnen Dateien
- TrueCrypt (zum Verschlüsseln von Festplattenbereichen)

vorgestellt.

Du findest folgende Infos:

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

5.1 Was ist Verschlüsselung?

Was ist Verschlüsselung?

Verschlüsseln von Texten heißt, aus einem Text (einer Datei/Mail) 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.

Zurück zum Inhalt dieses Kapitels

Warum Verschlüsselung auf der Festplatte?

Wenn eine unbefugte Person Zugang zu deinem Computer hat, kann diese Person mit wenigen Handgriffen auf alle Daten deines Computers zugreifen, die nicht verschlüsselt sind. Da nützt auch kein noch so gutes Windows- oder Linux-Passwort etwas.

Den einzigen Schutz davor bietet die Verschlüsselung deiner Daten. Da du wahrscheinlich nicht jede einzelne Datei manuell verschlüsseln willst, kannst du ganze Bereiche deiner Festplatte verschlüsseln und deine Dateien einfach darauf speichern.

Zurück zum Inhalt dieses Kapitels

Voraussetzungen zum Ver- und Entschlüsseln von Mails bzw. Texten

Alle beteiligten Personen (SenderIn und EmpfängerIn) benötigen das installierte Programm GnuPG (Gnu Privacy Guard, auf dem z.B. das hier vorgestellte Programm WinPT basiert), und ihren Schlüsselbund. Für Menschen, die zu Hause einen Computer haben und mit ihrem Computer arbeiten, ist das kein Problem, z.B. WinPT installieren und schon geht's los.

Befindest du dich aber bei einem anderen Computer, auf dem GnuPG bzw. WinPT nicht installiert ist, kannst du auch nicht Ver- und Entschlüsseln. Ist auf diesem anderen Computer jedoch das Programm GnuPG (z.B. mit WinPT) installiert, kannst du deinen sogenannten Schlüsselbund auf Diskette, USB-Stick oder CD mitnehmen und mit ihm auch auf dem anderen Computer Ver- und Entschlüsseln.

Zurück zum Inhalt dieses Kapitels

Kompatibilität mit PGP

WinPT (eigentlich GnuPG) ist voll kompatibel mit PGP (Pretty Good Privacy), das ist das Programm zum Verschlüsseln, das wir in den bisherigen Ausgaben dieses Handbuchs vorgestellt haben. Wenn eine andere Person ihre Mails mit PGP verschlüsselt, kannst du sie auch mit GnuPG (auch GPG abgekürzt) entschlüsseln. Umgekehrt funktioniert es natürlich auch.

Du kannst deine Schlüssel, die du mit WinPT erstellt hast, auch mit dem Programm PGP verwenden und umgekehrt.

Zurück zum Inhalt dieses Kapitels

Begriffsverwirrung

In Zusammenhang mit der Verschlüsselung von Texten (z.B. Mails) und einzelnen Dateien werden dir hier verschiedene Begriffe unterkommen. Wir versuchen, diese Begriffe kurz zu klären:

- GnuPG (oder kurz GPG): Gnu Privacy Guard, Basisprogramm für die Verschlüsselung, macht die eigentliche “Arbeit”.
- Windows Privacy Tools (oder kurz WinPT): Programm mit komfortabler grafischer Oberfläche zur Schlüsselverwaltung auf Basis von GnuPG. GnuPG ist in WinPT enthalten, muss also bei WinPT nicht extra installiert werden.
- Open PGP: ist ein Synonym für GnuPG und soll zeigen, dass das Ganze auf Basis des von Philip Zimmermann entwickelten PGP (Pretty Good Privacy) entwickelt wurde.

Zurück zum Inhalt dieses Kapitels

5.2 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 WinPT 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 sogenannten „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 (Secret Key)

Deinen privaten Schlüssel benötigst du, um für dich verschlüsselte Mails entschlüsseln zu können und um Mails „signieren“ zu können. Er ist durch ein Passwort geschützt.

Die öffentlichen Schlüssel (Public Keys)

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. Josefine kann mit dem öffentlichen Schlüssel von Maxi an Maxi verschlüsselte Texte schicken. Nur die BesitzerIn des privaten Schlüssels kann diesen Text entschlüsseln, in diesem Fall also Maxi.

Verschlüsselt z.B. Josefine eine Mail nur 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 über 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 bitte keine Panik.

Zurück zum Inhalt dieses Kapitels

Das Schützen des privaten Schlüssels mittels Passwort

Dein privater Schlüssel ist natürlich durch ein Passwort geschützt. Es versteht sich von selbst, dass das ein sehr gutes Passwort sein muss.

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

Zurück zum Inhalt dieses Kapitels

Das Sichern deines privaten Schlüssels

Du solltest deinen privaten Schlüssel irgendwo sichern, d.h. auf eine oder besser mehrere Disketten oder noch besser auf eine oder mehrere CDs 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 (entschlüsseln).

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. Sie kann aber z.B. den verschlüsselten Text nicht „signieren“.

Zur Absicherung dagegen kann mensch Texte sowohl ohne Passwort-Eingabe (unsigned, nicht signiert) oder mit Passwort-Eingabe (signed, signiert) verschicken. Die EmpfängerIn sieht beim 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 Entschlüsselns und des Verschickens von verschlüsselten Mails.

Angenommen werden zwei Personen, Maxi und Josefine, die beide

- GnuPG (z.B. mit WinPT) oder ein dazu kompatibles Programm (z.B. 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 WinPT auf seinem Computer		J. installiert WinPT 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
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

Maxi		Josefine
		J. schreibt eine Mail für Maxi
		J. verschlüsselt die Mail nur für 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 nur für 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 Windows Privacy Tools und zur Schlüsselverwaltung findest du im Kapitel WinPT – Installation und Schlüsselverwaltung.

Zurück zum Inhalt dieses Kapitels

5.3 Das Verschlüsseln von Festplatten-bereichen mit TrueCrypt

Was ist TrueCrypt?

Mit TrueCrypt kann mensch ganze Festplattenbereiche verschlüsseln (wenn hier von Festplatten die Rede ist, sind auch Disketten, Zip-Disketten, Daten auf CDs 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) „Partitionen“ zugreifen, natürlich nur, wenn du das Passwort zu diesem Laufwerk weißt.

Diese Festplattenbereiche („Partitionen“) 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. Z). Diesen Buchstaben kannst du unter noch nicht benutzten Laufwerksbuchstaben aussuchen.

Zurück zum Inhalt dieses Kapitels

Mounten (Öffnen)

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).

Zurück zum Inhalt dieses Kapitels

Unmounten (Schließen)

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

Während die verschlüsselten Daten gemounted sind, haben auch neugierige Menschen Zugriff darauf, also den Computer bei Verlassen immer abdrehen oder zumindest vorher das verschlüsselte Laufwerk unmounten.

Mehr zur Verschlüsselung von Festplattenbereichen erfährst du im Kapitel TrueCrypt.

Zurück zum Inhalt dieses Kapitels

5.4 Zusammenfassung

Eine der wichtigsten Funktionen von WinPT (bzw. eigentlich GnuPG) ist das Verschlüsseln von Texten, wie z.B. Mails. Der Vorgang ist:

- Du und alle Personen, die mit GnuGP verschlüsselte Nachrichten austauschen, müssen das Programm GnuPG oder ein kompatibles Programm (z.B. PGP) installieren (z.B. mit dem Programm WinPT).
- 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 (außer du hast sie auch gleich für dich selbst verschlüsselt).
- Der private Schlüssel muss gut aufgehoben und z.B. auf einer CD gesichert werden
- Der einzige Schutz deines privaten Schlüssels ist das zugehörige Passwort.
- 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 (entschlüsseln). Also irgendwo (z.B. auf Disketten oder besser CDs) sichern und gut aufpassen darauf.

Genauso wichtig ist das Verschlüsseln der Daten auf deinem Computer:

- Du kannst nicht nur einzelne Texte (Mails) verschlüsseln, du kannst mit TrueCrypt auch Teile oder fast die ganze Festplatte verschlüsseln.

Zurück zum Inhalt dieses Kapitels

6 WinPT – Installation und Schlüsselverwaltung

Überblick

In diesem Kapitel werden die Installation von WinPT (Windows Privacy Tools) und die Erstellung, Verwaltung, Hinterlegung und Sicherung von Schlüsseln erklärt.

Du findest folgende Infos zu folgenden Bereichen:

- Die Installation von WinPT
- Einen kurzen Überblick über die verschiedenen Teilprogramme von WinPT
- Die Erstellung des ersten Schlüsselpaars
- Das Versenden deines öffentlichen Schlüssels an einen 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

GPG Programme ⇔ Schlüssel ⇔ verschlüsselte Laufwerke

Bei WinPT (Windows Privacy Tools) und TrueCrypt ist immer zwischen dem Programm WinPT bzw. TrueCrypt und den mit WinPT bzw. TrueCrypt erstellten Schlüsseln und verschlüsselten Laufwerken zu unterscheiden.

Selbst wenn du die Programme WinPT oder TrueCrypt löschst (deinstallierst), mehrmals installierst (z.B. später andere Versionen installierst) u.a., gehen deine mit den Programmen erstellten Schlüssel und verschlüsselten Laufwerke nicht verloren.

Du benötigst jedoch die (oder ähnliche) Programme, um deine 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

6.1 Die Installation des Programms

Auf der CD im Verzeichnis WinPT findest du das Installationsprogramm von WinPT.

Für Windows öffne den Windows Explorer, wechsle auf der CD ins Verzeichnis WinPT//Windows und doppelklicke auf die Datei winpt-install-1.0rc2.exe. Das Installationsprogramm wird gestartet.

WinPT\Windows

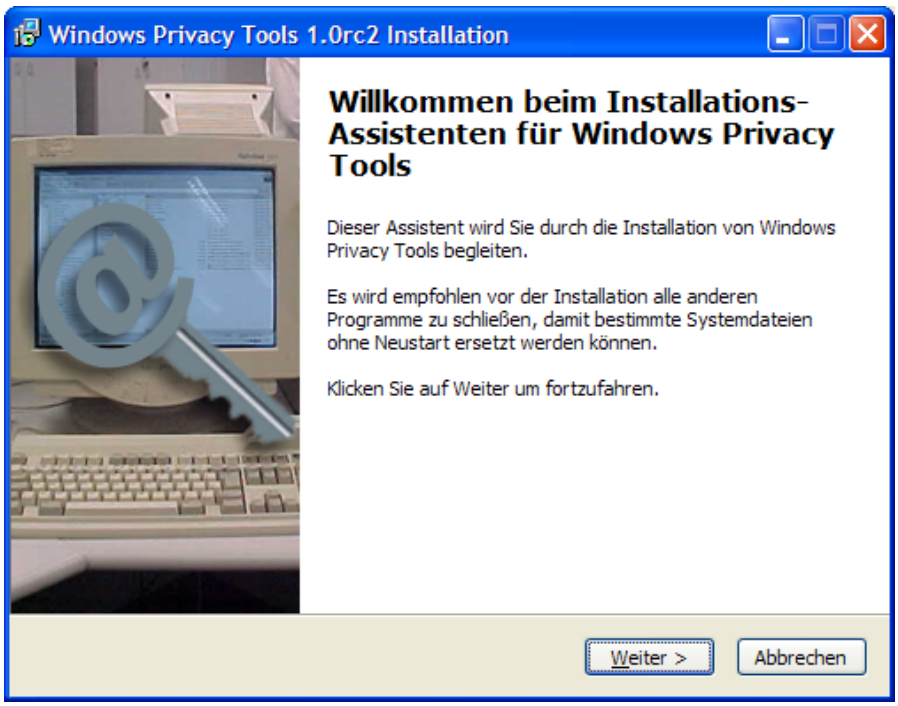
winpt-install-1.0rc2.exe

Die aktuelle Programmversion findest du immer im Internet unter http://winpt.sourceforge.net/de/download.php

Zurück zum Inhalt dieses Kapitels

Die Vorbereitung des Installationsprogramms beginnt:

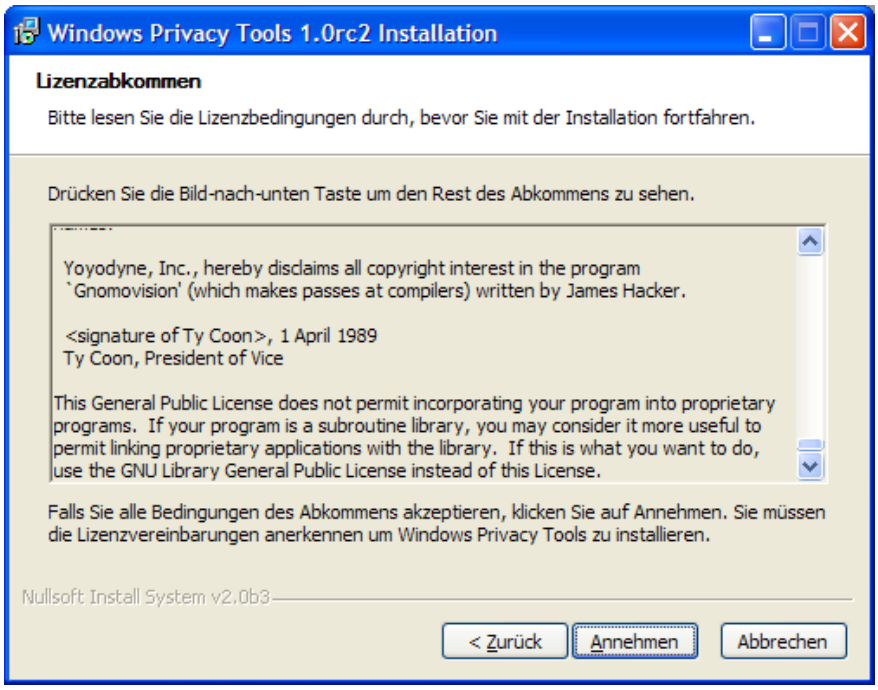
Wähle die gewünschte Sprache für die Installation aus und drücke den Button „OK“. Das Willkommensfenster erscheint:



Drücke den Button „Weiter“

Zurück zum Inhalt dieses Kapitels

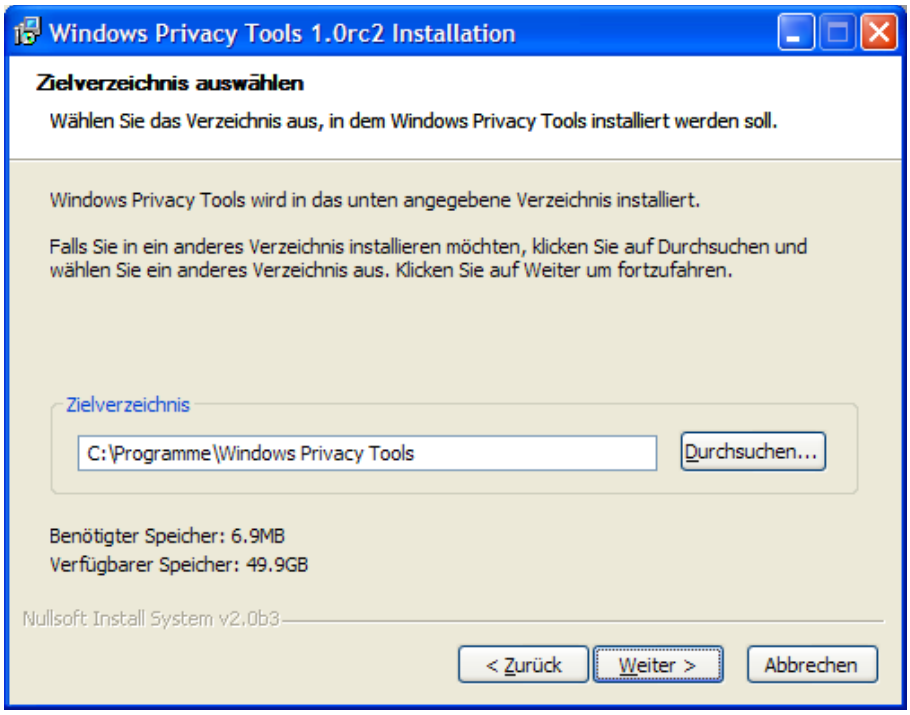
Es erscheint das Lizenzabkommen:



Lies es dir durch und drücke dann den Button „Annehmen“

Zurück zum Inhalt dieses Kapitels

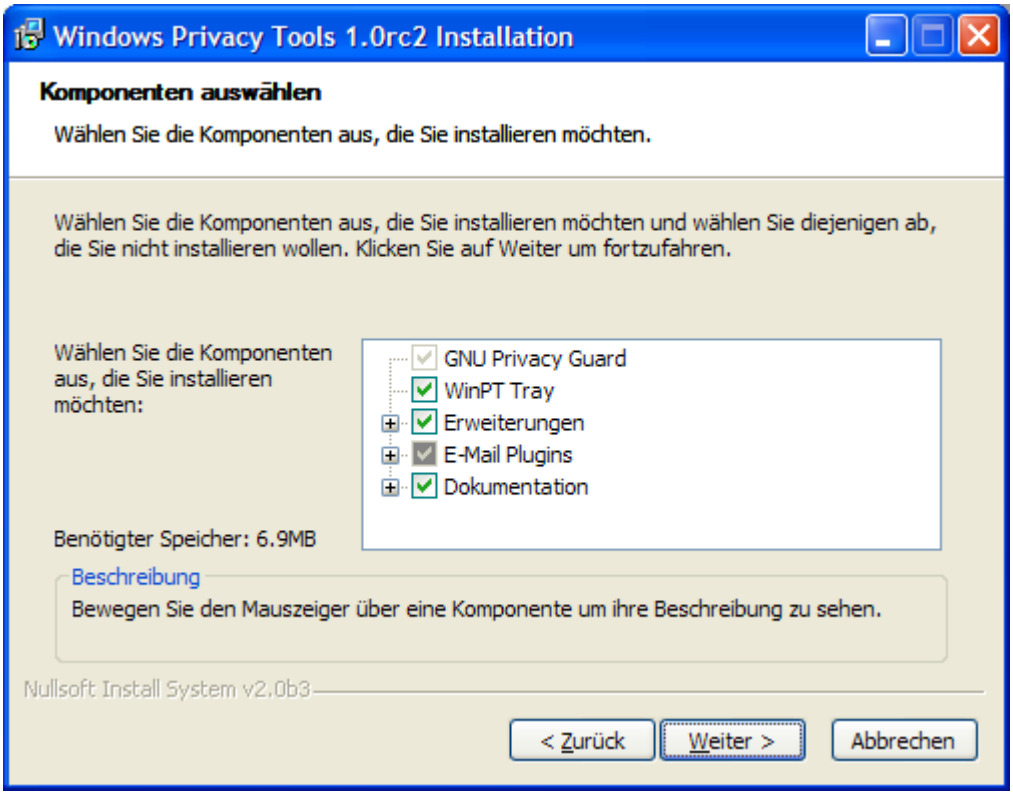
Nun erscheint ein Fenster, in dem du das Verzeichnis angeben kannst, wo das Programm installiert werden soll:



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

Zurück zum Inhalt dieses Kapitels

WinPT ist ein ganzes Programmpaket. Du kannst dir jetzt aussuchen, welche Bestandteile du installieren willst:

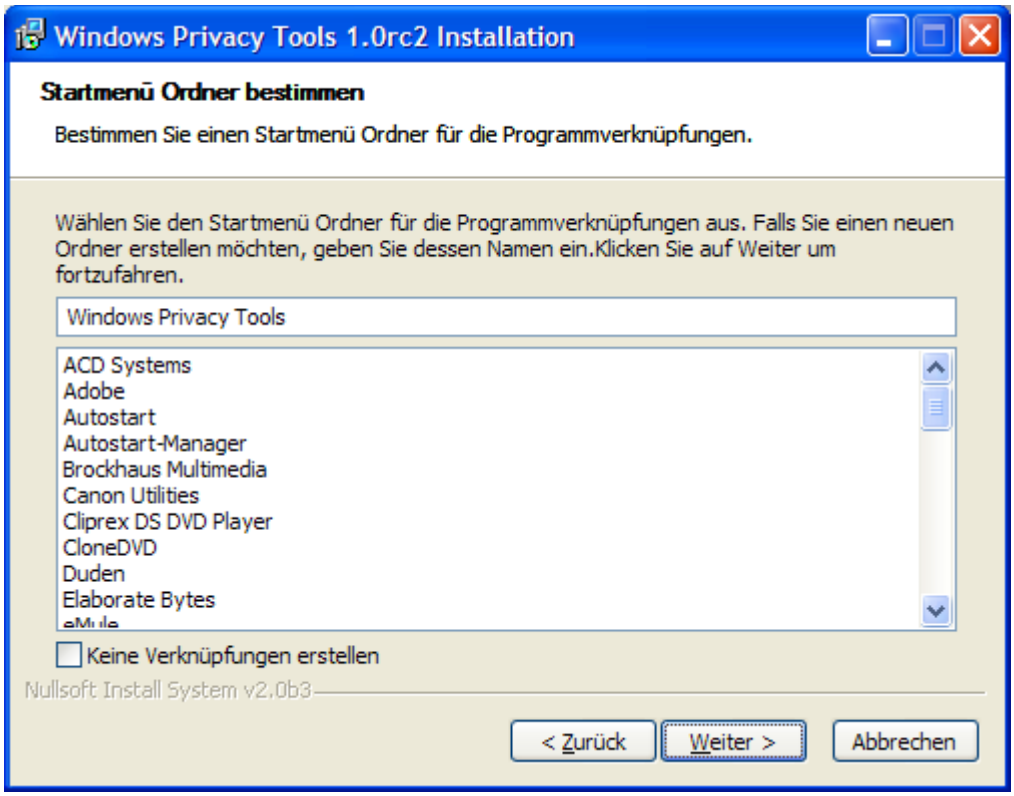


Wenn du die Mailprogramme Eudora oder Microsoft Outlook verwendest, findest du unter dem Punkt E-Mail Plugins die jeweiligen Programmbestandteile angekreuzt, die später das Ver- und Entschlüsseln von Mails bei den beiden Programmen sehr komfortabel machen.

Übernehme einfach den Vorschlag (alles installieren) oder wähle nur das Gewünschte aus. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

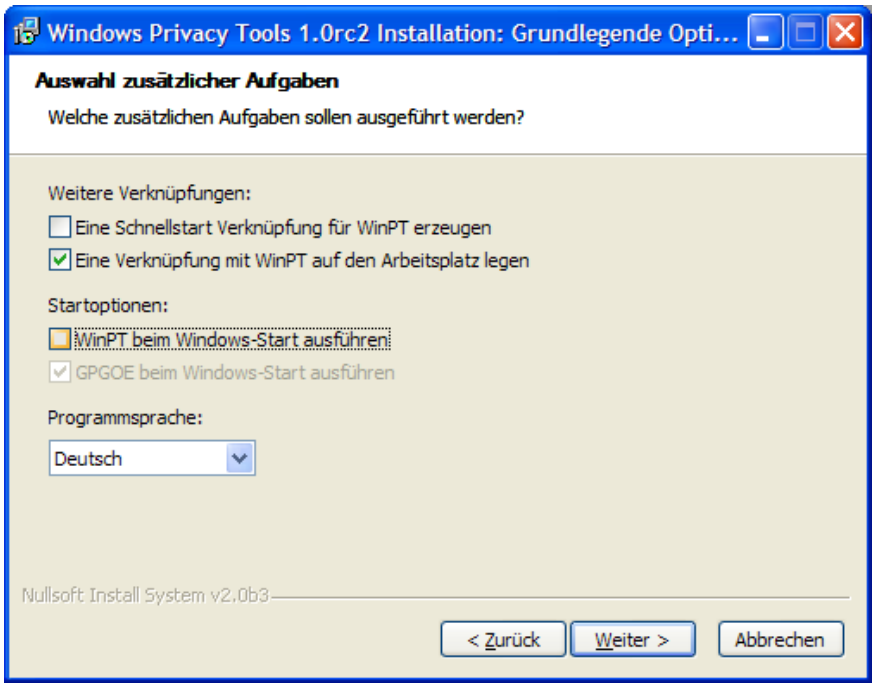
Jetzt erscheint ein Fenster, in dem du dir aussuchen kannst, wo das Programm in deinem Start-Menü zu finden sein soll:



Übernehme einfach den Vorschlag oder wähle einen anderen Ort bzw. Namen. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du dir noch aussuchen, ob du eine Verknüpfung auf deinem Desktop (auf deiner Windows Oberfläche) haben möchtest und ob WinPT bei jedem Start von Windows automatisch gestartet werden soll:

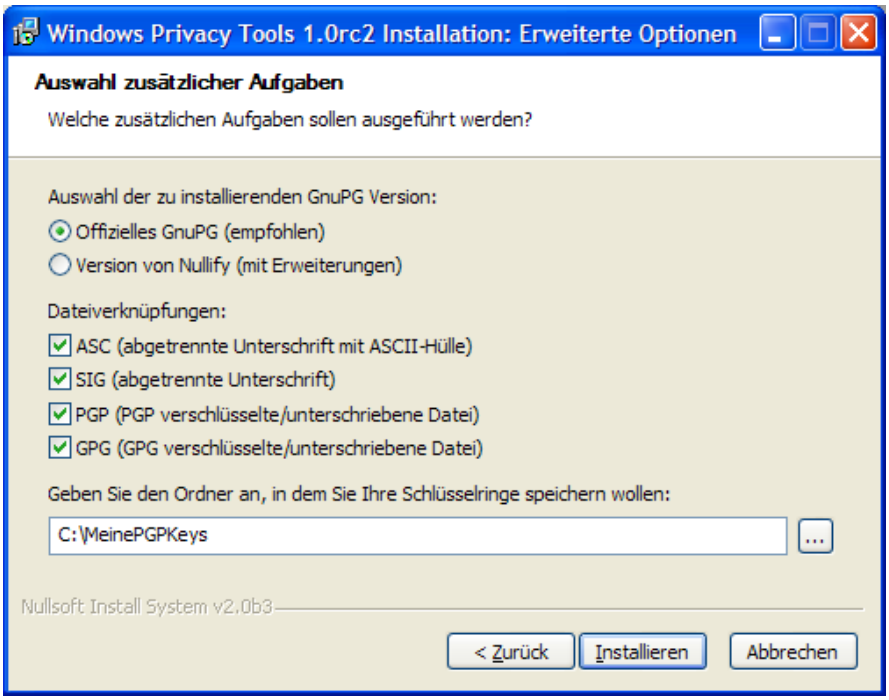


WinPT muss gestartet werden, bevor du Texte und Dateien damit verschlüsseln kannst. Du kannst es entweder automatisch bei jedem Start von Windows starten (durch Ankreuzen von „WinPT beim Windows-Start ausführen“) oder es bei Bedarf durch Doppelklick auf das WinPT-Symbol auf deinem Desktop starten.

Wähle das Gewünschte und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Ein weiteres Fenster zur Auswahl verschiedener Optionen erscheint:



Im oberen Teil ist die Verwendung des „offiziellen GnuPG“ gewählt, übernehme einfach diese empfohlene Einstellung.

Im mittleren Teil kannst du dir aussuchen, ob Dateien mit den 4 angeführten Endungen automatisch mit WinPT verknüpft werden sollen (dass z.B. bei Doppelklick in einem Ordner automatisch WinPT gestartet wird). Wähle die Gewünschten aus oder übernehme einfach die vorgeschlagene Einstellung.

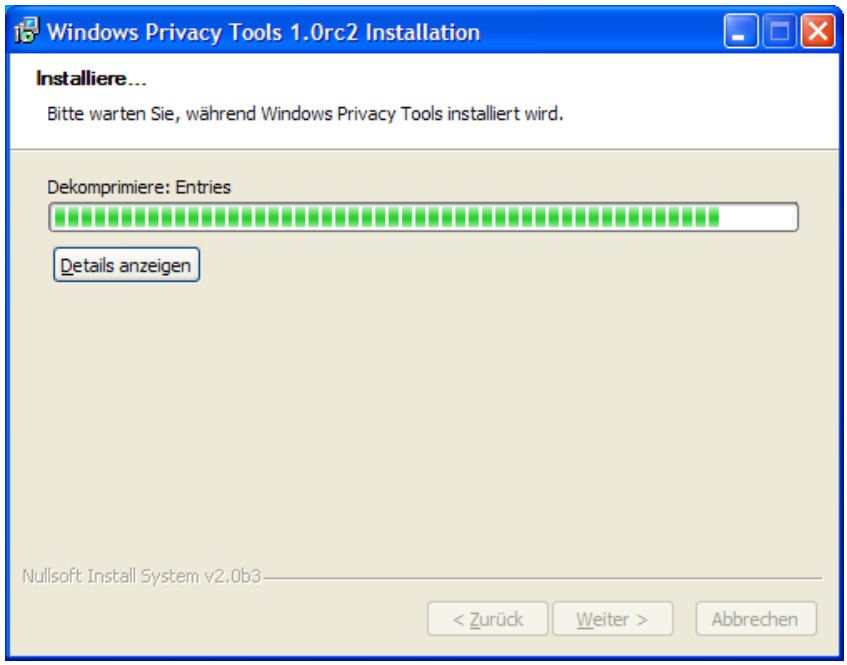
Im unteren Teil musst du angeben, wo deine Schlüsselringe gespeichert werden sollen, der Ordner wird automatisch angelegt. Am besten ist es natürlich, wenn diese Schlüsselringe auf einem verschlüsselten Teil deiner Festplatte gespeichert werden (siehe dazu das Programm TrueCrypt).

Diesen Ordner musst du dir merken, hier landen später die Dateien mit deinem Schlüsselbund.

Gib einen Ordner an und drücke den Button „Installieren“.

Zurück zum Inhalt dieses Kapitels

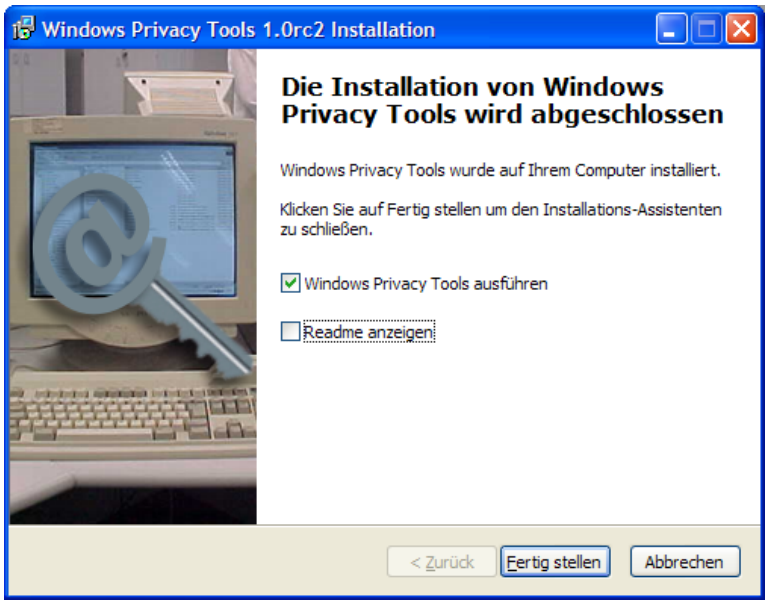
So, jetzt geht’s endlich los mit der Installation:



Die Installation dauert nicht lange.

Zurück zum Inhalt dieses Kapitels

Nach Abschluss der Installation erscheint das folgende Fenster:



Du kannst jetzt das Programm sofort starten und bei Interesse die Datei „Readme“ lesen. In diesen Dateien stehen u.a. immer die letzten aktuellsten Informationen zu einem Programm.

Wähle das gewünschte aus und drücke den Button „Fertig stellen“.

Wenn du im letzten Fenster „Windows Privacy Tools ausführen“ gewählt hast oder das Programm manuell gestartet hast, siehst du das WinPT-Symbol am rechten unteren Rand deines Bildschirms:

Es ist das Symbol mit dem Schlüssel ganz links.

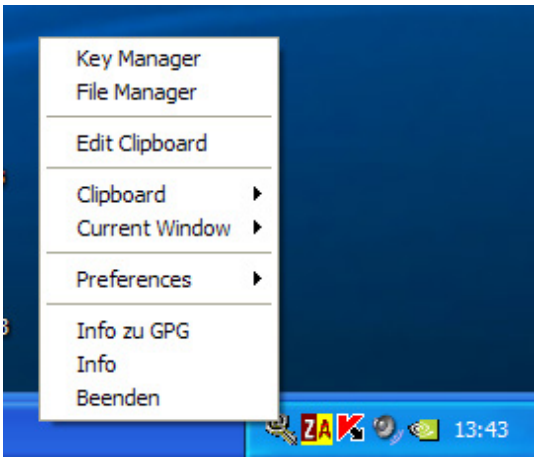
Zurück zum Inhalt dieses Kapitels

6.2 Die WinPT Programme

Nach der Installation von WinPT und dem Start des Programms siehst du auf deinem Desktop rechts unten ein neu hinzugekommenes Symbol, das wie ein Schloss aussieht (Symbol ganz links).

Zurück zum Inhalt dieses Kapitels

Wenn du mit der rechten Maustaste auf dieses Schlüsselsymbol klickst, wird das Auswahlmenü der WinPT-Programme geöffnet:



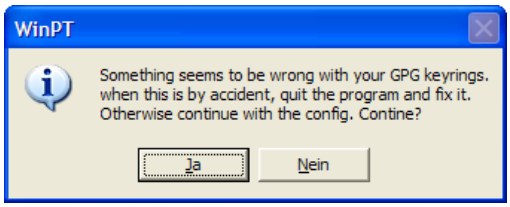
Die Bestandteile sind:

- Key Manager: alles zum Erstellen und Verwalten deines Schlüsselbundes.
- File Manager: alles zum Verschlüsseln und nachhaltig Löschen von Dateien und zum nachhaltigen Löschen des gesamten freien Platzes deiner Festplatte(n) – damit nichts Gelöschtes wiederhergestellt werden kann.
- Edit Clipboard: zum Lesen und Bearbeiten von Text in der Windows Zwischenablage, z.B. nach dem Markieren eines Textes und wählen des Menüpunktes „copy“ bzw. „kopieren“.
- Clipboard: hier findest du Untermenüs zum Ver- und Entschlüsseln von Texten in der Zwischenablage (dem Clipboard). Das ist sehr hilfreich, wenn du ein anderes Mailprogramm als Eudora, Thunderbird oder Outlook verwendest (siehe dazu auch das Kapitel zu Verschlüsselung mit anderen Mailprogrammen und Webmail).
- Preferences: hier kannst du einige Einstellungen nachträglich hinzufügen bzw. ändern.

Zurück zum Inhalt dieses Kapitels

6.3 Die Erstellung des ersten Schlüsselpaars

Wenn du das Teilprogramm „Key Manager“ das erste Mal startest, erscheint möglicherweise folgendes Fenster mit einer etwas verwirrenden Mitteilung:



Auch wenn da steht, dass irgendetwas mit deinem Schlüsselbund nicht stimmt – vergiss es, du musst ihn ja erst erstellen.

Drücke einfach den Button „Ja“, du willst weitermachen.

Zurück zum Inhalt dieses Kapitels

Dann wirst du gefragt, was du tun willst:

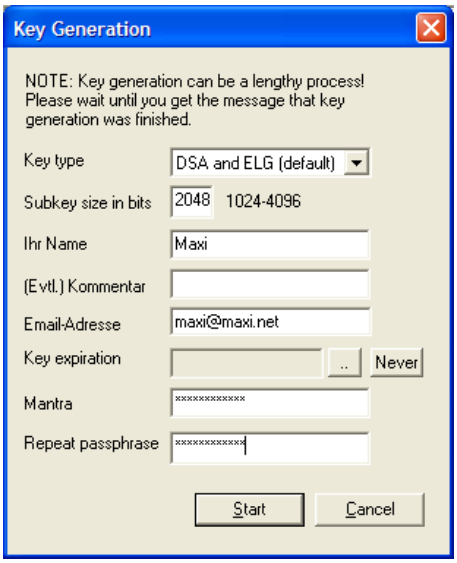
In diesem Fenster kannst du angeben, ob du

- einen neuen Schlüsselbund erstellen willst
- einen bestehenden Schlüsselbund importieren willst
- einen Ordner angeben willst, in dem sich bereits existierende Schlüsselbunde befinden

Hier wird beschrieben, wie du dein erstes Schlüsselpaar erstellen kannst. Wähle daher den Punkt „Have WinPT to generate a key pair“ und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Nun kannst du Details zu diesem Schlüsselpaar angeben:

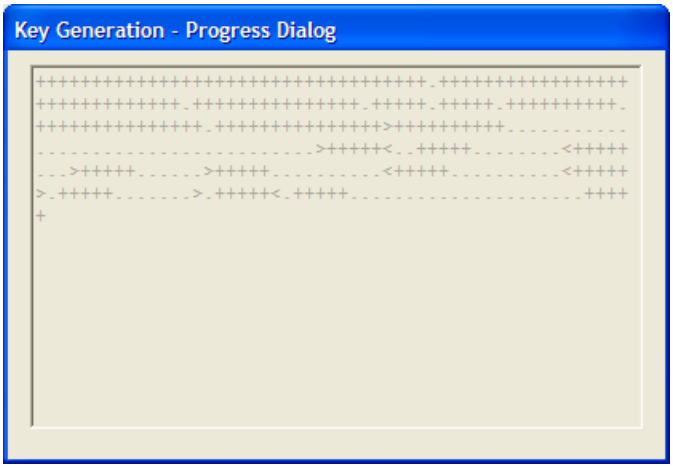


- Key type: es geht um den Algorythmus, mit dem deine Schlüssel erzeugt werden. Laut Dokumentation ist es egal, welchen Algorythmus du wählst, derzeit gelten alle aufgelisteten Möglichkeiten als sicher.
- Subkey size: Mittels „Subkey size in bits“ kannst du die Schlüssellänge angeben. Je länger ein Schlüssel ist, desto sicherer ist er auch. Allerdings dauert die Ver- und Entschlüsselung umso länger, je länger der Schlüssel ist. Auch die Größe der verschlüsselten Texte ist davon abhängig. Ein vernünftiger Wert ist sicher der vorgeschlagene bzw. eine Größe bis 2048 Bits, alles darüber ist eigentlich ziemlich sinnlos.
- Name und Email-Adresse kannst du, musst du aber nicht korrekt angeben. Es ist ratsam, einen fantasievollen Namen zu nehmen, der leicht am Keyserver wiedergefunden werden kann („Maxi“ ist da z.B. ein ganz schlechtes Beispiel). Auf keinen Fall solltest du deinen richtigen Namen angeben, das geht ja keineN etwas an.

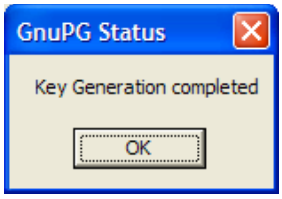
  Zur E-Mail Adresse: diese Adresse ist für jeden Mensch am Keyserver offen einsehbar. D.h., sie kann auch zum Spam verschicken dort gefunden werden. Andererseits erleichtert die richtige E-Mail Adresse das Verschlüsseln, weil sie durch Übereinstimmung von einigen E-Mail- bzw. den Verschlüsselungs- Programmen bereits automatisch richtig zugeordnet werden kann. Entscheide selbst, was dir wichtiger ist.

- Eine „Key expiration“ (ein Ablaufdatum) des Keys ist eigentlich selten notwendig. Lass daher einfach dieses Feld leer (Never).
- Und dass du dir bei jeder Art von Verschlüsselung ein besonders gutes Passwort (hier „Mantra“ genannt) einfallen lassen solltest, ist wohl selbstverständlich. Tipps dazu findest du im Kapitel Tipps für Passwörter/Passphrases.

Gib alles an und drücke dann den Button „Start“. Nun wird dein erstes Schlüsselpaar generiert:



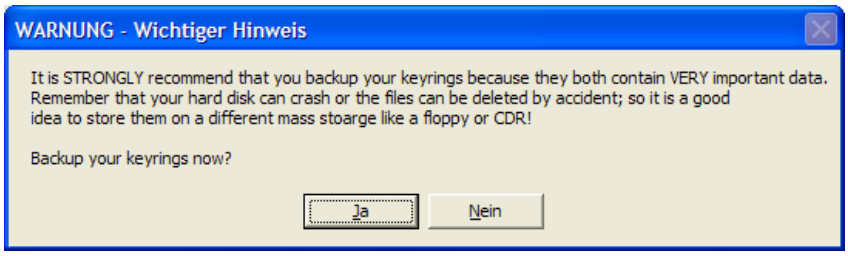
Nach Beendigung der Erstellung deiner Schlüssel erhältst du folgende Erfolgsmeldung:



Drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Nun erhältst du dankenswerter Weise den Hinweis, dass du deinen Schlüsselbund sofort sichern solltest.



Drücke den Button „Ja“, um die Sicherung sofort, „Nein“, um die Sicherung später vorzunehmen.

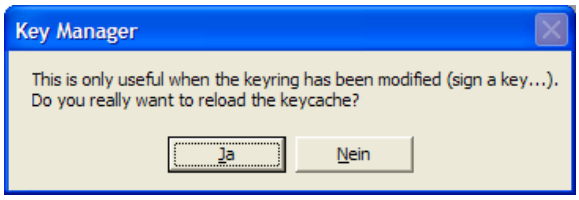
Wenn du dein Schlüsselpaar jetzt sofort sicherst, wirst du gefragt, in welchen Ordner es gesichert werden soll. Wie beim späteren Sichern werden Kopien von zwei Dateien angelegt:

- secring.gpg (dein privater Schlüssel, Secret Key)
- pubring.gpg (dein und andere öffentliche Schlüssel, Public Keys)

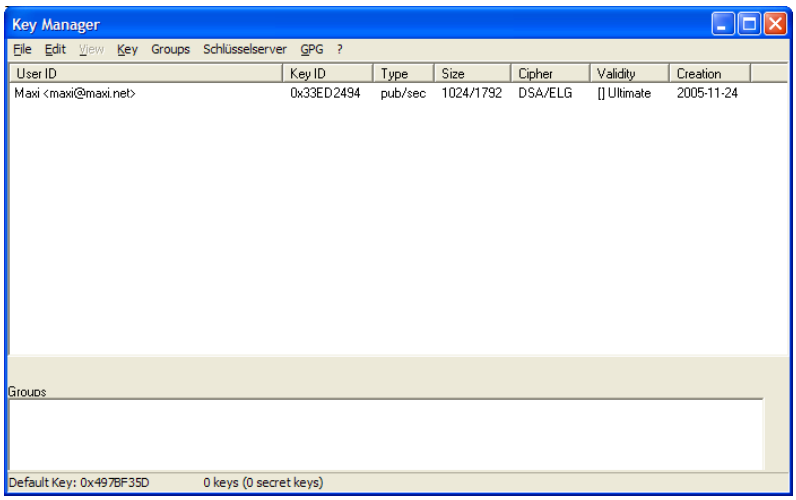
Wenn du keine zweite Festplatte in deinem Computer oder als externes Gerät dazugehängt hast, sichere dein Schlüsselpaar später. Wie das gemacht wird, erfährst du im Kapitel Das Anlegen von Sicherungskopien deiner Schlüssel.

Zurück zum Inhalt dieses Kapitels

Nach der Schlüsselerstellung erscheint noch eine Abfrage (ob das Fenster aktualisiert werden soll):



Drücke auf den Button „Ja“. Nun erscheint das Fenster zur Schlüsselverwaltung:



Du siehst dein soeben erstelltes Schlüsselpaar in der Liste (es gibt in diesem Fall nur einen Eintrag für privaten und öffentlichen Schlüssel). Als Typ siehst du „pub/sec“, es ist also ein Schlüsselpaar mit Public und Secret Key, dein Schlüsselpaar.

So, fertig. Du hast das Programm erfolgreich installiert und deinen ersten Schlüsselbund erstellt. Nach der Sicherung des Schlüsselpaars steht einem Ver- und Entschlüsseln von Texten/Mails und Dateien fast nichts mehr im Wege. Wie du das machst, erfährst du in den nächsten Kapiteln.

Zurück zum Inhalt dieses Kapitels

6.4 Das Anlegen von Sicherungskopien deiner Schlüssel

Überblick

Computer werden zeitweise kaputt, werden gestohlen... Es ist ganz wichtig, dass du zumindest eine Kopie deines Schlüssels anlegst, sonst kannst du bisher für dich verschlüsselte Texte und Dateien nie wieder lesen (entschlüsseln).

Und diese Kopie darf sich natürlich nicht auf dem gleichen Computer oder sogar auf der gleichen Festplatte wie dein Hauptschlüssel befinden. Eine Möglichkeit ist z.B., den Schlüssel auf eine oder mehrere CDs zu brennen (auch CDs werden ja nach einiger Zeit kaputt).

Das Anlegen von Sicherungskopien deiner Schlüssel

Um Kopien von deinem Schlüsselbund anzufertigen, kopiere einfach die beiden betroffenen Dateien an einen anderen Ort:

- pubring.gpg (dein und andere öffentlichen Schlüssel, Public Keys)
- secring.gpg (dein privater Schlüssel, Secret Key)

Sie befinden sich im Ordner, den du bei der Installation von WinPT angegeben hast.

Wenn dir eine Kopie deines privaten Schlüssels (Secret Key) 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 dein Passwort geschützt, und dieses Passwort ist ja sicherlich so ausgeklügelt, dass es niemand knacken kann.

Zurück zum Inhalt dieses Kapitels

6.5 Das Exportieren deines öffentlichen Schlüssels

Überblick

Damit andere Personen deinen öffentlichen Schlüssel (Public Key) auf ihrem Schlüsselbund aufnehmen können, kannst du unter drei verschiedenen Varianten wählen:

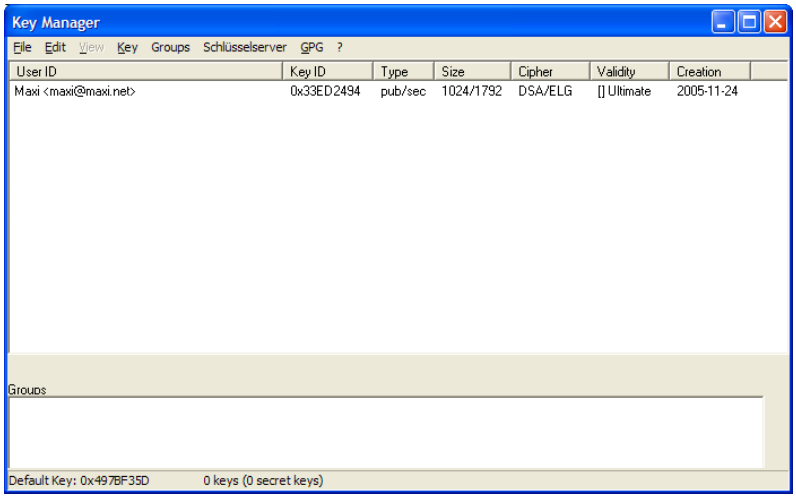
- Das Hinterlegen deines öffentlichen Schlüssels auf einem Keyserver (Schlüsselserver)
- Du speicherst deinen Schlüssel in einer Datei und schickst ihn anderen Personen per E-Mail bzw. übergibst ihn mittels Diskette, CD o.ä.
- Du hast eine eigene Webseite und stellst ihn dort in Textform oder als Datei zum Download bereit.

Auf den nächsten Seiten stellen wir die ersten beiden Möglichkeiten vor.

Zurück zum Inhalt dieses Kapitels

Das Hinterlegen des öffentlichen Schlüssels auf einem Keyserver

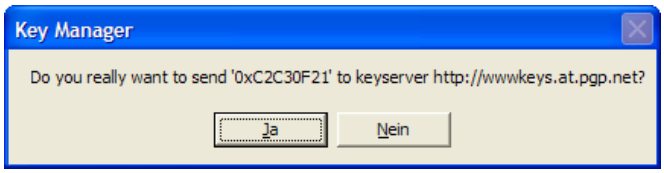
Um deinen öffentlichen Schlüssel (Public Key) an einen Keyserver zu senden, starte das Schlüsselverwaltungs-Programm durch Klicken mit der rechten Maustaste auf das Schlüsselsymbol rechts unten auf deinem Bildschirm und wähle den Menüpunkt „Key Manager“.



Markiere die Zeile mit deinem eigenen Schlüssel, drücke die rechte Maustaste und wähle den Menüpunkt Send to Keyserver ⇨ entsprechender Keyserver (in Österreich z.B. den Keyserver wwwkeys.at.pgp.net).

Zurück zum Inhalt dieses Kapitels

Es erscheint eine Abfrage, ob du das alles ernst meinst:



Bestätige die Abfrage durch Drücken des Buttons „Ja“. Kurz danach erhältst du (hoffentlich) die Erfolgsmeldung:

Der Schlüssel wurde erfolgreich hinterlegt.

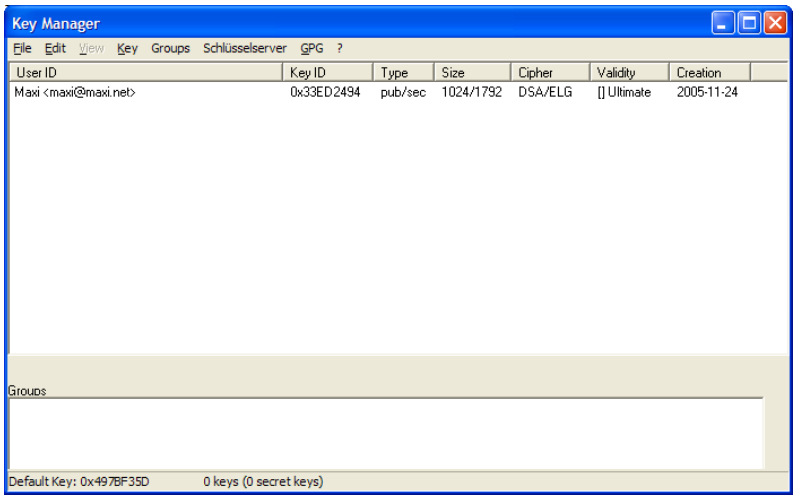
Andere Personen finden den Schlüssel nun auf diesem Keyserver mit der angeführten Key-Id (die siehst du auch im Schlüsselverwaltungs-Fenster bei deinem Schlüssel), dem angegeben Namen oder der angegebenen E-Mail-Adresse. Wie ein Schlüssel über den Keyserver an den Schlüsselbund gehängt werden kann, erfährst du im Kapitel Das Importieren von öffentlichen Schlüsseln von anderen Personen.

Zurück zum Inhalt dieses Kapitels

Das Speichern des Schlüssels in einer Datei

Du kannst deine beiden Schlüssel getrennt in Dateien speichern. Um anderen Personen deinen öffentlichen Schlüssel schicken bzw. übergeben zu können, speicherst du aber natürlich nur den öffentlichen Schlüssel.

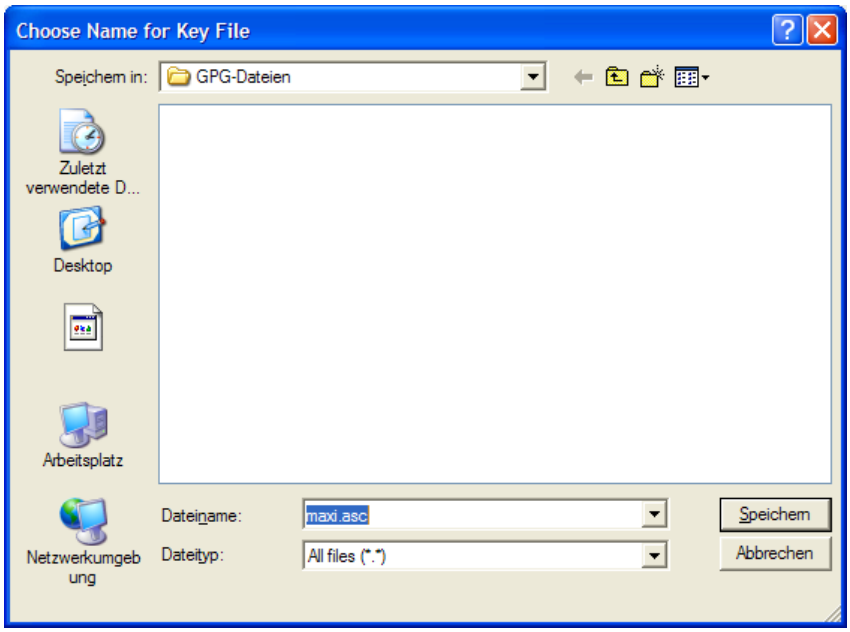
Starte das Schlüsselverwaltungs-Programm durch Klicken mit der rechten Maustaste auf das Schlüsselsymbol rechts unten auf deinem Bildschirm und wähle den Menüpunkt „Key Manager“.



Markiere die Zeile mit deinem eigenen Schlüssel und wähle den Menüpunkt Key ⇨ Export.

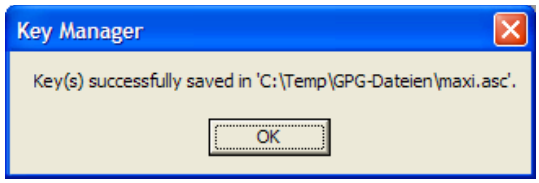
Zurück zum Inhalt dieses Kapitels

Nun wird ein Fenster geöffnet, in dem du den Ordner und den Namen der Datei angeben musst, in der dein öffentlicher Schlüssel gespeichert wird.



Ordner und Name der Datei sind frei wählbar, du musst sie nur nachher wieder finden.

Gib Ordner und Dateinamen an und drücke dann den Button „Speichern“. Es erscheint dann folgende Erfolgsmeldung:



Diese Datei kannst du nun per E-Mail verschicken oder auf Diskette, CD o.ä. kopieren und anderen Personen übergeben.

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: GnuPG v1.2.1 (MingW32)

mQGiBEOFv5kRBACYQ37gkYqqxvsDb5aueV1KekhRbhy5gyUS85h5LegH1GgkPpjB
v8/dVTTv9WkGfImDgoN3Bxc4eonvoyGoem7b+WIJ3bWjhh0d2Z7D4nKDpOJT57lA
5xmx1txQPdZGxeGLjscwEyuZI1QkXvy38FCiPzwMZCO78SWPyG7Cmyq0pwCggLBn
iNVuU4TPioHpvg4ASeYfbmsD/02LJM3R3ZDXs2OFKwjuYTNrstrgENEt/CdcRY1I
CR0yaWwgXk73Oa+trc1wIbqpB7ySDt7x2WMal1Aq5pDsohGn0fyvzhYcTpG4j/l4
u9gWmJXxIET4t4f5hHcS2gvNVJSoXw85gV4IPX8YaCf4VE0kcRccYms/doMVhc+B
kolYA/9jmV/lEv/3zbUXOhzw7EAWwxQsrHkmYGwpoC7RwOp2gyhw44s0U/wy7Il9
f4tUDFGlNUa4tH2NyhnhMdpye2Pcc/Lwi2Drn5F4HCqw+BFJZMEeTerlr+R5nmTi
Ey6dfYkjQ4P+eEgaBWk3Cyl1jDhXbRhqnJBQ7rjawKcD0ngJgbQUTWF4aSA8bWF4
aUBtYXhpLm5ldD6IWQQTEQIAGQUCQ4W/mQQLBwMCAxUCAwMWAgECHgECF4AACgkQ
3mNAcsLDDyGzrwCfcZnUn0aY5KkfuynxRZWfCpN0VLUAn286Cwxs7D8wazr/miq9
SUJwUNn6uQINBEOFv6QQCADgRqXZ0Ru/6YOfu2/a+Tk9RfZpXVzOJFltEMby5I0W
dWM+muW/FZ4z6d1GvgOZvUKdRnurdhUkaLvitVHGNs05kJRmkHikPTC/rQiid2Pd
r5gdnSTaRHquZCHNKQMwdPWuHZs9mhn3ZjDuY2FdCl593iNblwxJU/IIA+ILqV3y
xz4TAHj2IU0YX9YGVRhxhl92b9suRNJaEytcJJZSfZ20lJpHqJOT4fI6eZ+V5qnv
0zXPAo0WEjpVZ+LFvK2Hzw2F0Vv5kLbH2O4UNWCdARarlouiqi424y3IGVoTycxu
wGz7lteVqXHEoFDHySyNpp31uevyZk49QMGeQgs0CZIjAAMGB/sGB8UawTba0bb1
FmNZ9MpEj4q7C1ZMimI4ZyeLt/01SxcHN9n6bU8Ggh+i3QKPXgaoz0k1PuMemQDM
Z8yUCW+j1qlo+faD/F22lGleTYSFUZYOLSxC8p0AyrenIzUk1m8vF6rEBeldsU6e
w6TWuNDDS8kGv33YdjSnBaSihdK8H+QCvmwjidTdiBKtggY/uawdq9igMlFcVSM6
eIPrFwhz5j4+3tjbp+q1ip+za1wvtOUPYNqnezTXtBpQe3/xsiNWXUH9bdKrezbR
sIm8EgSJIRU4osi4x2ScBKgEjvGnyjhl3fiohRILFXbW3BrL7DTAkCWOpTxxp1nh
Ml/oEXhYiEYEGBECAAYFAkOFv6QACgkQ3mNAcsLDDyF7UwCfULQSWOBue6FnuJUt
GJOW9dRuD1cAnj8NZJNeqyKVLjTLogcqNIFr6FM1
=Kjk0
-----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

6.6 Das Importieren von öffentlichen Schlüsseln von anderen Personen

Überblick

Um einer anderen Person eine verschlüsselte Mail oder eine verschlüsselte Datei schicken zu können, musst du noch die öffentlichen Schlüssel (Public Keys) dieser Personen importieren (an deinen Schlüsselbund hängen).

Es gibt mehrere Möglichkeiten dazu:

- Das Importieren von einem Keyserver (Schlüsselserver)
- Das manuelle Importieren einer Datei mit dem Schlüssel
- Das manuelle Importieren eines Schlüssel über die Zwischenablage (Clibboard, durch Markieren des Schlüssel in Textform und wählen der Menüpunkte Bearbeiten ⇨ Kopieren bzw. Edit ⇨ Copy).

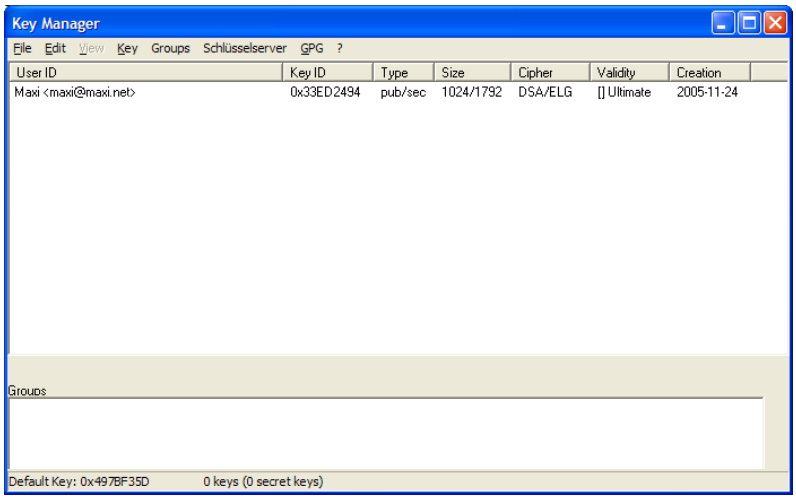
Auf den nächsten Seiten stellen wir alle 3 Möglichkeiten vor.

Nach dem Aufnehmen von öffentlichen Schlüsseln von anderen Personen musst du bei WinPT unbedingt extra angeben, dass du diesen Schlüsseln vertraust. Andernfalls erhältst du beim Verschlüsseln eine Fehlermeldung.

Wie das geht, erfährst du im Kapitel Die Markierung des importierten Schlüssels als vertrauenswürdig

Zurück zum Inhalt dieses Kapitels

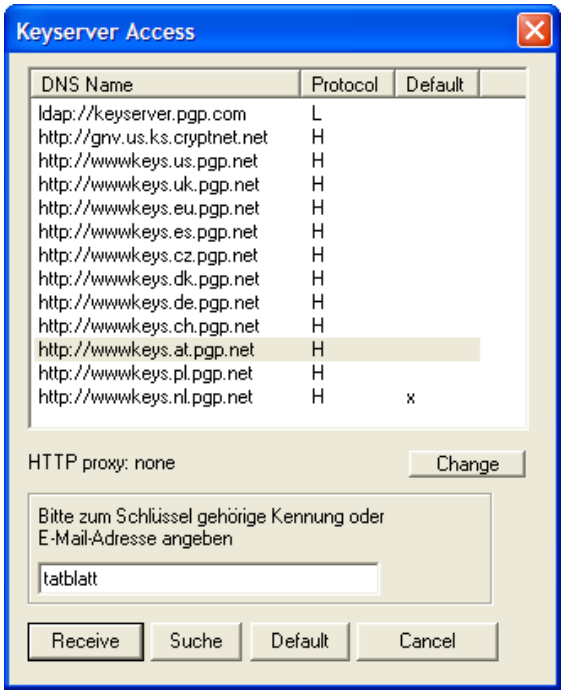
Das Importieren von Schlüsseln erfolgt mit dem Key Manager (Schlüsselverwaltungsprogramm). Starte das Programm durch Klicken mit der rechten Maustaste auf das Schlüsselsymbol rechts unten auf deinem Bildschirm und wähle den Menüpunkt „Key Manager“.



Zurück zum Inhalt dieses Kapitels

Das Importieren von einem Keyserver

Um einen Schlüssel, der auf einem Keyserver hinterlegt ist, zu importieren, wähle den Menüpunkt „Schlüsselserver“. Folgendes Fenster erscheint:



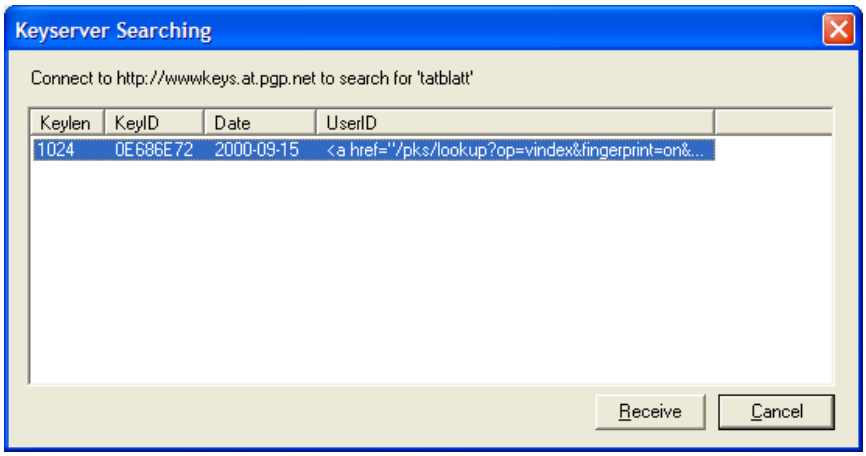
Als Beispiel wird hier der öffentliche Schlüssel der Zeitschrift TATblatt gesucht.

Wähle einen der Keyserver aus (es funktionieren nicht alle problemlos, bei Problemen probiere einfach einen anderen) und gib die E-Mail-Adresse oder den Namen an.

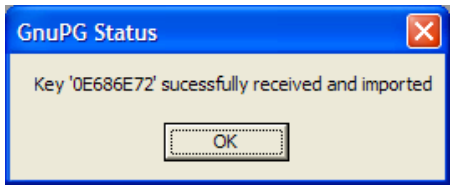
Drücke dann den Button „Suche“.

Zurück zum Inhalt dieses Kapitels

Mit etwas Glück wird der Schlüssel gefunden.



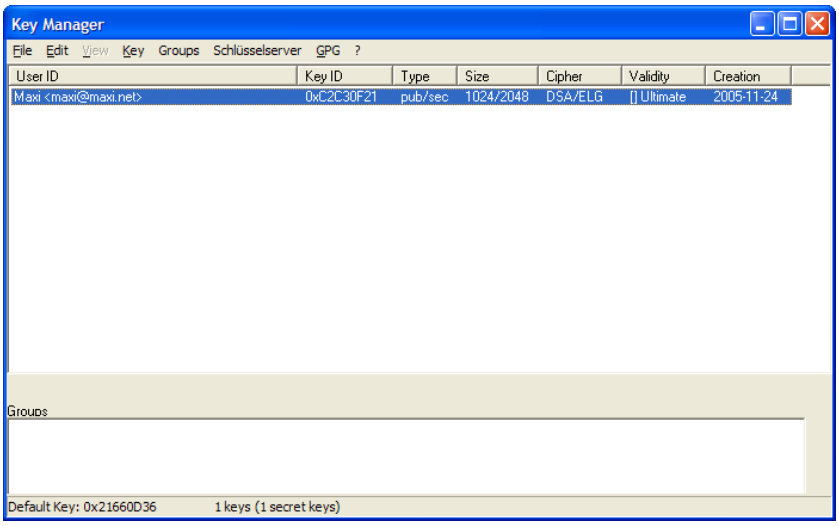
Markiere den gefundenen Eintrag und drücke den Button „Receive“, der Schlüssel wird dann an deinen Schlüsselbund gehängt. Es erscheint die Erfolgsmeldung:



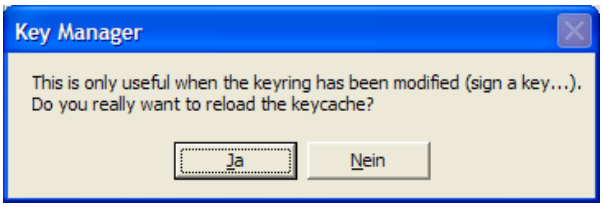
Bestätige durch Drücken des Buttons „OK“ und schließe auch das „Keyserver Searching“ und das „Keyserver Access“-Fenster von vorher (z.B. durch Drücken des Buttons „Cancel“).

Zurück zum Inhalt dieses Kapitels

Im Schlüsselverwaltungs-Fenster siehst du den eben importieren Schlüssel nicht sofort:



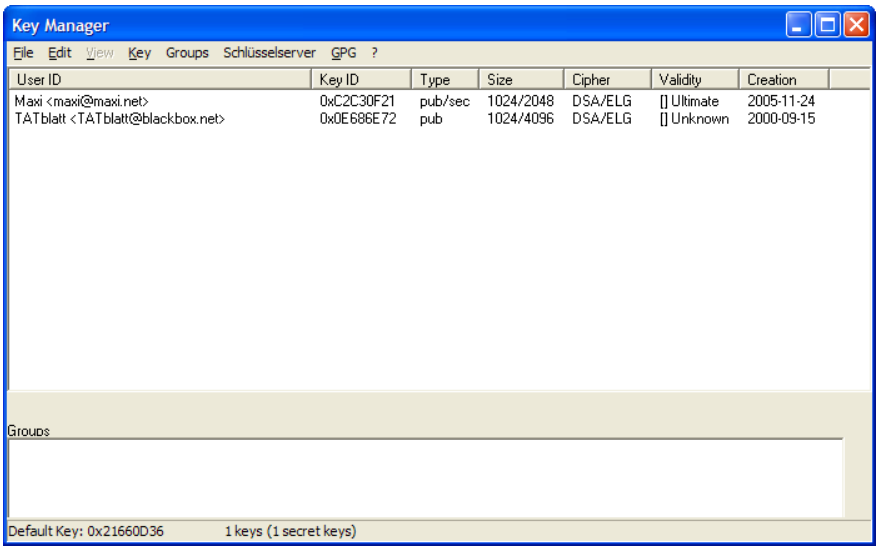
Aktualisiere den Fensterinhalt durch Wählen des Menüpunkts Key ⇨ Reload Key Cache, es erscheint eine Bestätigungsabfrage:



Drücke den Button „Ja“.

Zurück zum Inhalt dieses Kapitels

Nun erscheint endlich das aktualisierte Fenster mit dem eben importieren Key des TATblatt:



Beim importierten Schlüssel ist jetzt als Typ „pub“ für public angegeben, was ja korrekt ist – du hast den Public Key vom TATblatt importiert.

Werden mehrere Schlüssel zu einem Namen gefunden, musst du den richtigen Schlüssel herausfinden (probier es z.B. mal mit einer Suche nach Maxi). Bei der Suche nach einem gewissen Maxi erhältst du mehrere Ergebniszeilen mit verschiedenen gefundenen Schlüsseln.

Leider bekommst du bei diesem Programm keinerlei Hinweise auf zusätzliche Informationen wie z.B. die E-Mail-Adresse eines Keys.

Eine Möglichkeit ist in diesem Fall, im Suchfenster nach der genauen E-Mail-Adresse statt nur nach dem Namen zu suchen. Dazu musst du aber die E-Mail-Adresse wissen, welche die andere Person bei ihrer Schlüsselerstellung angegeben hat (auch ein Grund, warum du doch überlegen solltest, deine richtige E-Mail-Adresse anzugeben).

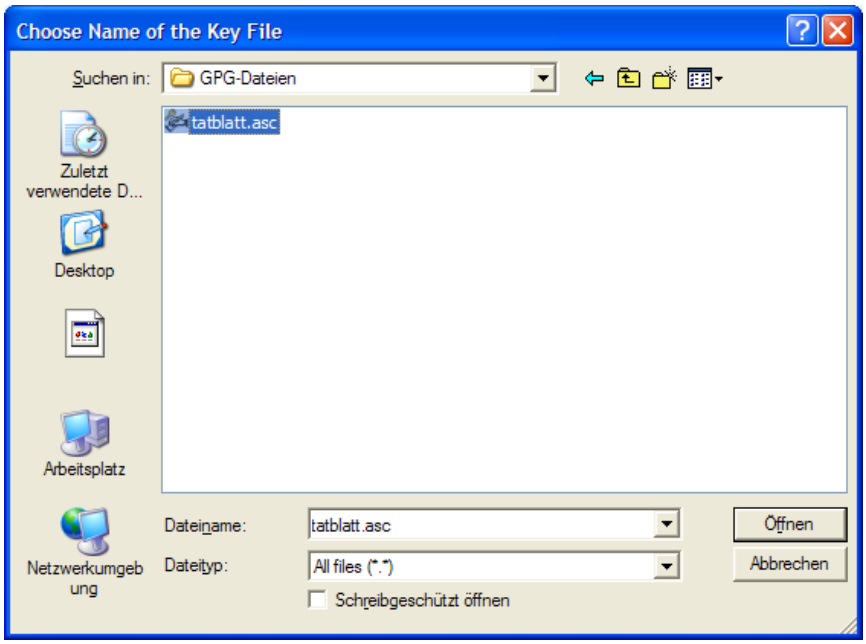
Zurück zum Inhalt dieses Kapitels

Das Importieren eines Schlüssels mit einer Datei

Die Person, deren Schlüssel du aufnehmen willst, kann dir auch eine Datei mit dem Schlüssel schicken, so eine Datei hat meistens die Endung .asc.

Du musst aber sicher sein, dass dieser Schlüssel wirklich von der Person ist, mit der du verschlüsselt kommunizieren willst.

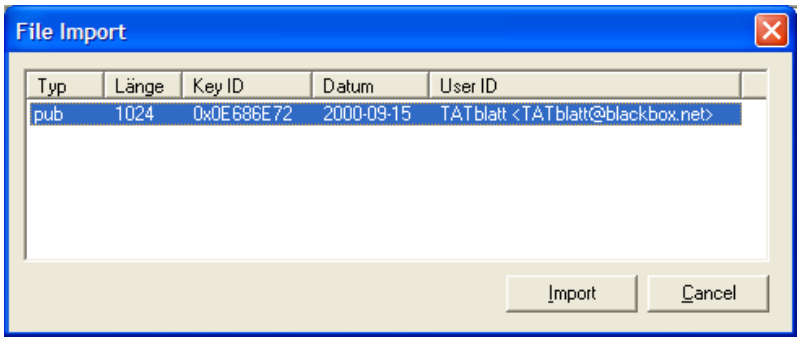
Wähle dazu im Schlüsselverwaltungs-Fenster den Menüpunkt Key ⇨ Import. Es wird ein Fenster geöffnet, in dem du den Ordner und die Datei angeben musst:



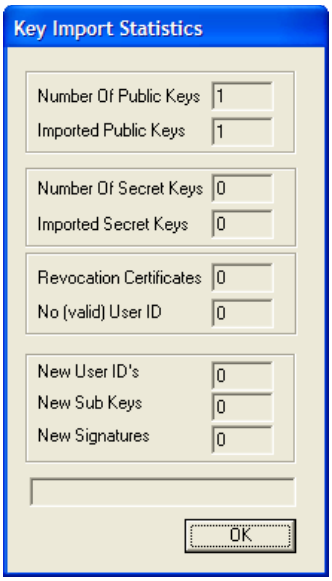
Suche die Datei, markiere sie und drücke dann den Button „Öffnen“.

Zurück zum Inhalt dieses Kapitels

Es erscheint ein Bestätigungsfenster mit dem Schlüssel, der importiert werden soll:



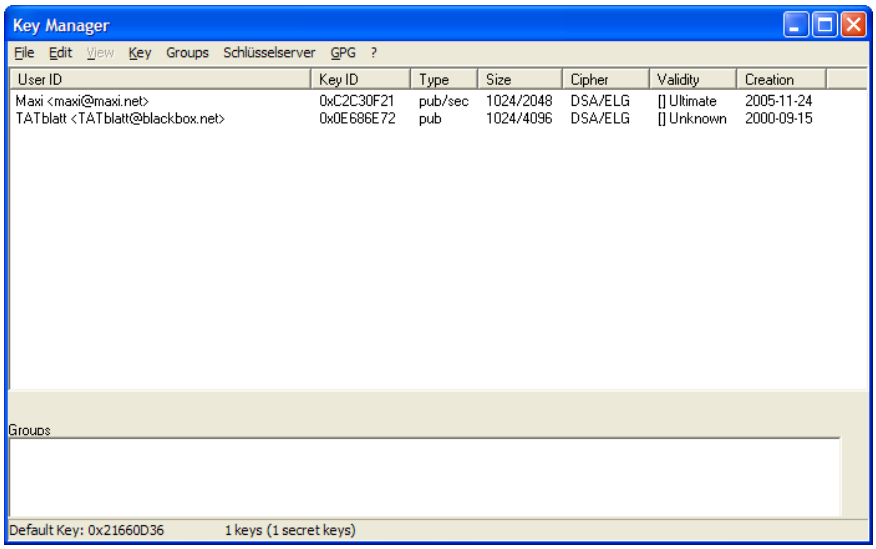
Markiere die Zeile und drücke den Button „Import“. Es erscheint noch ein Infofenster mit der Information, dass ein Public Key importiert wurde:



Bestätige durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

Im Schlüsselverwaltungs-Fenster musst du wieder das Fenster durch Auswählen des Menüpunkts Key ⇨ Reload Key Cache aktualisieren, dann siehst du den importierten Schlüssel:



Zurück zum Inhalt dieses Kapitels

Das manuelle Importieren eines Schlüssel über die Zwischenablage (Clibboard)

Oft werden auf Internetseiten Public Keys in Textform angeboten, im Fall des TATblatt z.B. Unter http://tatblatt.mediaweb.at/Tb-PGP.htm.

Du musst den Textteil von

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

bis

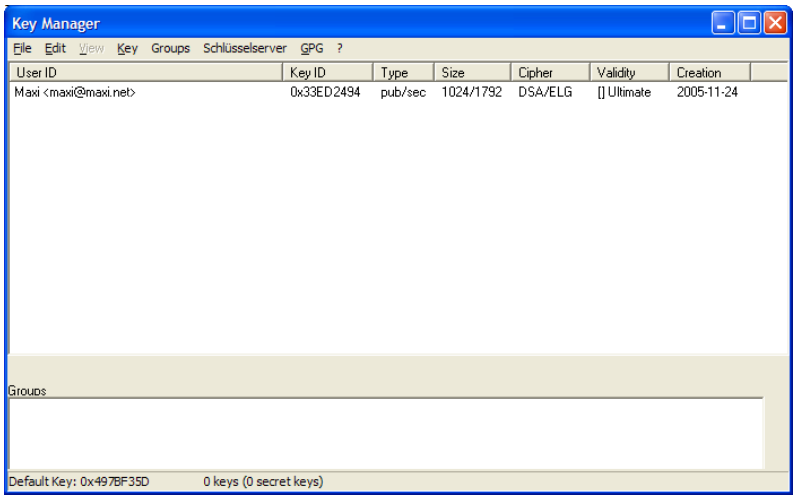
```
-----END PGP PUBLIC KEY BLOCK-----
```

markieren - inklusive der beiden angeführten Zeilen!

Wähle dann den Menüpunkt Bearbeiten ⇨ Kopieren. Jetzt ist der Schlüssel in Textform in der Windows Zwischenablage (dem Clipboard) gelandet.

Zurück zum Inhalt dieses Kapitels

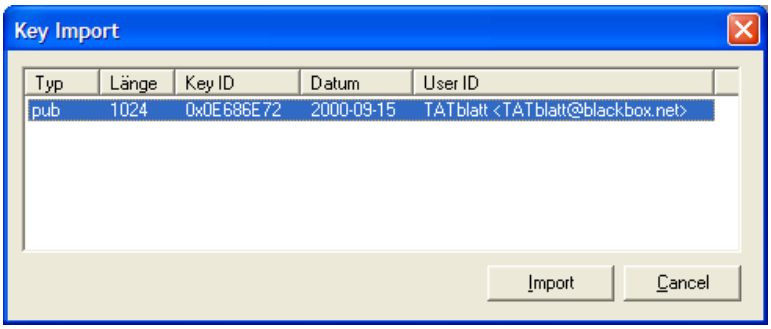
Starte das Schlüsselverwaltungs-Programm durch Klicken mit der rechten Maustaste auf das Schlüsselsymbol rechts unten auf deinem Bildschirm und wähle den Menüpunkt „Key Manager“.



Klicke mit der rechten Maustaste auf irgendeine bestehenden Zeile und wähle im Kontextmenü den Punkt „Paste Key from Clipboard“ (d.h. „füge den Schlüssel aus der Zwischenablage ein“).

Zurück zum Inhalt dieses Kapitels

Es erscheint ein Bestätigungs-Fenster mit dem Schlüssel:

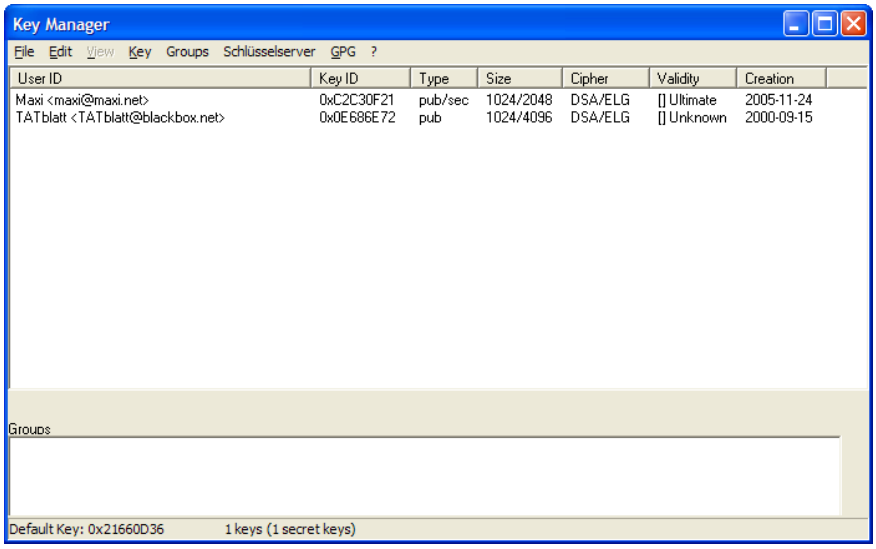


Markiere die Zeile und drücke zur Bestätigung den Button „Import“.

Es erscheint noch ein Fenster mit der Information, dass du einen Public Key importiert hast. Bestätige die Information durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

Im Schlüsselverwaltungs-Fenster musst du wieder das Fenster durch Auswählen des Menüpunkts Key ⇨ Reload Key Cache aktualisieren, dann siehst du den importierten Schlüssel:

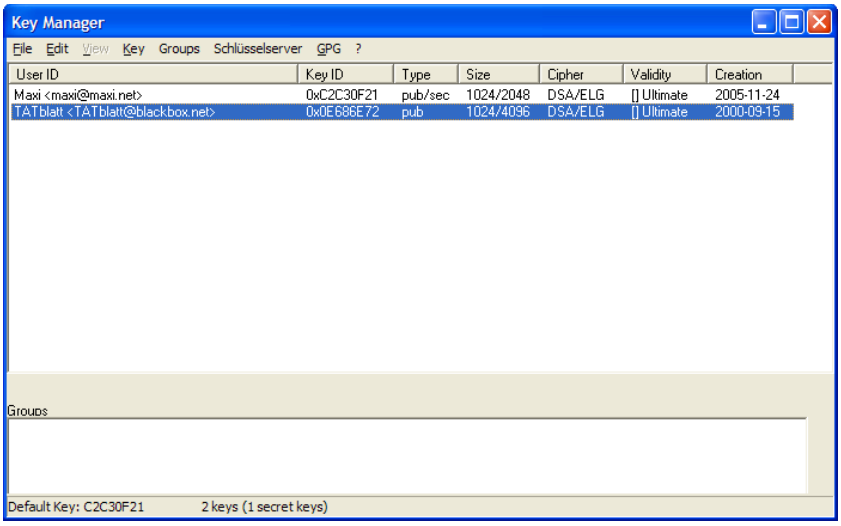


Zurück zum Inhalt dieses Kapitels

Die Markierung des importierten Schlüssels als vertrauenswürdig

Wie schon erwähnt, musst du den importierten Schlüssel als vertrauenswürdig einstellen, sonst kannst du ihn nicht zum Verschlüsseln verwenden.

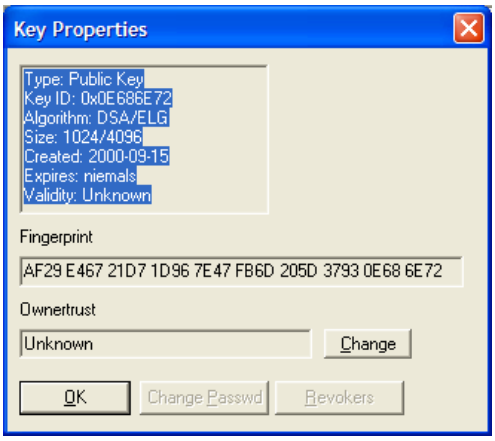
Starte dazu das Schlüsselverwaltungs-Programm durch Klicken mit der rechten Maustaste auf das Schlüsselsymbol rechts unten auf deinem Bildschirm und wähle den Menüpunkt „Key Manager“.



Zeige mit dem Mauszeiger auf die Zeile mit dem eben importierten Schlüssel und drücke die rechte Maustaste. Im sich öffnenden Kontextmenü wähle den Menüpunkt „Key Properties“.

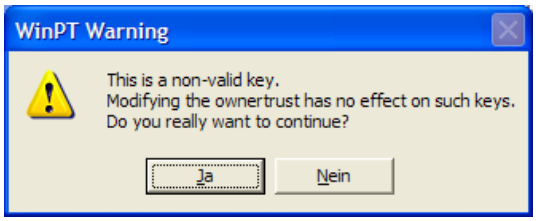
Zurück zum Inhalt dieses Kapitels

Es öffnet sich ein Fenster mit den Schlüsseleigenschaften:



Unter „Ownertrust“ siehst du den Vertrauensstatus zum Schlüssel, in diesem Fall ist er nach dem Importieren auf „Unknown“ (unbekannt) gesetzt. Und das musst du ändern.

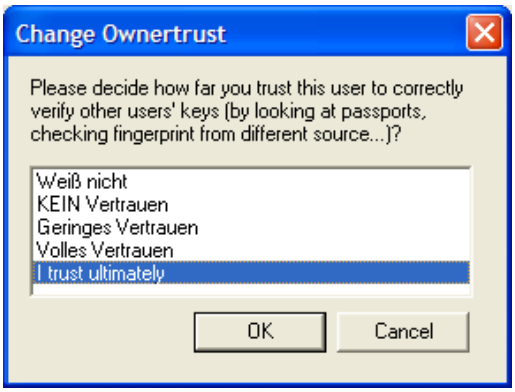
Drücke den Button „Change“. Es folgt eine Warnung, dass der Schlüssel ungültig ist.



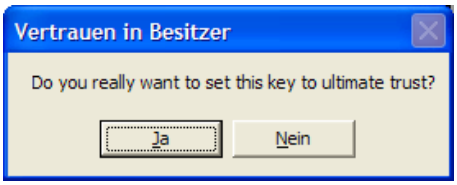
Ignoriere diese Warnung und drücke den Button „Ja“ zum Fortsetzen.

Zurück zum Inhalt dieses Kapitels

Es erscheint ein Fenster mit den möglichen Vertrauensstufen:



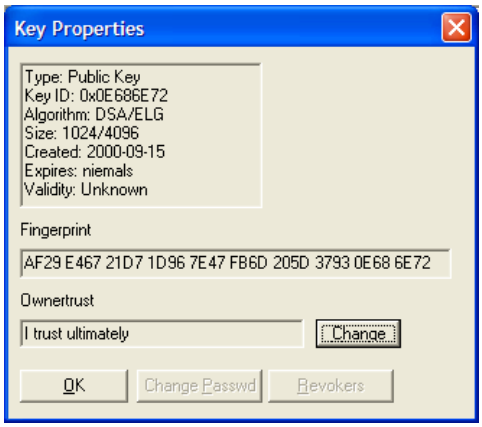
Markiere die Zeile mit „I trust ultimately“ und drücke den Button „OK“. Wieder erscheint eine Abfrage, ob du das alles ernst meinst:



Bestätige die Abfrage durch Drücken des Buttons „Ja“. Jetzt kommt noch eine Erfolgsmeldung:

Zurück zum Inhalt dieses Kapitels

Im Fenster mit den Schlüssel-Eigenschaften wurde der Status jetzt entsprechend geändert:



Schließe das Fenster durch Drücken des Buttons „OK“.

So, endlich geschafft – du kannst dem TATblatt jetzt verschlüsselte Mails schicken (aber probier das bitte nicht mit dem TATblatt, sondern z.B. mit einer FreundIn aus).

Zurück zum Inhalt dieses Kapitels

7 Die Verwendung von GPG 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
- Mozlla Thunderbird
- Andere Mailprogramme und Web-Mail

Leider ist die Verwendung von GPG im Mailprogramm Thunderbird noch nicht direkt integriert. In Zukunft wird diese Funktionalität aber wahrscheinlich angeboten (es gibt bereits ein Projekt dazu).

Bei Verwendung von Thunderbird musst du entweder ein kleines Zusatzprogramm (die Extension Enigmail) installieren oder wie im Kapitel Andere Mailprogramme und Web-Mail beschrieben vorgehen.

7.1 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 für Windows die derzeit aktuelle Version 7.0, für MacOS die Version 6.2. Das Programm Eudora selbst wird aber hier nicht erklärt, sondern nur die Integration von GPG.

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\7.0


Eudora_7.0.0.16.exe


Diese kostenlosen Versionen von Eudora haben aber leider keinen Spam-Filter, er ist deaktiviert. Nur die kostenpflichtige Version aktiviert diese Funktion.

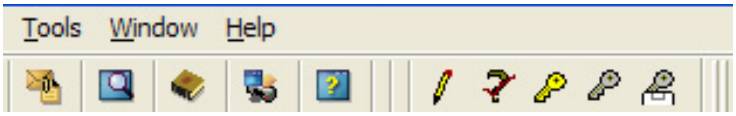
Das ebenfalls vorgestellte kostenlose Mailprogramm Thunderbird hat einen sehr guten integrierten Spam-Filter.

Zurück zum Inhalt dieses Kapitels

Überblick

Mit Eudora ist die Ver- und Entschlüsselung besonders komfortabel. Grund dafür ist, dass GPG in Eudora voll integriert ist.

Wenn du Eudora nach der Installation von GPG (z.B. durch Installation von WinGP) startest, siehst du in der Toolbar fünf Symbole, die mit Verschlüsselung mittels GPG zu tun haben:



Die Symbole werden erst aktiviert, wenn du eine Mail erstellst oder liest, sonst sind sie nicht anwählbar.

Du siehst jetzt die fünf neuen Symbole (die Gruppe mit den Schlüsselsymbolen) mit folgender Bedeutung (von links nach rechts):

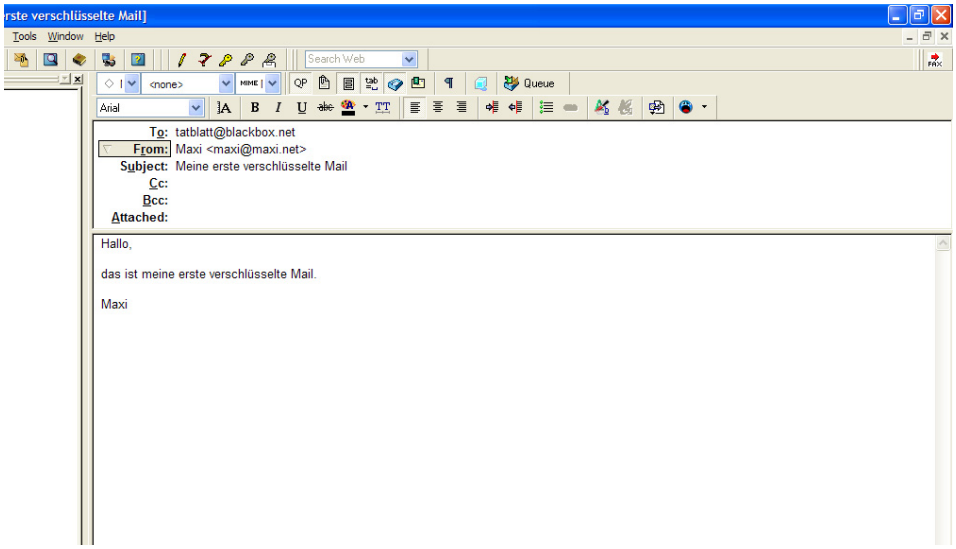
- GPG Signieren: du „unterschreibst“ die Mail mit Hilfe deines GPG-Schlüssels um zu beweisen, dass die Mail wirklich von dir ist.
- GPG Unterschrift prüfen: du prüfst die „Unterschrift“ einer Mail, die du erhalten hast, mit Hilfe des Public Keys der AbsenderIn
- GPG Verschlüsseln: zum Verschlüsseln einer Mail, die du geschrieben hast
- GPG Entschlüsseln: zum Entschlüsseln einer Mail, die du erhalten hast
- GPG In Zwischenablage entschlüsseln: die verschlüsselte Mail nicht verändern, den entschlüsselten Text in die Windows Zwischenablage (Clipboard) kopieren.

  Du kannst den entschlüsselten Text dann in einem anderen Programm (z.B. in einem Texteditor) durch Wählen des Menüpunkts Bearbeiten ⇨ Einfügen sichtbar machen.

Zurück zum Inhalt dieses Kapitels

Das Verschlüsseln

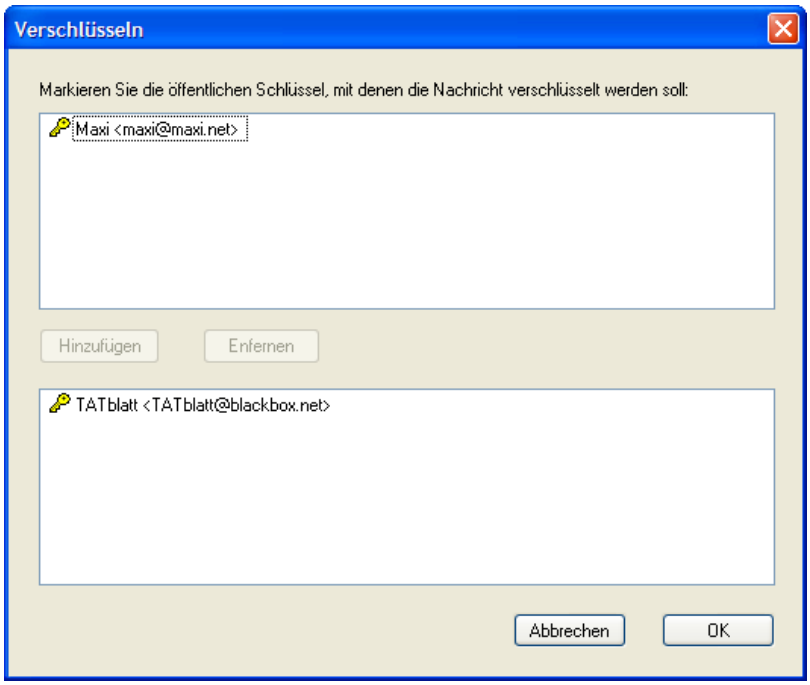
Wenn du nun eine Mail in Eudora geschrieben hast, sieht das ungefähr so aus:



Wenn du die Mail für das TATblatt verschlüsseln willst, drücke auf das entsprechende Schlüsselsymbol für „GPG Verschlüsseln“ (der gelbe Schlüssel).

Zurück zum Inhalt dieses Kapitels

Es erscheint jetzt ein Fenster, in dem du die EmpfängerInnen angeben musst:



Doppelklicke auf die richtige EmpfängerIn(nen), der Eintrag scheint dann im unteren Teil des Fensters auf.

Nachdem du einen Text für eine bestimmte EmpfängerIn verschlüsselt hast, kannst auch du sie nicht mehr lesen.

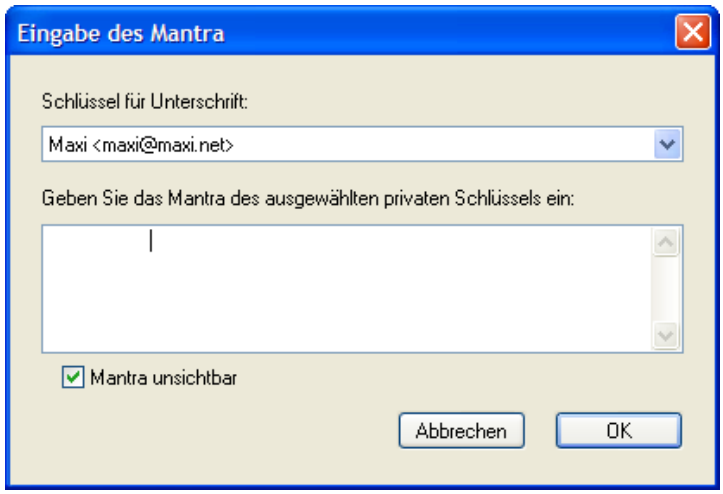
Ein Tipp dazu: wenn du die Mail auch für dich selbst verschlüsselst, kannst auch du sie nachher nochmals entschlüsseln und lesen.

Also in diesem Fall einfach auch auf die Zeile mit Maxis Schlüssel doppelklicken, es stehen dann beide im unteren Teil des Fensters.

Klicke nach der Wahl der EmpfängerIn(nen) den Button „OK“.

Zurück zum Inhalt dieses Kapitels

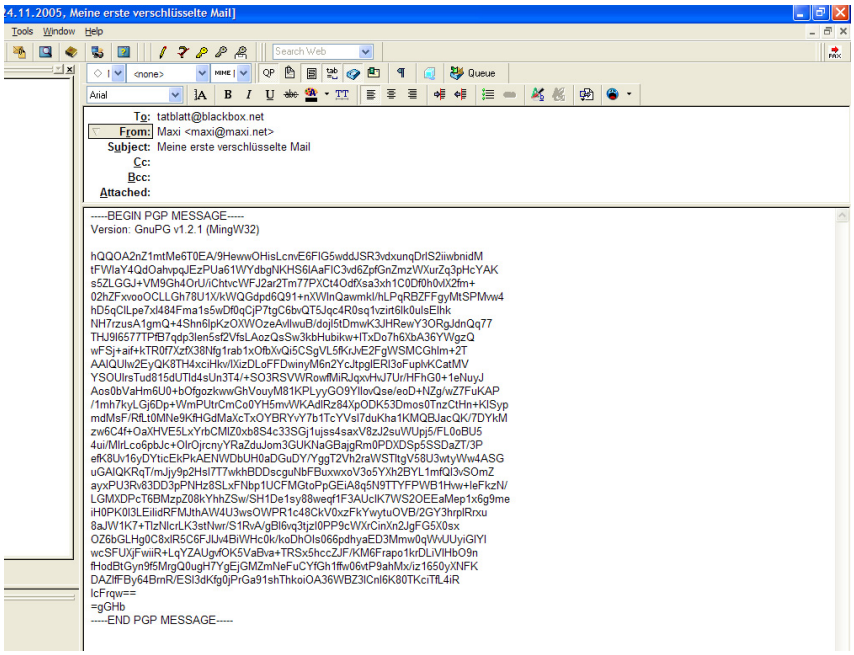
Nun erscheint ein Fenster zur Eingabe deines Passworts (das Passwort deines Secret Keys):



Gib dein Passwort (hier Mantra genannt) ein und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Und schon ist die Mail für das TATblatt verschlüsselt, falls angewählt, natürlich auch für dich selbst:



Und diesen wilden Haufen von Buchstaben, Ziffern und Sonderzeichen kann jetzt nur das TATblatt entschlüsseln (bzw. alle EmpfängerInnen, für die du den Text verschlüsselt hast).

Tja, das war's schon, abschicken und fertig. So einfach geht das...

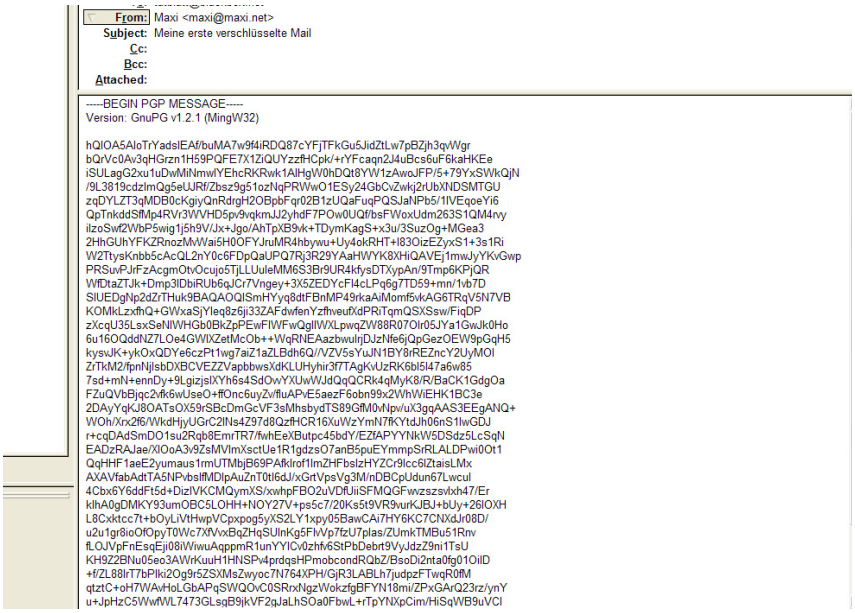
Der verschlüsselte Text schaut im Verhältnis zu den paar wenigen Worten, die hier im Beispiel geschrieben wurden, sehr sehr lange aus.

Aber keine Angst, in diesem Text sind auch Schlüssel-Informationen enthalten. Wenn du einen längeren Text schreibst, wird die verschlüsselte Version nicht um ein Vielfaches länger.

Zurück zum Inhalt dieses Kapitels

Das Entschlüsseln

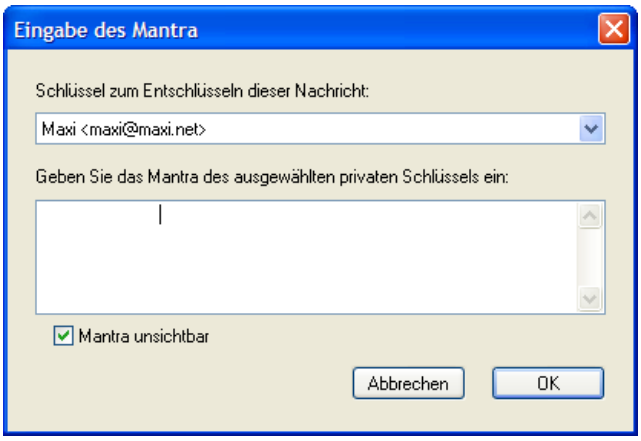
Wenn du eine verschlüsselte Nachricht erhältst, schaut der verschlüsselte Text so wie der, der vorher im Beispiel für das Verschlüsseln erstellt wurde, aus:



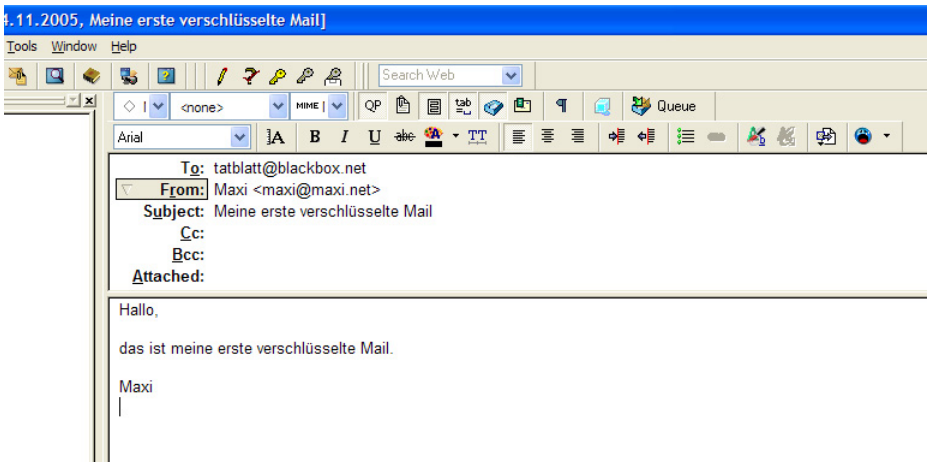
Drücke mit der Maus einfach auf das Symbol für das Entschlüsseln (GPG Entschlüsseln).

Zurück zum Inhalt dieses Kapitels

Natürlich musst du jetzt auch dein Passwort eingeben, alles andere wäre ja äußerst sinnlos (dann könnte jeder Mensch den Text entschlüsseln):



Und schon ist der entschlüsselte Text sichtbar:



Auch nicht allzu kompliziert, oder? Beachte aber bitte noch ein paar Hinweise auf der nächsten Seite.

Zurück zum Inhalt dieses Kapitels

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 TrueCrypt 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

7.2 Thunderbird

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

Dieses Mail-Programm kannst du auch von der CD aus installieren. Auf der CD befindet sich für Windows die derzeit aktuelle Version 1.0.7.

Installation von Thunderbird

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



Thunderbird\Windows


Thunderbird Setup 1.0.7.exe

Bei Thunderbird ist leider die Installation eines kleinen Zusatzprogramms (einer Extension) notwendig, um danach genauso komfortabel ver- und entschlüsseln zu können wie in Eudora.

Du findest anschließend im Kapitel Die Installation von Enigmail eine Anleitung, wie du dieses Zusatzprogramm mit dem Namen Enigmail zu Thunderbird dazuinstallieren kannst. Es befindet sich natürlich auch auf der CD.


Auf der Webseite von Thunderbird http://www.mozilla.com/thunderbird/ findest du zahlreiche gute Anleitungen und Hinweise zu diesem Mailprogramm.

Zurück zum Inhalt dieses Kapitels

Überblick

Mit Thunderbird ist die Ver- und Entschlüsselung genauso komfortabel wie bei Eudora. Grund dafür ist, dass GPG auch hier voll integriert ist, wenn du ein kleines Zusatzprogramm (die Extension Enigmail) dazuinstallierst.

Im nächsten Kapitel findest du die Anleitung, wie du dieses Zusatzprogramm installieren kannst.

Wenn du Thunderbird nach der Installation von GPG (z.B. durch Installation von WinGP) startest und eine Mail schreibst, findest du zugehörige Menüpunkte, die mit Verschlüsselung mittels GPG zu tun haben.

Zurück zum Inhalt dieses Kapitels

Die Installation von Enigmail

Du findest das Zusatzprogramm Enigmail für Thunderbird auf der CD im gleichen Verzeichnis wie das Mailprogramm selbst:



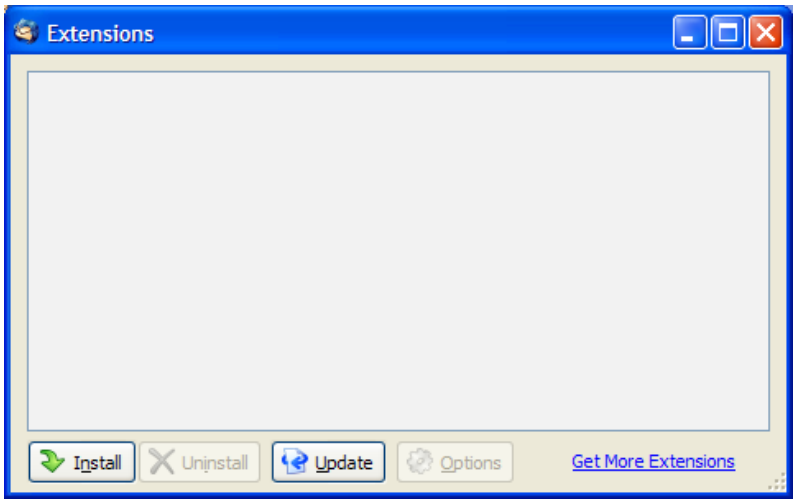
Thunderbird\Windows


enigmail-0.93.0-tb10-win32.xpi

Zur Installierung dieser Extension starte das Programm Thunderbird und wähle den Menüpunkt Tools ⇨ Extensions.

Zurück zum Inhalt dieses Kapitels

Du siehst wahrscheinlich ein recht leeres Fenster vor dir:

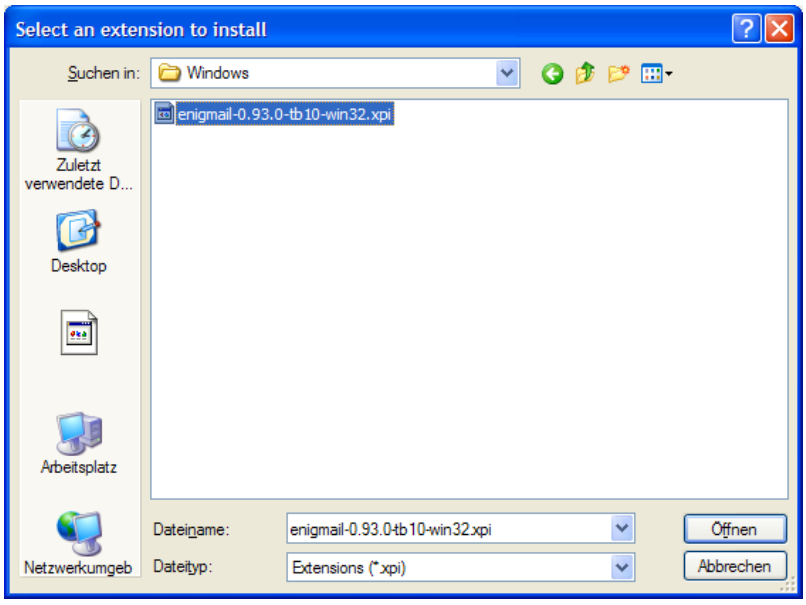


Hier werden alle Extensions (Erweiterungen) angezeigt, die du installierst hast. In diesem Beispiel wurde noch keine Extension installiert.

Drücke den Button „Install“.

Zurück zum Inhalt dieses Kapitels

Im nun erscheinenden Fenster musst du angeben, wo sich diese Extension zum Installieren befindet:

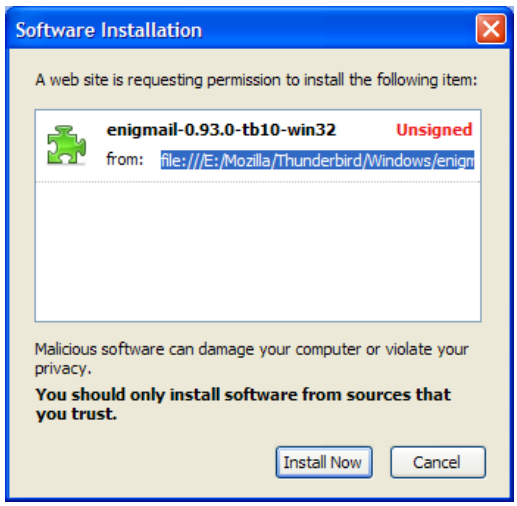


Suche den Ordner Mozilla\Thunderbird\Windows auf der CD und markiere die Datei enigmail-0.93.0-tb10-win32.xpi.

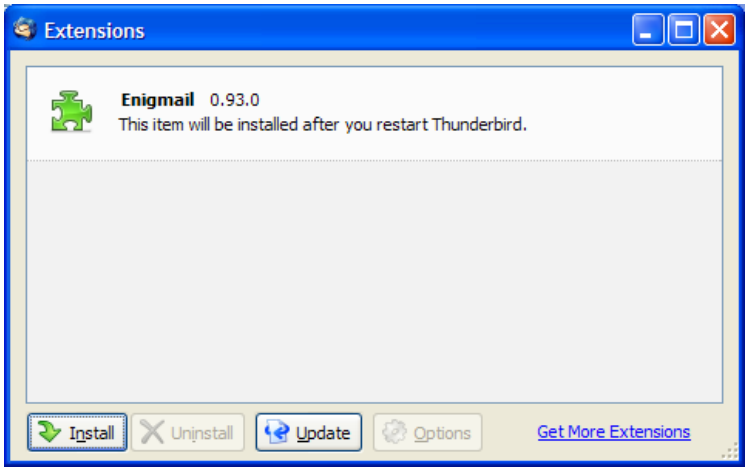
Drücke dann den Button „Öffnen“.

Zurück zum Inhalt dieses Kapitels

Es erscheint ein Fenster mit der Extension:



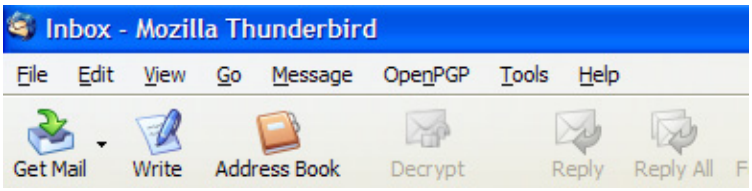
Drücke den Button „Install Now“. Kurz danach erscheint wieder das Fenster mit deinen Extensions:



Die Extension Enigmail ist jetzt aufgelistet. Du erhältst auch den Hinweis, dass du Thunderbird schließen und neu starten musst, um die Extension zu installieren. Schließe das Fenster und das Mailprogramm Thunderbird und starte das Mailprogramm neu.

Zurück zum Inhalt dieses Kapitels

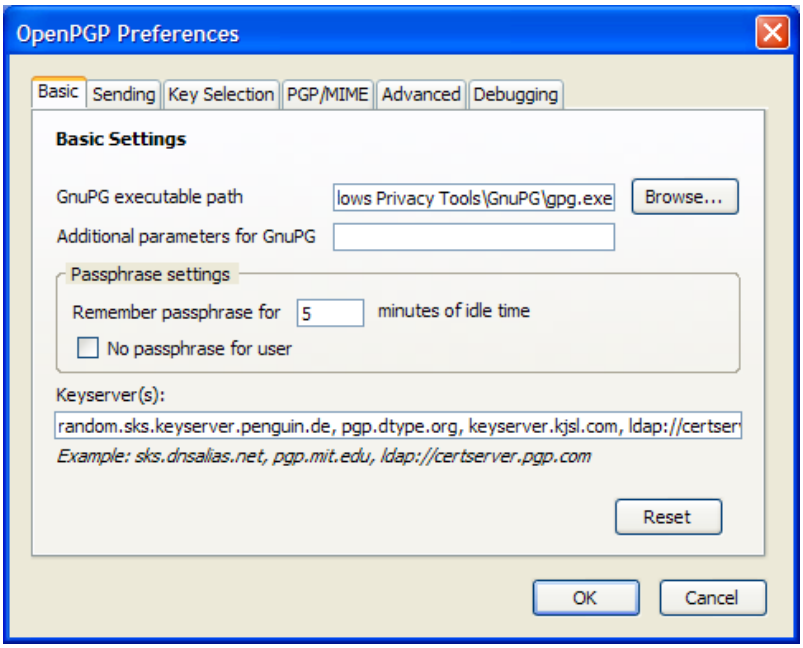
Es ist jetzt ein neuer Menüpunkt hinzugekommen, nämlich OpenPGP:



Du musst noch ein paar Einstellungen vornehmen. Wähle dazu den Menüpunkt OpenGPG ⇨ Preferences.

Zurück zum Inhalt dieses Kapitels

Folgendes Konfigurationsfenster erscheint:

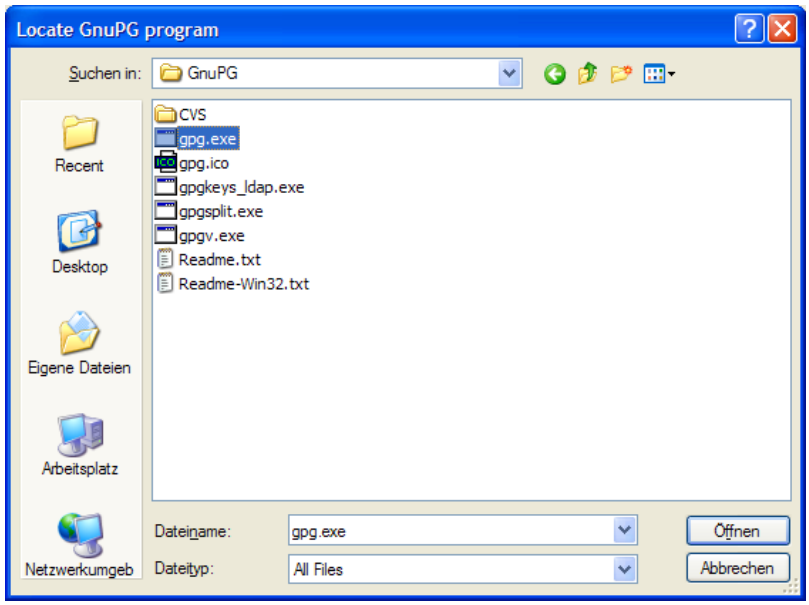


Das Wichtigste ist, dass du bei „GnuPG executable path“ den Pfad zur Datei gpg.exe angibst. Diese Datei wird bei der Installation von WinPT mitinstalliert. Drücke den Button „Browse“, dann kannst du die Datei suchen (siehe auch nächste Seite).

Wichtig ist unserer Meinung nach auch, dass du bei den „Passphrase settings“ angibst, dass dein Passwort nicht im Speicher „gemerkt“ wird, nicht für 5 Minuten (wie hier vorgeschlagen) und auch nicht für weniger.

Zurück zum Inhalt dieses Kapitels

In diesem Fenster musst du die gesuchte Datei finden (das Programm GPG):



Sie befindet sich nach einer Standard-Installation von WinPT in folgendem Ordner (der Pfad kann aber bei dir leicht abweichen):

- C:\Programme\Windows Privacy Tools\GnuPG\gpg.exe

Wähle die Datei gpg.exe aus und drücke den Button „Öffnen“.

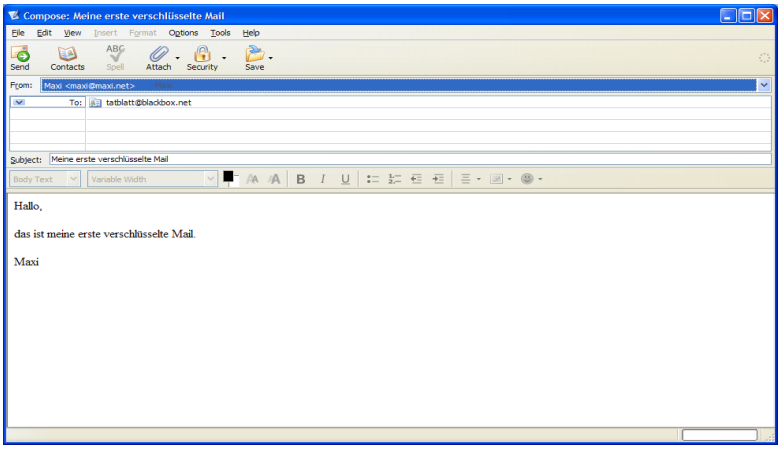
Bei den anderen Reitern findest du noch eine ganze Reihe weiterer Einstellungsmöglichkeiten, z.B. ob du eine verschlüsselte Mail immer auch für dich selbst verschlüsseln willst – was ja ganz praktisch ist.

Wenn du fertig bist, drücke den Button „OK“. So, fertig, jetzt ist das Mailprogramm bereit zum Verschlüsseln.

Zurück zum Inhalt dieses Kapitels

Das Verschlüsseln

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



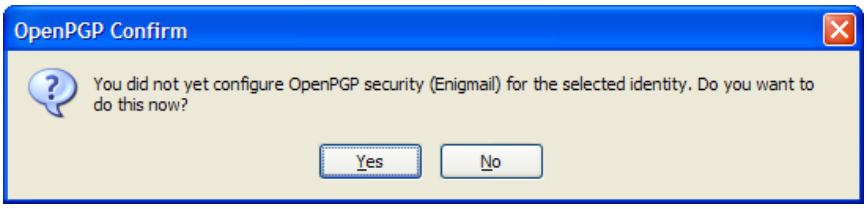
Wenn du die Mail verschlüsseln willst, wähle den Menpunkt OpenPGP ⇨ Encrypt Message.

Wenn du deine erste (verschlüsselte) Mail mit Thunderbird schickst, solltest du noch eine wichtige Einstellung vornehmen. Die kannst du nur im hier gezeigten Fenster wählen, in dem du deine Mails schreibst.

Wähle den Menüpunkt OpenPGP ⇨ Default Composition Options ⇨ Signing/Encryption Options. Hake den Punkt „Sign encrypted messages by default“ an, so erhält jede verschlüsselte Mail deine „Unterschrift“ und du musst dein Passwort angeben. Das zeigt der EmpfängerIn, dass die Mail wirklich von dir ist (solange keine andere Person dein Passwort herausfindet).

Zurück zum Inhalt dieses Kapitels

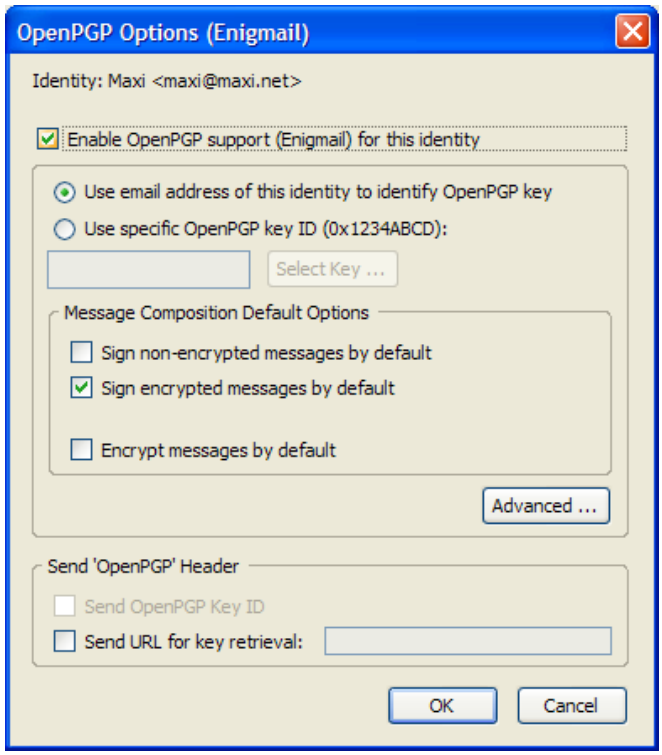
Nach dem Wählen des Menüpunkts „Encrypt Message“ passiert vorerst mal gar nichts. Erst wenn du die Mail abschickst, wird sie auch verschlüsselt. Sie ist jetzt mal nur zum Verschlüsseln vorgemerkt. Drücke den Button „Send“.



Diese Meldung erscheint nur das erste Mal, wenn du eine Mail in Thunderbird verschlüsseln willst. Drücke den Button „Yes“,

Zurück zum Inhalt dieses Kapitels

Im jetzt erscheinenden Fenster ermöglichst du das Verschlüsseln für den Account:



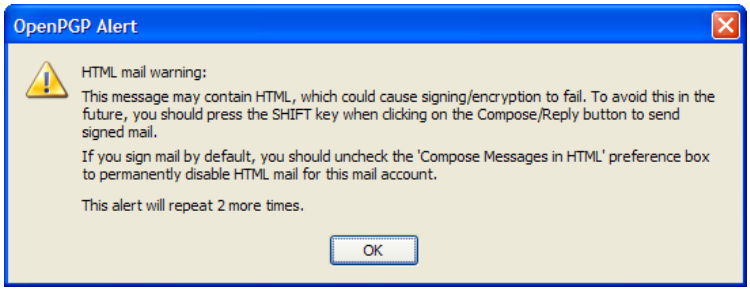
Hake den Punkt „Enable OpenPGP support (Enigmail) for this identity“ und den Punkt „Sign encrypted messages by default“ an.

Zweiteres bedeutet, dass du bei jeder Verschlüsselung dein Passwort angeben musst und damit der EmpfängerIn bestätigst, dass diese Mail wirklich von dir ist.

Drücke dann den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Eine Warnung erscheint:



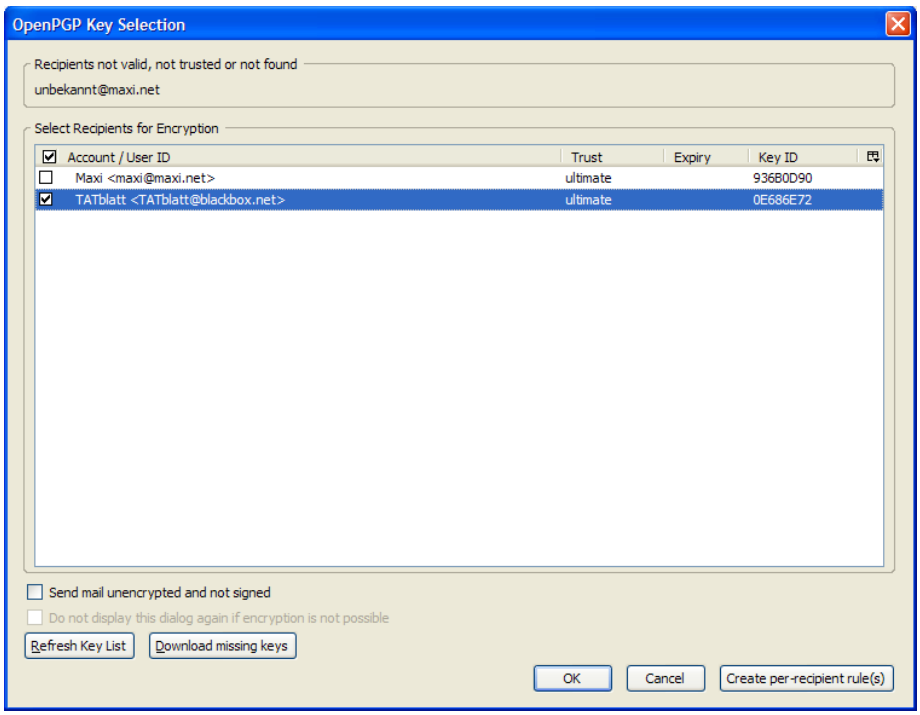
Die Warnung weist dich darauf hin, dass diese Mail unter Umständen eine Mail in HTML-Format (wie bei Webseiten) sein könnte und dass dann die Verschlüsselung schief gehen könnte.

Diese Warnung wird laut Information im Fenster noch zwei Mal erscheinen. Bestätige sie einfach jedes Mal durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

Jetzt gibt es zwei Möglichkeiten: die erste ist, dass der zugehörige Schlüssel zu der angegebenen E-Mail-Adresse gefunden wurde, das nächste Fenster zum Aussuchen des Schlüssels erscheint in diesem Fall nicht, sondern gleich die Aufforderung zur Eingabe deines Passworts.

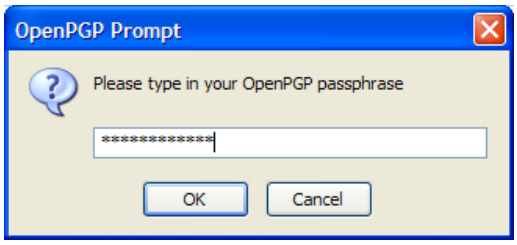
Wurde kein übereinstimmender Schlüssel gefunden, musst du ihn im folgenden Fenster angeben:



Du erhältst alle öffentlichen Schlüssel deines Schlüsselbundes aufgelistet (auch deinen eigenen). Markiere den richtigen Schlüssel und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

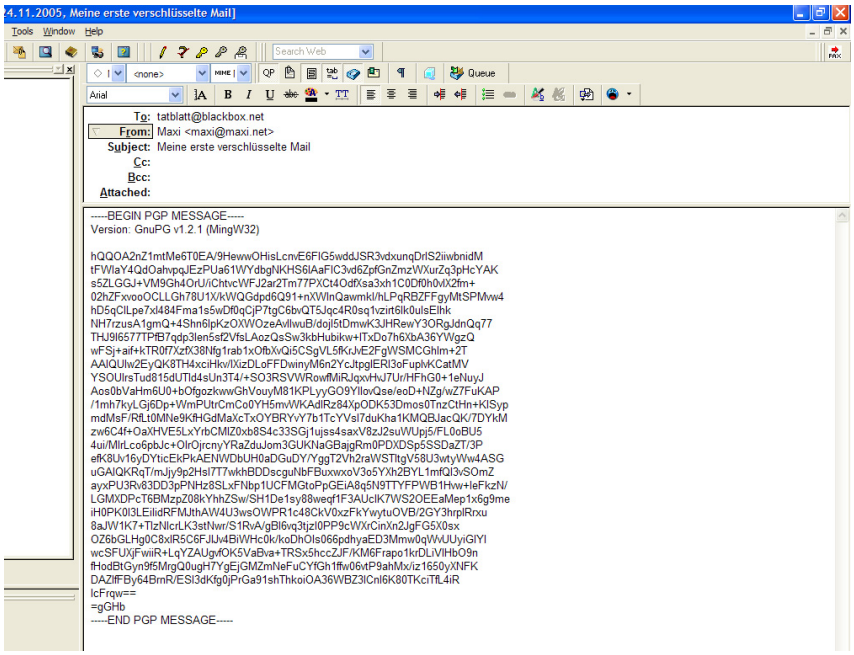
Da du angegeben hast, dass du zu verschlüsselnde Mails automatisch auch signieren willst, erscheint nun die Aufforderung zur Eingabe des Passworts:



Tippe dein Passwort ein und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Und schon ist die Mail für das TATblatt verschlüsselt, falls angewählt, natürlich auch für dich selbst:



Und diesen wilden Haufen von Buchstaben, Ziffern und Sonderzeichen kann jetzt nur das TATblatt entschlüsseln (bzw. alle EmpfängerInnen, für die du den Text verschlüsselt hast).

Tja, das war's schon, abschicken und fertig. So einfach geht das...

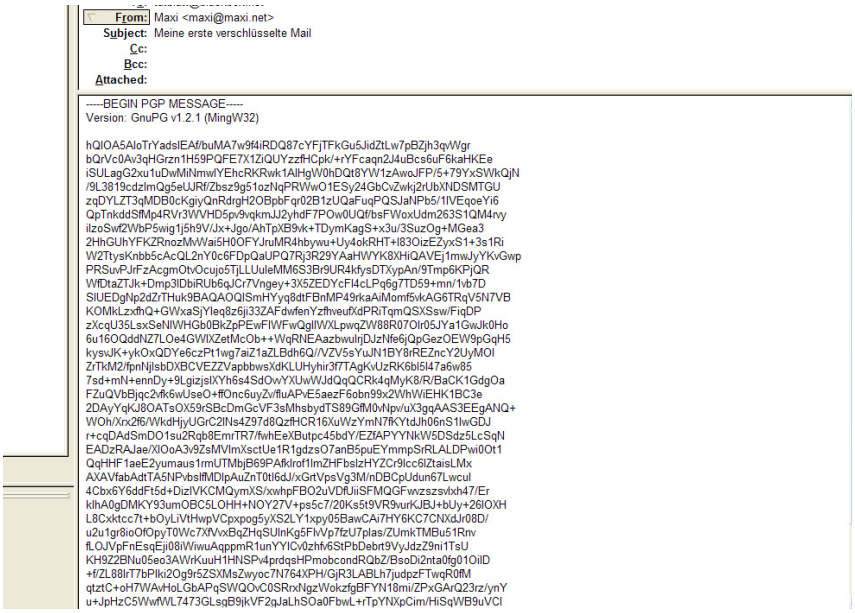
Der verschlüsselte Text schaut im Verhältnis zu den paar wenigen Worten, die hier im Beispiel geschrieben wurden, sehr sehr lange aus.

Aber keine Angst, in diesem Text sind auch Schlüssel-Informationen enthalten. Wenn du einen längeren Text schreibst, wird die verschlüsselte Version nicht um ein Vielfaches länger.

Zurück zum Inhalt dieses Kapitels

Das Entschlüsseln

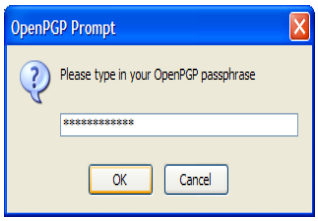
Wenn du eine verschlüsselte Nachricht erhältst, schaut der verschlüsselte Text so wie der, der vorher im Beispiel für das Verschlüsseln erstellt wurde, aus:



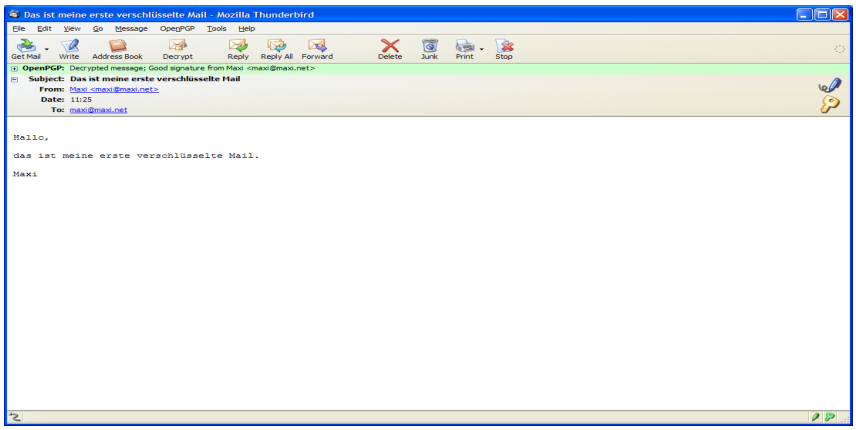
Öffne die Mail durch Doppelklicken im Übersichtsfenster und drücke dann den Button „Decrypt“.

Zurück zum Inhalt dieses Kapitels

Natürlich musst du jetzt auch dein Passwort eingeben, alles andere wäre ja äußerst sinnlos (dann könnte jeder Mensch den Text entschlüsseln):



Und schon ist der entschlüsselte Text sichtbar:



Auch nicht allzu kompliziert, oder?

Zurück zum Inhalt dieses Kapitels

7.3 Andere Mailprogramme und Web-Mail

Wenn du weder Eudora noch Thunderbird als Mailprogramm verwendest und GPG nicht im Mailprogramm integriert ist oder du z.B. über eine Internetseite zu deinen Mails kommst (z.B. bei gmx), musst du ein wenig anders vorgehen.

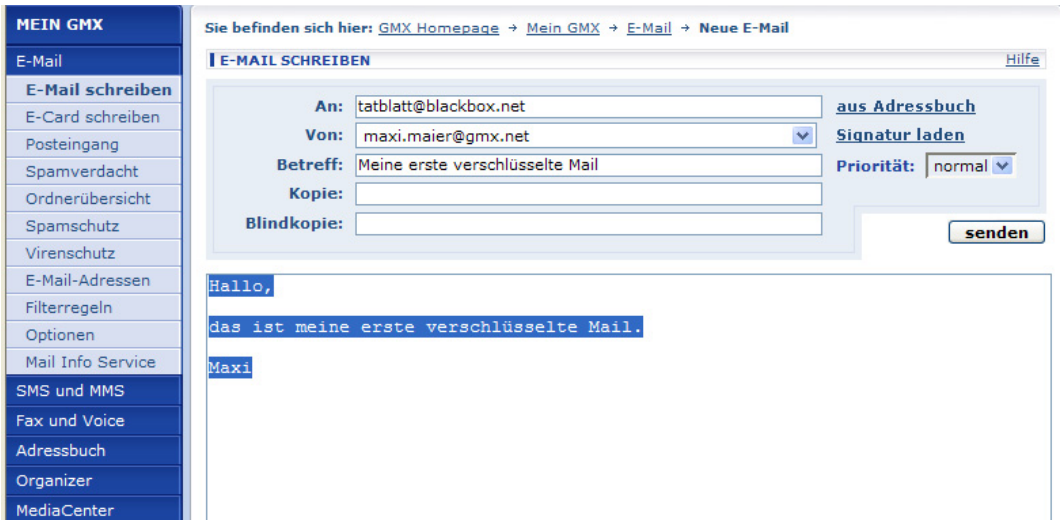
Du kannst aber trotzdem deine Nachrichten ver- und entschlüsseln, wenn GPG (z.B. mit WinPT) auf dem Computer installiert ist. Du musst einfach den Text in die Zwischenablage kopieren, ver- bzw. entschlüsseln und wieder in die Mail zurückkopieren.

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

Zurück zum Inhalt dieses Kapitels

Das Verschlüsseln

Wenn du bei gmx eine Mail schreibst, sieht das ungefähr so aus:



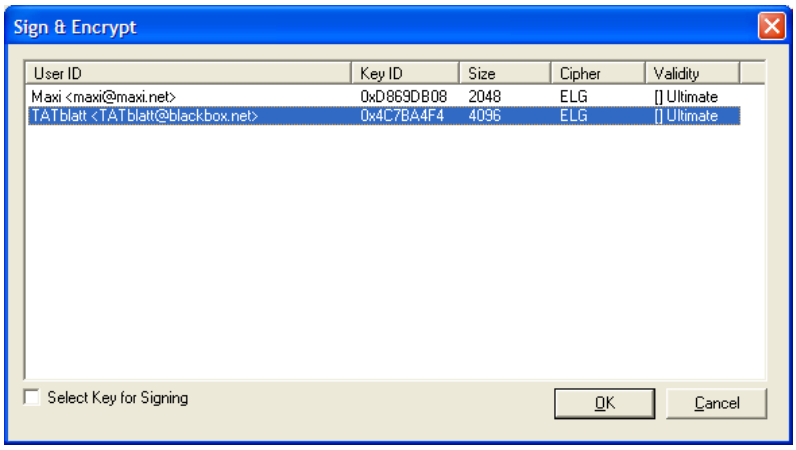
Schreib den Text der Mail und markiere ihn mit der Maus. Wähle dann im Menü des Internet Browsers den Punkt „Bearbeiten ⇨ Kopieren“ oder „Edit ⇨ Copy“.

Der markierte Text befindet sich jetzt in der Zwischenablage (im Clipboard).

Klicke mit der rechten Maustaste auf das Schlüsselsymbol von WinPT am rechten unteren Rand deines Bildschirms. Wähle den Menüpunkt „Clipboard ⇨ Sign & Encrypt“, damit wird dieser Text nachher innerhalb der Zwischenablage verschlüsselt.

Zurück zum Inhalt dieses Kapitels

Es öffnet sich ein Fenster mit allen öffentlichen Schlüsseln deines Schlüsselbunds inkl. deinem eigenen:

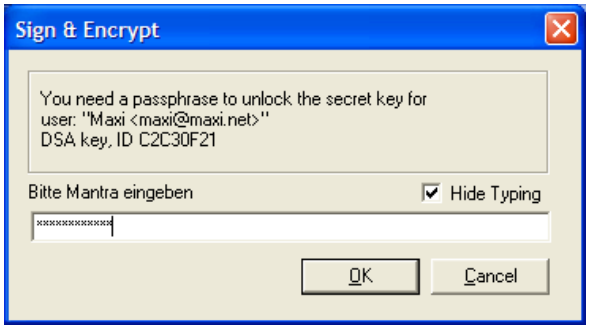


Markiere den oder die richtigen Schlüssel (es können mehrere sein, wenn du die Nachricht gleich für mehrere Personen verschlüsseln willst und/oder auch für dich selbst).

Drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

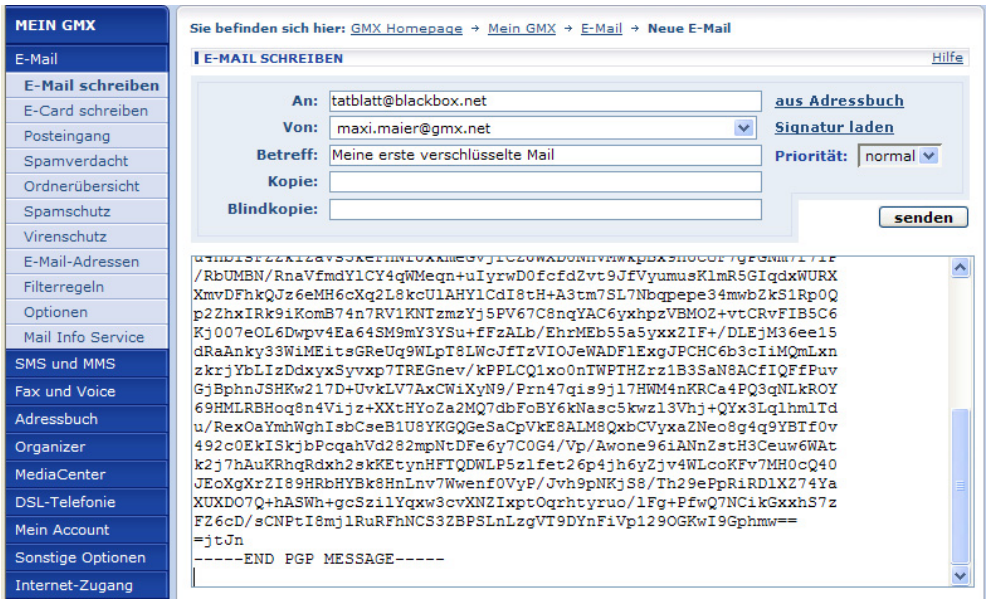
Nun musst du natürlich dein Passwort eingeben:



Gib dein Passwort (hier Mantra genannt) ein und drücke den Button „OK“. Das Fenster wird automatisch geschlossen.

Zurück zum Inhalt dieses Kapitels

Kehre ins Fenster mit der Mail zurück, sie ist noch unverschlüsselt. Falls der Originaltext nicht mehr markiert ist, markiere ihn vollständig und wähle dann im Menü des Internet Browsers den Menüpunkt „Bearbeiten ⇨ Einfügen“ bzw. „Edit ⇨ Paste“.



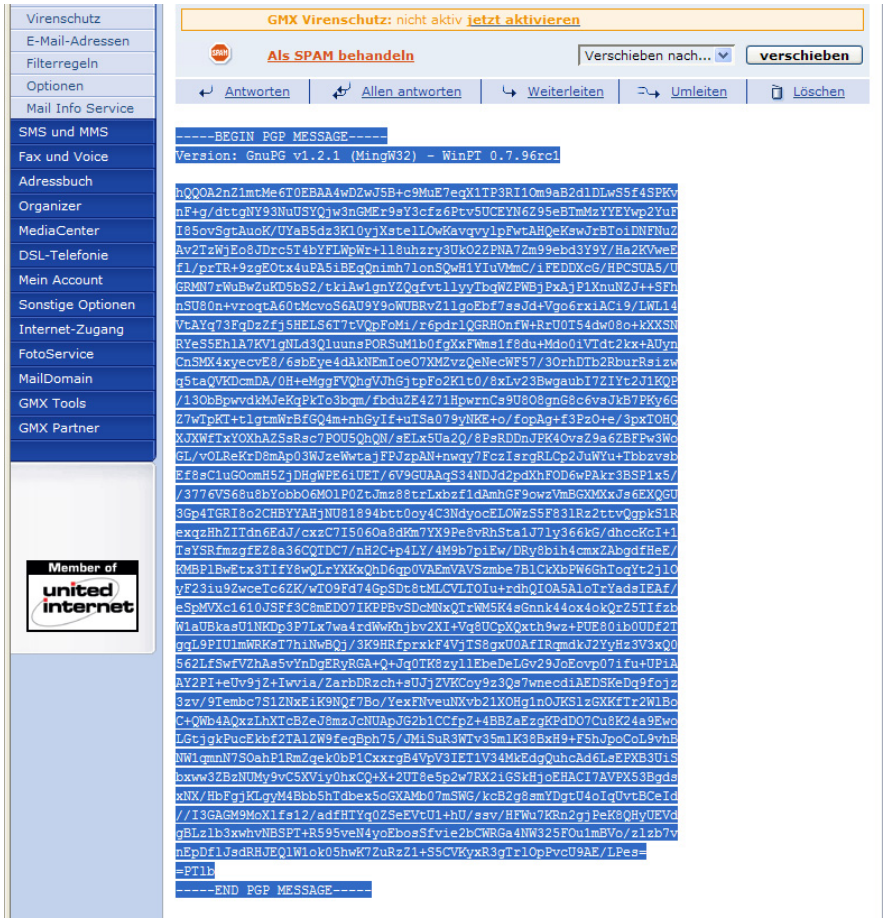
Jetzt wurde der verschlüsselte Text aus der Zwischenablage eingefügt und der Originaltext überschrieben (wenn er markiert war).

Fertig, du kannst die verschlüsselte Mail schon abschicken.

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.

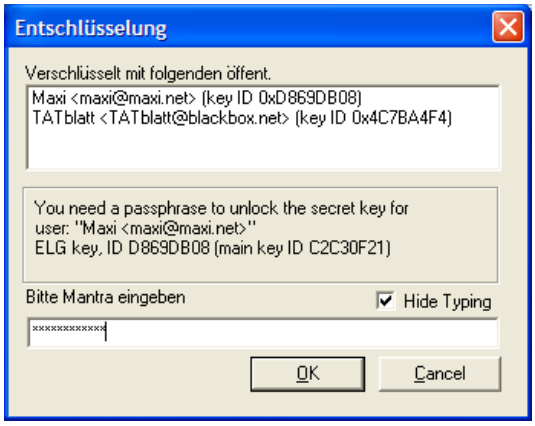


Markiere den verschlüsselten Text (von -----BEGIN PGP MESSAGE----- bis -----END PGP MESSAGE-----, alles inklusive). Wähle dann im Menü „Bearbeiten ⇨ Kopieren" bzw. „Edit ⇨ Copy".

Zurück zum Inhalt dieses Kapitels

Der markierte Text befindet sich jetzt in der Zwischenablage (im Clipboard).

Klicke mit der rechten Maustaste auf das Schlüsselsymbol von WinPT am rechten unteren Rand deines Bildschirms. Wähle den Menüpunkt „Clipboard ⇨ Decrypt / Verify“, damit wird dieser Text nachher innerhalb der Zwischenablage entschlüsselt.



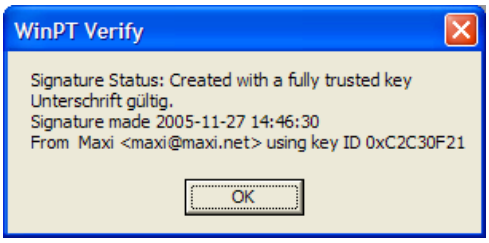
Du siehst, mit welchen Schlüsseln die Nachricht verschlüsselt wurde (fürs TATblatt und für Maxi).

Jetzt musst du natürlich dein Passwort (hier Mantra genannt) eingeben. Drücke dann den Button „OK“.

Der Text befindet sich jetzt unverschlüsselt in der Zwischenablage (im Clipboard). Du kannst jetzt den Text in irgendeinem Programm ansehen, z.B. in einem Textprogramm wie Notepad, Word oder OpenOffice Writer.

Zurück zum Inhalt dieses Kapitels

Nun erscheint noch eine Bestätigung, dass der Schlüssel gültig ist:



Bestätige die Meldung durch Drücken des Buttons „OK“.

Starte dann z.B. einen einfachen Texteditor (Notepad), das Programm OpenOffice Writer oder Microsoft Word und wähle im Menü „Bearbeiten ⇨ Einfügen“ bzw. „Edit ⇨ Paste“.

Und schon siehst du den unverschlüsselten Text vor dir, er wurde aus der Zwischenablage eingefügt.

Zurück zum Inhalt dieses Kapitels

8 TrueCrypt

Überblick

In diesem Kapitel erfährst du Näheres zum Programm TrueCrypt. 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 des Passworts kann mensch die Daten wieder lesen.

Du findest Beschreibungen zu folgenden Bereichen:

- Die prinzipielle Funktionsweise von TrueCrypt
- Die Installation von TrueCrypt
- Das Anlegen eines verschlüsselten Bereichs auf deiner Festplatte
- Das Mounten und Unmounten von angelegten verschlüsselten Bereichen (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 Thunderbird-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 z.B. einfach nichts, auf dem Computer die Daten fein verschlüsselt zu haben, neben dem Computer aber die Sicherungs-CDs mit unverschlüsselten Daten liegen zu haben.

8.1 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 erste Festplatte in Windows den Laufwerksbuchstaben C besitzt.

In dieser Datei werden von dir mehr oder weniger unbemerkt deine eigentlichen Dateien (z.B. Word Dokumente, 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 mitTrueCrypt aussuchen kannst (also z.B. Z).

Jeder Mensch mit Zugang zu deinem Computer kann diese angelegte 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 irgendetwas eingebaut). Trotzdem ist für dich die Handhabung genauso einfach wie mit einer zusätzlichen Festplatte oder einem Diskettenlaufwerk.

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

Dieses Laufwerk wird auf deinen Wunsch und nach Eingabe des Passworts 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 „Laufwerk“ ab, genauso wie du es bisher auf C getan hast. Du kannst natürlich auch auf deinem verschlüsselten Laufwerk Ordner erstellen, Dateien umbenennen, löschen 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, die das Passwort nicht kennt, entschlüsselt werden können.

Zurück zum Inhalt dieses Kapitels

8.2 Die Installation von TrueCrypt

Auf der CD im Verzeichnis TrueCrypt findest du das Installationsprogramm von TrueCrypt.

Für Windows öffne den Windows Explorer, wechsle auf der CD ins Verzeichnis WinPT//Windows und doppelklicke auf die Datei winpt-install-1.0rc2.exe. Das Installationsprogramm wird gestartet.

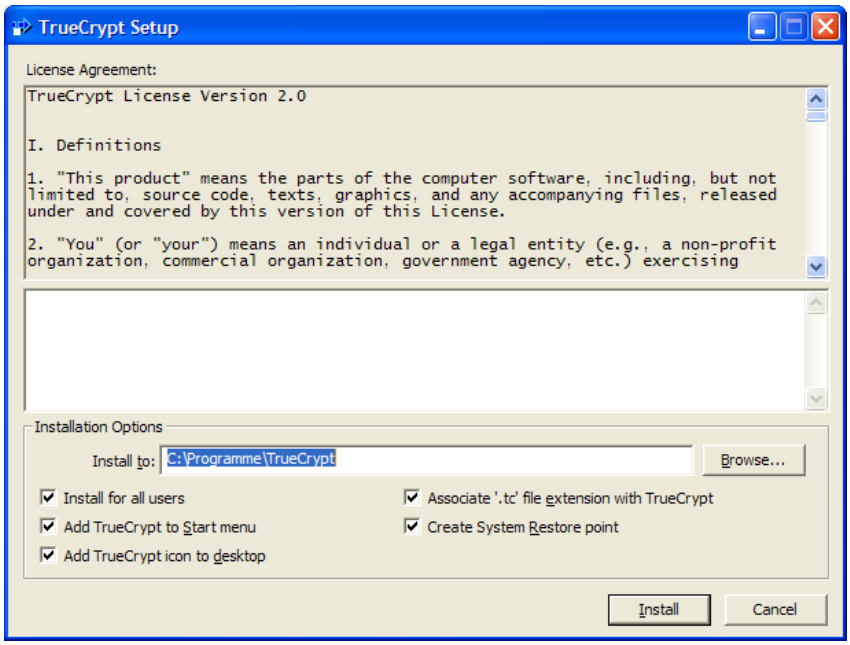
TrueCrypt\Windows

TrueCrypt Setup.exe

Das aktuelle Programm findest du immer im Internet unter http://www.truecrypt.org/downloads.php.

Zurück zum Inhalt dieses Kapitels

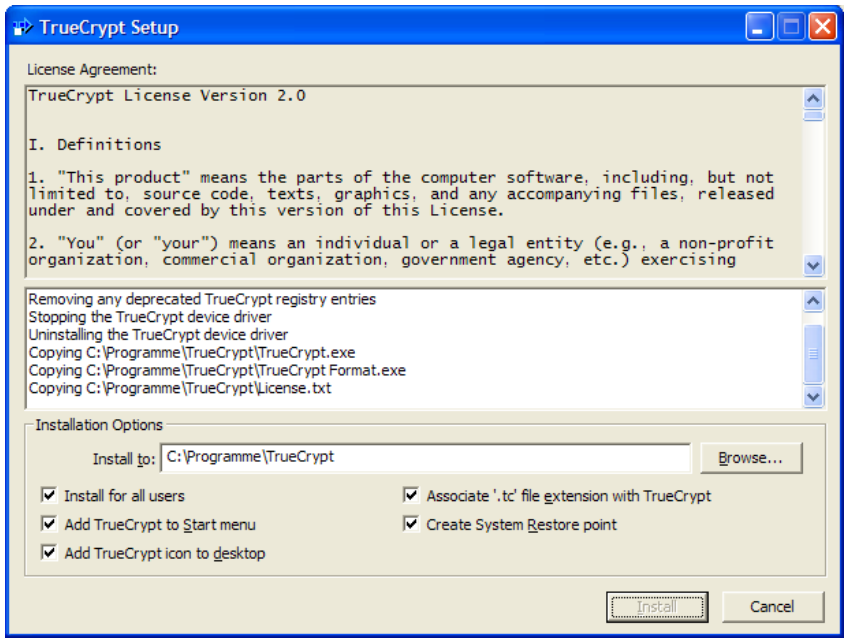
Gleich zu Beginn erscheint ein Fenster mit den Lizenzbedingungen:



Gib einen Ordner an, in dem das Programm installiert werden woll und akzeptiere die Lizenzbedingungen durch Drücken des Buttons „Install“.

Zurück zum Inhalt dieses Kapitels

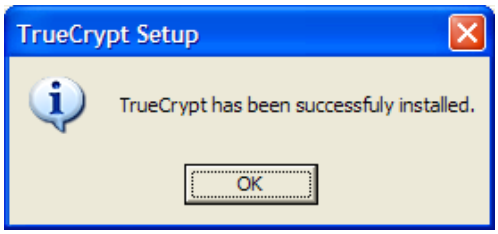
Die Installation beginnt sofort:



Es wird angezeigt, was das Installationsprogramm gerade tut.

Zurück zum Inhalt dieses Kapitels

Nach dem Ende des Installationsvorgangs erscheint eine Erfolgsmeldung:



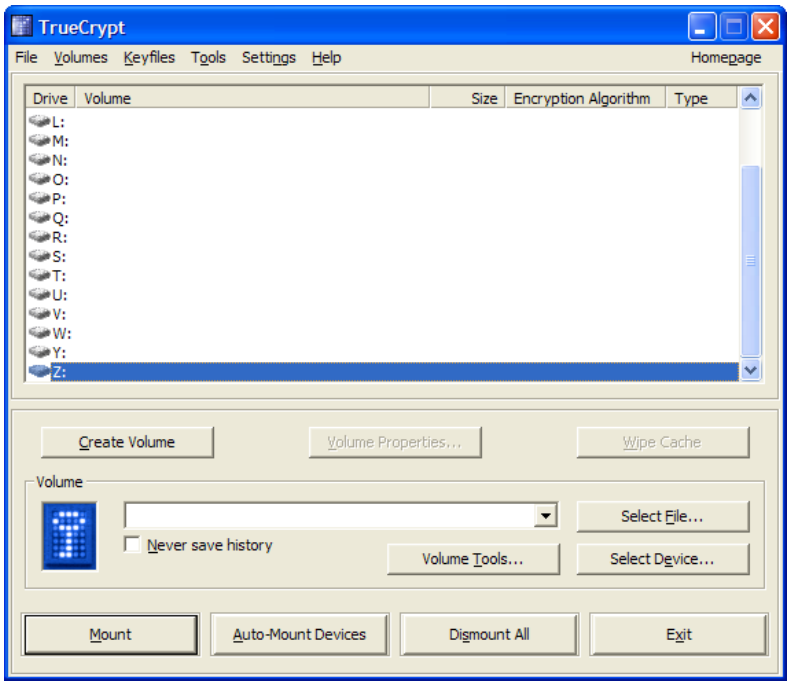
Bestätige die Meldung durch Drücken des Buttons „OK“ und schließe das Installationsfenster durch Drücken des Buttons „Exit“.

Das war's auch schon, das Programm wurde installiert. In den nächsten Kapiteln erfährst du, wie du verschlüsselte Bereiche auf deiner Festplatte anlegen und verwenden kannst.

Zurück zum Inhalt dieses Kapitels

8.3 Das Erstellen von verschlüsselten Bereichen der Festplatte

Starte das Programm TrueCrypt, du findest es im Start-Menü unter „Programme ⇨ TrueCrypt ⇨ TrueCrypt“.:



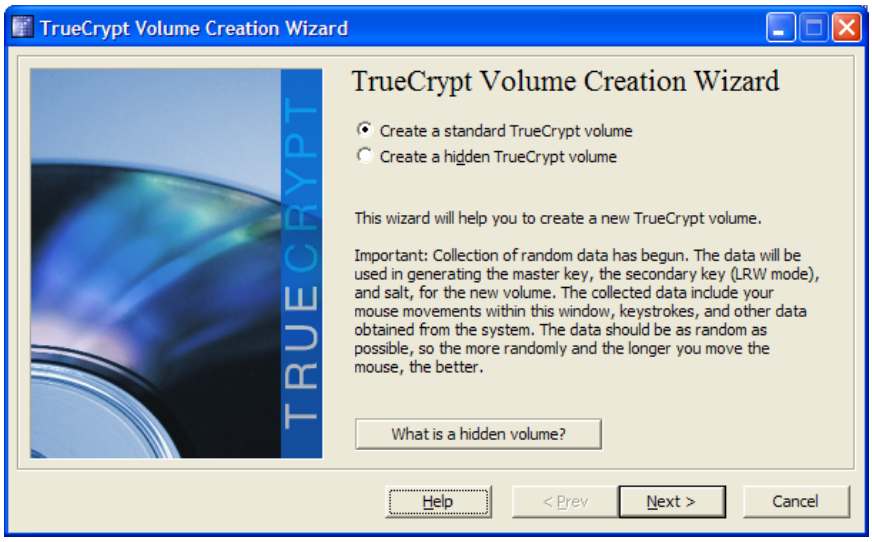
Du siehst das Hauptfenster von TrueCrypt vor dir. Durch Drücken des Buttons „Create Volume“ kannst du so einen verschlüsselten Teil auf deiner Festplatte anlegen.

Markiere die Zeile mit dem von dir gewünschten Laufwerksbuchstaben und drücke den Button „Create Volume“.

Ein Tipp: wenn du den Button “Help” drückst, erscheint das BenutzerInnen-Handbuch von TrueCrypt. Da findest du detaillierte Informationen zu dem Programm.

Zurück zum Inhalt dieses Kapitels

Folgendes Fenster erscheint:



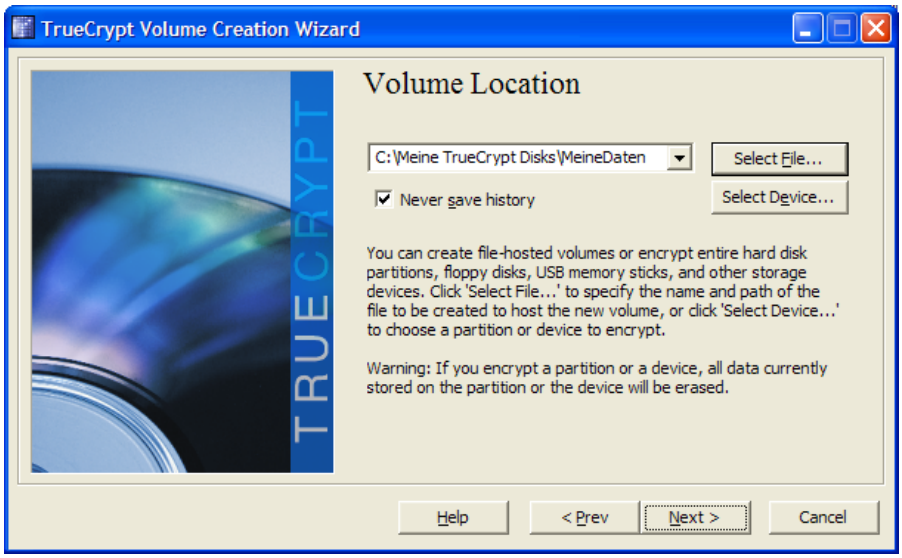
Du kannst dir aussuchen, welchen Typ von verschlüsselter Datei du anlegen möchtest.

Um zu erfahren, was eine „versteckte Partition“ (ein Hidden Volume) ist, lies dir bitte dieTrueCrypt-Dokumentation durch oder drücke einfach den Button „What is a hidden volume“, im Beispiel hier wird eine normale Standard-Datei gewählt.

Bestätige die Auswahl durch Drücken des Buttons „Next“.

Zurück zum Inhalt dieses Kapitels

Nun kannst du dir aussuchen, in welchem Ordner und unter welchem Namen die Datei für die verschlüsselten Daten angelegt werden soll:



Gib Ordner und Dateinamen an, durch Drücken des Buttons „Select File“ ist es etwas einfacher, die beiden Informationen anzugeben.

Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

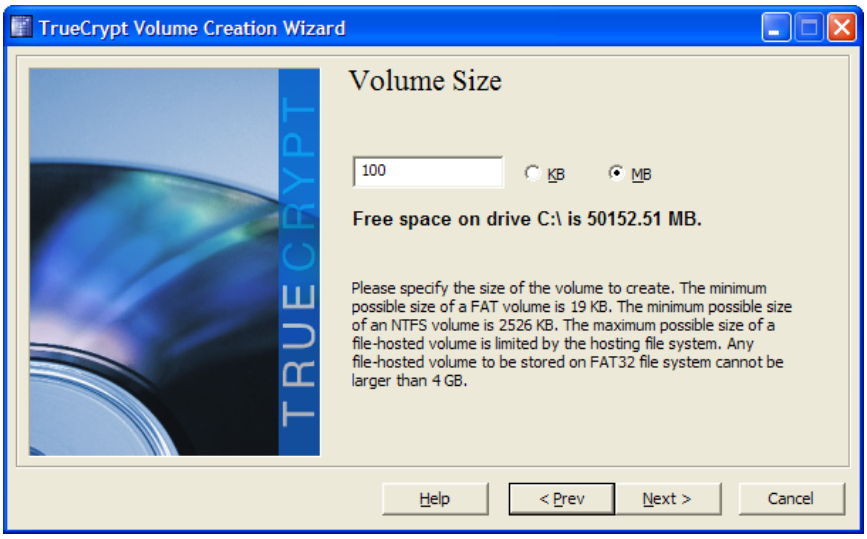
Nun folgen Auswahlmöglichkeiten zur Art der Verschlüsselung:

Das BenutzerInnen-Handbuch von TrueCrypt beinhaltet Informationen zu den verschiedenen Verschlüsselungs- und Hash-Algorithmen.

Du kannst aber auch einfach die Vorschläge übernehmen und den Button „Next“ drücken.

Zurück zum Inhalt dieses Kapitels

Nun musst du angeben, wie groß dieser verschlüsselte Teil sein soll:



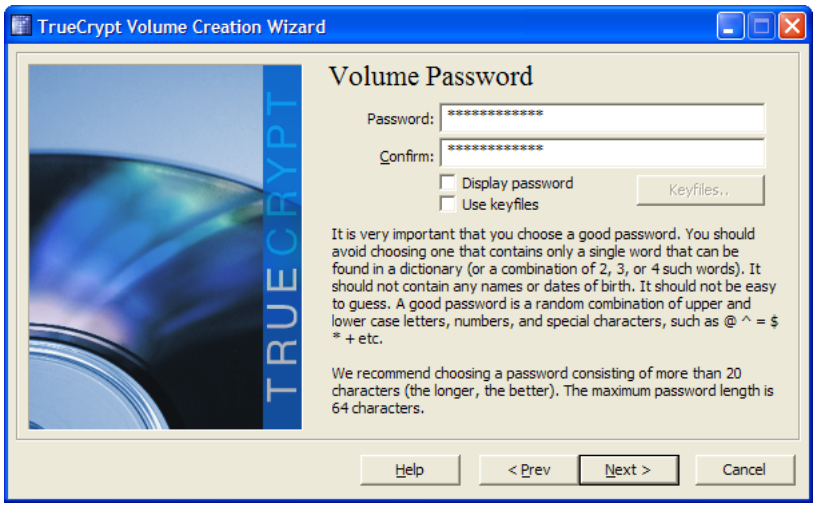
Du kannst eine beliebige Größe angeben, die Datei muss halt Platz auf deiner Festplatte haben. Du kannst auch nachher bei Bedarf weitere solche verschlüsselten „Disks“ (Volumes) anlegen.

Hier im Beispiel werden 100 MegaBytes angegeben, du musst halt halbwegs abschätzen, wie viel Platz du jetzt und in Zukunft brauchen wirst.

Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Nun musst du ein Passwort angeben:



Beachte, dass das ein eigenes Passwort ist. Wenn du Textverschlüsselung mit GPG (WinPT) verwendest, hat dein Schlüsselbund auch ein eigenes Passwort. Also nicht verwechseln.

Du musst natürlich ein sehr gutes Passwort wählen, es bietet den einzigen Schutz vor unbefugtem Zugriff auf deine verschlüsselten Daten.

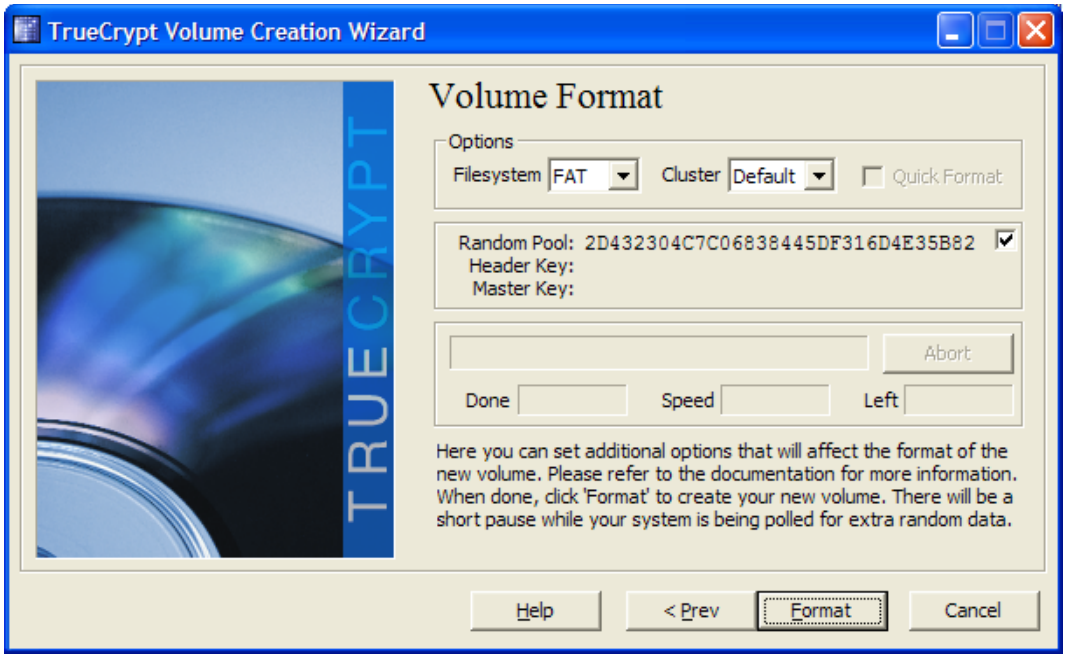
Merke dir dieses Passwort gut. Ohne das Passwort kannst du die Daten auf der verschlüsselten “Disk” nie wieder lesen.

Ein paar Tipps zur Wahl von guten Passwörtern findest du im Kapitel Tipps für Passwörter/Passphrases.

Gib das Passwort zwei Mal ein und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Jetzt werden noch irgendwelche Zufallinformationen für die Verschlüsselung gesammelt:



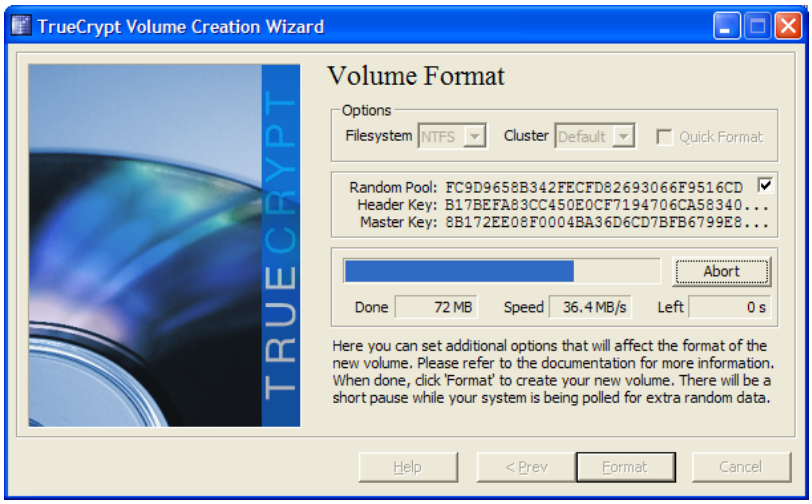
Du kannst auch noch angeben, mit welchem Dateisystem der verschlüsselte Bereich formatiert werden soll. Bei Windows-XP ist das Filesystem NTFS üblich, bei älteren Windows Versionen FAT.

Wähle das entsprechende Dateisystem und drücke den Button „Format“.

Und keine Angst, es wird nicht deine ganze Festplatte formatiert, sondern nur die eine Datei, die du angegeben hast, in der angegebenen Größe für die Verschlüsselung vorbereitet.

Zurück zum Inhalt dieses Kapitels

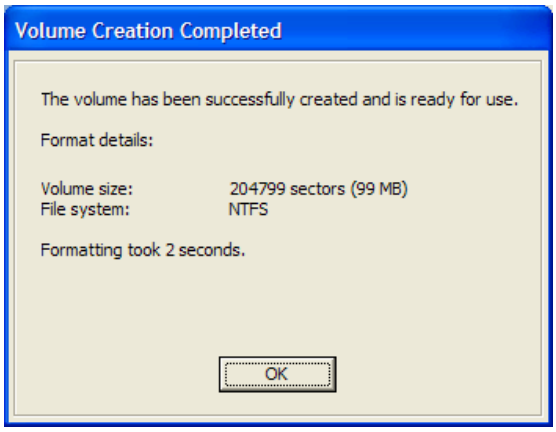
Du bekommst den Fortschritt der Formatierung angezeigt:



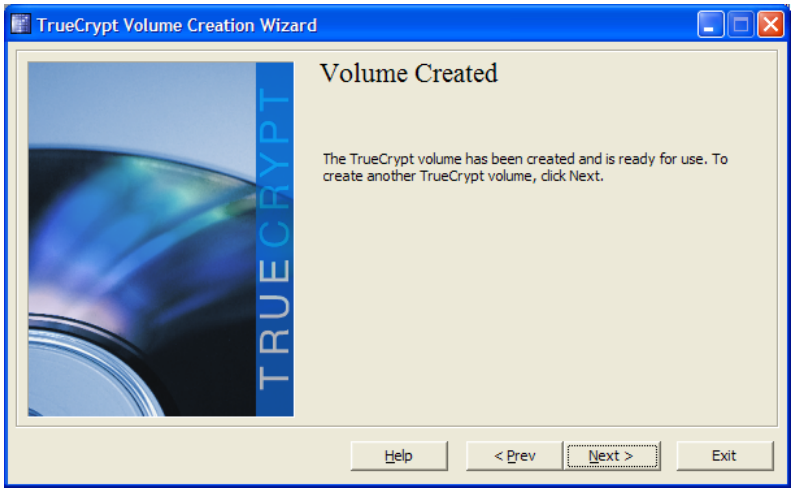
Je größer der verschlüsselte Teil sein soll, desto länger dauert auch die Erstellung.

Zurück zum Inhalt dieses Kapitels

Nach der Fertigstellung erhältst du zwei Erfolgsmeldungen:



Die Erstellung war erfolgreich und deine verschlüsselte „Disk“ ist bereit für eine Verwendung. Bestätige diese Information durch Drücken des Buttons „OK“.



Du kannst durch Drücken des Buttons „Next“ eine weitere verschlüsselte „Disk“ anlegen. Bist du fürs erste fertig, drücke den Button „Exit“.

Zurück zum Inhalt dieses Kapitels

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

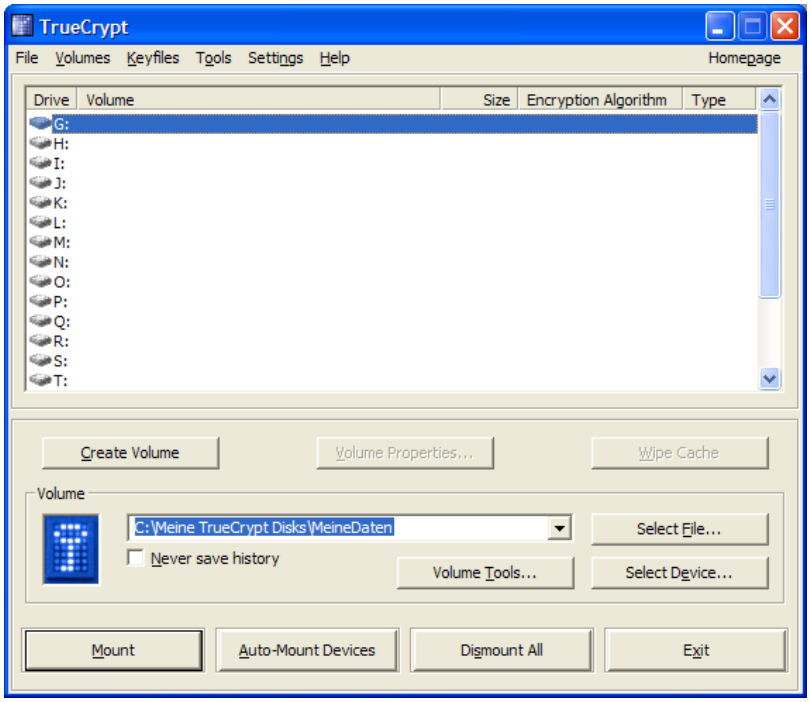
Wie schon erwähnt, musst du deine verschlüsselte(n) Partition(en) (deine verschlüsselten „Disks“) nach jedem Start des Betriebssystems (also z.B. von Windows) an dein Dateisystem anhängen, um den Inhalt öffnen und lesen zu können. Dieser Vorgang des Anhängens wird „mount“ genannt.

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

Zurück zum Inhalt dieses Kapitels

Das Mounten von verschlüsselten Disks

Wenn du das Programm TrueCrypt startest, siehst du wieder das Hauptfenster vor dir:

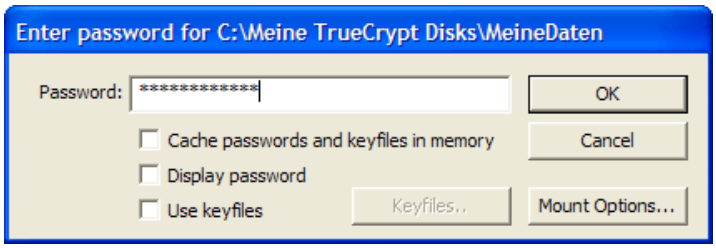


Wähle den gewünschten Laufwerksbuchstaben durch Markieren der entsprechenden Zeile und gib die Datei an, in der sich deine verschlüsselten Daten befinden. Durch Drücken des Buttons „Select File“ ersparst du dir das manuelle Eintippen des Pfades und des Dateinamens.

Drücke dann den Button „Mount“.

Zurück zum Inhalt dieses Kapitels

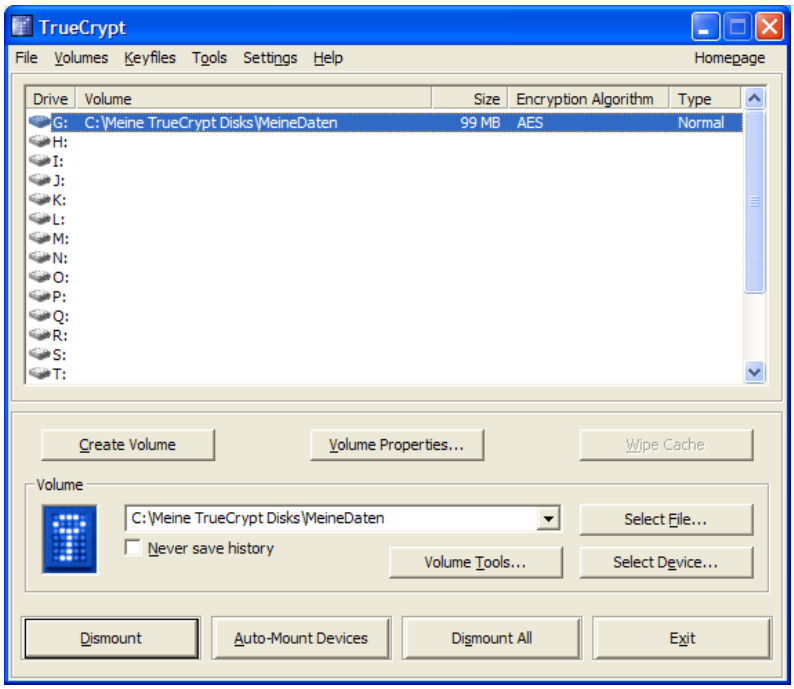
Natürlich musst du jetzt das Passwort angeben:



Tippe dein Passwort ein und drücke dann den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Du kehrst jetzt ins Hauptfenster zurück:

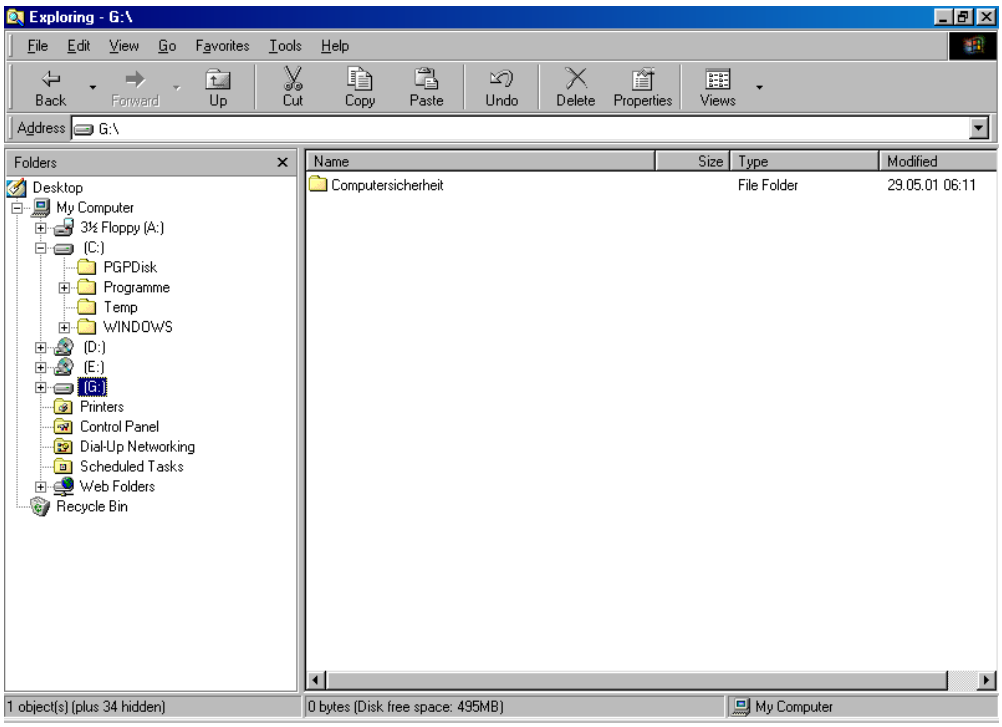


Neben dem vorher gewünschten Laufwerksbuchstaben siehst du jetzt Informationen zu deiner verschlüsselten „Disk“.

Fertig, du kannst jetzt diesen verschlüsselten Teil deiner Festplatte benützen. Drücke zum Schließen des Programms den Button „Exit“ (die verschlüsselte „Disk“ bleibt gemountet, auch wenn du aus dem Programm aussteigst).

Zurück zum Inhalt dieses Kapitels

Wenn du die „Disk“ gemountet hast, erscheint im Windows Explorer das gewünschte Laufwerk. Du kannst nun auf alle Dateien ganz normal zugreifen.



Wenn du schon vor dem Mounten einer verschlüsselten Disk ein Fenster des Windows Explorer geöffnet hast, wird der Laufwerksbuchstabe danach nicht gleich korrekt angezeigt.

Falls dir das auffällt, schließe den Windows Explorer einfach und öffne ihn neu, dann wird alles richtig angezeigt.

Zurück zum Inhalt dieses Kapitels

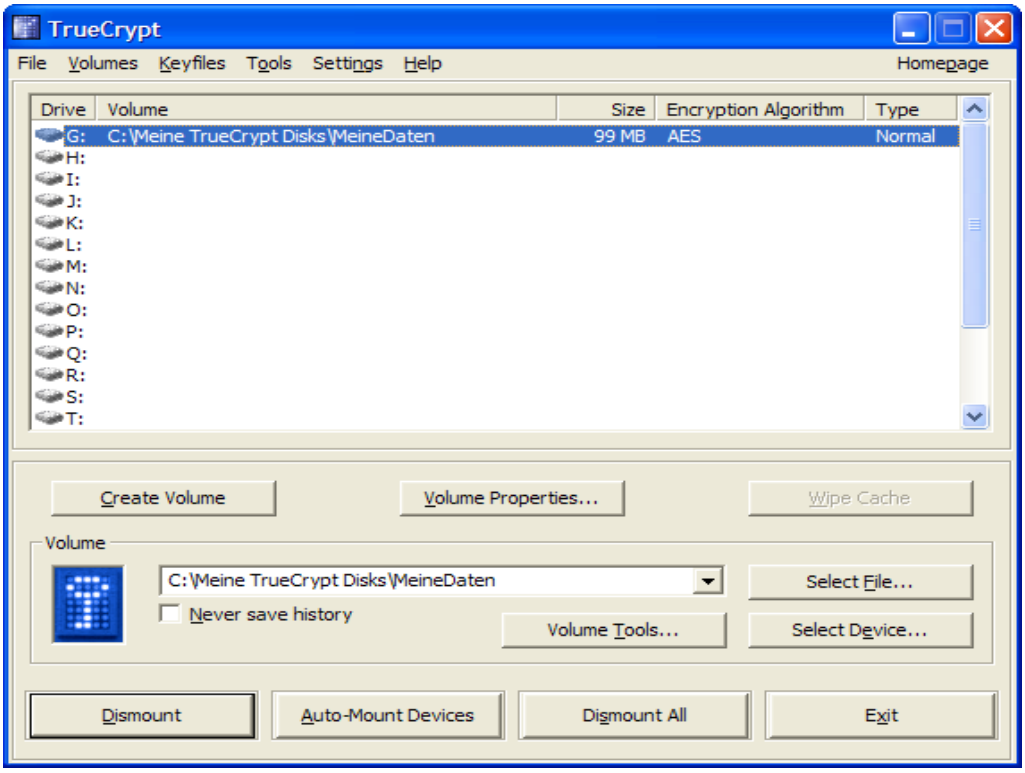
Das Unmounten von verschlüsselten Disks

So wie du verschlüsselte „Disks“ an dein Dateisystem anhängen (mounten) kannst, kannst du sie natürlich auch wieder abhängen (unmounten oder dismounten). 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.

Solange diese verschlüsselten „Disks“ gemountet sind, sind die Inhalte auch für jede Person einsichtbar, die Zugang zu deinem Computer hat.

Zurück zum Inhalt dieses Kapitels

Zum Unmounten (Dismounten) starte das Programm TrueCrypt.



Markiere die Zeile mit dem Laufwerksbuchstaben, den du unmounten möchtest und drücke den Button „Dismount“ oder den Button „Dismount All“ zum unmounten aller geöffneten verschlüsselten „Disks“.

Die Informationen zu deinen verschlüsselten „Disks“ verschwinden wieder, die Daten können nicht mehr gelesen werden, der Laufwerksbuchstabe ist auch aus dem Windows Explorer verschwunden.

Zurück zum Inhalt dieses Kapitels

8.5 Das Sichern von verschlüsselten Daten

Wie schon erwähnt, ist deine verschlüsselte „Disk“ eine einfache Datei auf deinem Computer. Das Schöne daran ist, dass du diese Datei als Sicherung einfach irgendwo hinkopieren kannst, die Daten darauf bleiben verschlüsselt und lassen sich nur nach dem Mounten mit Eingabe des Passworts entschlüsseln.

Du darfst auf keinen Fall einfach einzelne Dateien von deinem verschlüsselten Laufwerk auf ein nicht verschlüsseltes kopieren. Die Dateien bleiben nur verschlüsselt, solange sie sich auf einer deiner verschlüsselten „Disks“ befinden.

Daher muss zum Sichern auch eine ganze solche „Disk“ z.B. auf CD gebrannt werden, also die Datei, in der sich die verschlüsselten Daten befinden.

Zurück zum Inhalt dieses Kapitels

Das Sichern auf CD mit einem CD Brenner

Folgende Angaben sind nur Tipps, du kannst dir natürlich auch andere Vorgangsweisen einfallen lassen. Ein Problem beim Sichern ist oft, dass die Dateien mit deinen verschlüsselten Daten (deine verschlüsselte „Disk“) größer ist, als auf einer CD Platz hat.

Falls deine verschlüsselte „Disk“ größer als 600-700 MB ist, lege dir neben deiner „Hauptdisk“, auf die du deine Dateien speicherst, noch eine zweite verschlüsselte 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 von der „Original-Disk“ auf diese zweite „Sicherungs-Disk“ kopieren und die ganze „Sicherungs-Disk-Datei“ auf eine CD brennen. Die Daten sind dann verschlüsselt auf der CD, du kannst sie zum Ansehen wieder zurück auf deine Festplatte kopieren und wie jede deiner verschlüsselten Disks mounten. Das musst du halt so oft machen, bis alle Daten gesichert sind.

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 TrueCrypt-Disk notwendig.

Zurück zum Inhalt dieses Kapitels

8.5 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.

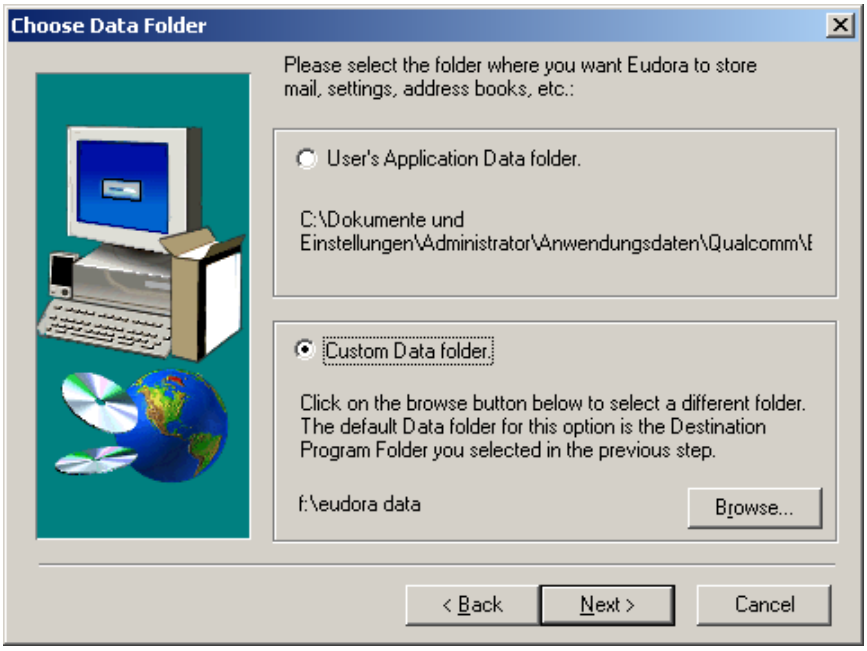
Abhilfe schafft da die Verwendung von TrueCrypt und das Speichern der Maildaten auf einem verschlüsselten Laufwerk. Alle deine persönlichen Daten und Einstellungen werden dann auf einem verschlüsselten Bereich gespeichert und können nur nach Mounten dieses Bereichs gelesen werden. Eudora lässt sich ohne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

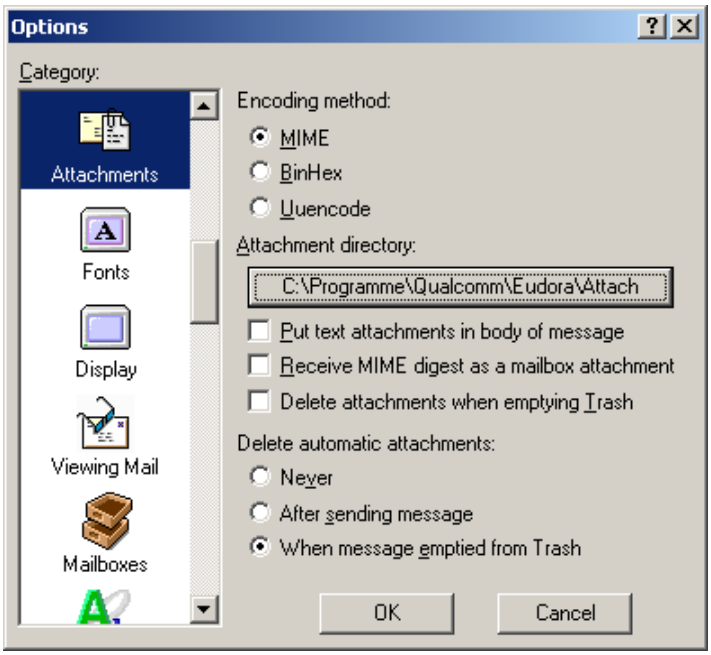
Um deine Mails nach dem Start von Eudora lesen zu können, musst du natürlich immer den gleichen hier angegebenen Laufwerksbuchstaben wählen, im Beispiel oben also F.

Zurück zum Inhalt dieses Kapitels

Attachments

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

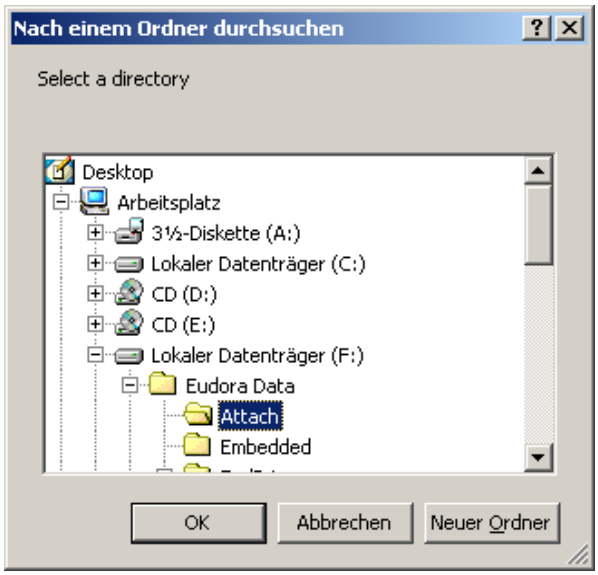
Starte Eudora und wähle im Menü den Punkt „Tools ⇨ Options“. Wähle dann im Fenster die Kategorie „Attachments“.



Drücke den Button bei „Attachment directory“.

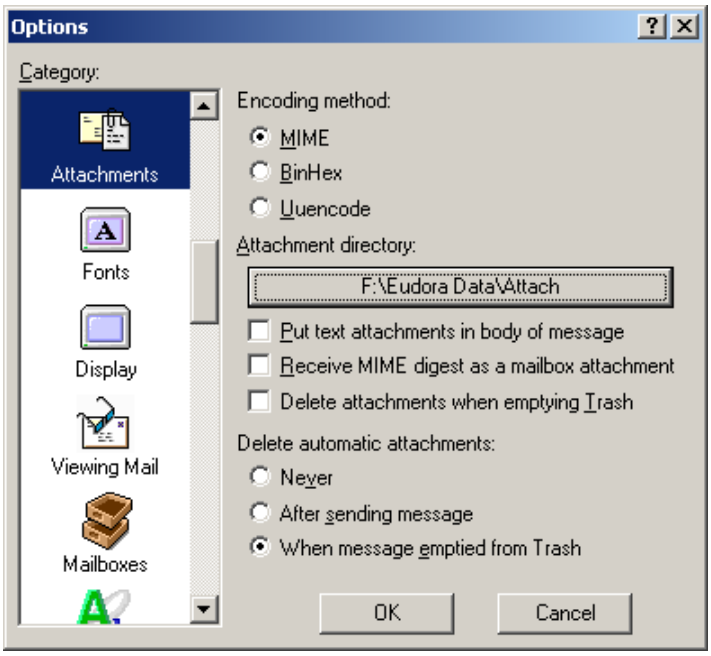
Zurück zum Inhalt dieses Kapitels

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

8.6 Das Speichern von Thunderbird-Daten auf einem verschlüsselten Laufwerk

Wie schon beim Mailprogramm Eudora besprochen: 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 TrueCrypt 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.

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

Zurück zum Inhalt dieses Kapitels

Thunderbird Daten

Originalordner mit den Daten

Bei der Installation von Thunderbird kannst du dir leider nicht wie bei Eudora aussuchen, in welchem Ordner deine Mails gespeichert werden, es wird einfach ein Standard-Ordner verwendet.

Du musst diesen Ordner nachher manuell auf ein anderes Laufwerk (z.B. das verschlüsselte Laufwerk) verschieben und Thunderbird mitteilen, wo sich jetzt die Mails befinden.

Nach der Installation von Thunderbird befinden sich die Mails in Windows in einem Ordner ähnlich wie

⇨ C:\Dokumente und Einstellungen\<Dein Windows-Login-Name>\Anwendungsdaten\Thunderbird\Profiles\sn97lbmo.default\Mail

Ein bisschen DetektivInnenarbeit ist leider notwendig, den richtigen Ordner zu finden. Du findest den Ordner aber auch nach dem Starten des Programms Thunderbird bei den Einstellungen des Accounts (siehe nächstes Kapitel).

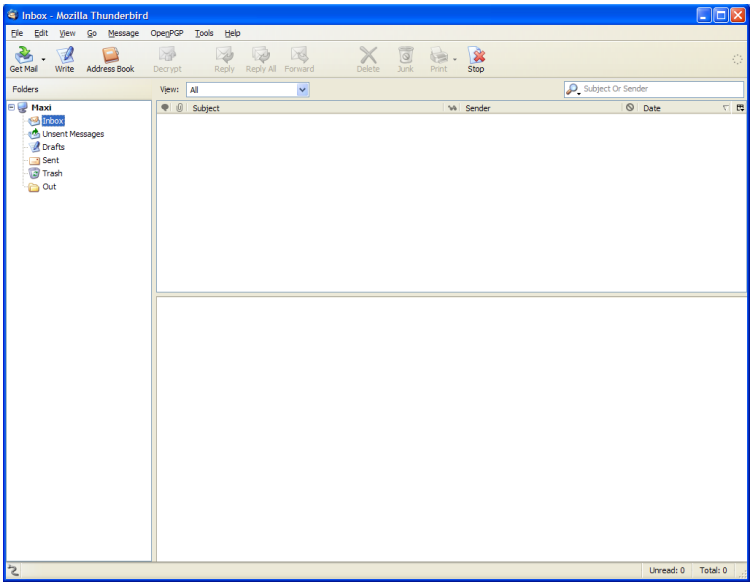
Zurück zum Inhalt dieses Kapitels

Verschieben des Ordners

Hast du den Mail-Ordner gefunden, verschiebe ihn einfach durch Wahl von „Bearbeiten ⇨ Ausschneiden“ bzw. „Einfügen“ auf ein verschlüsseltes Laufwerk.

Einstellungen in Thunderbird

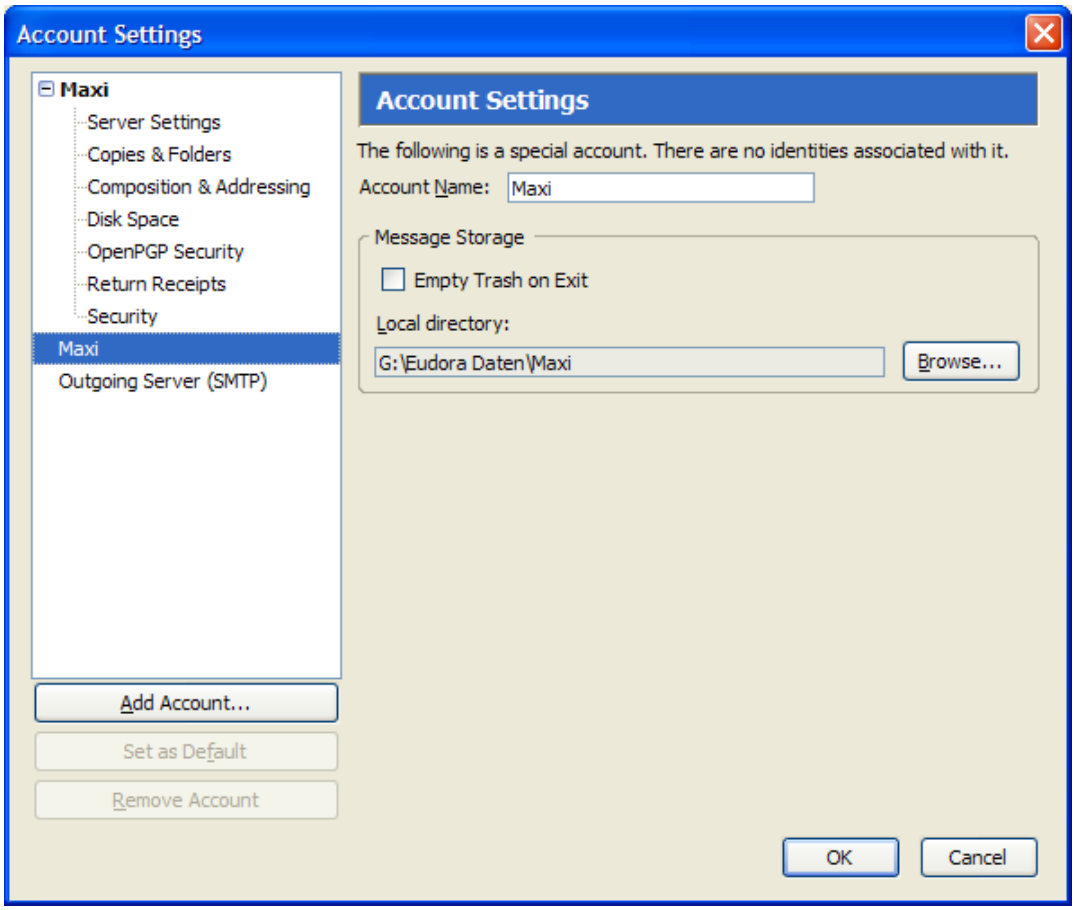
Starte das Mailprogramm Thunderbird



Klicke mit der rechten Maustaste auf deinen „Account“ (hier heißt dieser Account „Maxi“) und wähle den Menüpunkt „Properties“.

Zurück zum Inhalt dieses Kapitels

Das Fenster für die Einstellungen wird geöffnet.

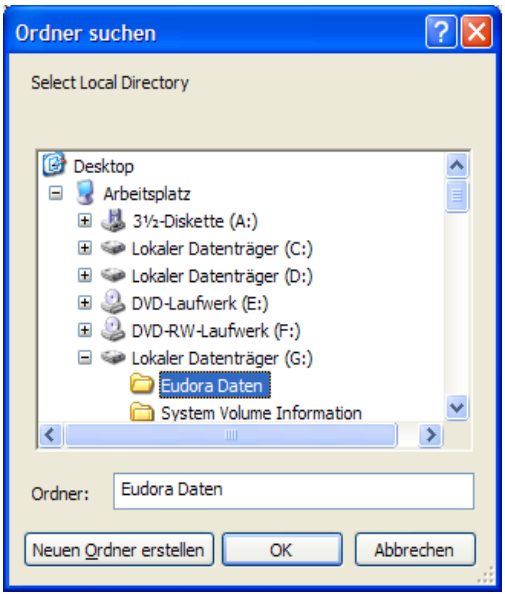


Wähle auf der linken Seite den Account, für den du die Einstellungen ändern willst (das Ganze musst du für jeden angelegten Account durchführen).

Rechts siehst du eine Ordnerangabe bei „Local directory“, zuerst ist der aktuelle Ordner angegeben, in dem die Maildaten gespeichert werden. Drücke auf den Button „Browse…“ zur Auswahl eines anderen Verzeichnisses auf deiner verschlüsselten Partition.

Zurück zum Inhalt dieses Kapitels

Ein Fenster zur Auswahl des Ordners wird geöffnet:



Suche den Ordner, in den du die Mails verschoben hast oder verschieben wirst. Drücke dann den Button „OK“. Bei der Verzeichnisangabe wird jetzt der neue Ordner angezeigt.

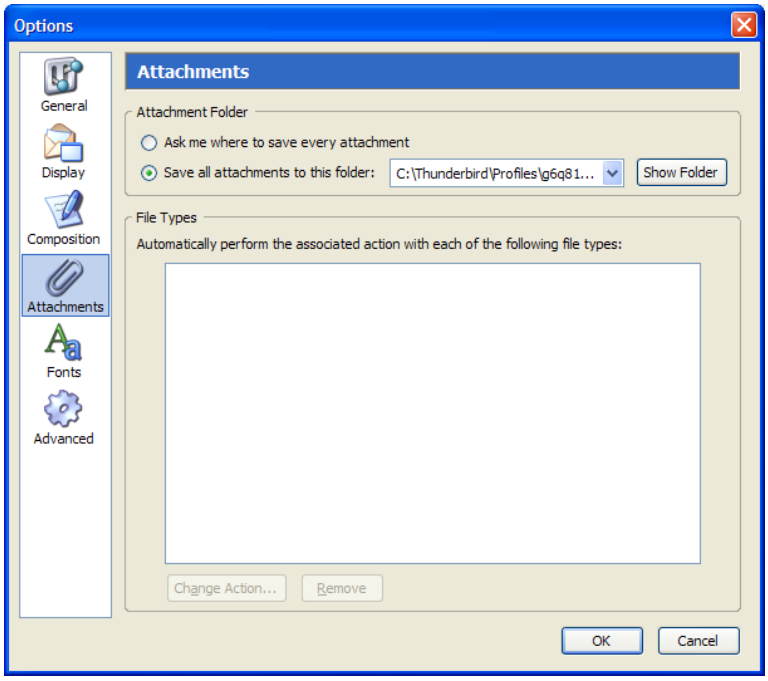
Wiederhole diesen Vorgang für jeden angelegten Account, falls du mehrere angelegt hast. Wenn du fertig bist, bestätige deine Angaben durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

Attachments

Nun musst du noch angeben, wo die Anhänge vom Mails (die Attachments) gespeichert werden sollen. Wähle dazu in Thunderbird den Menüpunkt „Tools ⇨ Options“.

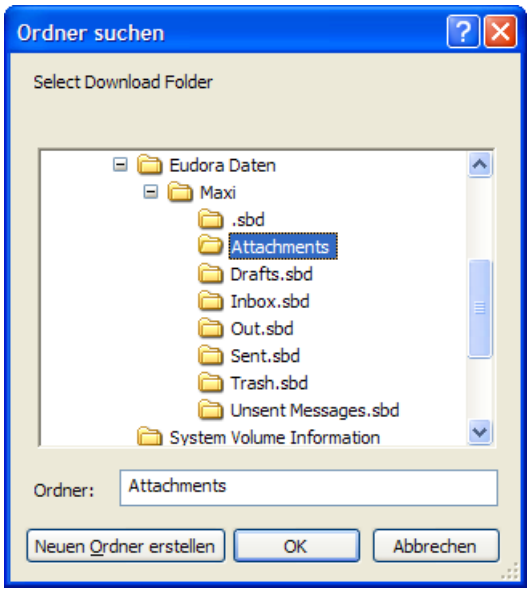
Wähle auf der linken Seite den Punkt „Attachments“:



Durch Auswählen des Listeneintrags „Other...“ in der ComboBox (Auswahlliste) bei „Save all attachments to this folder“ kannst du einen anderen Ordner angeben, also z.B. einen auf deiner verschlüsselten Partition.

Zurück zum Inhalt dieses Kapitels

Im sich öffnenden Fenster kannst du dir den Ordner aussuchen:



Du kannst auch einen neuen Ordner auf deiner verschlüsselten Partition erstellen.

Gib den Ordner an und drücke den Button „OK“. Schließe dann auch das Hauptfenster, fertig – deine Attachments werden zukünftig auf der verschlüsselten Partition gespeichert.

Zurück zum Inhalt dieses Kapitels

9 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

Die jeweils aktuellste Version von ZoneAlarm findest du unter http://www.zonelabs.com. Die kostenlose Version ist auf den Webseiten sehr versteckt, aber nach ein bisschen Herumsuchen findest du sie sicher.

9.1 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.

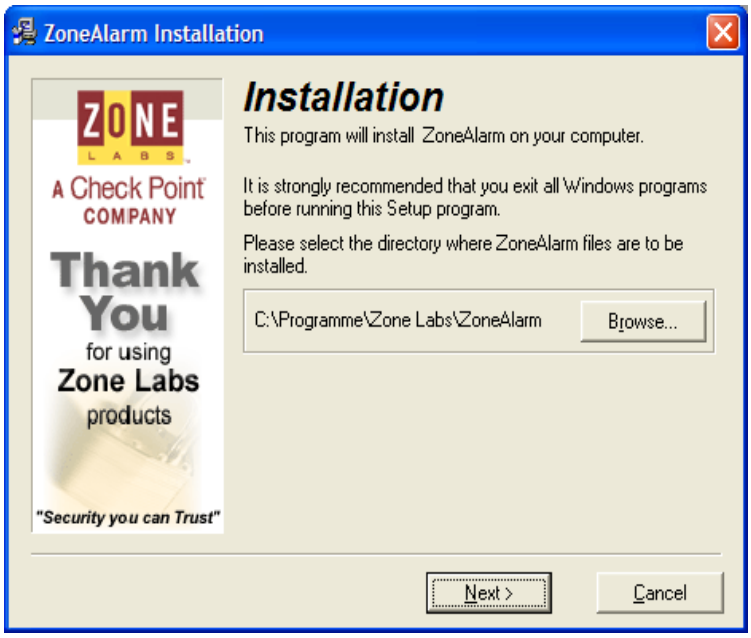
Doppelklicke auf der CD auf die Datei zlsSetup_61_737_000_en.exe, dann erscheint der Willkommenstext mit der Möglichkeit zur Auswahl des Installationsverzeichnisses.

ZoneAlarm\Windows\

zlsSetup_61_737_000_en.exe

Zurück zum Inhalt dieses Kapitels

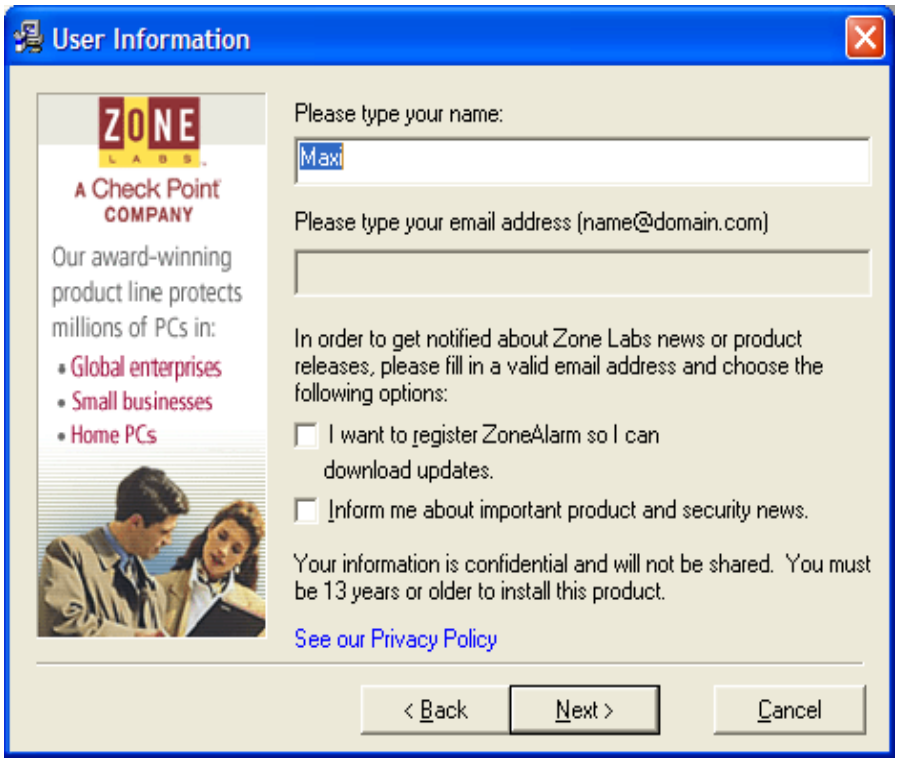
Es erscheint der Willkommens-Dialog, bei dem du dir gleich das Installationsverzeichnis aussuchen kannst.



Du kannst das vorgeschlagene Installationsverzeichnis annehmen oder auch ein anderes angeben. Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann sollst du (d)einen Namen und (d)eine E-Mail Adresse angeben.



Hier antwortest du natürlich absolut wahrheitsgetreu ;-) mit einem Phantasienamen und einer Phantasie-E-Mail-Adresse, geht ja alles niemanden etwas an.

Auch die Kästchen mit „I want to register...“ und „Inform me about...“ kannst du ruhig entmarkieren. Da ZoneAlarm ein kostenloses Programm ist, kannst du dir sowieso immer eventuell neuere Versionen aus dem Internet herunterladen.

Drücke dann den Button „Weiter“.

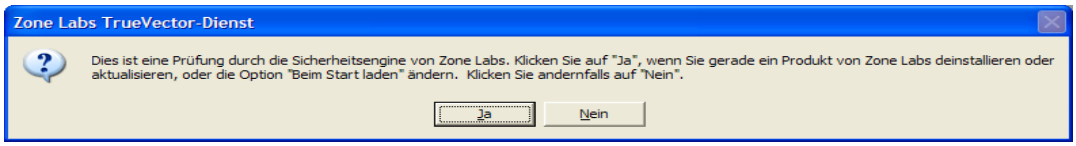
Zurück zum Inhalt dieses Kapitels

Dann erscheint die Lizenzvereinbarung.

Markiere das Kästchen mit „I accept the terms of the preceding License Agreement“ und drücke den Button „Install“.

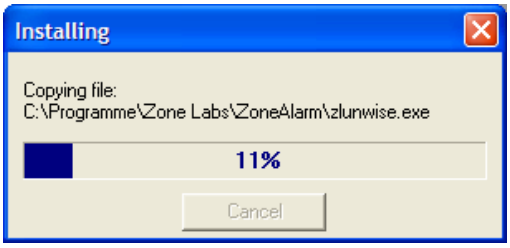
Zurück zum Inhalt dieses Kapitels

Es folgt eine Sicherheitsabfrage. Sie fragt, ob du wirklich gerade dabei bist, ZoneAlarm zu installieren.



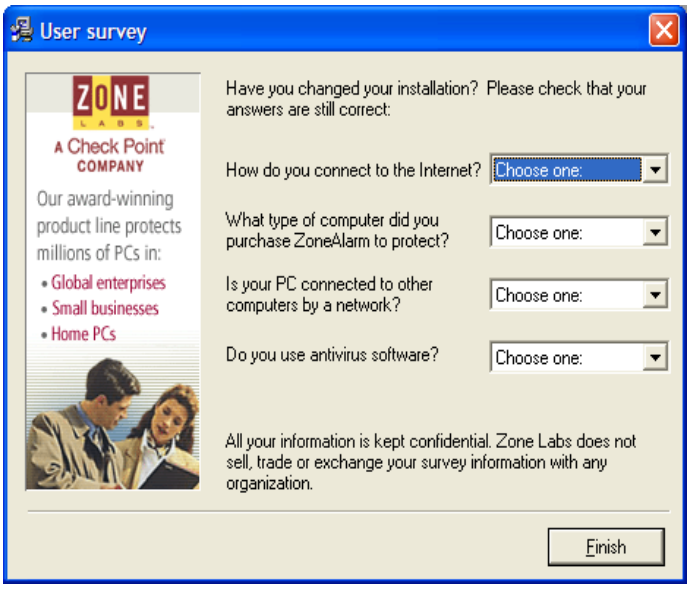
Diese Abfrage dient dazu zu verhindern, dass ein anderes Programm die Firewall manipuliert.

Drücke den Button „Ja“. Dann beginnt die Installation, die nicht sehr lange dauert.



Zurück zum Inhalt dieses Kapitels

Für die anschließende „BenutzerInnenumfrage“ hast du voraussichtlich gerade leider keine Zeit.



Einfach „Finish“ drücken.

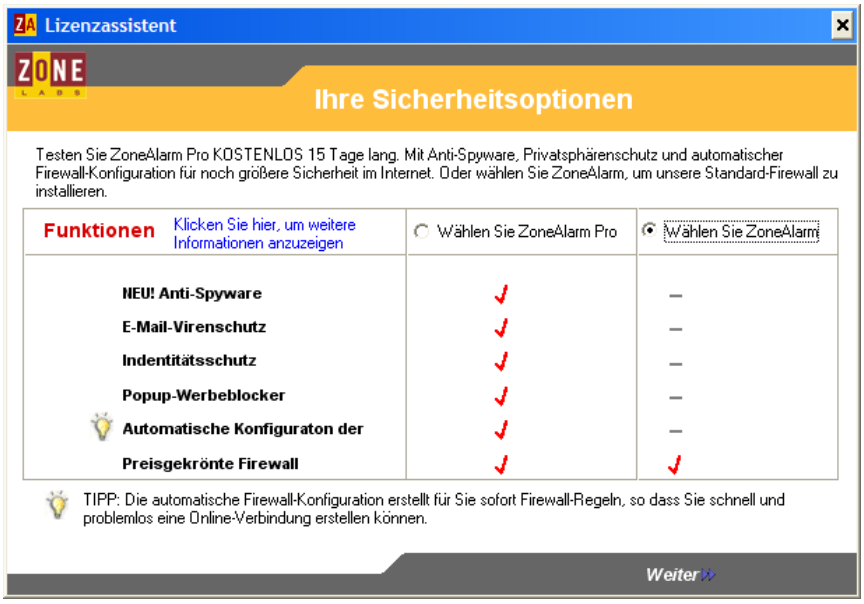
Zurück zum Inhalt dieses Kapitels

Die Installation ist jetzt abgeschlossen. Du wirst gefragt, ob du das Programm gleich starten willst.

Drücke den Button „Yes“.

Zurück zum Inhalt dieses Kapitels

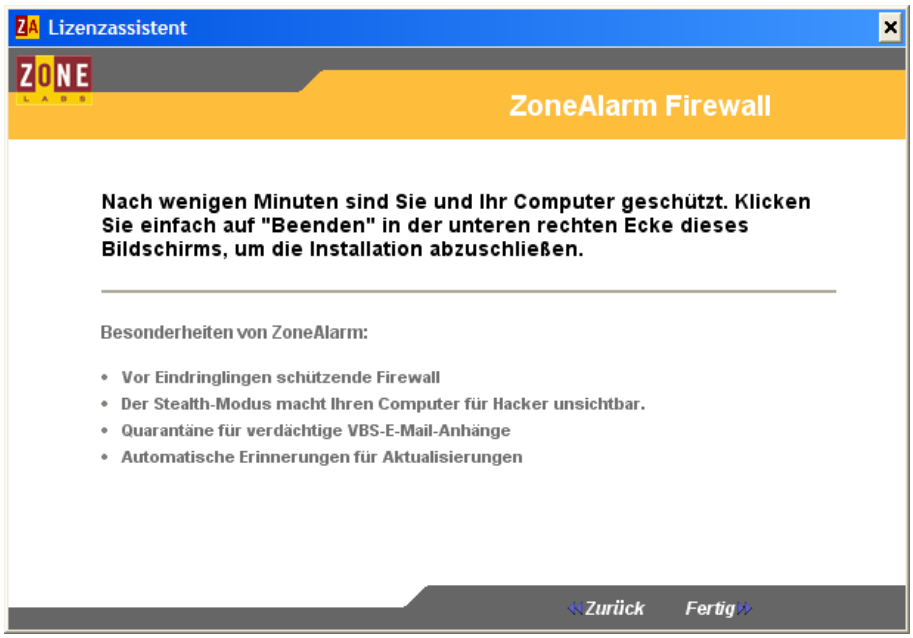
Danach erscheint der „Lizenzassistent“. Hier muss angegeben werden, ob du eine Testversion des kostenpflichtigen ZoneAlarm Pro oder das kostenlose ZoneAlarm verwenden willst.



Markiere „Wählen Sie ZoneAlarm“ (das ohne „Pro“) und drücke „Weiter“.

Zurück zum Inhalt dieses Kapitels

Es erscheint ein weiterer Abschluss-Dialog.



Nach dem Drücken von „Fertig“ bist du vorerst mal wirklich fertig mit der Installation.

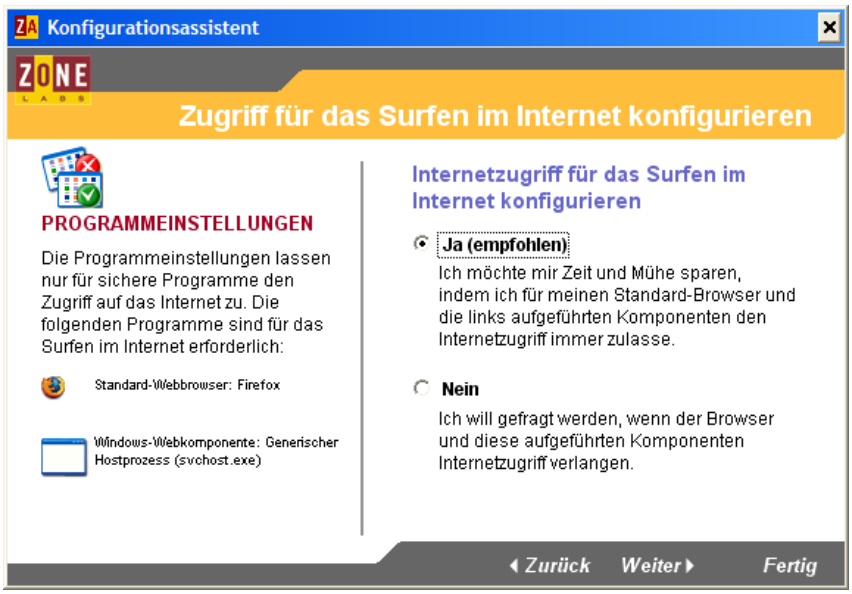
Zurück zum Inhalt dieses Kapitels

Beim ersten Start des Programms folgen noch Konfigurationsmöglichkeiten (Einstellungen) des Programms.

Drücke „Weiter“. Es erscheint der „Konfigurationsassistent“. Die anschließend vorzunehmenden Einstellungen kannst du aber auch später jederzeit vornehmen bzw. ändern. Trotzdem ist es eine gute Idee, gleich mal ein paar grundlegende Dinge vorzunehmen (falls du die gesamte Grund-Konfiguration manuell vornehmen willst, drücke „Fertig“ statt „Weiter“).

Zurück zum Inhalt dieses Kapitels

Du wirst gefragt, ob ein paar Programme die Erlaubnis zum Zugriff auf das Internet bekommen sollen oder nicht.

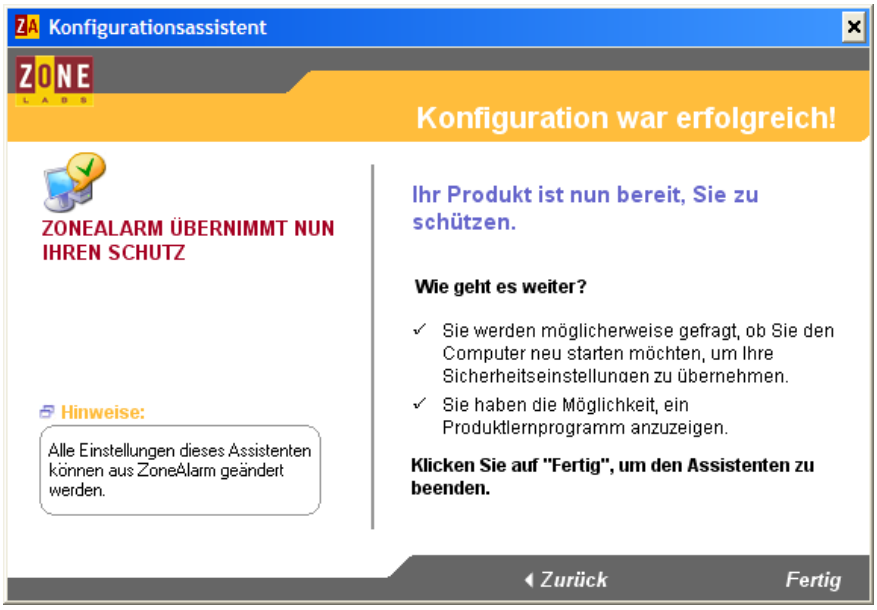


Auf der linken Seite siehst du diese Programme, in diesem Fall ist es der Standard-Webbrowser (hier Firefox) und das Windows-Programm „Generischer Hostprozess“ (ohne den bekommst du überhaupt keine Verbindung ins Internet).

Du kannst also ruhig das „Ja“ (Erlaubnis erteilen) auf der rechten Seite markieren und „Weiter“ drücken.

Zurück zum Inhalt dieses Kapitels

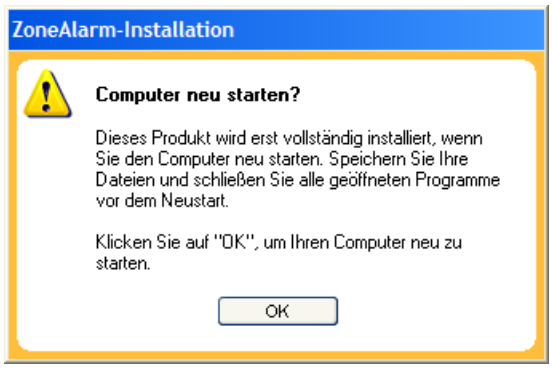
Es folgt der Abschluss-Dialog des Konfigurationsassistenten.



Drücke auf „Fertig“.

Zurück zum Inhalt dieses Kapitels

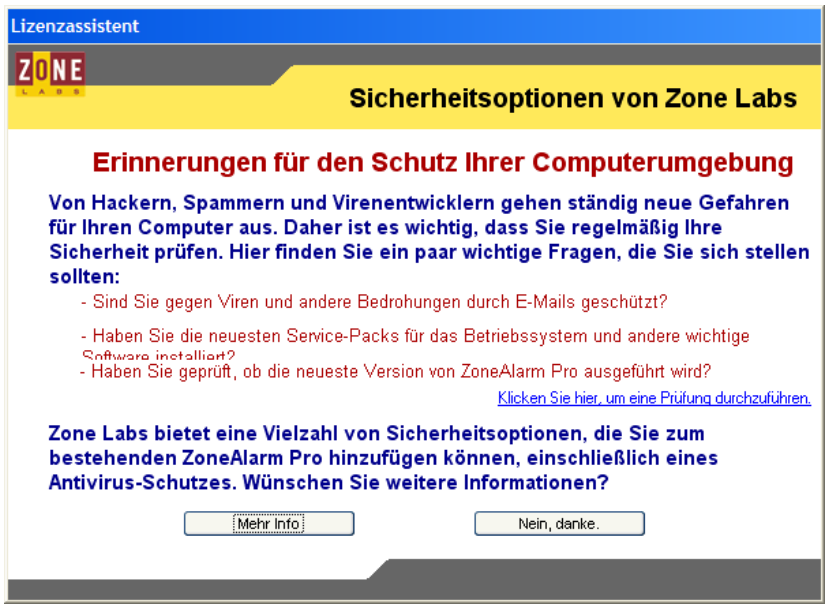
Der Computer muss dann neu gestartet werden.



Nach Drücken des Buttons „Ok“ wird der Computer neu gestartet.

Zurück zum Inhalt dieses Kapitels

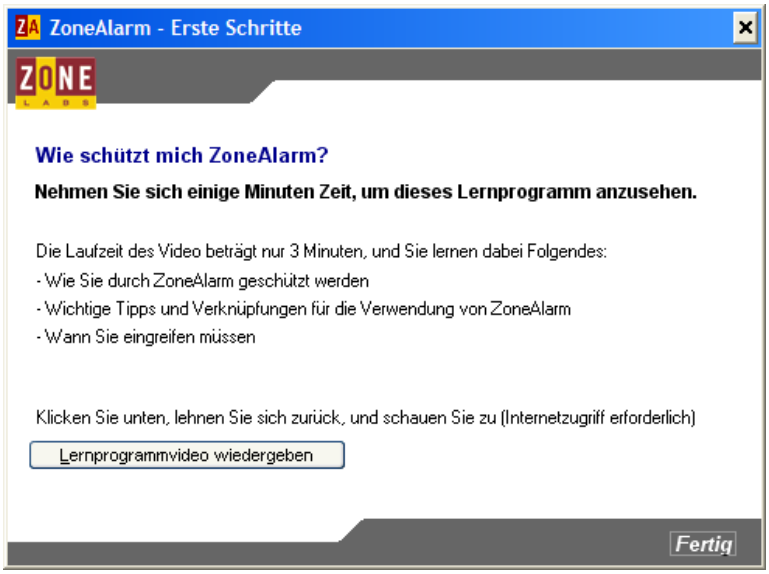
Nach dem Neustart wird ZoneAlarm automatisch gestartet.



Es wird noch ein bisschen Werbung für eine kostenpflichtige Version von ZoneAlarm gemacht. Drücke einfach den Button „Nein, danke“.

Zurück zum Inhalt dieses Kapitels

Du kannst dir jetzt, wenn du willst, ein Lernvideo ansehen:

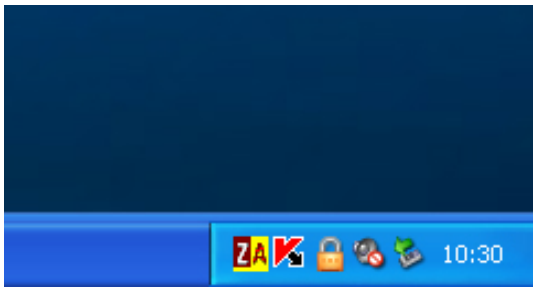


Wenn du das Video sehen willst, drücke „Lernprogrammvideo wiedergeben“.

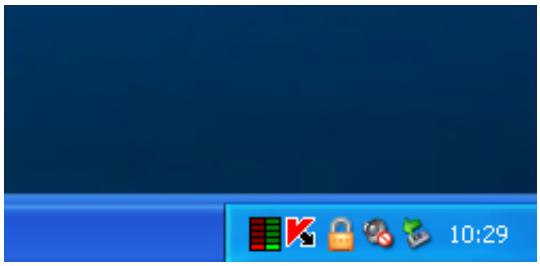
Drücke dann den Button „Fertig“.

Zurück zum Inhalt dieses Kapitels

Nach jedem Start von Windows wird ab sofort ZoneAlarm automatisch gestartet. Du erkennst, dass ZoneAlarm gestartet wurde und darüber wacht, was von außen an deinen Computer kommt und was von deinem Computer ins Internet gesendet wird, an einem kleinen Symbol rechts unten auf deinem Bildschirm – ein ZA in rot/gelb.

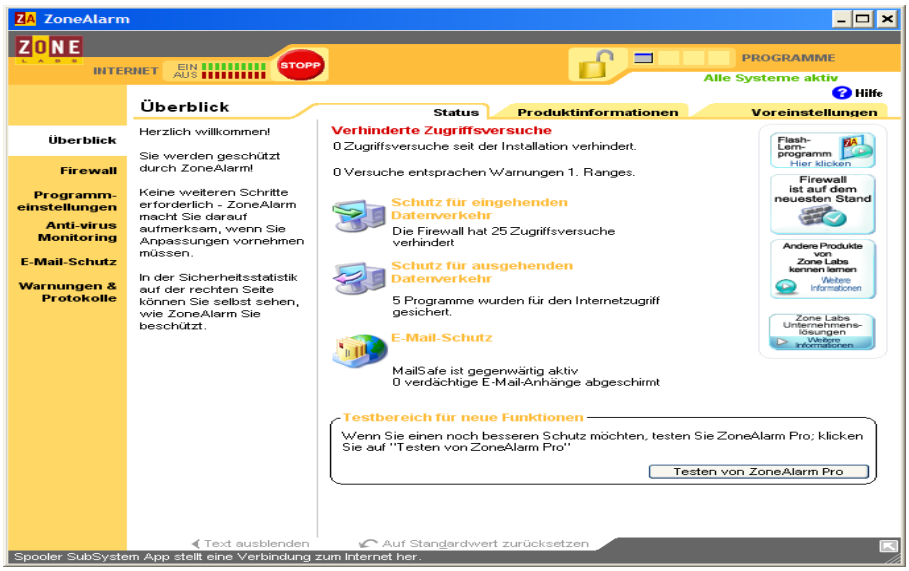


Wenn Daten zu deinem Computer gesendet werden oder Daten von deinem Computer gesendet werden, verwandelt sich das kleine Bild in eine gestreifte Version.



Zurück zum Inhalt dieses Kapitels

Nach dem ersten Start nach der Installation erscheint das Hauptfenster von ZoneAlarm.



Hier kannst du einige Einstellungen vornehmen. Z.B. Programmen erlauben oder verbieten, sich ins Internet zu verbinden und vieles andere. Klick dich einfach mal durchs Menü auf der linken Seite und durch die einzelnen Tabs bei jedem Menüpunkt.

Du kannst das Fenster durch Drücken des „x“ am rechten oberen Rand des Fensters schließen.

Zurück zum Inhalt dieses Kapitels

Tja, trotz der vorherigen Angabe, dass der Standard-Browser aufs Internet zugreifen darf, erscheint die Abfrage zur Erlaubnis nochmals, nachdem du ihn startest. Na ja, ist halt ein kleiner Fehler…

Mehr dazu, z.b. wie Programmen erlaubt/verboten wird, Verbindung mit dem Internet aufzunehmen, findest du im nächsten Kapitel.

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.

Vergiss also nicht, den meisten anderen in diesem Handbuch vorgestellten Programmen diese Erlaubnis zu erteilen (z.B. dem Virenscanner, den Anti-Spyware-Programmen zum Aktualisieren u.a.).

Ob du die automatischen Updates aktivierst, bleibt dir überlassen. Du erhältst dadurch die Garantie, immer am aktuellsten Stand zu sein – ist halt eine Frage des Vertrauens.

Zurück zum Inhalt dieses Kapitels

9.2 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.

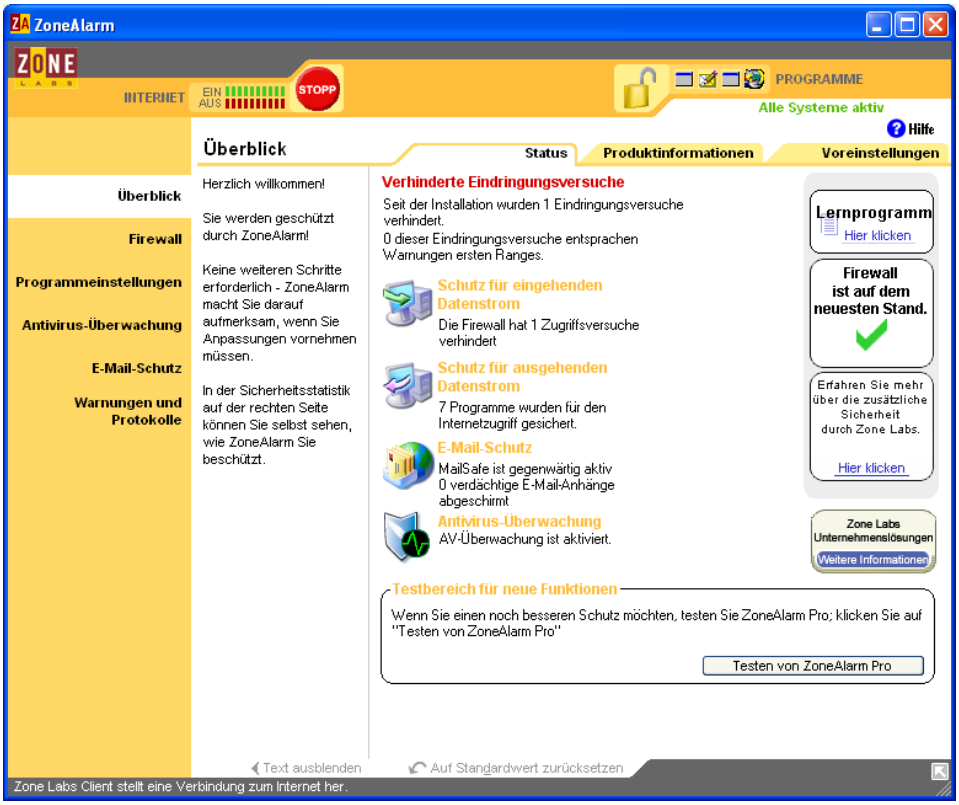
Auch diesen Verbindungen musst du deine Erlaubnis erteilen.

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

Zurück zum Inhalt dieses Kapitels

Einstellungen/Konfiguration

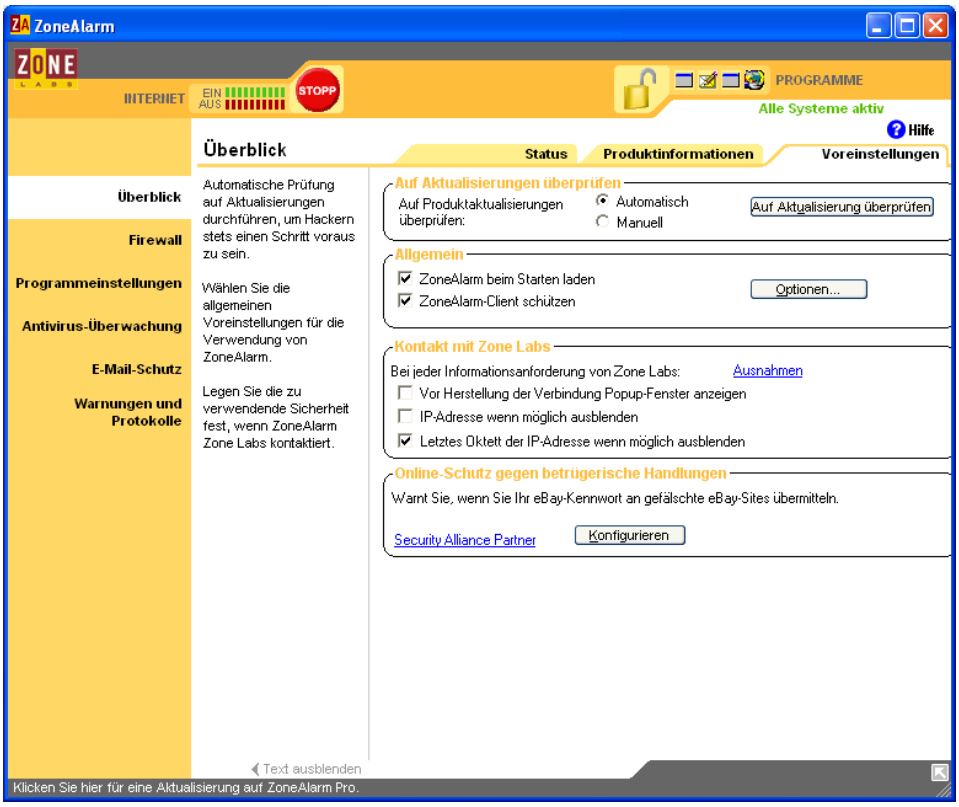
Starte das Programm im Start-Menü durch Wählen des Menüpunktes „Start ⇨ Programme ⇨ Zone Labs ⇨ Zone Labs Security“ oder doppelklicke auf das ZoneAlarm-Symbol am rechten unteren Rand deines Bildschirms. Folgendes Konfigurationsfenster erscheint.



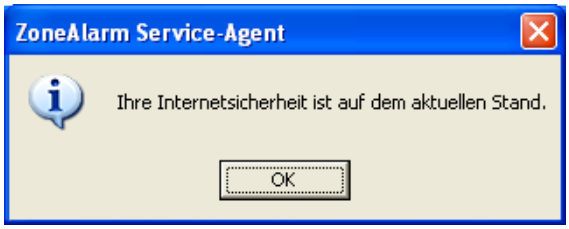
In diesem Konfigurationsfenster kannst du alle Einstellungen vornehmen, dir Protokolle ansehen und prüfen, ob es schon neuere Versionen von ZoneAlarm gibt.

Zurück zum Inhalt dieses Kapitels

Zum Prüfen, ob es schon neuere Versionen von ZoneAlarm gibt, wähle im linken Hauptmenü den Menüpunkt „Überblick“ und im Untermenü den Tab „Voreinstellungen“.



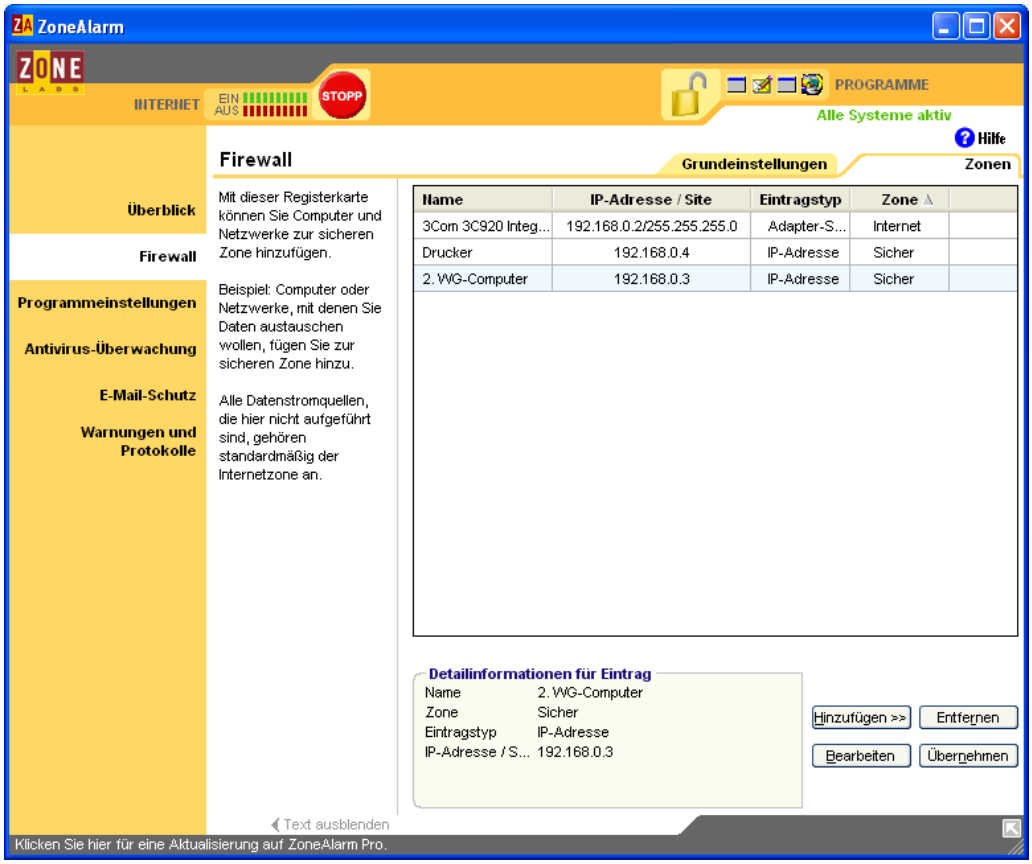
Nach Drücken des Buttons „Auf Aktualisierung überprüfen“ verbindet sich das Programm mit der Zone Labs-Seite und prüft die Version. Ist die Version aktuell, erhältst du die folgende Meldung.



Zurück zum Inhalt dieses Kapitels

Falls sich dein Computer in einem lokalen Netzwerk befindet und du willst, dass andere Computer auf deinen Zugriff haben bzw. du Geräte im Netzwerk nützen willst, kannst du die IP-Adressen dieser Computer/Geräte hinzufügen.

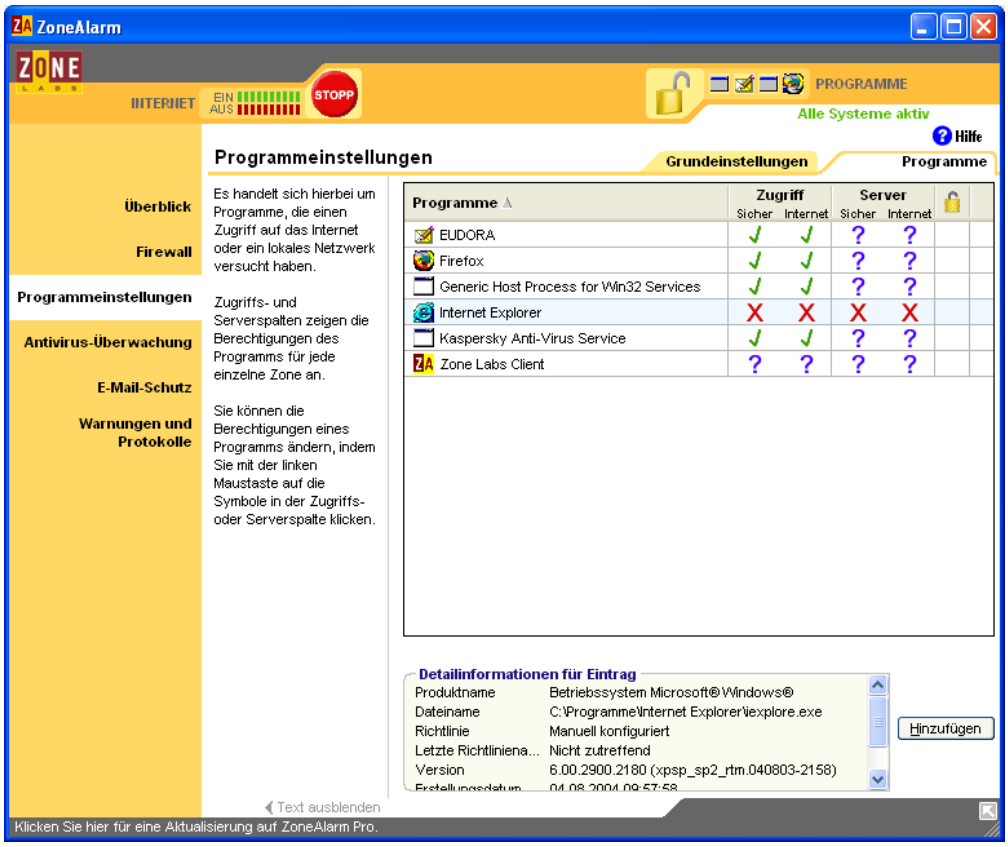
Wähle dazu links den Hauptmenüpunkt „Firewall“ und den Tab „Zonen“.



Hier kannst du die IP-Adressen hinzufügen, in diesem Beispiel wurde ein anderer „WG-Computer“ und der Netzwerkdrucker hinzugefügt, die erste Zeile beinhaltet die eigene Netzwerkkarte.

Zurück zum Inhalt dieses Kapitels

Um die einzelnen Programme zu prüfen/ändern, die Zugriff aufs Internet bzw. vom Internet haben, wähle auf der linken Seite den Hauptmenüpunkt „Firewall“.



Zu jedem Programm, das für ZoneAlarm registriert wurde, gibt es 3 Einstellungsmöglichkeiten:

- Ein grünes Häkchen: hat immer Zugriff
- Ein blaues Fragezeichen: bei jedem Zugriff wird gefragt
- Ein rotes X: das Programm hat nie Zugriff

Zurück zum Inhalt dieses Kapitels

Jede dieser Einstellungen wird für beide mögliche Funktionen des Programms angegeben:

- Zugriff: einfache Verbindung des Programms ins Internet
- Server: das Programm stellt Dienste fürs Internet zur Verfügung (das ist z.B. bei Filesharing-Programmen nötig)

„Zugriff“ und „Server“ werden jeweils für zwei Zonen angegeben:

- Sicher: alles, was im Menüpunkt „Firewall“ für die Zone „Sicher“ registriert wurde (z.B. der Netzwerkdrucker, ein anderer Computer im lokalen Netzwerk)
- Internet: alles außerhalb der Zone „Sicher“

Es gibt noch eine Reihe anderer Einstellungen, wir stellen sie aber hier nicht alle einzeln vor. Mehr dazu findest du im Lernprogramm und in der Hilfe-Funktion des Programms (Button rechts oben).

Schließen kannst du das Konfigurationsfenster durch Drücken des X ganz rechts oben am Konfigurationsfenster – auch nicht gerade elegant, aber was soll’s.

Schließt du das Konfigurationsfenster zum ersten Mal, erhältst du noch einige „Tipps“.

Willst du diese „Tipps“ nicht jedes Mal sehen, wenn du das Konfigurationsfenster schließt, markiere „Diese Meldung nicht erneut anzeigen“ und drücke den Button „OK“.

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 des Filesharing-Programms eMule sieht das z.B. so aus:

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

Wenn du vorher das Kästchen bei „Diese Einstellung speichern“ anhakst, erlaubst du diesem Programm ohne zukünftige Abfrage, sich mit dem Internet zu verbinden. Dieses Recht kannst du natürlich über die Konfiguration in „Programmeinstellungen“ jederzeit wieder entziehen.

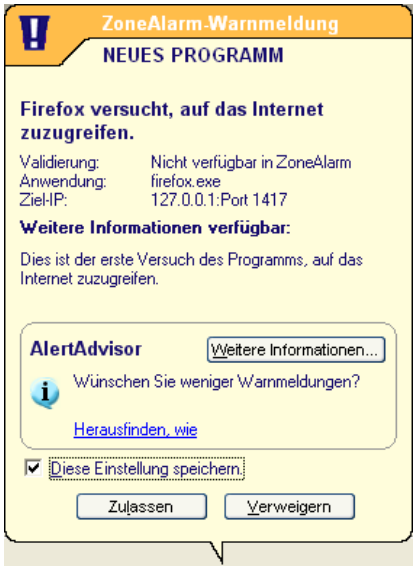
Zurück zum Inhalt dieses Kapitels

Du willst wahrscheinlich nicht jedes Mal, wenn du deinen Internet Browser startest, die Erlaubnis zur Verbindung geben. 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 „Verweigern".

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

Beim Starten eines Internet-Browsers (hier Firefox) sieht es sehr ähnlich aus.



Auch hier gilt: mit deinem Internet-Browser willst du ja immer aufs Internet zugreifen und surfen. Es wäre daher etwas mühsam, jedes Mal extra die Erlaubnis geben zu müssen.

Kreuze also hier auch das Kästchen bei „Diese Einstellung speichern" an und bestätige mit „Zulassen" die Erlaubnis.

Zurück zum Inhalt dieses Kapitels

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

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 „Verweigern".

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

Wenn du dir nicht sicher bist, ist es auch empfehlenswert, vorher der Erlaubnis mal im Internet nachzugoogeln, was es an Infos zu diesem Programm gibt.

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 (angeblich) 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 „Warnungen und Protokolle“ angegeben ist, wird in jedem Fall so ein Kontaktaufnahmeversuch vermerkt.

Bestätige die Warnung durch Drücken von „OK“.

Zurück zum Inhalt dieses Kapitels

10 AntiVir (Anti-Virenprogramm)

Überblick

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

Es gibt zahlreiche Viren-Schutzprogramme, AntiVir für Windows ist nur eines davon (in einem eigenen Dokument auf der CD wird auch noch das kostenpflichtige Anti-Virenprogramm Kaspersky Anti-Virus vorgestellt).

Wichtig ist aber vor allem, überhaupt einen sogenannten Viren-Scanner auf dem Computer zu installieren und diesen unbedingt immer auf aktuellem Stand zu halten (mit zumindest täglicher Aktualisierung), denn es tauchen ständig neue Computerviren auf.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von AntiVir
- Die Verwendung von AntiVir
- Einstellungen in AntiVir
- Das Durchsuchen des Computers nach Computerviren
- Das Prüfen einzelner Ordner und Dateien

Die aktuellste Version von AntiVir findest du im Internet unter http://www.free-av.de/

Das Installationsprogramm für eine Testversion des Antiviren-Programms Kaspersky-Antivirus findest du auf der CD im Ordner Kaspersky Anti-Virus Testversion.

Dort findest du auch eine Beschreibung der Installation und Verwendung von Kaspersky Anti-Virus.

Word-Dokumente

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).

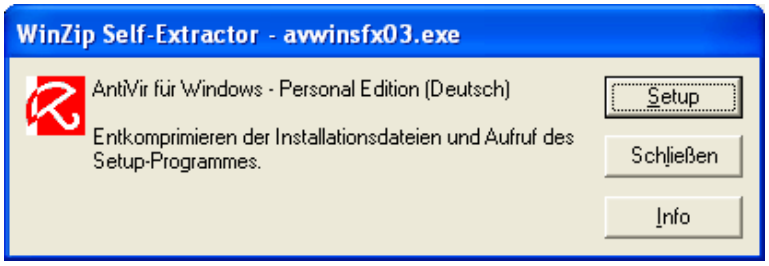
Auch wissen das Menschen zu schätzen, die keinen Kabel- oder ADSL-Anschluss zu Hause haben und mit einem Modem zum Internet verbunden sind. Word-Dokumente sind ja meist aufgrund der vielen Formatierungen sehr groß, reine Texte, wie du sie in deinem E-Mail Programm eintippst, sind jedoch für alle blitzschnell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

Zurück zum Inhalt dieses Kapitels

10.1 Die Installation von AntiVir

Du findest das Installationsprogramm von AntiVir für Windows auf der zugehörigen CD im Verzeichnis „AntiVir\Windows“. 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 auf die Datei avwinsfx.exe, dann erscheint gleich mal folgende Information



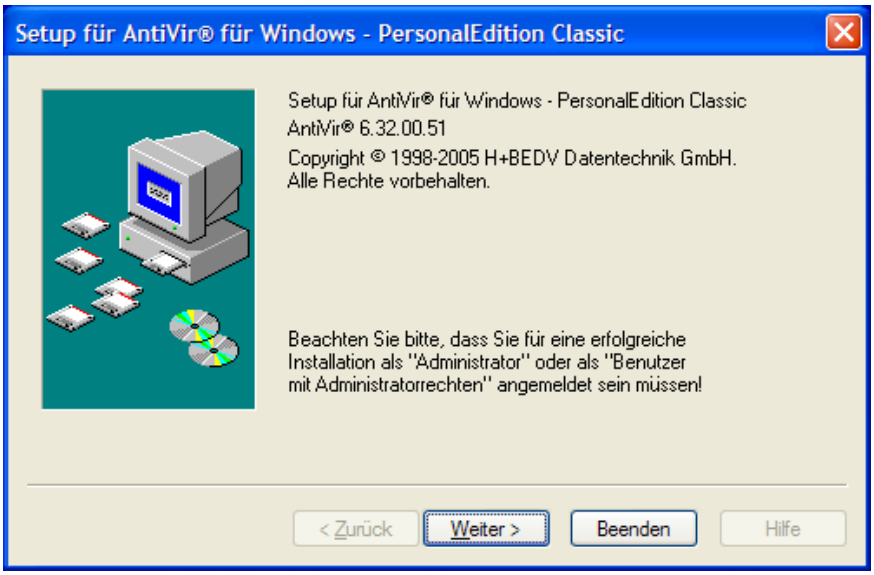
Der Installationsvorgang beginnt nach Drücken des Buttons „Setup“.

Beseitige/deinstalliere unbedingt eventuell bereits installierte andere Anti-Virenprogramme. Du erhältst im Laufe der Installation noch einen entsprechenden Warnhinweis.

Dieser Hinweis ist bei AntiVir wirklich ernst zu nehmen, AntiVir verträgt andere installierte Virenscanner meist überhaupt nicht – dein Computer könnte völlig lahm gelegt werden.

Zurück zum Inhalt dieses Kapitels

Als erstes erscheint folgendes Fenster:



Drücke einfach den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

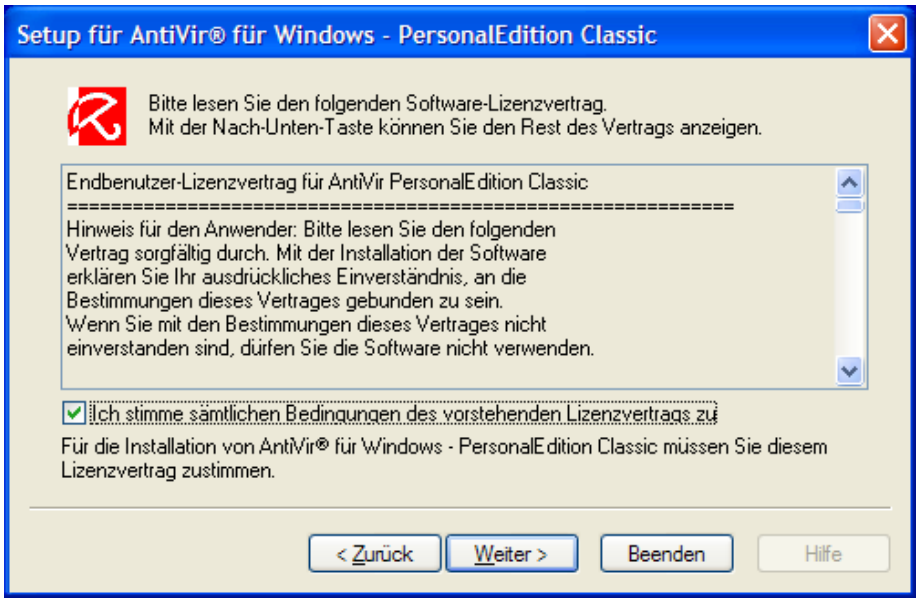
Dann erscheint der Hinweis, dass du alle Programme schließen sollst, insbesondere bereits installierte Anti-Virenprogramme:

Nimm vor allem den Hinweis ernst, dass eventuell bereits installierte Anti-Virenprogramme (Virenwächter) vor der Installation von AntiVir deinstalliert werden müssen.

Bestätige das Fenster durch Drücken des Buttons „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann kommt natürlich der Lizenzvertrag:



Hake „Ich stimme sämtlichen Bedingungen zu“ an und drücke den Button „Weiter“.

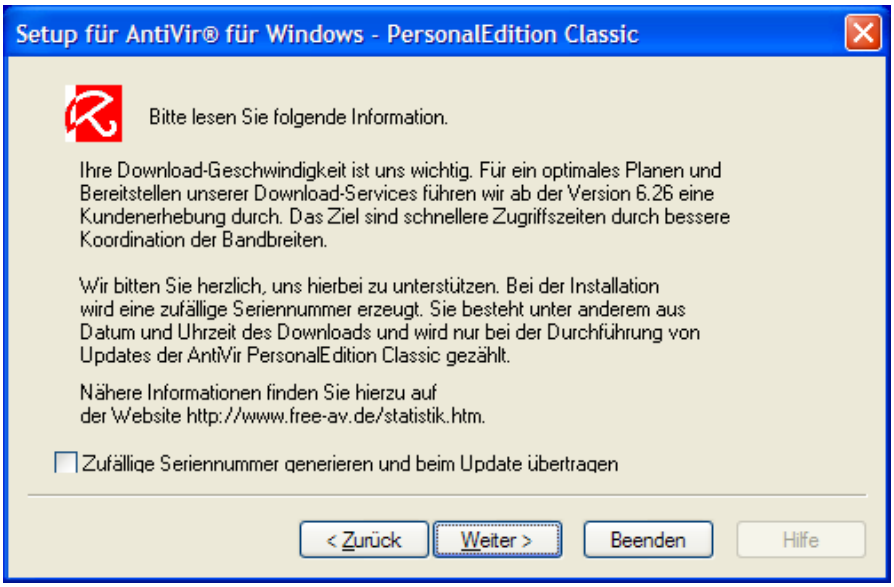
Zurück zum Inhalt dieses Kapitels

Nun musst du bestätigen, dass du das Programm nur privat nutzt:

Bestätige das durch Anhaken der Bestätigung und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt wirst du gebeten zuzustimmen, dass eine „Seriennummer“ für dich generiert wird, mit der dein Computer eindeutig zu identifizieren ist.

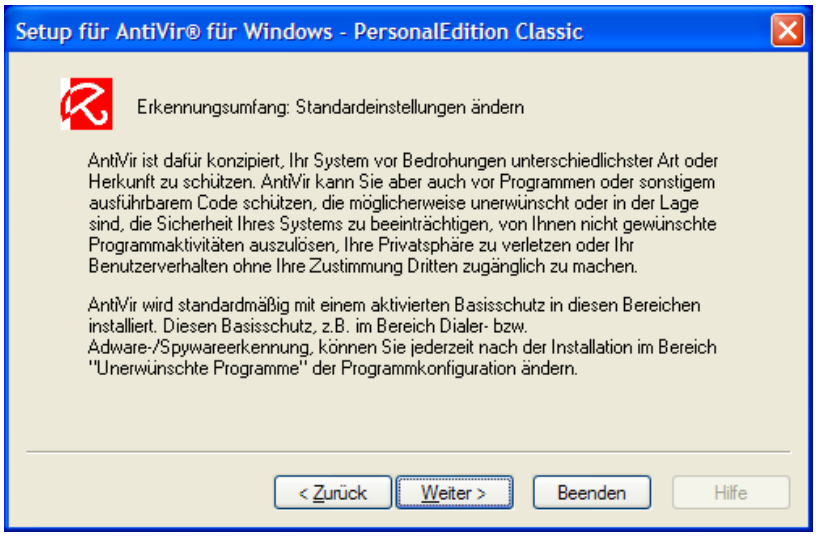


Tja, tut uns ja wirklich leid, aber das wollen wir eigentlich nicht.

Klicke das Häkchen bei „Zufällige Seriennummer generieren“ weg und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

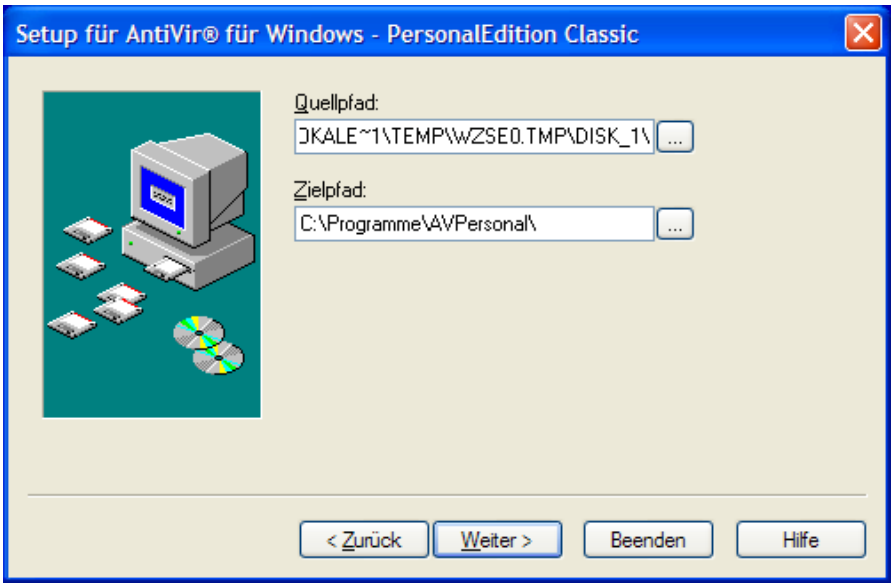
Nun erhältst du noch einen Hinweis zum Programmumfang:



Lies es dir durch und drücke den Buton „Weiter“.

Zurück zum Inhalt dieses Kapitels

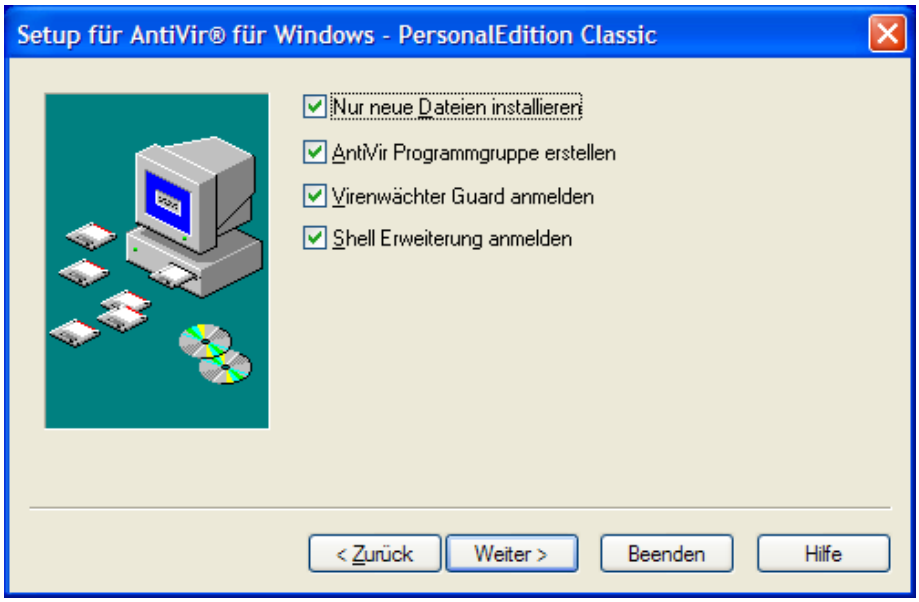
Nun kannst du dir den Ordner aussuchen, in den das Programm installiert wird:



Nimm einfach den vorgeschlagenen Ordner oder gib einen anderen an, drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

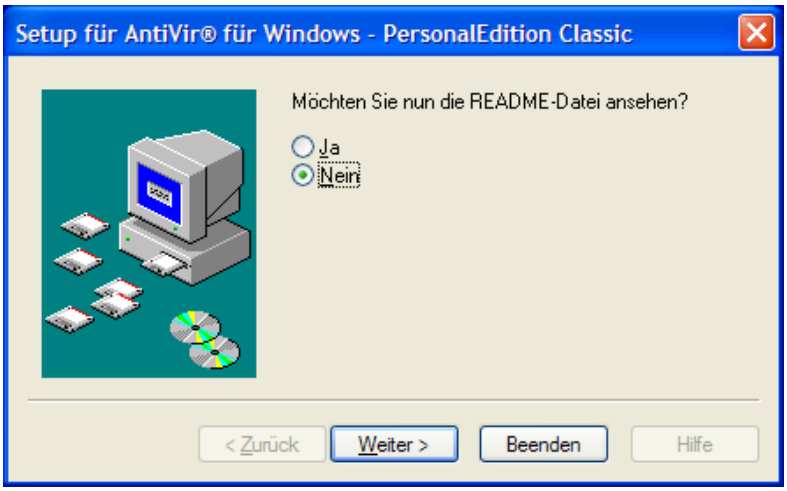
Nun kannst du dir die zu installierenden Komponenten aussuchen:



Du willst natürlich wie vorgeschlagen alles installieren. Lass alles angehakt und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann beginnt die eigentliche Installation des Programms. Das dauert nur ein paar Sekunden.



Du wirst noch gefragt, ob du die README-Datei lesen möchtest. In diesen Dateien stehen meist die allerneuesten Informationen zu einem Programm.

Wähle das Gewünschte und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Dann wirst du gefragt, ob du ein AntiVir-Icon am Desktop haben willst oder nicht.

Wähle das von dir Gewünschte aus und drücke den Button „Weiter“.

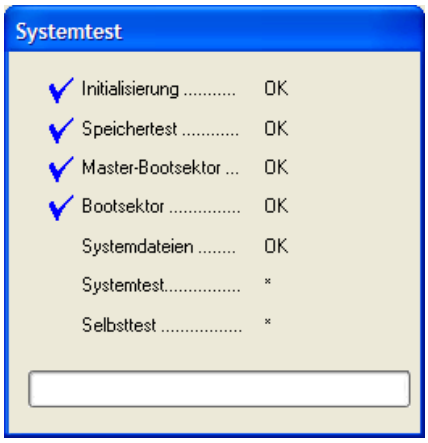
Zurück zum Inhalt dieses Kapitels

So, nun hast du es geschafft, die Erfolgsmeldung erscheint:

Du erhältst auch den Hinweis, dass du das Programm sofort aktualisieren solltest. Drücke den Button „Fertig stellen“.

Zurück zum Inhalt dieses Kapitels

Jetzt wird dein Computer gleich mal durchgecheckt. Es beginnt immer mit einem System- und Selbsttest (auch ein Anti-Virenprogramm könnte ja von einem Virus befallen worden sein).



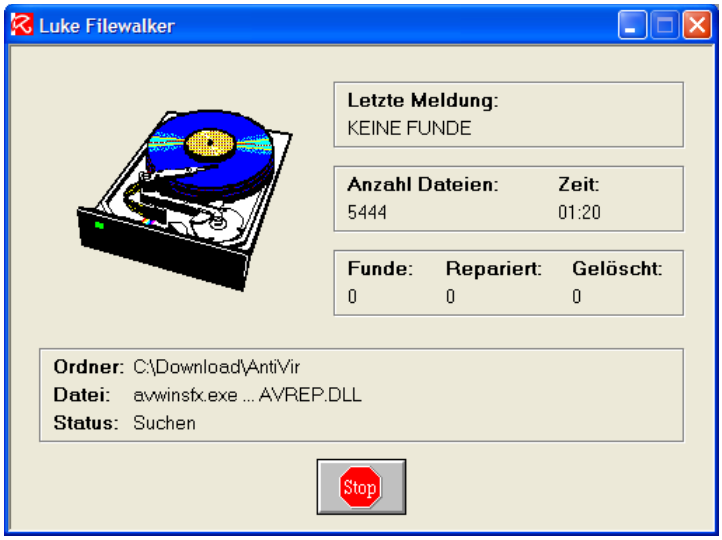
Falls du aber gerade keine Zeit dafür hast, den doch etwas zeitraubenden Virensuchvorgang abzuwarten, kannst du natürlich auch zu einem späteren Zeitpunkt jederzeit deinen Computer nach Viren durchsuchen lassen.

Im 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.

Was du tun kannst, wenn ein Virus gefunden wurde, wird im Kapitel Das Durchsuchen des Computers nach Viren beschrieben.

Zurück zum Inhalt dieses Kapitels

Nun 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.

Achtung: wenn der Regenschirm geschlossen angezeigt wird, heißt das, dass der Virenwächter nicht aktiv ist, du bist in diesem Fall nicht vor Viren geschützt.

Zurück zum Inhalt dieses Kapitels

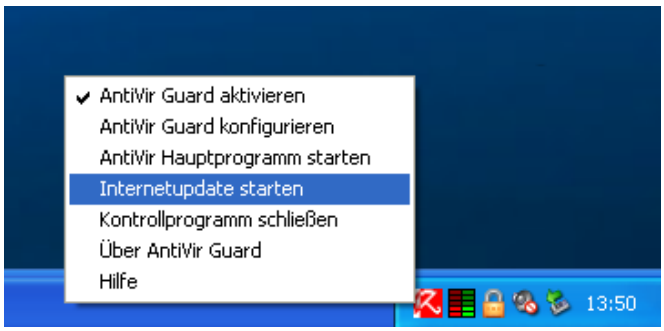
10.2 Die Verwendung von AntiVir

Das Aktualisieren der Viren-Signaturen

Wie schon mehrfach erwähnt, es ist ungemein wichtig, deinen Virenscanner immer aktuell zu halten. Aktuell heißt, ihn zumindest täglich zu aktualisieren.

Diese Aktualisierung läßt sich im Gegensatz zum Programm Kaspersky Anti-Virus bei AntiVir leider nicht automatisieren, du musst immer daran denken, das Programm manuell zu aktualisieren. Mehr dazu in den folgenden Kapiteln.

Am einfachsten findest du diese Aktualisierungsmöglichkeit durch Anklicken des Regenschirm-Symbols von AntiVir in der Taskleiste am rechten unteren Rand deines Bildschirms.



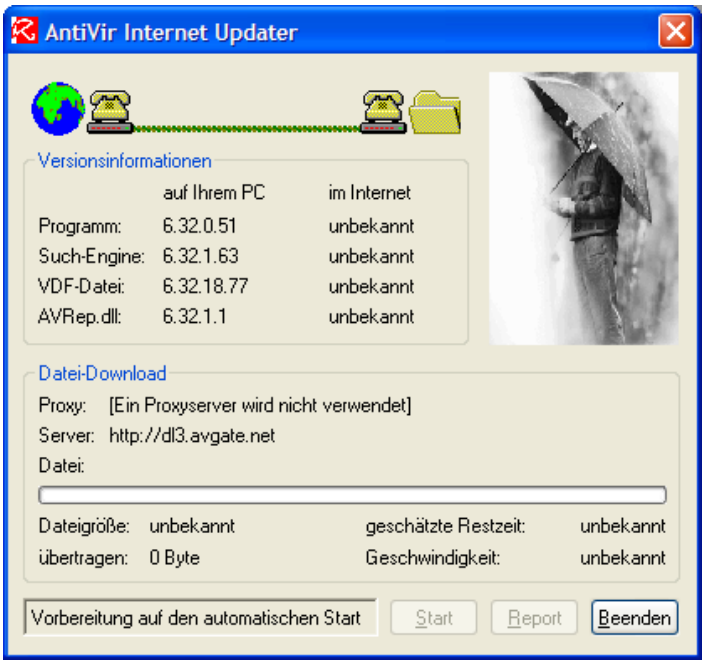
Zurück zum Inhalt dieses Kapitels

Hast du längere Zeit auf die Aktualisierung vergessen, erhältst du vom Programm eine Warnung:

Prüfe in diesem Fall, dass dein Computer mit dem Internet verbunden ist und drücke den Button „Jetzt updaten“.

Zurück zum Inhalt dieses Kapitels

Es erscheint das Aktualisierungsprogramm:

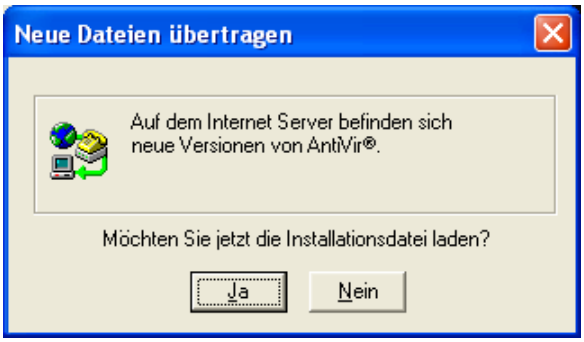


Falls das nicht automatisch passiert, starte die Prüfung deiner Version durch Drücken des Buttons „Start“.

Wenn du ZoneAlarm installiert hast, musst du auch diesem Programm die Erlaubnis erteilen, sich mit dem Internet zu verbinden.

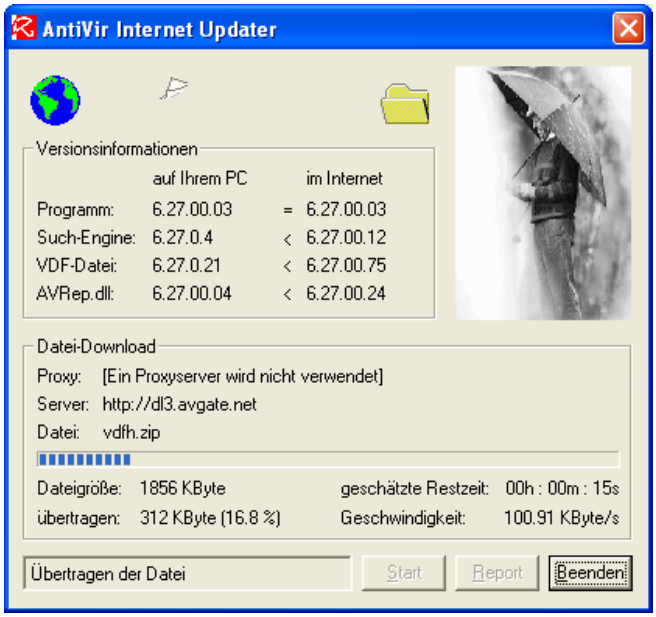
Zurück zum Inhalt dieses Kapitels

Wird eine neuere Version gefunden, wirst du gefragt, ob du das Programm aktualisieren willst:



Beantworte die Frage durch Drücken des Buttons „Ja“.

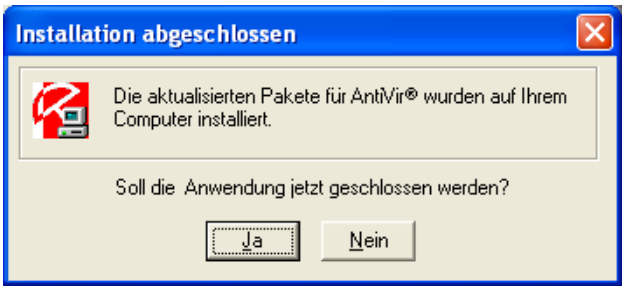
Die Aktualisierung des Programms beginnt jetzt:



Der Fortschritt der Übertragung und Installation wird angezeigt.

Zurück zum Inhalt dieses Kapitels

Wenn die Übertragung der neuesten Virensignaturen abgeschlossen wurde, erhältst du folgende Erfolgsmeldung:



Bestätige die Frage mit „Ja“. Dein Programm ist jetzt wieder aktuell.

Zurück zum Inhalt dieses Kapitels

Der AntiVir Guard

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

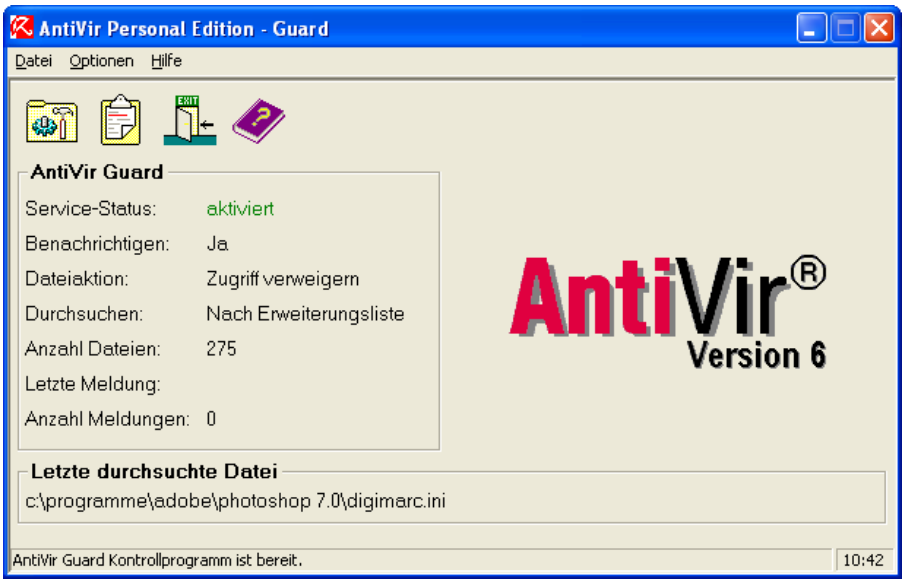
Dieser Guard wacht die ganze Zeit im Hintergrund darauf, dass dir kein Computervirus auf den Computer kommt. Alle Dateien, die einen Virus enthalten könnten, werden vor dem Starten schnell auf Viren geprüft. Beinhaltet eine Datei einen Virus, wirst du sofort informiert und kannst den Virus entfernen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

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

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

Du kannst hier aber auch wichtige Einstellungen vornehmen.



So kannst du aus diesem Fenster heraus das Internet-Update (die Aktualisierung des Programms) starten. Wähle dazu im Menü Datei ⇨ Internetupdate starten.

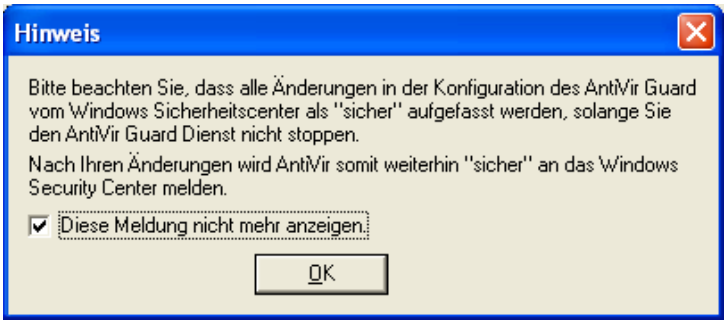
Der Vorgang ist dann genau so wie im vorherigen Kapitel beschrieben.

Zurück zum Inhalt dieses Kapitels

10.3 Einstellungen in AntiVir

Nach einem Doppelklick auf das Regenschirm-Symbol in der Taskleiste deines Desktops ganz rechts unten öffnet sich das Hauptprogramm, in dem du verschiedene Einstellungen vornehmen kannst.

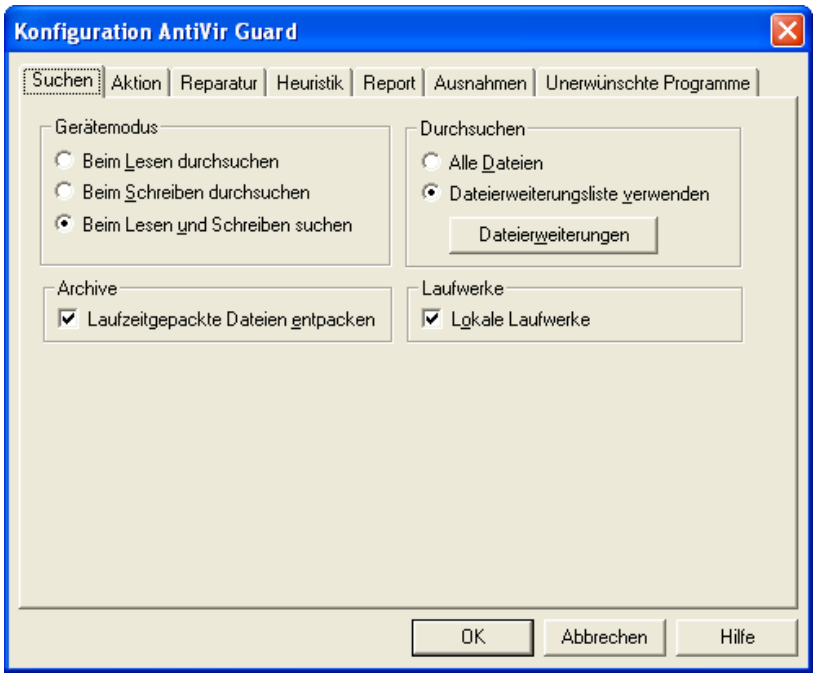
Öffne das Hauptprogramm und wähle im Menü den Punkt Optionen ⇨ Konfiguration. Es folgt ein Hinweis in Zusammenhang mit dem Windows XP Security Center.



Wenn du diesen Hinweis nicht jedes Mal sehen willst, wenn du das AntiVir Hauptprogramm startest, hake „Diese Meldung nicht mehr anzeigen“ an und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Das Konfigurationsmenü bietet einige Einstellungsmöglichkeiten:



Schau dir das Ganze mal an. Du kannst die voreingestellten Optionen belassen oder je nach Wunsch andere angeben.

Zurück zum Inhalt dieses Kapitels

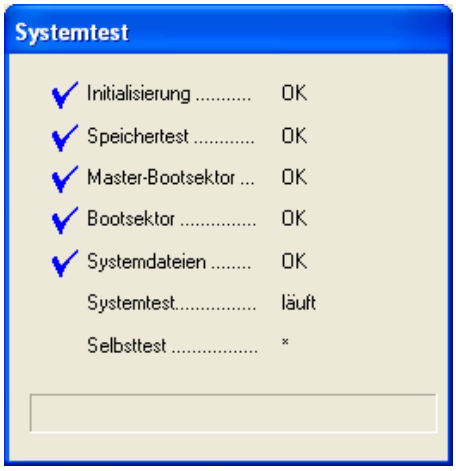
10.4 Das Durchsuchen des Computers nach Viren

Das Prüfen von ganzen Laufwerken (Festplatten, Disketten)

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.

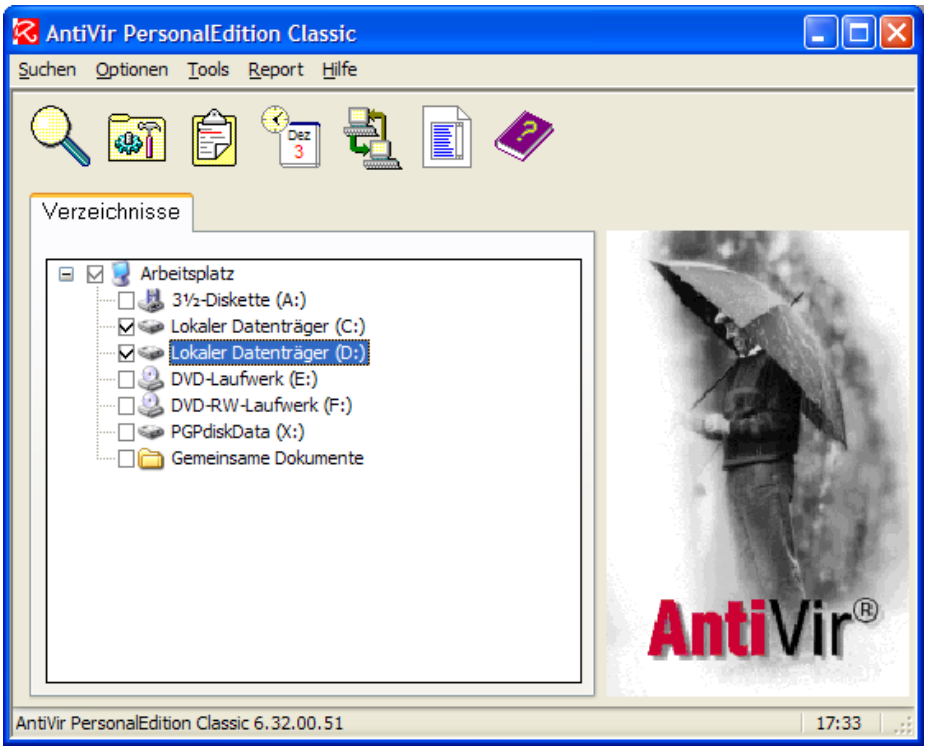
Du findest es im Startmenü unter „Start ⇨ Programme ⇨ AntiVir Personal Edition ⇨ AntiVir“ oder durch Klicken der rechten Maustaste auf das Regenschirmsymbol von AntiVir und wählen des Menüpunkts „AntiVir Hauptprogramm starten“.

Zu Beginn wird wie immer der System- und Selbsttest durchgeführt:



Zurück zum Inhalt dieses Kapitels

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:



Über diesen Weg kannst du leider nur ganze Laufwerke prüfen lassen und nicht einzelne Ordner oder Dateien auf einem Laufwerk. Wie du einzelne Ordner und/oder Dateien prüfen kannst, erfährst du im nächsten Kapitel.

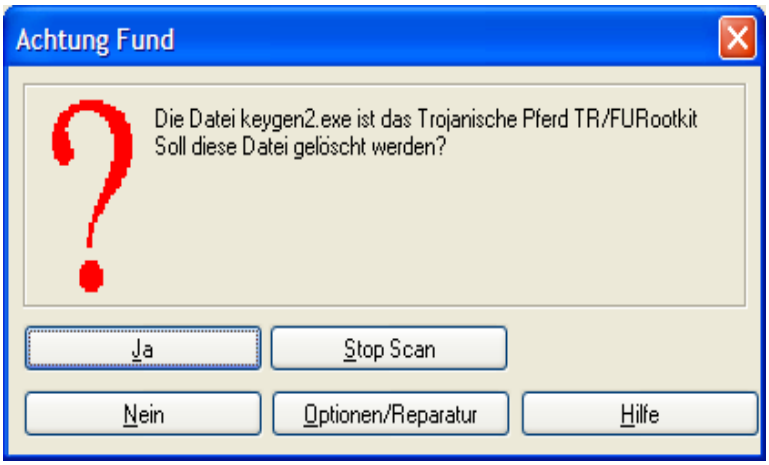
Markiere die Kästchen bei den Laufwerken, die du prüfen willst. Zum Starten der Prüfung drücke die Lupe links oben.

Zurück zum Inhalt dieses Kapitels

Die Laufwerke werden jetzt nach Viren durchsucht.

Zurück zum Inhalt dieses Kapitels

Wird ein Virus gefunden, wird das jedes Mal angezeigt. Du kannst dir dann aussuchen, was du damit machen willst.



Besteht die Möglichkeit einer „Reparatur“ (d.h. des Entfernens des Virus aus einer Datei bzw. einem Programm), kannst du auch das auswählen.

Hier ist nur ein Löschen möglich, drücke daher den Button „Löschen“.

Zurück zum Inhalt dieses Kapitels

Die Meldung kann auch so aussehen:

Hier kannst du du dir nicht aussuchen, was passieren soll, Viren in komprimierten (gezippten) Archiven werden von AntiVir nicht entfernt.

Tipp: auf der Webseite der Zeitschrift c't kannst du dir unter E-Mail-Check Testmails mit Anhängen, die Viren enthalten, zuschicken lassen. Diese Viren sind nur simuliert und richten keinen Schaden an.

Damit kannst du testen, ob der von dir verwendete Virenscanner die Viren erkennt und auch loswird.

⇨ c't Email-Check (Dummyviren)

Zurück zum Inhalt dieses Kapitels

Nach dem Durchsuchen erhältst du einen Report über die Suche.

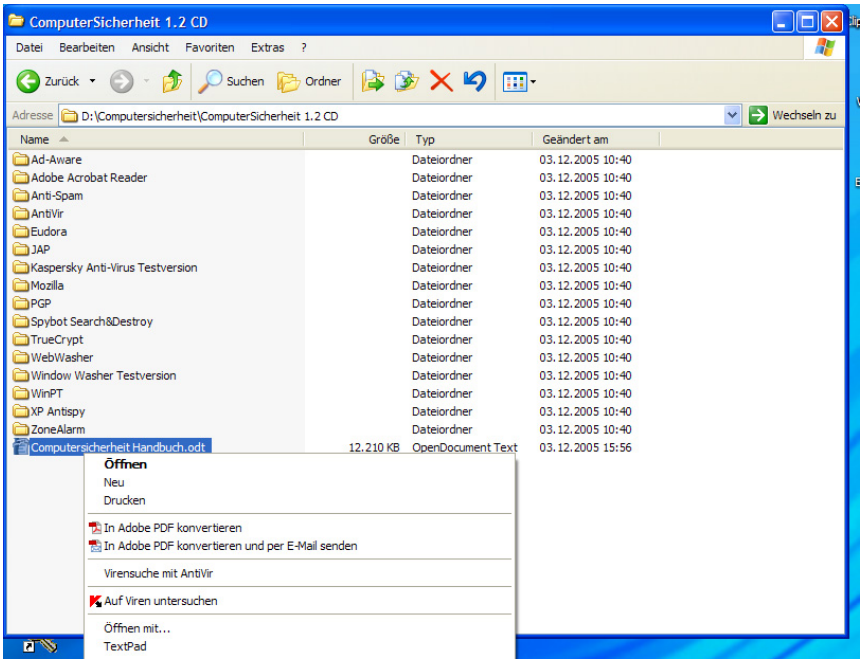
In diesem Beispiel wurden 2.753 Ordner durchsucht, dabei wurde 1 Virus gefunden (den habe ich mir übrigens mittels oben erwähntem E-Mail-Check der Webseite der Zeitschrift c't zuschicken lassen).

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

Zurück zum Inhalt dieses Kapitels

Das Prüfen einzelner Ordner und Dateien

Oft willst nicht ganze Laufwerke durchsuchen, sondern nur einzelne Ordner und/oder Dateien (z.B. eine Datei, die mittels E-Mail geschickt wurde).



Klicke in diesem Fall auf das Symbol „Arbeitsplatz“ auf deinem Windows Desktop. Suche den Ordner oder die Datei, die du prüfen willst und klicke mit der rechten Maustaste auf die Datei oder den Ordner.

Es öffnet sich ein Kontextmenü, ein Menüpunkt ist „Virensuche mit AntiVir“. Wähle diesen Menüpunkt aus.

Es folgt dann sofort der schon beschriebene System- und Selbsttest, dann gleich die Prüfung der von dir gewählten Datei(en).

Zurück zum Inhalt dieses Kapitels

Wurde kein Virus gefunden, erhältst du eine entsprechende Meldung:

Es wurde 1 Datei geprüft und kein Virus gefunden, alles ok.

Zurück zum Inhalt dieses Kapitels

11 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. Mit JAP kannst du wirklich anonym surfen.

Du findest Beschreibungen zu folgenden Bereichen:

- Was ist JAP?
- Die Installation von JAP
- Die Verwendung von JAP
- Was du für Einstellungen im Internet Browser vornehmen musst

Die aktuellste Version von JAP findest du im Internet unter http://anon.inf.tu-dresden.de/

11.1 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 (wir bitten die penetrant männliche Schreibweise zu entschuldigen, wir haben hier den Originaltext übernommen):

„Mit JAP ist es möglich, anonym und unbeobachtbar im Internet zu surfen.

Ohne Anonymisierung kommuniziert jeder Computer im Internet unter einer eindeutigen Adresse. Das bedeutet,

- der besuchte Webserver,
- der Internet-Zugangsprovider,
- jeder Lauscher auf den Verbindungen

kann ermitteln, welche Webseiten vom Nutzer dieser Adresse besucht und, wenn unverschlüsselt kommuniziert wird, welche Informationen abgerufen werden.

Mit JAP benutzen Sie zum Internet-Surfen eine feste Adresse, die Sie sich mit den anderen JAP Nutzern teilen. Dadurch erfährt weder der angefragte Server noch ein Lauscher auf den Verbindungen, welcher Nutzer welche Webseite aufgerufen hat.

Funktion

Die Anonymisierung der Internetzugriffe wird erreicht, indem sich die Computer der Nutzer nicht direkt zum Webserver verbinden, sondern ihre Kommunikationsverbindungen verschlüsselt über einen Umweg mehrerer Zwischenstationen, sogenannter Mixe, schalten.

Da viele Benutzer gleichzeitig diese Zwischenstationen des Anonymitätsdienstes nutzen, werden die Internetverbindungen jedes Benutzers unter denen aller anderen Benutzer versteckt: Niemand, kein Außenstehender, kein anderer Benutzer, nicht einmal der Betreiber des Anonymitätsdienstes kann herausbekommen, welche Verbindungen zu einem bestimmten Benutzer gehören.

Info: Eine Kommunikationsbeziehung kann nur dann aufgedeckt werden, wenn alle Zwischenstationen bzw. deren Betreiber zusammen die Anonymisierung sabotieren.

Im Regelfall werden die Zwischenstationen (Mixe) von unabhängigen Institutionen betrieben, die in einer Selbstverpflichtung erklären, dass sie weder Log-Files über die geschalteten Verbindungen speichern, noch derartige Daten mit den anderen Mix Betreibern austauschen.

Zukünftig werden auch unabhängige Prüfstellen sich im Namen der JAP-Benutzer davon überzeugen, dass die Selbstverpflichtung tatsächlich eingehalten wird.“

Kurz gesagt, deine Internetverbindung muss über diese speziellen 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 etwas langsamer als gewohnt macht.

Zurück zum Inhalt dieses Kapitels

11.2 Die Installation von JAP

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

Für Windows muss nur das Installationsprogramm im entsprechenden Ordner gestartet werden, die JAVA-Umgebung wird nötigenfalls gleich mitinstalliert.

Bei anderen Betriebssystemen muss die JAVA-Umgebung vor der JAP-Installation installiert werden. Anweisungen dazu erhältst du auf der unten angegebenen Webseite.

JAP\Windows

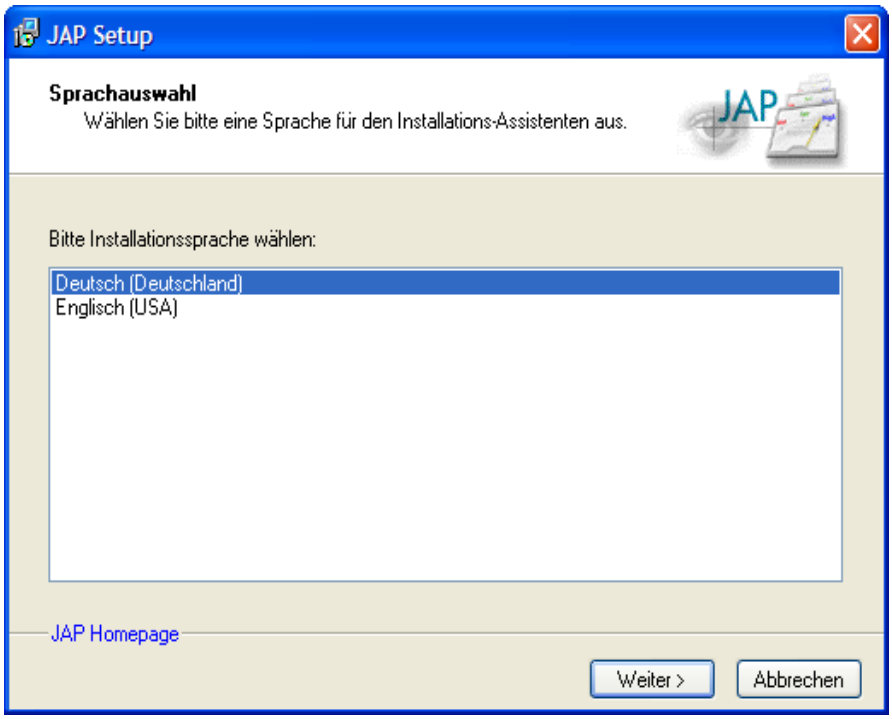
japsetup.exe

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, falls etwas fehlt.

Zurück zum Inhalt dieses Kapitels

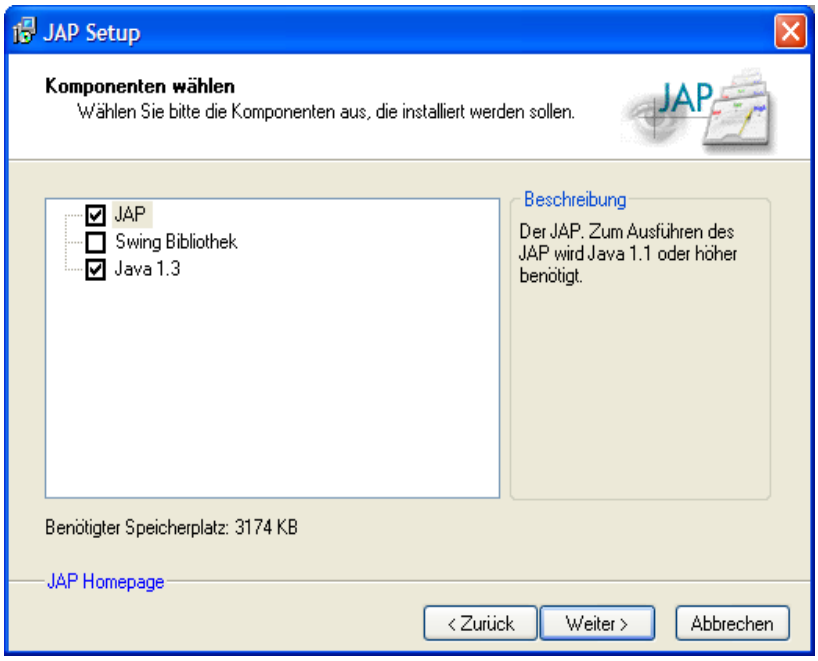
Starte das Installationsprogramm durch Doppelklick auf die Installationsdatei. Zu Beginn kannst du dir die Installationssprache auswählen:



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

Zurück zum Inhalt dieses Kapitels

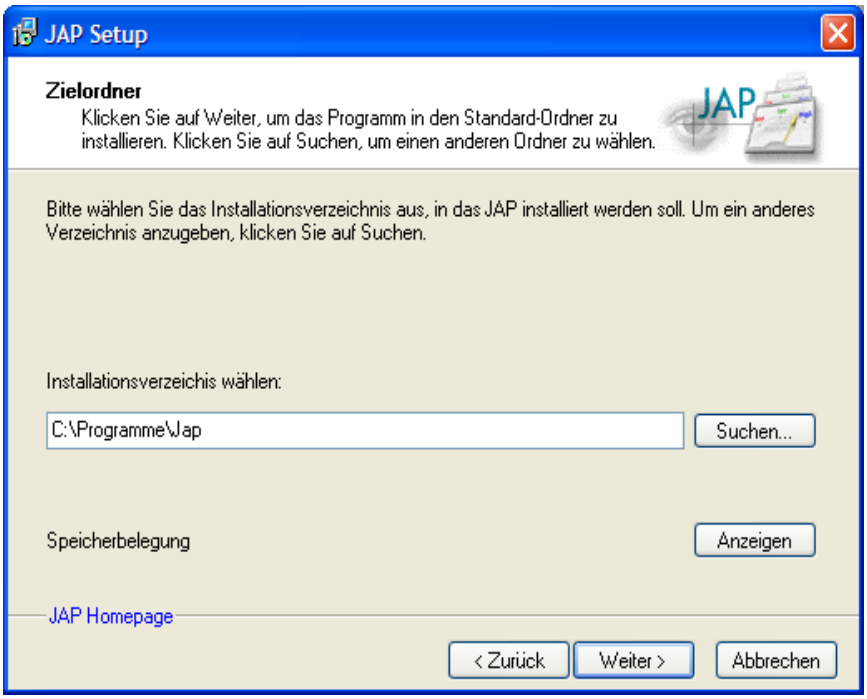
Nun musst du angeben, was du alles installieren willst.



Nimm einfach das Vorgeschlagene und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

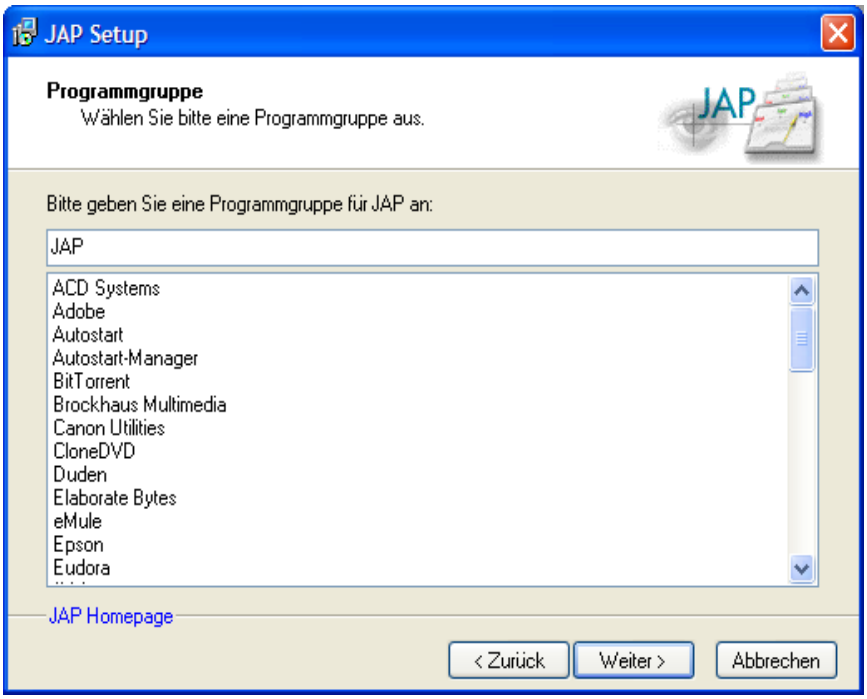
Dann kannst du das Installationsverzeichnis angeben, in welches das Programm installiert werden soll:



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

Zurück zum Inhalt dieses Kapitels

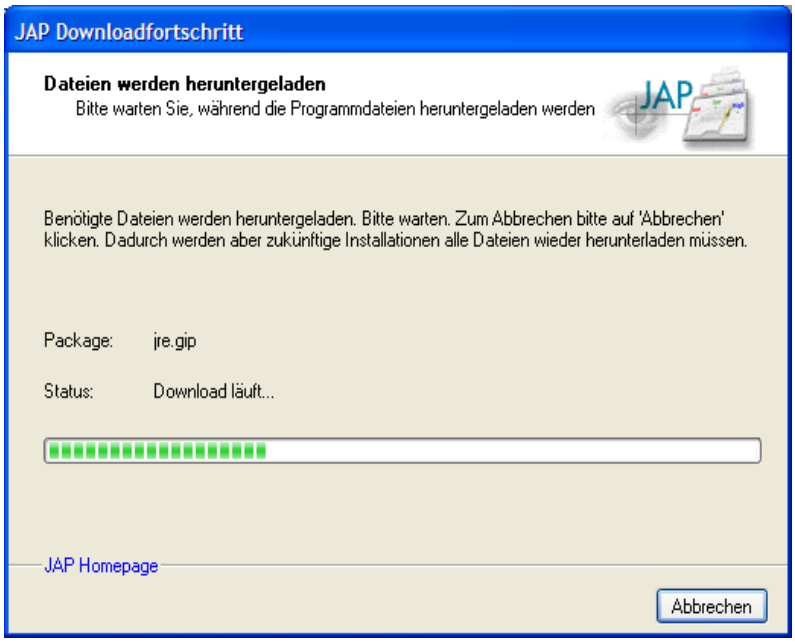
Jetzt kannst du noch angeben, unter welchem Namen das Programm im Start-Menü eingetragen werden soll:



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

Zurück zum Inhalt dieses Kapitels

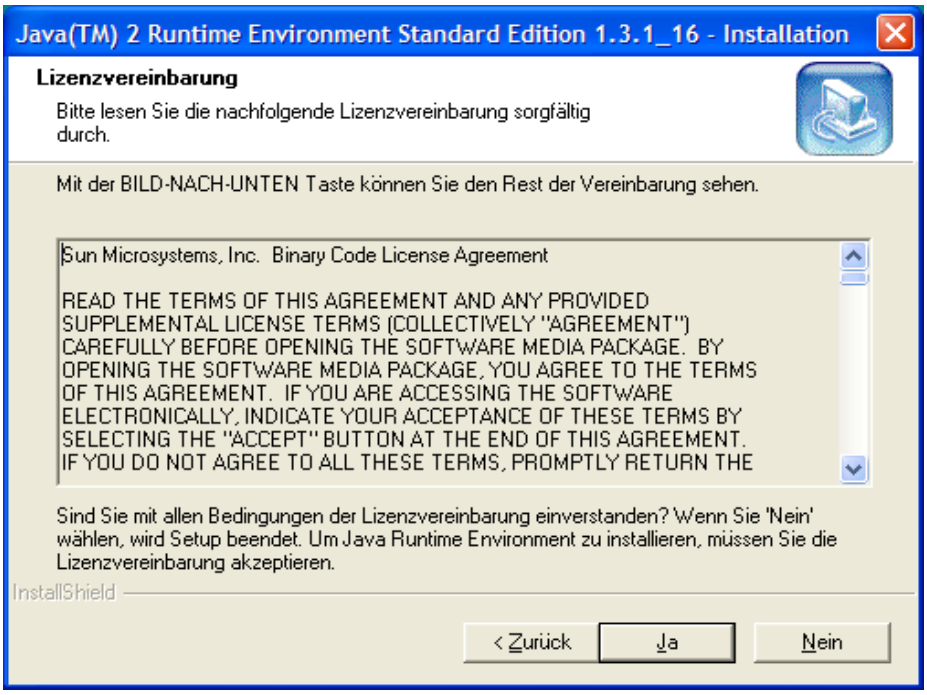
Nun wird das Programm installiert:



Du siehst im Fenster, was das Programm gerade tut.

Zurück zum Inhalt dieses Kapitels

Wenn du auch Java mitinstallierst, musst du den Lizenzbedingungen für Java zustimmen.



Drücke den Button „Ja“.

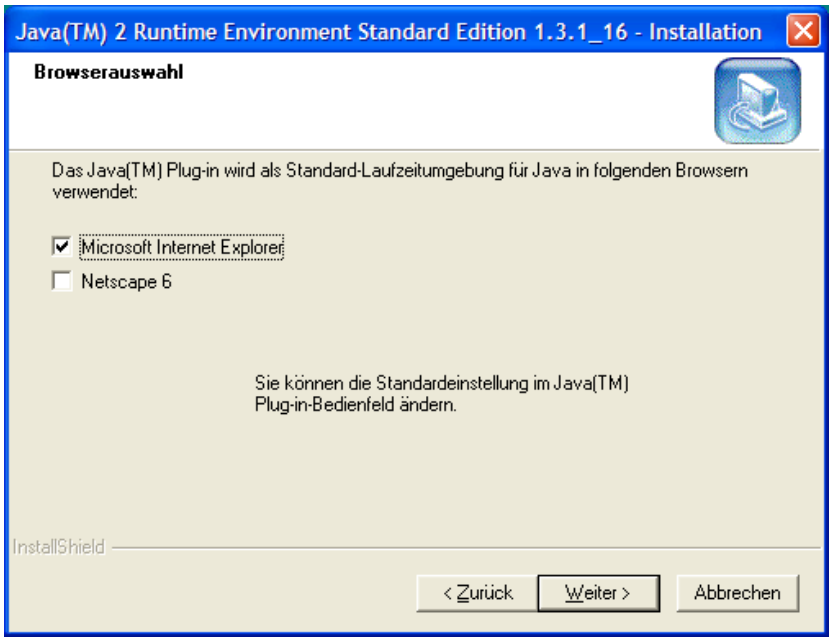
Zurück zum Inhalt dieses Kapitels

Auch hier kannst du dir das Verzeichnus aussuchen, in das Java installiert wird:

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

Zurück zum Inhalt dieses Kapitels

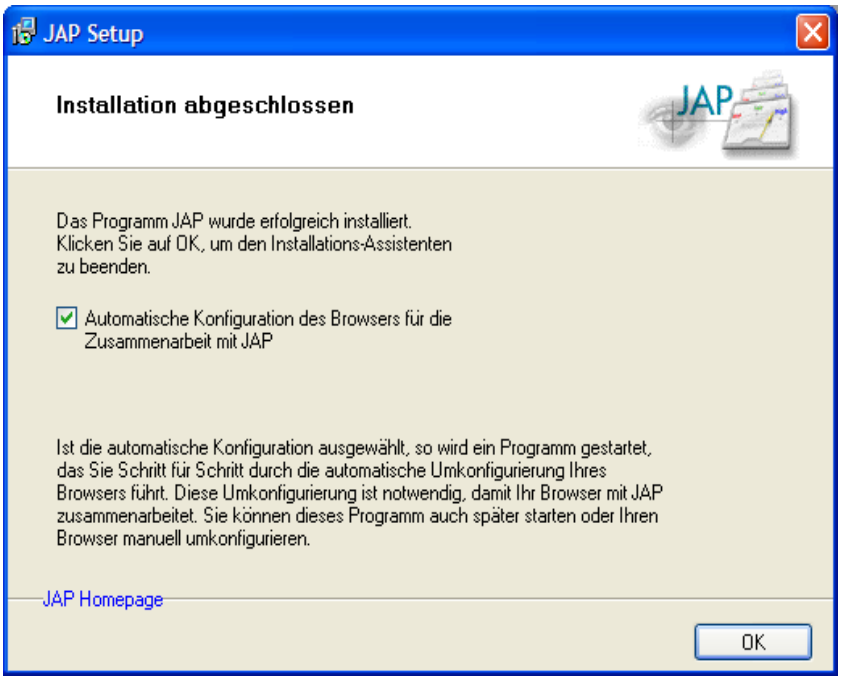
Dann erhältst du noch eine Information, von welchen Internet Browsern diese Java-Version verwendet werden kann.



Drücke einfach den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Nach dem Ende des Installationsvorgangs wirst du darüber informiert, dass es fertig ist:



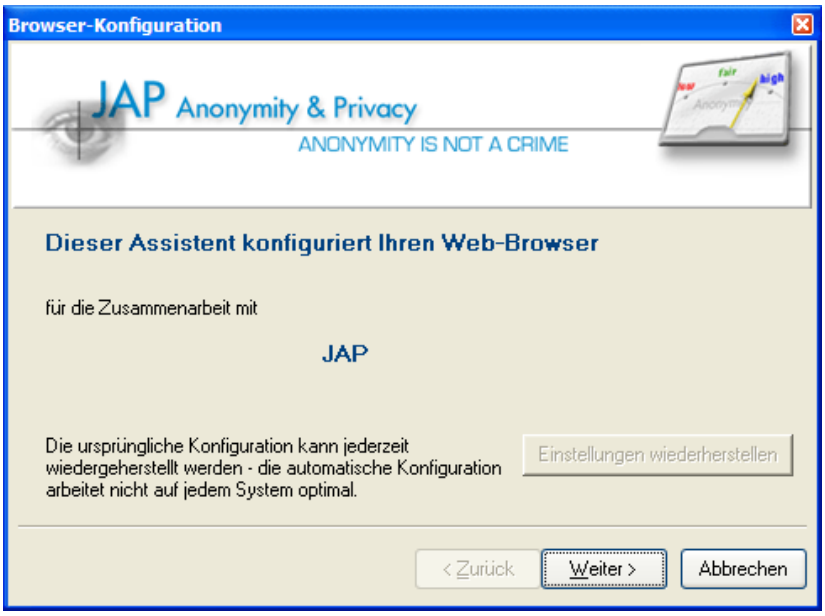
Du kannst dir aussuchen, ob du die Konfiguration der Internet-Browser gleich vornehmen willst. Wenn du das willst, lasse den Punkt „Starten der automatischen Konfiguration“ angekreuzt.

Wenn du das nicht willst und die Einstellungen wie in den nächsten Kapiteln beschrieben vornehmen willst, entmarkiere den Punkt.

Bestätige die Meldung durch Drücken des Buttons „OK“.

Zurück zum Inhalt dieses Kapitels

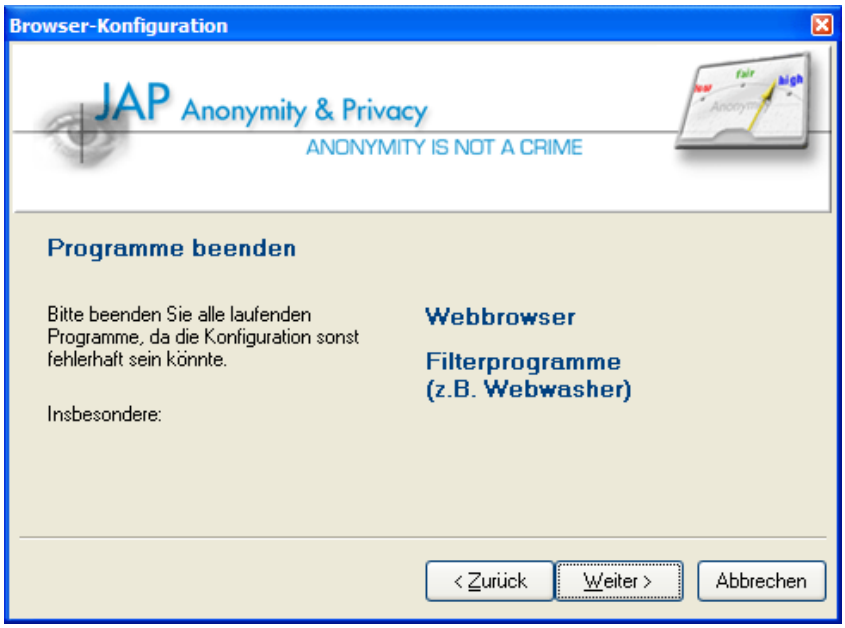
Da wir im Beispiel den Punkt „Starten der automatischen Konfiguration“ angekreuzt angekreuzt haben, geht es gleich weiter mit dem Konfigurieren der Internet-Browser.



Bestätige die Information durch Drücken des Buttons „Weiter“.

Zurück zum Inhalt dieses Kapitels

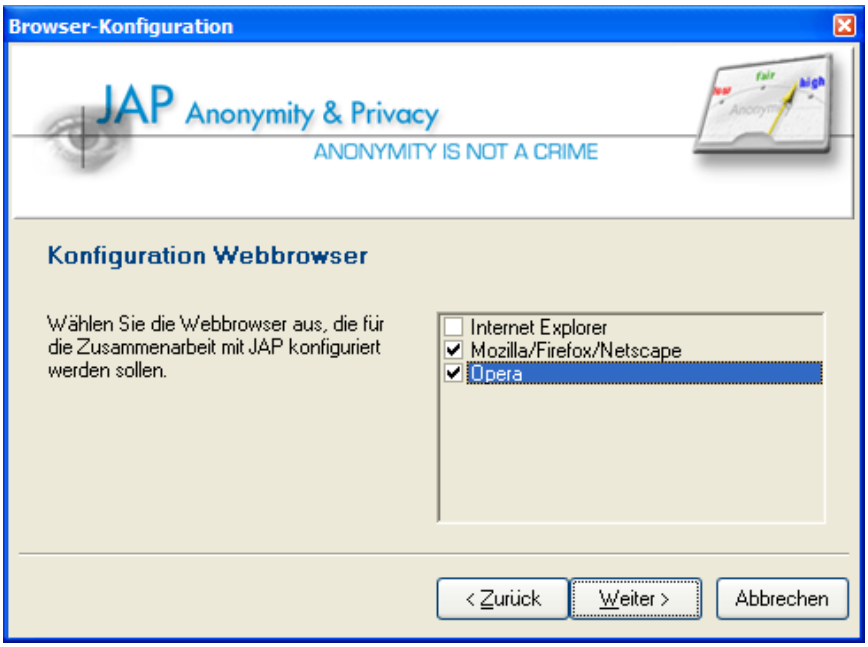
Nun erhältst du noch einen Hinweis, dass du andere Programme schließen sollst.



Falls du einen Internet-Browser geöffnet hast, schließe ihn. Drücke dann „Weiter“.

Zurück zum Inhalt dieses Kapitels

Du erhältst nun eine Liste von Browsern, die du konfigurieren kannst:



Markiere die zu konfigurierenden Browser und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Gleich danach erscheint ein Fenster mit der Mitteilung, dass die Konfiguration der gewählten Browser durchgeführt wurde.

Ein wichtiger Hinweis bezieht sich auf die Möglichkeit zu prüfen, ob JAP im Internet Browser korrekt funktioniert. Das wird auch im nächsten Kapitel dieses Handbuchs beschrieben.

Lies dir die Information durch und drücke den Button „Beenden“.

Auf der Homepage von JAP http://anon.inf.tu-dresden.de/ findest du einiges an Informationen zu dieser Art von Anonymisierung. Weiters findest du Beschreibungen und Hilfe zum Programm selbst.

Zurück zum Inhalt dieses Kapitels

11.3 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 deines jeweiligen Internet-Browser ändern, falls das nicht automatisch bei der Installation geschehen ist.

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

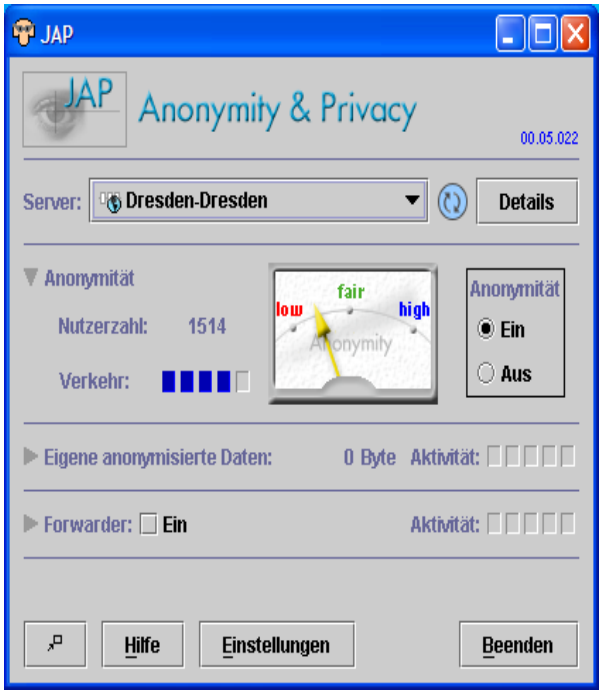
Eine Möglichkeit ist, Opera als Browser zu verwenden, bei Opera kannst du ganz einfach im Menü zwischen der Verwendung dieses Proxy Servers von JAP und dem normalen Internetzugang ohne Proxy Server hin- und herwechseln.

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

Das Starten von JAP / Einstellungen

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

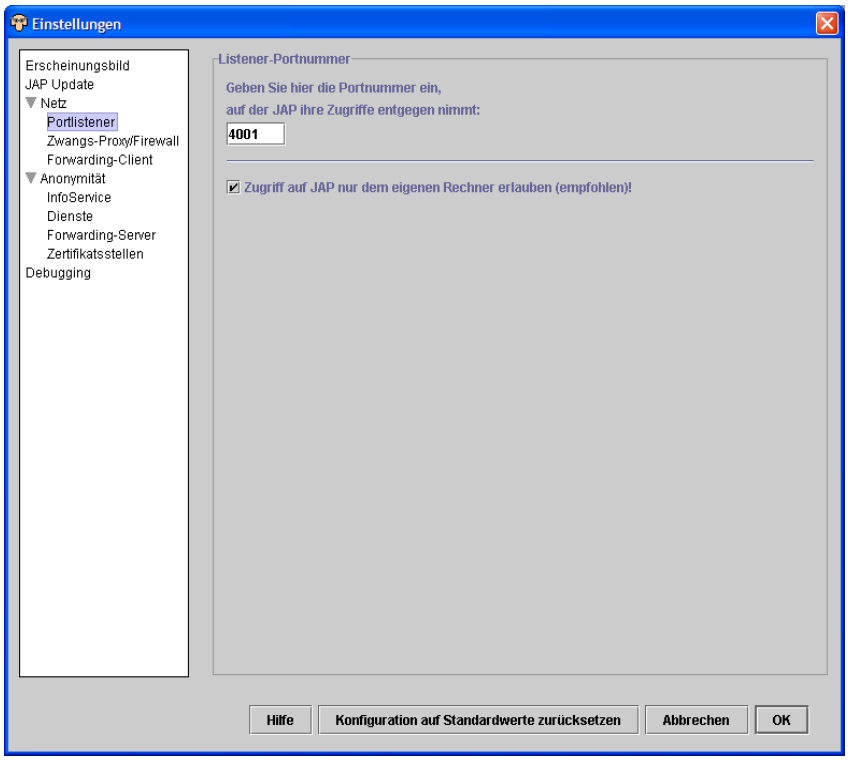


Das Programm verbindet sich sofort mit einem der Anonymisierungsdienst (hier mit dem Dienst in Dresden). Wenn bei „Anonymität“ der Punkt „Ein“ ausgewählt ist, bist du mit dem Anonymisierungsdienst verbunden.

Nun ist alles klar zum anonymen Surfen, wenn du die in den nächsten Kapiteln beschriebenen Einstellungen des Proxy Servers vorgenommen hast (siehe auch Kapitel Einstellungen im Browser).

Zurück zum Inhalt dieses Kapitels

Du benötigst noch Informationen, die nach Drücken des Buttons „Einstellungen“ angezeigt werden.



Wähle im Menü links den Punkt „Portlistener“.

Hier siehst du die Angabe des Ports, an dem das Programm JAP nach seinem Start lauscht, ob es Anforderungen eines Internet-Browsers gibt. Es ist die Nummer, über die JAP mit deinem Internet-Browser kommuniziert.

Du kannst diese vorgeschlagene Nummer 4001 belassen oder auch eine andere auswählen. Du musst dir diese Nummer auf jeden Fall merken. Drücke dann den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Einstellungen im Internet 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.

Du findest Anleitungen zu folgenden Internet Browsern:

- Firefox
- Opera
- Microsoft Internet Explorer

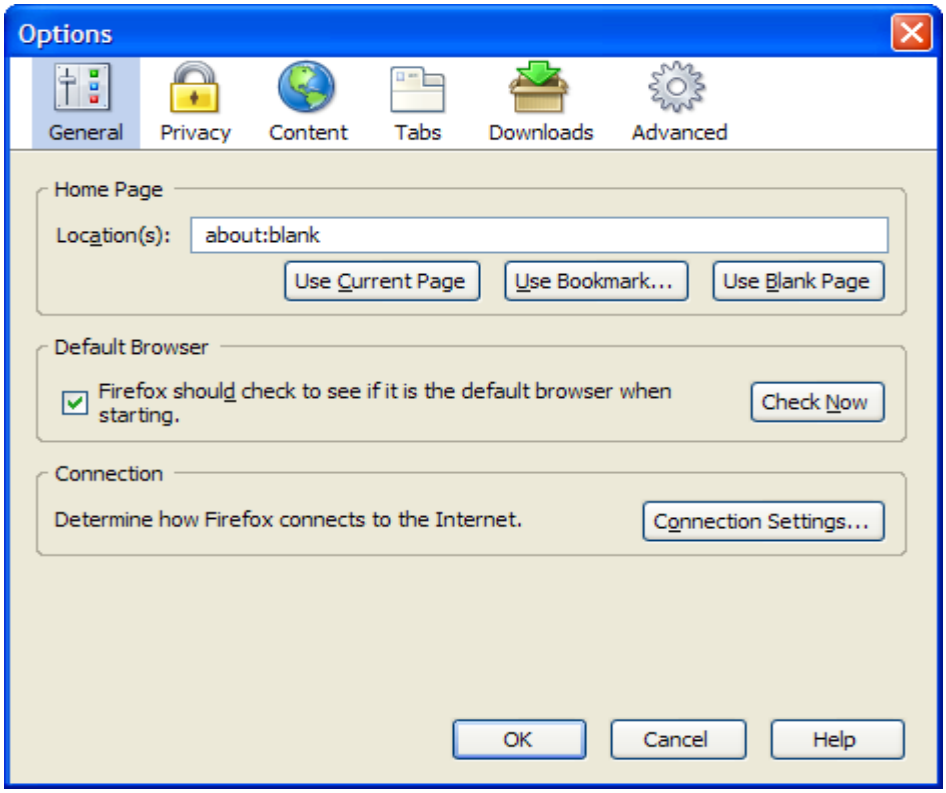
Weiters findest du Informationen, wie du das Funktionieren der Verbindung mit dem Anonymisierungsdienst überprüfen kannst:

- Die Kontrolle der anonymen Verbindung

Zurück zum Inhalt dieses Kapitels

Firefox

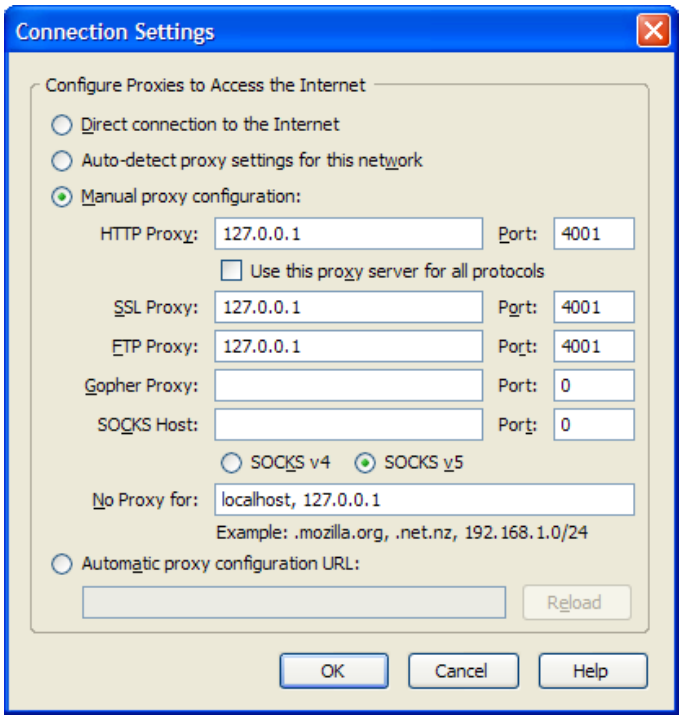
Im Menü findest du unter Tools ⇨ Options die benötigten Einstellungen.



Drücke den Button „Connection Settings...“.

Zurück zum Inhalt dieses Kapitels

Das Fenster mit den Verbindungs-Einstellungen wird geöffnet:



Wähle „Manual proxy configuration“ aus und trage als HTTP Proxy 127.0.0.1 (das ist dein eigener Computer) und als Port 4001 (bzw. das in der JAP-Konfiguration angegebene, das du dir gemerkt hast) ein, drücke dann den Button OK.

Schließe dann das Hauptfenster ebenfalls durch Drücken des Buttons „OK“.

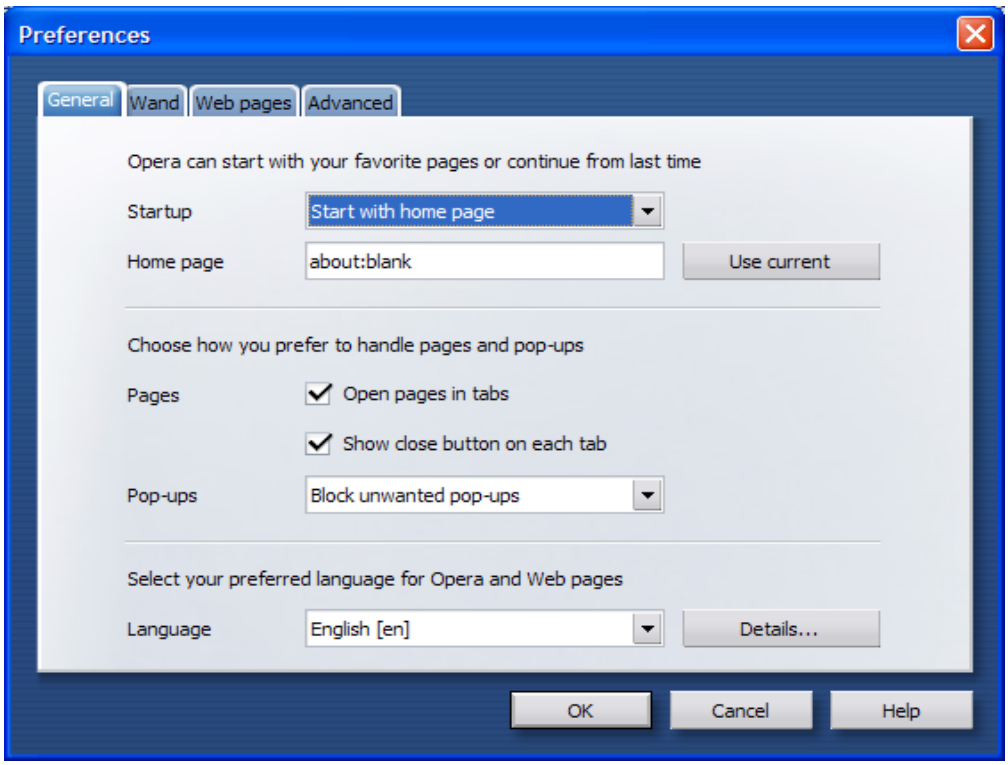
Mit dieser Einstellung kannst du nur mehr mit dem Programm JAP surfen. Wenn JAP nicht gestartet wurde, bekommst du mit dieser Einstellung keine Verbindung mehr zum Internet.

Wenn du ohne Verwendung von JAP surfen willst, musst du im gleichen oben abgebildeten Fenster „Direct Connection to the Internet“ statt „Manual proxy configuration“ auswählen. Dann kannst du wieder normal ohne JAP und damit nicht anonym surfen.

Zurück zum Inhalt dieses Kapitels

Opera

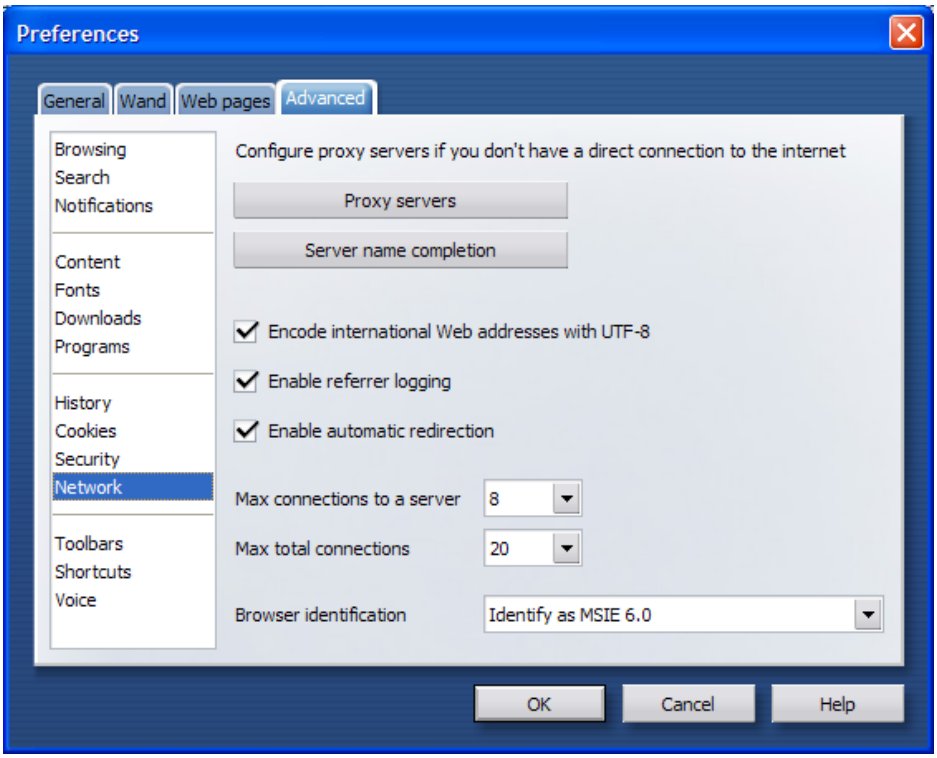
Wähle im Menü den Punkt „Tools ⇨ Preferences“, es geht dann folgendes Fenster auf:



Wähle den Punkt „Advanced“ und dann „Network“ auf der linken Seite.

Zurück zum Inhalt dieses Kapitels

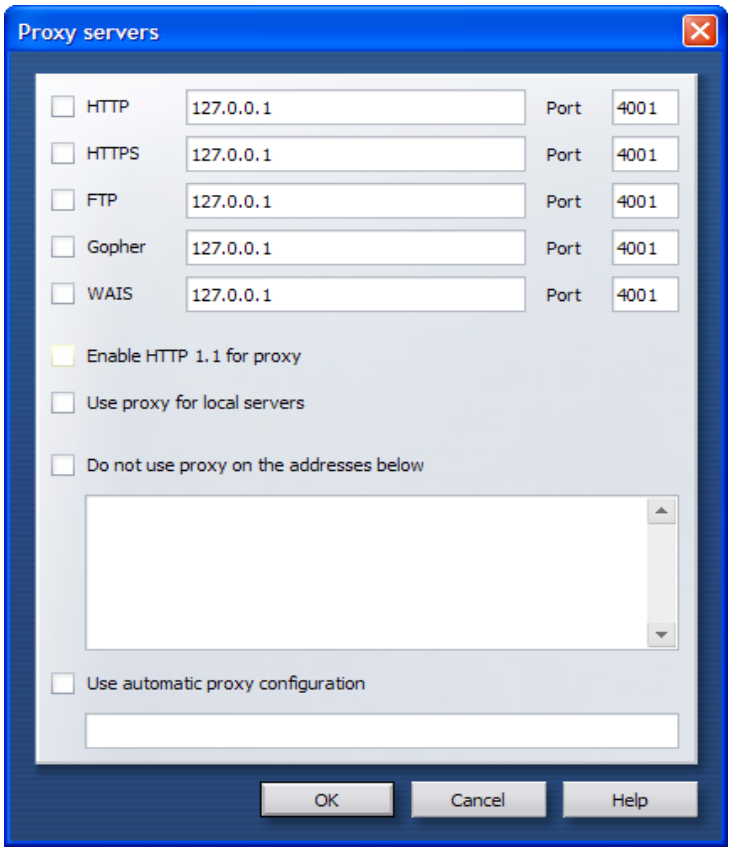
Wähle den Punkt „Advanced“.



Drücke jetzt den Button „Proxy servers“.

Zurück zum Inhalt dieses Kapitels

Es erscheint ein weiteres Fenster, in dem du die Einstellungen eingeben kannst. Hier kannst du die Portnummer angeben:

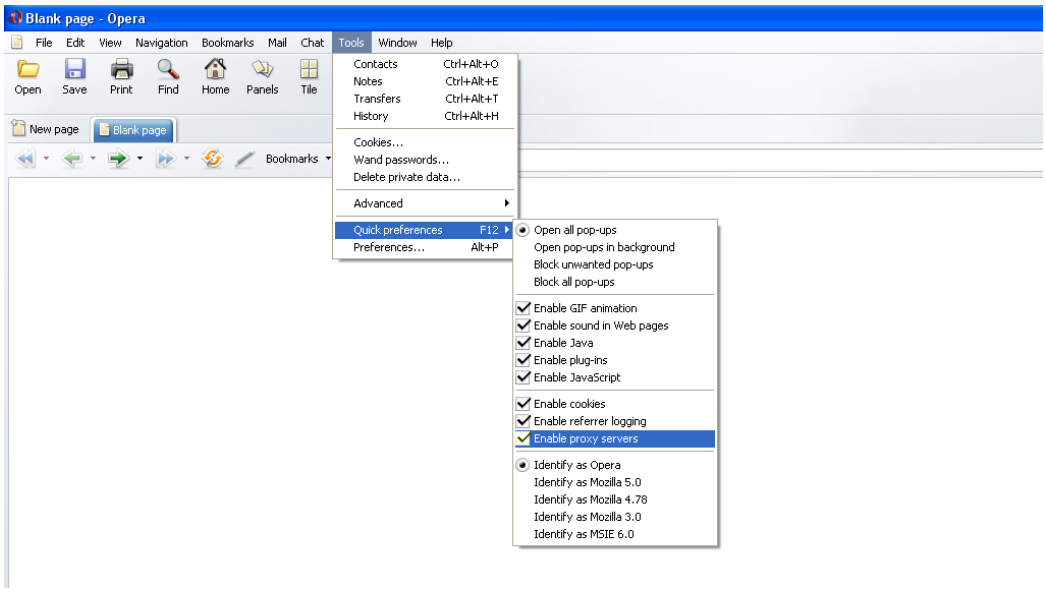


Falls das noch nicht geschehen ist, trage unter HTTP 127.0.0.1 und als Port 4001 (bzw. das bei der JAP-Konfiguration angegebene, das du dir gemerkt hast) ein, drücke dann den Button OK.

Schließe dann das Konfigurationsfenster ebenfalls durch Drücken des Buttons „OK“.

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 (zum anonymen Surfen) und der Nichtverwendung (zum nicht anonymen Surfen) hin- und herschalten kann.



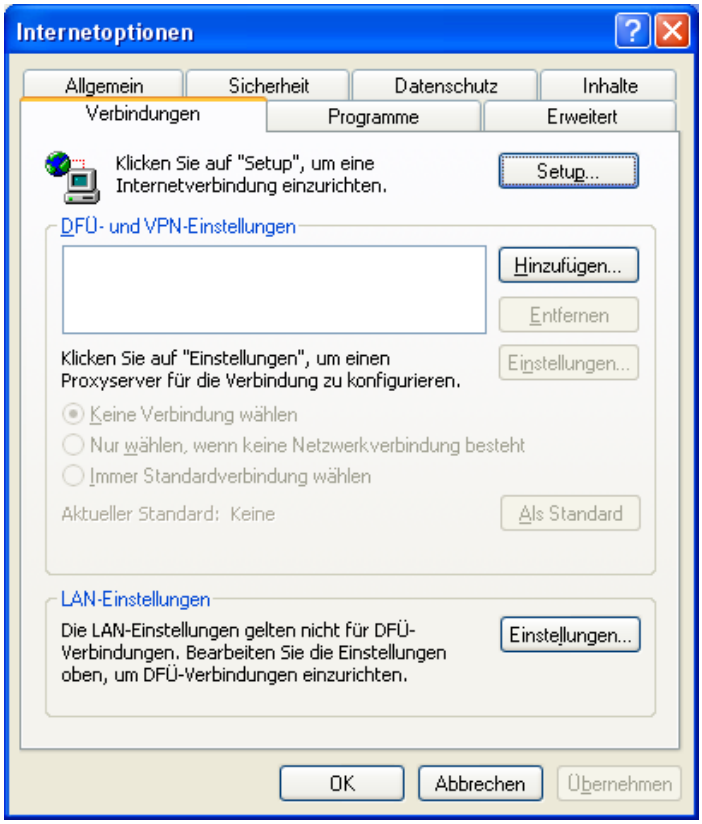
Jedes Mal, wenn du den Menüpunkt Tools ⇨ Quick preferences ⇨ Enable proxy servers wählst, wird die Verwendung des Proxy Serves aus- bzw. eingeschaltet.

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

Microsoft Internet Explorer 6

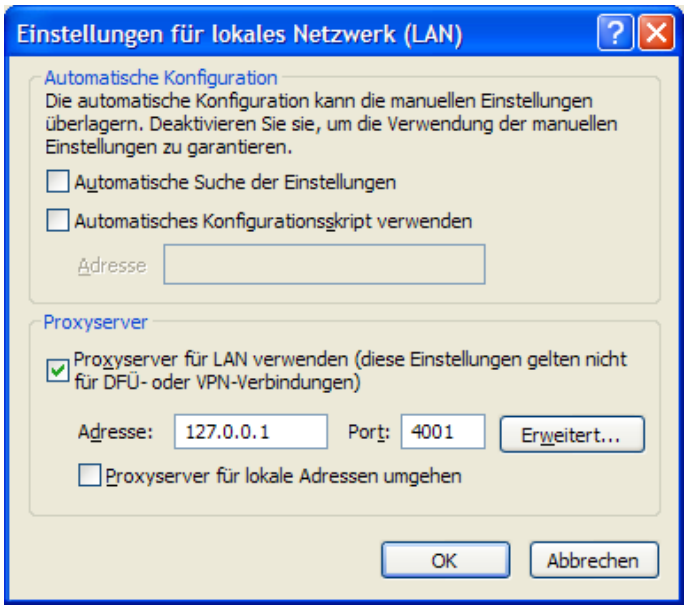
Im Menü findest du unter „Extras ⇨ Internetoptionen“ in der Karteikarte „Verbindungen“ Einstellungsmöglichkeiten für Modem- und für Kabel(LAN)-Verbindungen.



Drücke den Button „Einstellungen...“.

Zurück zum Inhalt dieses Kapitels

Es wird ein Fenster geöffnet, in dem du die Portnummer angeben kannst:



Hake „Proxyserver für LAN verwenden an und trage als Adresse 127.0.0.1 oder – wie von JAP automatisch eingefügt – localhost und als Port 4001 (bzw. das in der JAP-Konfiguration angegebene, das du dir gemerkt hast) 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.

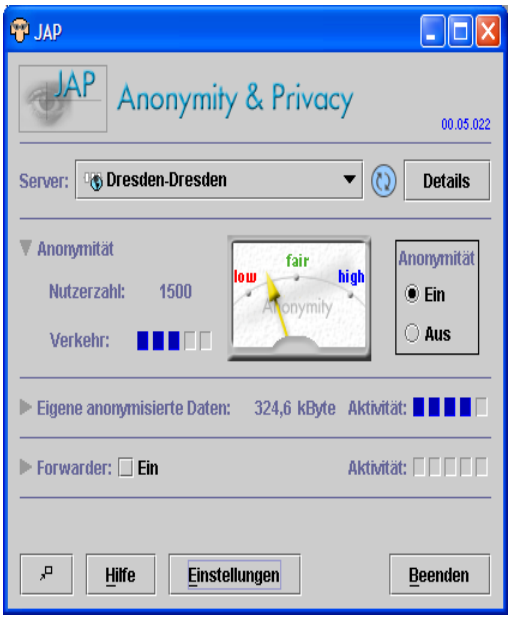
Wenn du ohne Verwendung von JAP surfen willst, musst du im gleichen oben abgebildeten Fenster das Kreuzchen bei „Proxyserver für LAN verwenden“ wegklicken. Dann kannst du wieder normal ohne JAP und damit nicht anonym surfen.

Zurück zum Inhalt dieses Kapitels

Die 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:

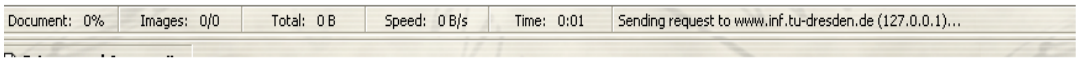


Wenn du eine Webseite aufrust, sollte sich rechts neben der Beschriftung „Eigene anonymisierte Daten: Aktivität" etwas tun, das Übertragungsvolumen wird größer bzw. behält nach dem fertigen Laden einer Seite einen bestimmten Wert. Das zeigt, dass du über den Anonymisierungsdienst surfst.

Zurück zum Inhalt dieses Kapitels

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:



Auch der Anonymisierungsdienst (hier im Beispiel die Uni Dresden) wird zumindest kurz angezeigt.

Zurück zum Inhalt dieses Kapitels

12 Ad-Aware

Überblick

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

Solche Spyware ist meist in Programmen integriert, die du installierst. Meist weißt du gar nicht, dass dieses Programm Spyware beinhaltet. Diese Programmteile schicken dann 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 (wie das nachfolgend ebenfalls vorgestellte Programm Spybot) nach solchen Programmen, du kannst dir bei Auffinden eines solchen Programms bzw. einer solchen Einstellung aussuchen, ob dieser Teil des Programms bzw. das gesamte Spyware-Programm gelöscht werden soll oder nicht.

Du solltest das Programm hin und wieder laufen lassen, zumindest dann, wenn du ein neues Programm installiert hast. Im Doppelpack mit dem Programm Spybot ist Ad-Aware bei der Beseitigung von Spyware sehr gründlich.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Ad-Aware
- Die Verwendung von Ad-Aware

Die aktuellste Version von Ad-Aware findest du im Internet unter http://www.lavasoft.com/software/adaware/

12.1 Die Installation von Ad-Aware

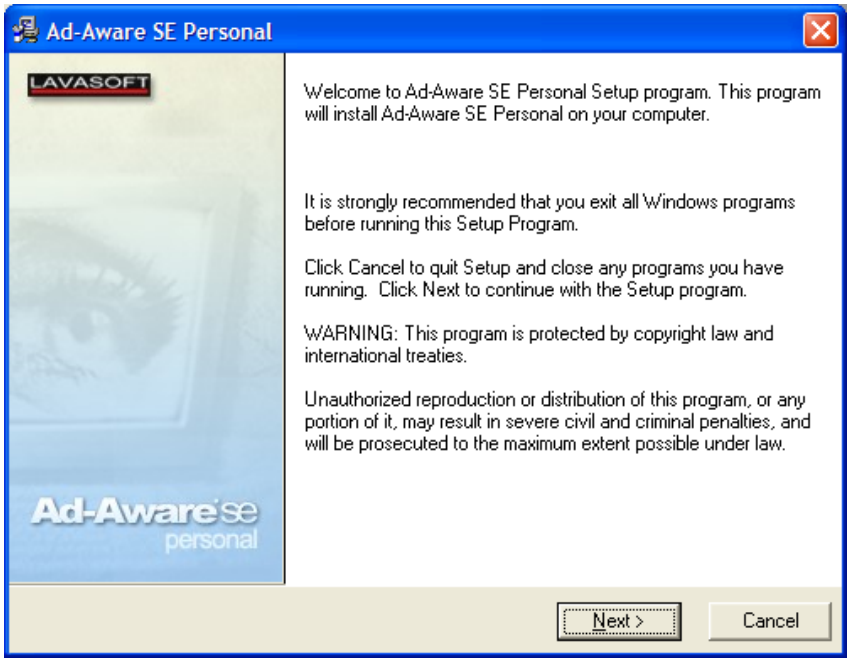
Die Installation von Ad-Aware ist denkbar einfach. Starte das Installationsprogramm durch Doppelklick auf das Programm aawsepersonal.exe im Ordner Ad-Aware\Windows auf der CD.

Ad-Aware/Windows

aawsepersonal.exe

pllangs.exe (optional: verschiedene Sprachen für die Oberfläche des Programms, z.B. Deutsch)

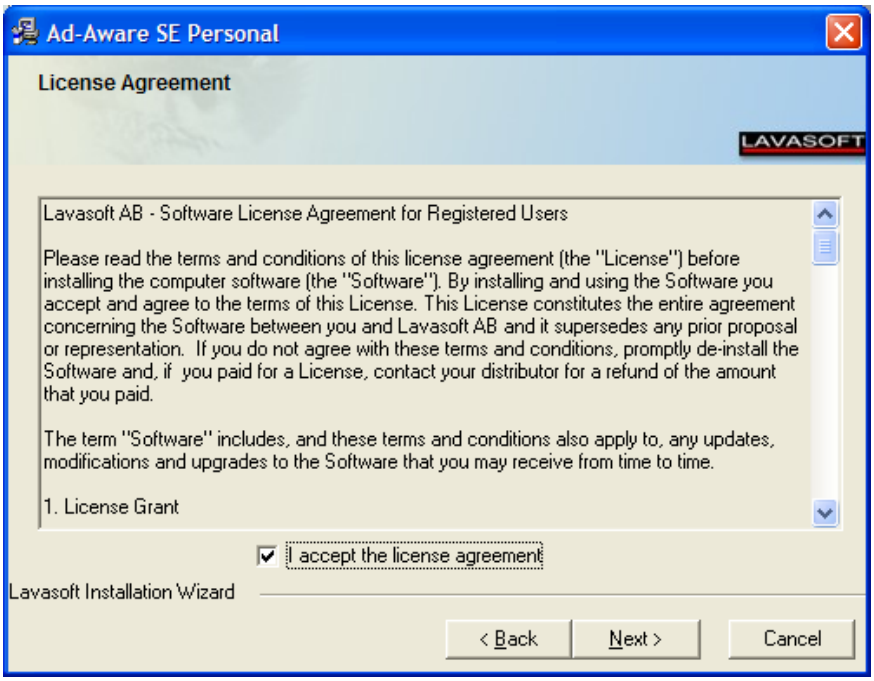
Nach dem Start des Installationsprogramms erscheint ein Begrüßungsfenster:



Drücke auf den Button „Next“.

Zurück zum Inhalt dieses Kapitels

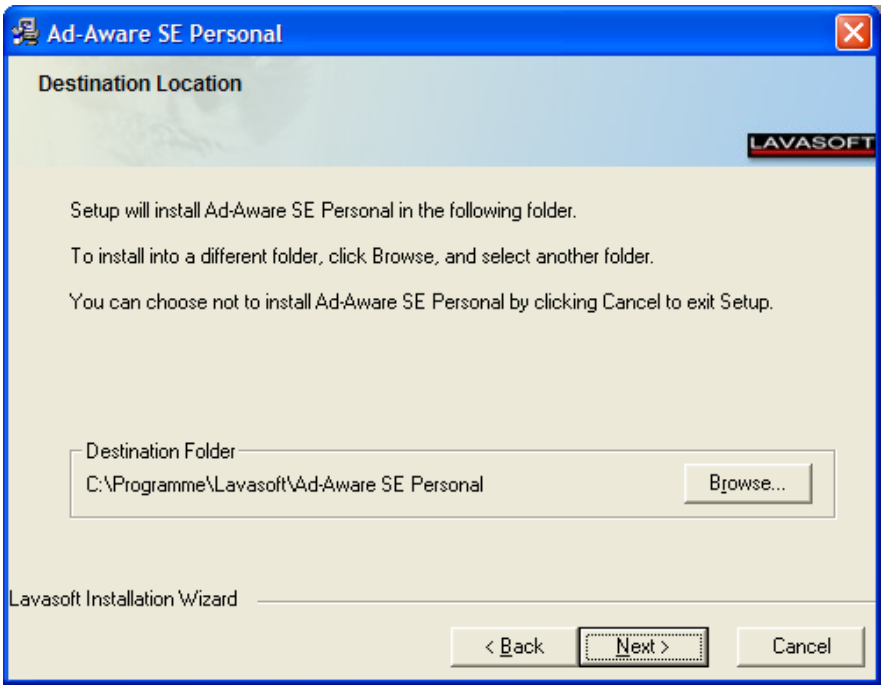
Es folgt die Lizenzvereinbarung:



Natürlich liest du dir alles gut durch, hake dann das Kästchen bei „I accept the license agreement“ an und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

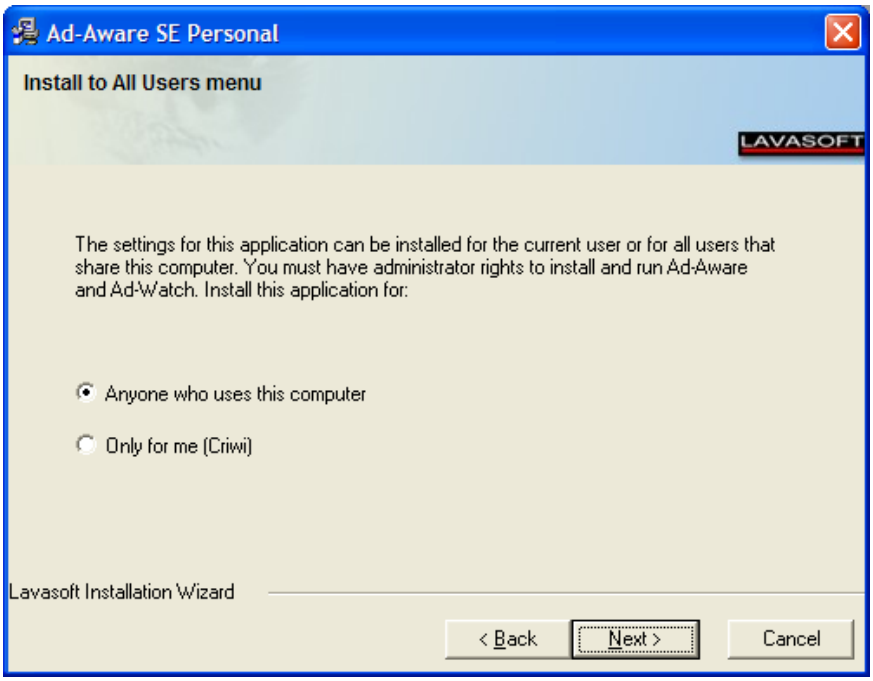
Jetzt kannst du dir den Ordner aussuchen, in dem das Programm installiert werden soll:



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

Zurück zum Inhalt dieses Kapitels

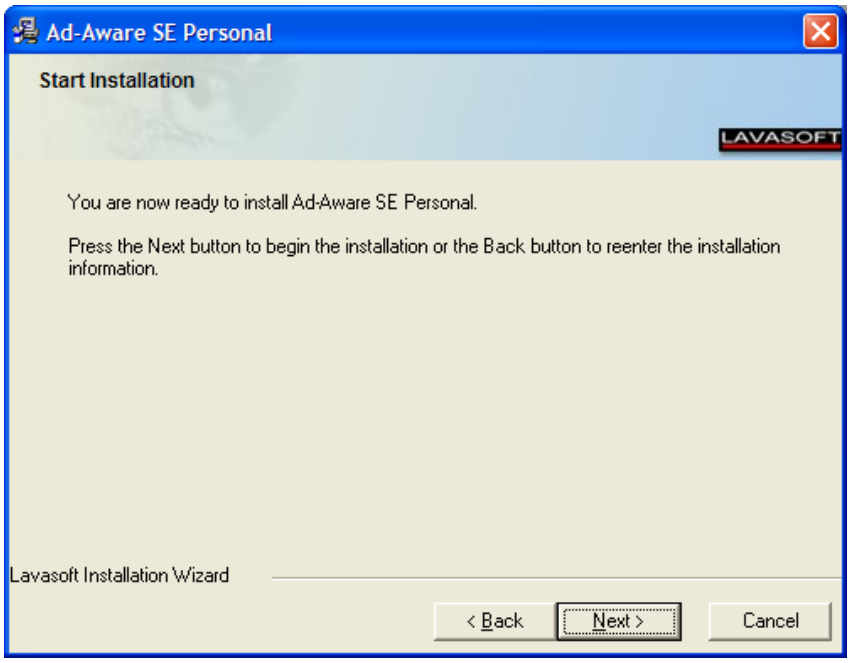
Jetzt kannst du angeben, ob jedeR BenutzerIn deines Computers das Programm verwenden darf oder nur du selbst:



Gib das Gewünschte an und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

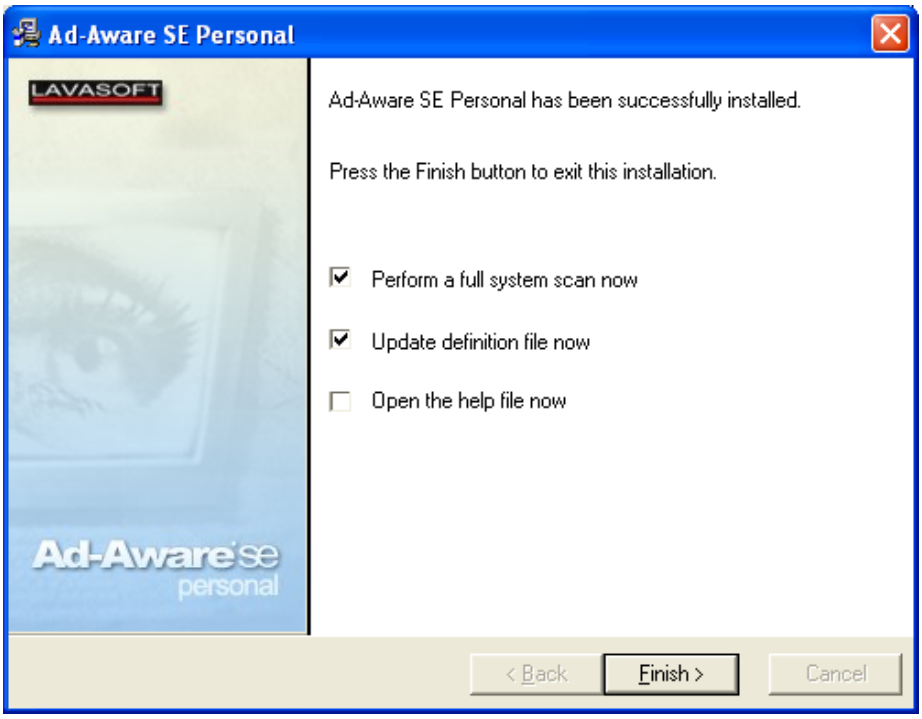
Vor der wirklichen Installation erscheint noch ein Hinweis, dass alles für die Installation bereit ist:



Drücke einfach den Button „Next“ und schon geht’s los mit der Installtion.

Zurück zum Inhalt dieses Kapitels

Nach ein paar Sekunden ist die Installation abgeschlossen:



Du kannst nun gleich

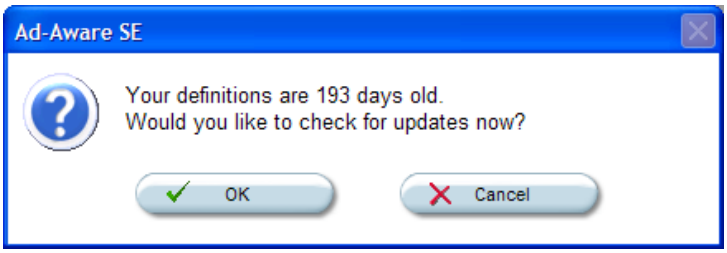
- Die neueste Definitionsdatei von Lavasoft laden („Update definition file now“)
- Deinen Computer nach Spyware durchsuchen lassen („Perform a full system scan now“)

Die Definitionsdatei mit der Liste aller bedenklichen Programme und Einstellungen musst du regelmäßig aus dem Internet laden. Das geht ganz einfach. Wie es geht, erfährst du in Kürze.

Markiere die beiden Punkte „Perform a full system scan now“ und „Update definition file now“. Drücke dann den Button „Finish“.

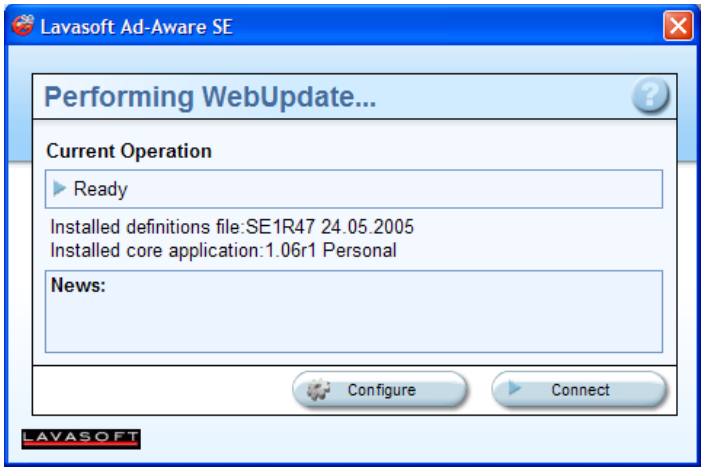
Zurück zum Inhalt dieses Kapitels

Du wirst nun gefragt, ob du die neuesten Definitionsdateien laden willst:



Das willst du natürlich, drücke den Button „OK“.

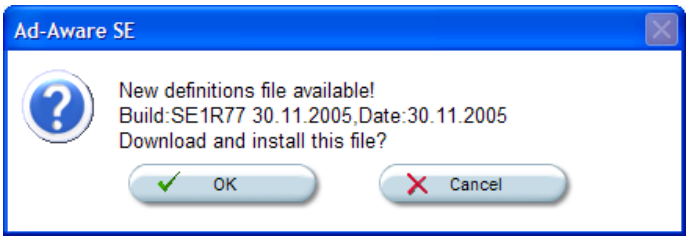
Nun geht ein Fenster auf, mit dem du das Herunterladen starten kannst:



Drücke den Button „Connect“.

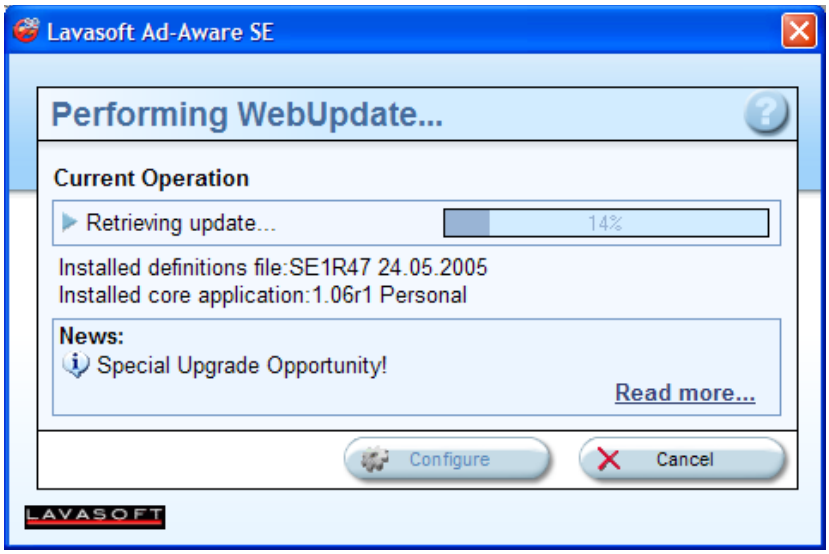
Zurück zum Inhalt dieses Kapitels

Jetzt wird geprüft, ob neue Definitionsdateien verfügbar sind. Werden neuere Versionen gefunden, erscheint folgendes Fenster:



Drücke den Button „OK“ zum Starten des Downloads.

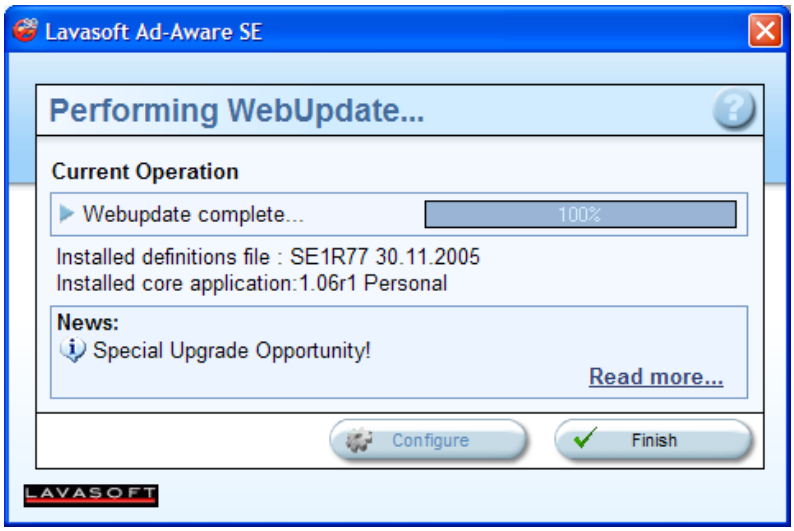
Nun wird endlich die neueste Definitionsdatei aus dem Internet geladen:



Du bekommst den Fortschritt angezeigt.

Zurück zum Inhalt dieses Kapitels

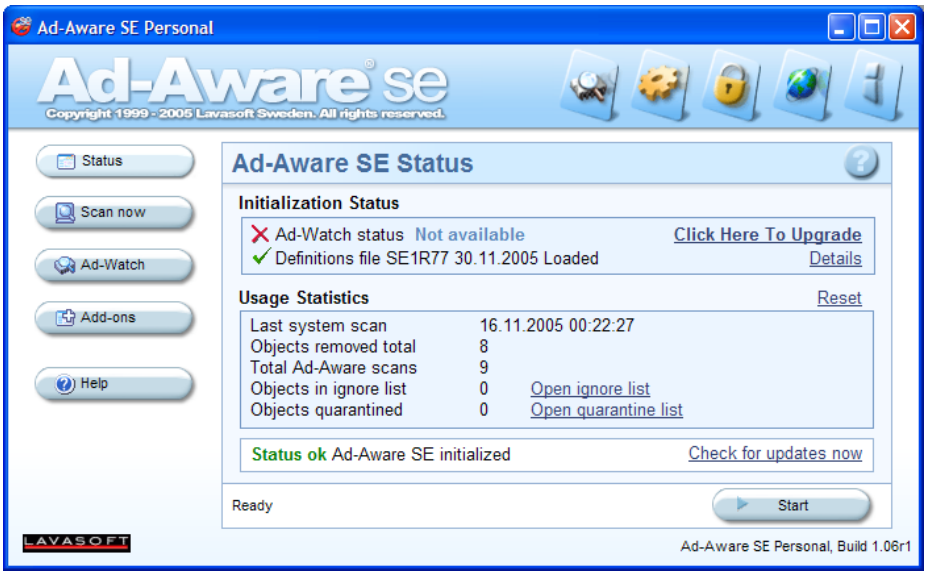
Nach dem Laden der Definitionsdatei erhältst du folgende Erfolgsmeldung:



Drücke den Button „Finish“ zum Schließen des Fensters.

Zurück zum Inhalt dieses Kapitels

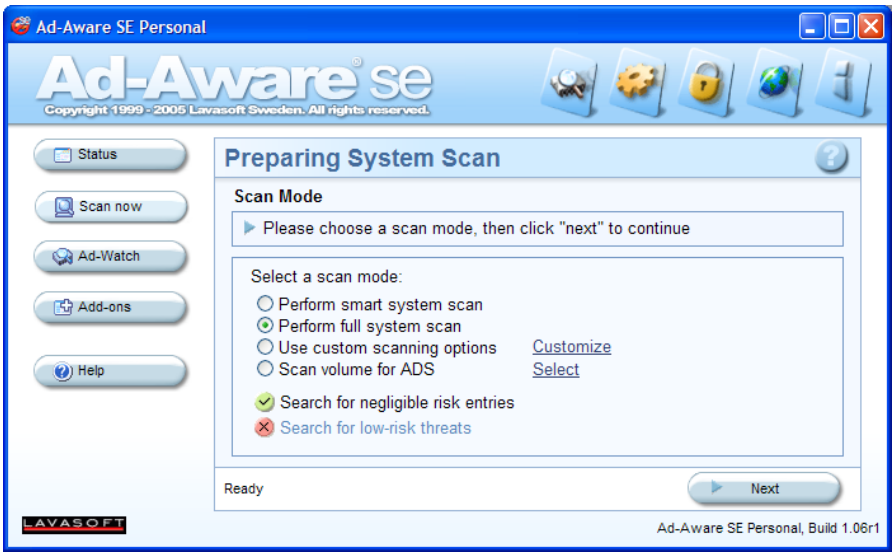
Nun erscheint das Hauptfenster von Ad-Aware:



Drücke den Button „Start“ zum Starten der Prüfung deines Computers (des „Scans“ deines Computers).

Zurück zum Inhalt dieses Kapitels

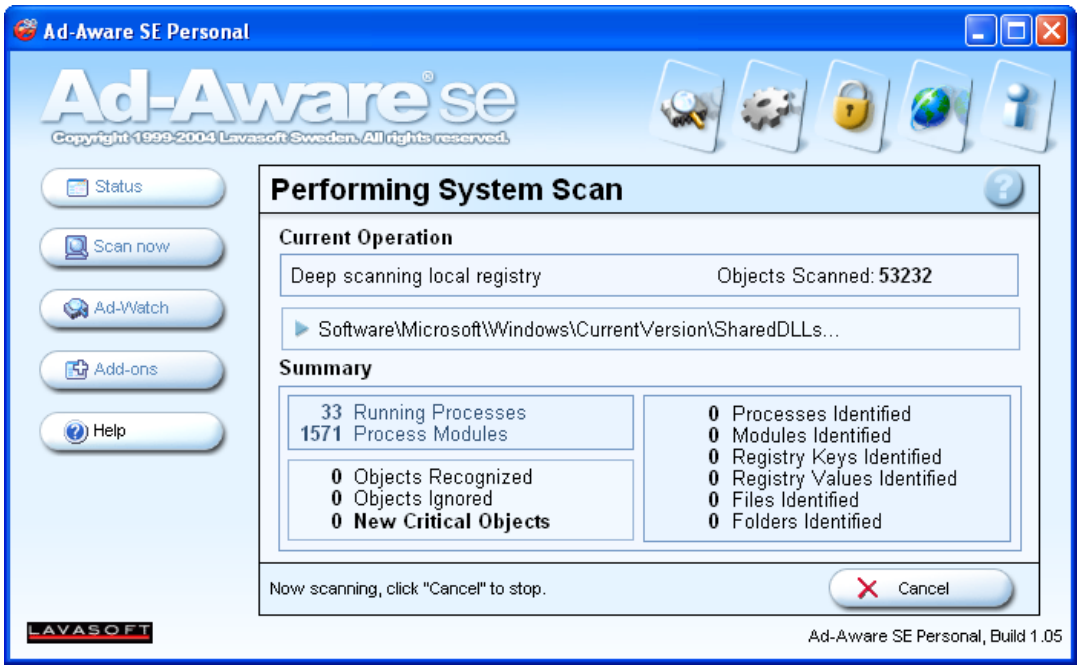
Du kannst dir noch die Art und Weise (die Gründlichkeit) aussuchen, mit der dein Computer gecheckt wird:



Wähle „Perform full system scan“ und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Du bekommst den Fortschritt der Prüfung angezeigt:



Und dieses Scannen kann jetzt eine Weile dauern, natürlich abhängig von der Anzahl und Größe der auf deinem Computer installierten Programme bzw. der Größe deiner Registry.

Wenn's dir gerade zu lange dauert, kannst du den Vorgang jederzeit durch Drücken des Buttons „Cancel" abbrechen.

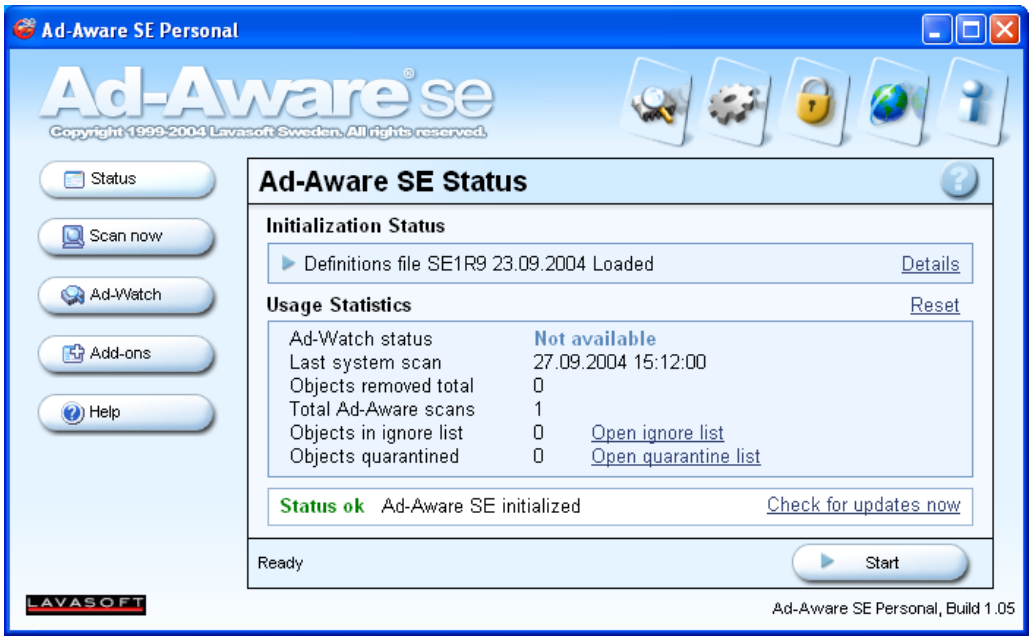
Wenn du durchhältst (und z.B. in dieser Zeit dein nächtliches Schlafbedürfnis befriedigst) und bedenkliche Programme und/oder Einstellungen gefunden wurden, kannst du diese anschließend entfernen lassen. Wie das geht, erfährst du am Ende des nächsten Kapitels.

Zurück zum Inhalt dieses Kapitels

12.2 Die Verwendung von Ad-Aware

Das Laden von neuen Definitionsdateien und Programmversionen

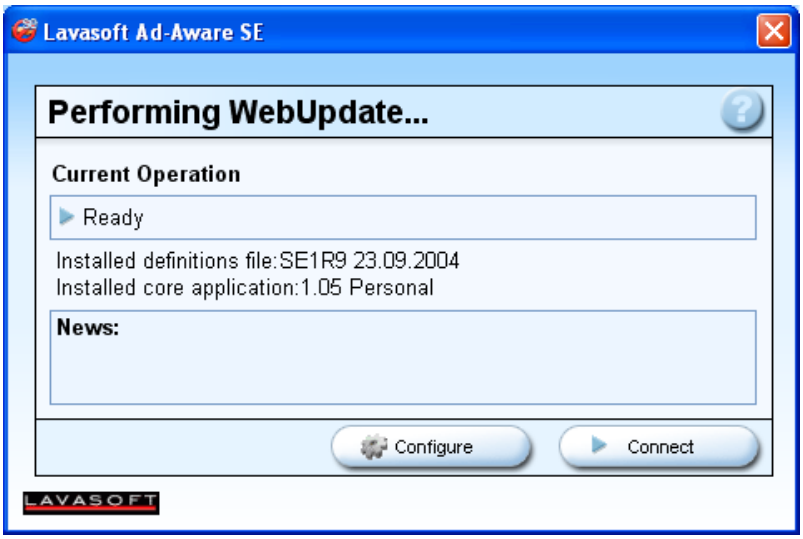
Nach dem Start von Lavasoft Ad-aware erscheint folgendes Fenster:



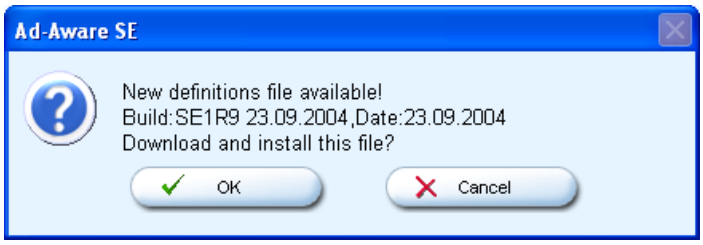
Du kannst durch Drücken des Buttons „Check for updates now“ prüfen, ob eine neue Programmversion und/oder eine neue Definitionsdatei verfügbar ist.

Zurück zum Inhalt dieses Kapitels

Ist dies der Fall, wird es gleich installiert. Drücke den Button „Check for updates now”. Folgender Hinweis erscheint:



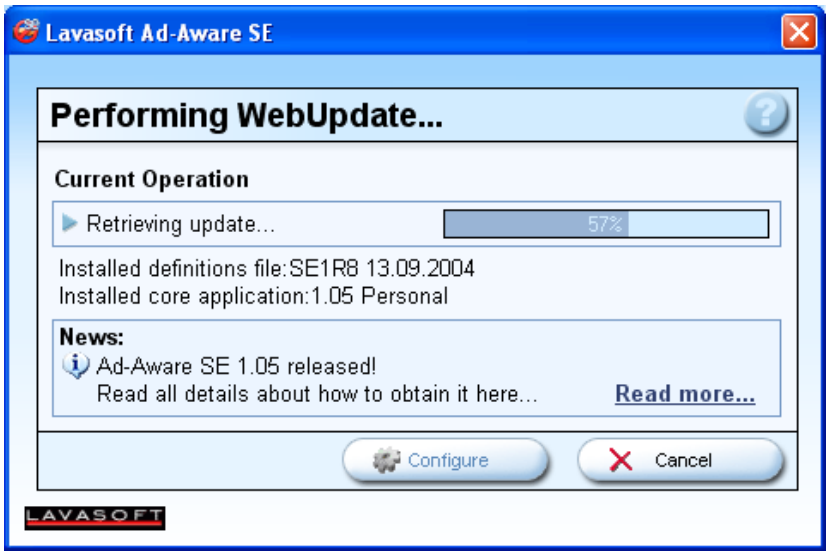
Drücke nun den Button “Connect”.



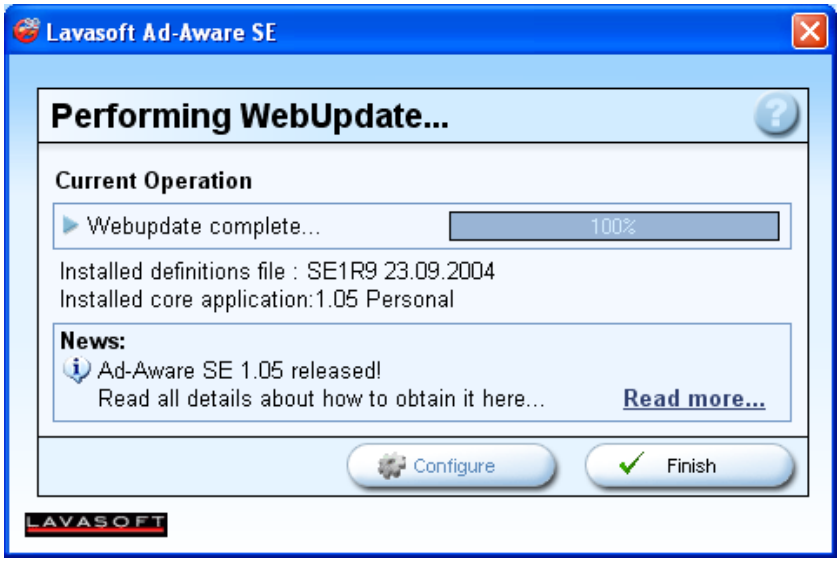
Nach Herstellung der Verbindung erhältst du den Hinweis, dass alles aktuell ist, oder – wie hier – dass es eine neue Defintionsdatei gibt. Drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

Die Aktualisierung beginnt jetzt:



Wurde die Aktualisierung beendet, zeigt der Fortschrittsbalken 100% an:

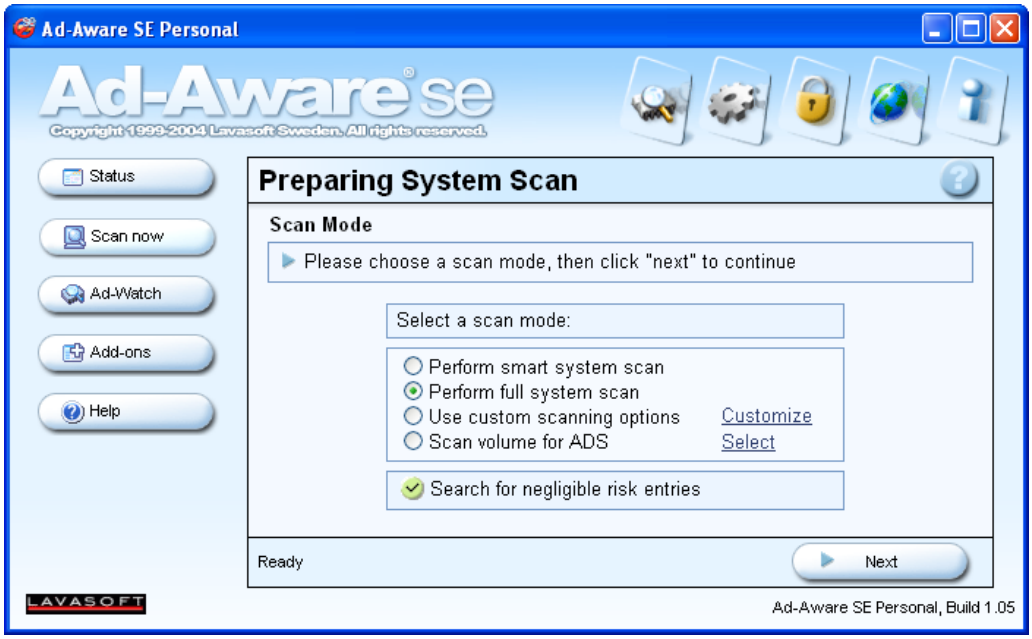


Drücke den Button „Finish“.

Zurück zum Inhalt dieses Kapitels

Das Prüfen des Computers

Nach dem Starten des Programms kannst du im Hauptmenü den Punkt „Scan now“ wählen:

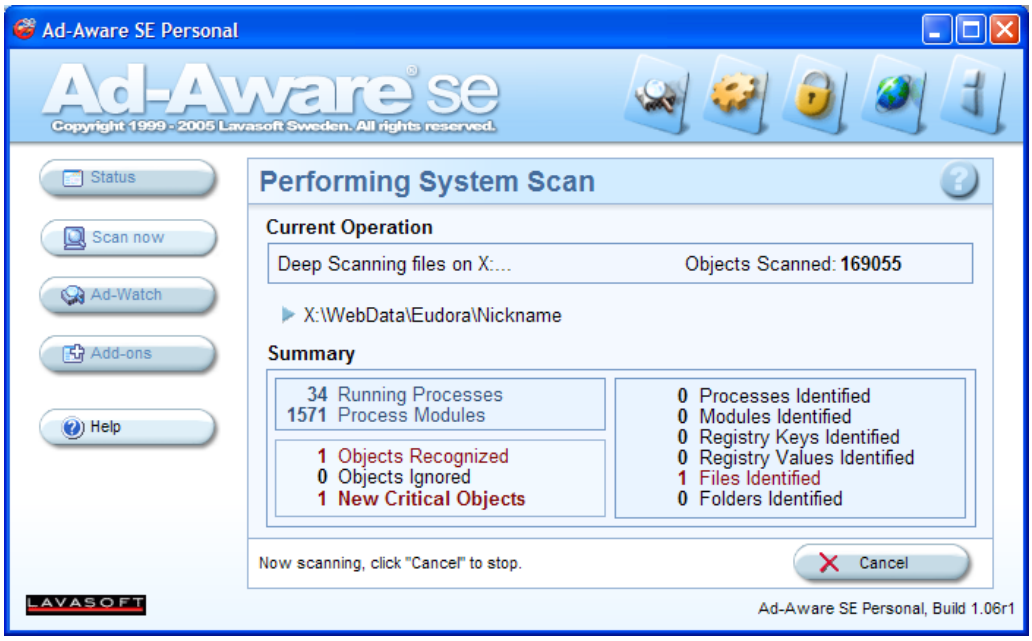


Du kannst dir nun die Art der Prüfung aussuchen (mehr Info dazu gibt’s in der Hilfe des Programms). Nimm einfach die vorgeschlagenen Einstellungen oder wähle das intensivere „Perform full system scan“.

Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Jetzt prüft das Programm deinen Computer auf bedenkliche Programme und Einstellungen:

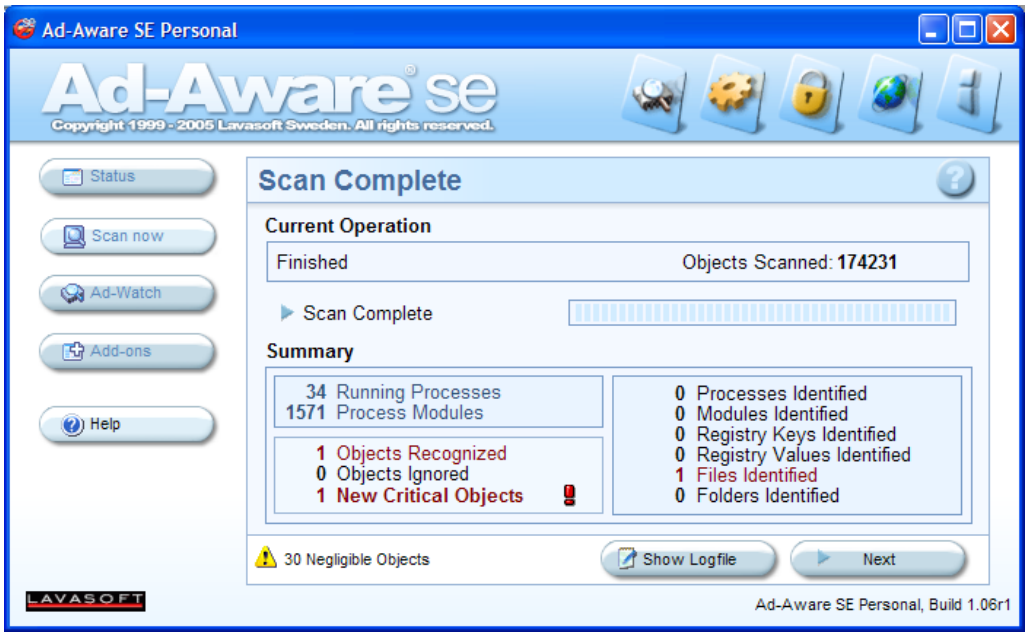


Aber keine Angst, noch passiert nichts mit deinem Computer, nichts wird deinstalliert oder geändert. Es wird nur eine Liste von Spyware-Programmen und Einstellungen erstellt.

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 „Scan complete“ mit einer Liste der gefundenen Programme/Einstellungen:



Die Chancen, dass zumindest ein verdächtiges Programm gefunden wird, stehen erfahrungsgemäß sehr gut. Wie du den Mist loswirst, erfährst du auf den folgenden Seiten.

Hier wurden ein „kritisches“ und 30 „vernachlässigbare“ Probleme entdeckt. Drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Nun siehst du die Details zu den gefundenen Objekten:

Wähle den Karteikarte mit „Critical Objects“. Du kannst jetzt aus der angezeigten Liste alle Programme/Einstellungen ankreuzen, die Spyware beinhalten und die du loswerden willst. Drücke dann den Button „Next“.

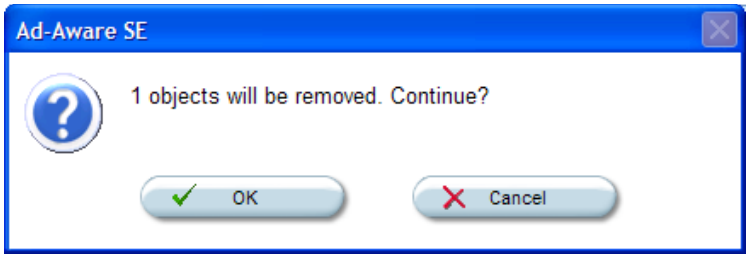
Zurück zum Inhalt dieses Kapitels

Wenn du von einem Programm den Spyware-Teil entfernst, wird nicht garantiert, dass das Programm nachher noch vollständig funktioniert. Du musst selbst entscheiden, was du tun möchtest.

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 zu suchen – nämlich Programme, die keine Spyware beinhalten.

Es erscheint noch eine Sicherheitsabfrage:



Drücke den Button „OK“. Die ausgewählten Programme und/oder Dateien werden jetzt entfernt, das Hauptfenster erscheint wieder.

Zurück zum Inhalt dieses Kapitels

13 Spybot – Search & Destroy

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Spybot, wie Ad-Aware ein kostenloses Programm zum Auffinden und Entfernen von Windows-Programmen, die deinen Computer ausspionieren (Spyware)

Ad-Aware und Spybot sind gemeinsam im Doppelpack ein äußerst wirkungsvolles Mittel gegen solche Spyware.

Warum beide Programme installieren und verwenden? Weil es Programme und Einstellungen gibt, die von Ad-Aware nicht aufgespürt werden, von Spybot aber schon – und natürlich umgekehrt auch. Beide zusammen finden aber so gut wie alles.

Wichtig ist, dass du deinen Computer regelmäßig mit beiden Programmen nach Spyware durchsuchen lässt, es kann sich ja immer wieder mal etwas auf deinen Computer schleichen.

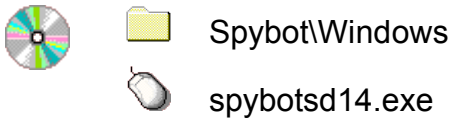
Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Spybot
- Die Verwendung von Spybot

Die aktuellste Version von Sypbot findest du im Internet unter http://www.safer-networking.org/de/spybotsd/

13.1 Die Installation von Spybot

Die Installation von Spybot ist sehr einfach. Starte das Installationsprogramm durch Doppelklick auf das Programm spybotsd14.exe im Ordner Spybot\Windows auf der CD.

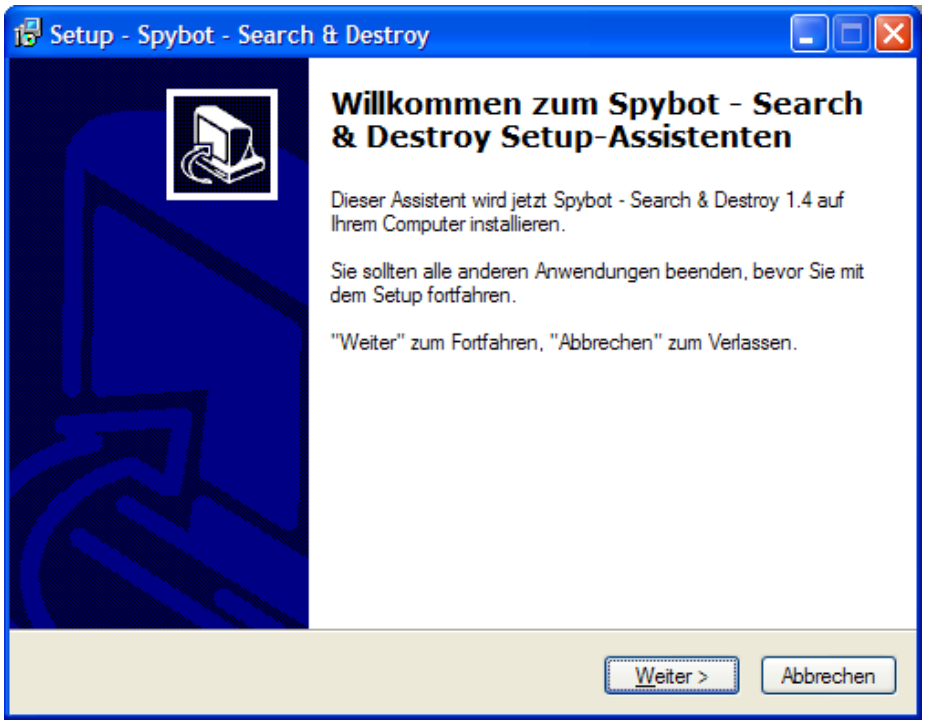


Nach dem Start des Installationsprogramms kannst du dir die Sprache für die Installation auswählen:

Wähle die von dir gewünschte Sprache und drücke den Button „OK“.

Zurück zum Inhalt dieses Kapitels

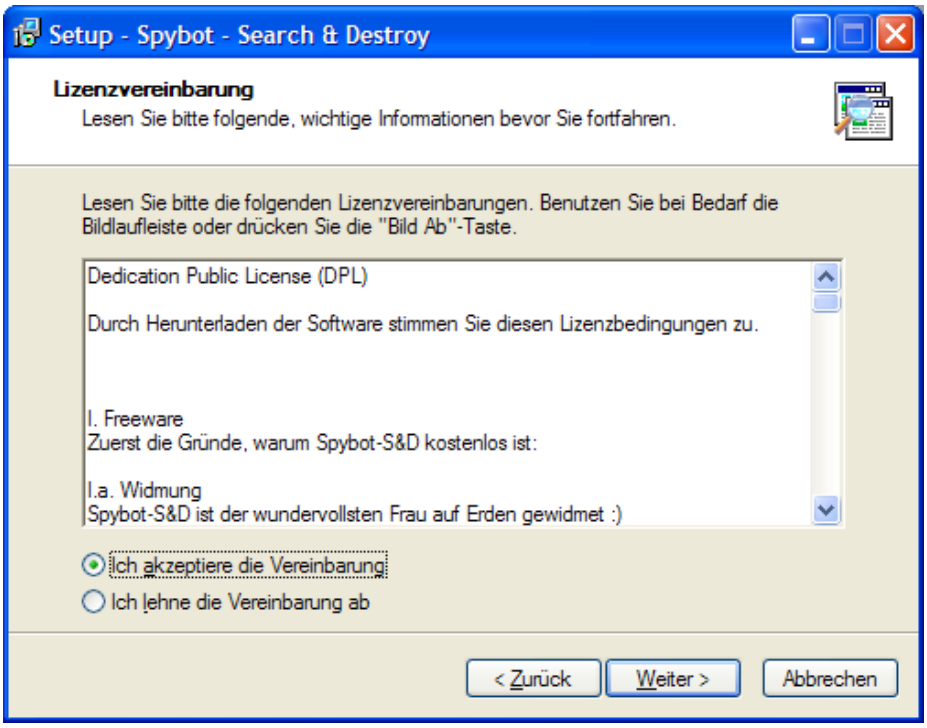
Dann erscheint das Willkommensfenster:



Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

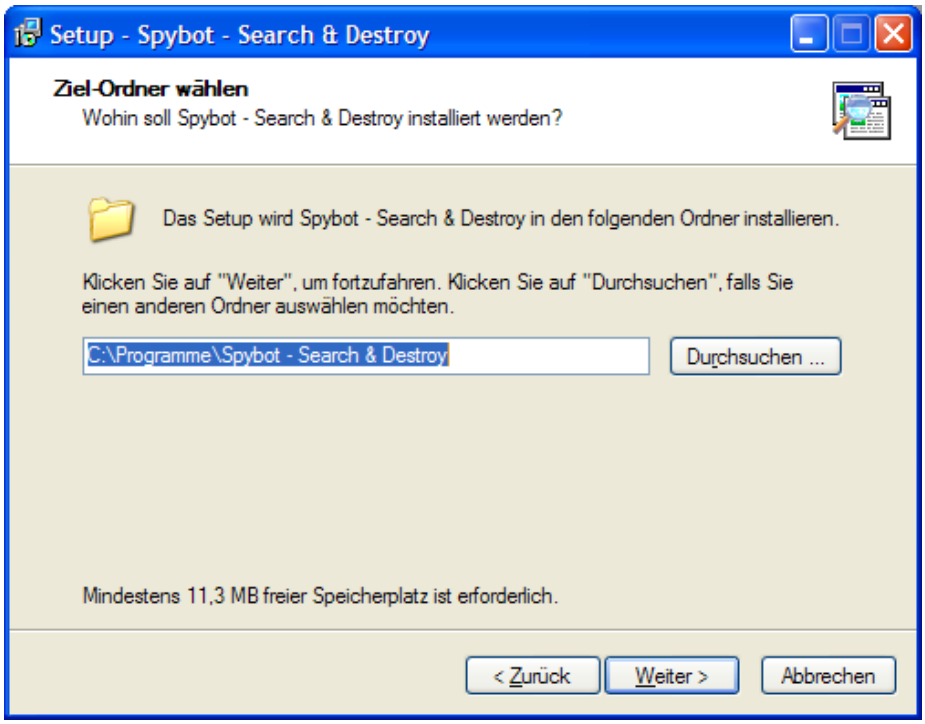
Es folgt die Lizenzvereinbarung:



Aktzeptiere die Lizenzvereinbarung durch Auswählen des Punkts „Ich akzeptiere die Vereinbarung“, drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

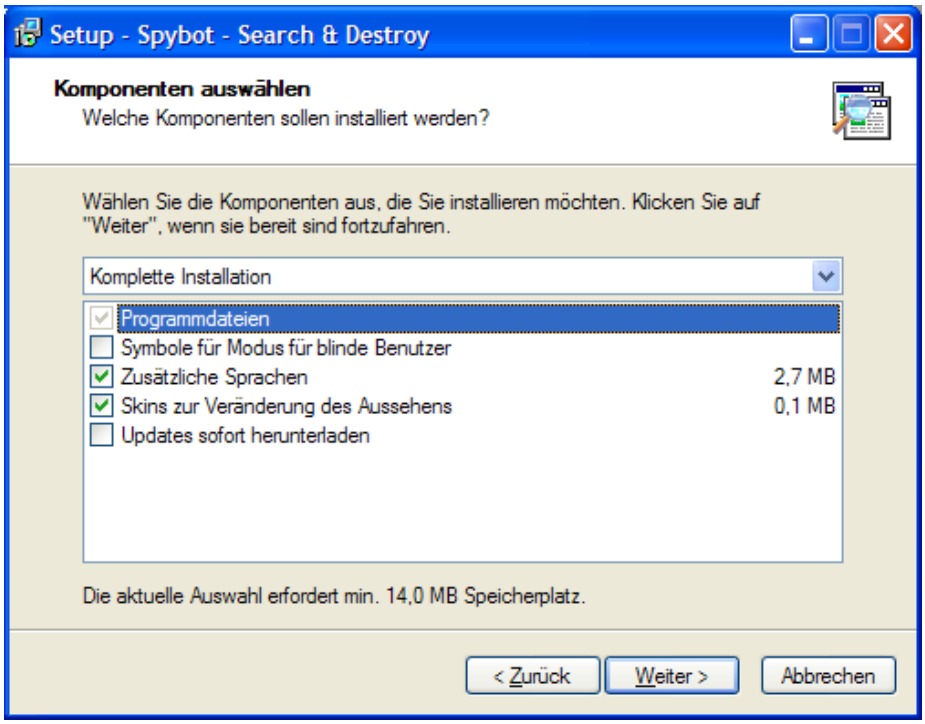
Nun kannst du dir den Ordner aussuchen, in dem Spybot installiert wird:



Nimm den vorgeschlagenen Ordner oder wähle einen anderen, drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du dir aussuchen, welche Komponenten installiert werden sollen:

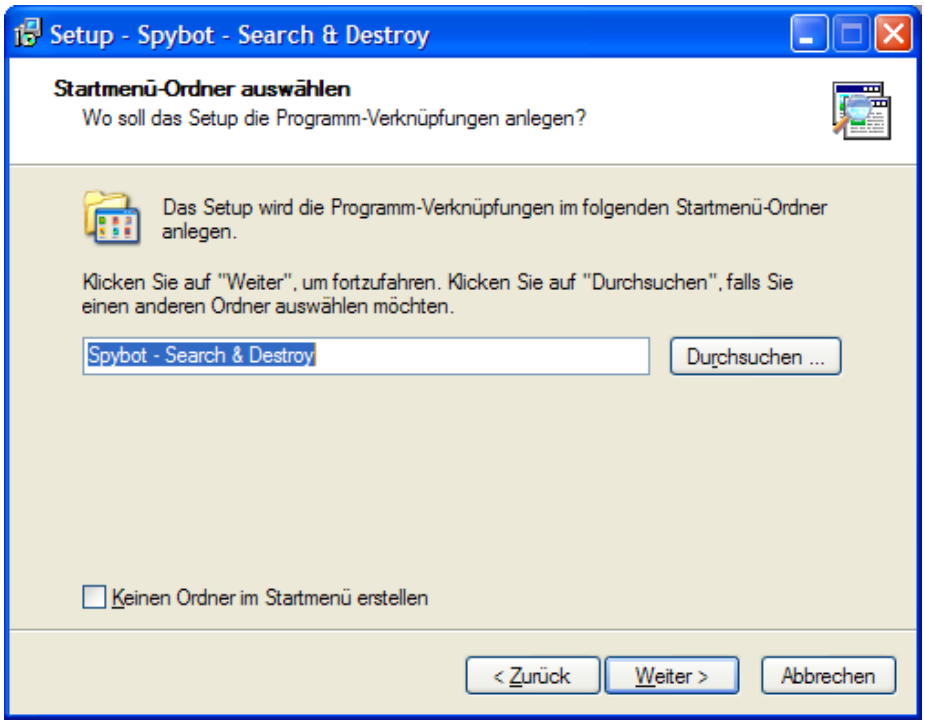


Wähle aus, was du installieren willst, und drücke dann den Button „Weiter“.

Die Updates kannst du dir auch später vor der Prüfung deines Computers auf Spyware herunterladen.

Zurück zum Inhalt dieses Kapitels

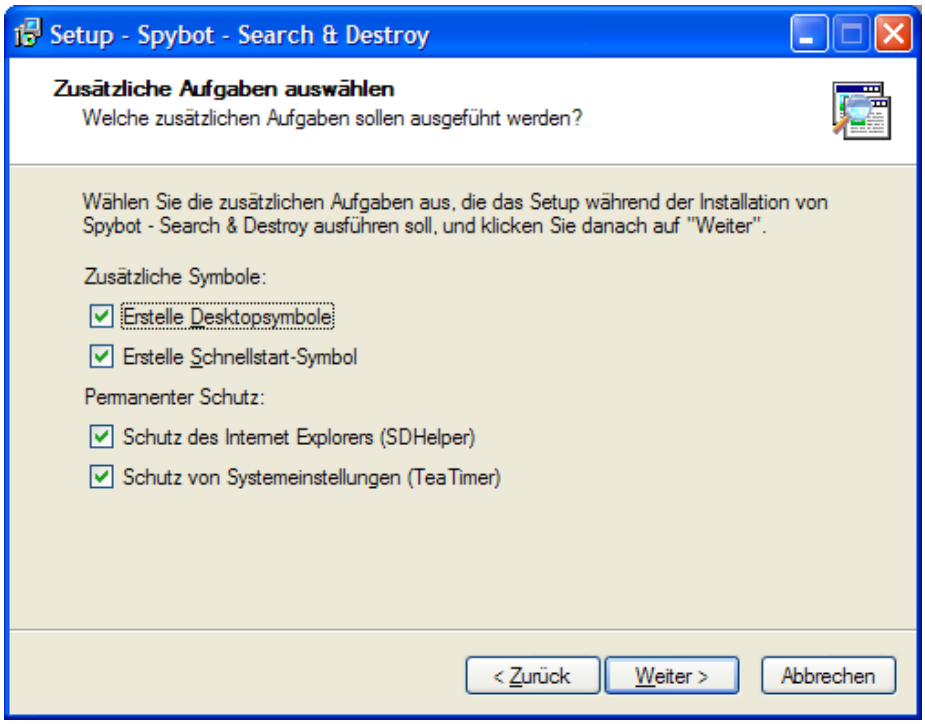
Hier kannst du dir aussuchen, wie der Ordner in deinem Startmenü mit Spybot heißen soll:



Nimm den vorgeschlagenen Namen oder gib einen anderen an, drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

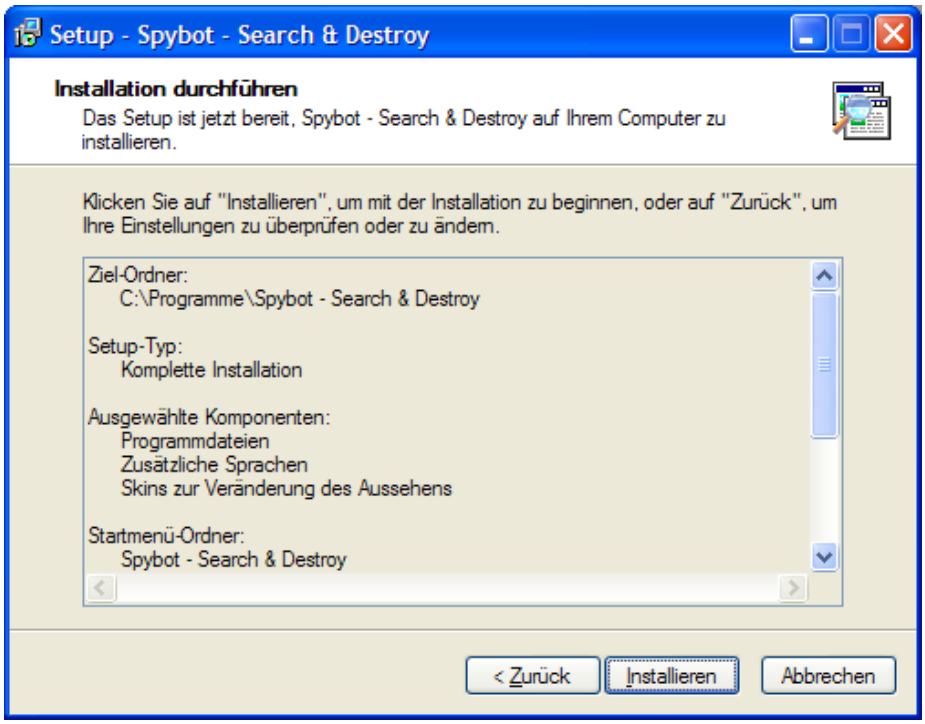
Jetzt kannst du dir noch zusätzliche Dinge aussuchen:



Du kannst z.B. angeben, ob du ein Symbol auf dem Desktop haben willst. Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

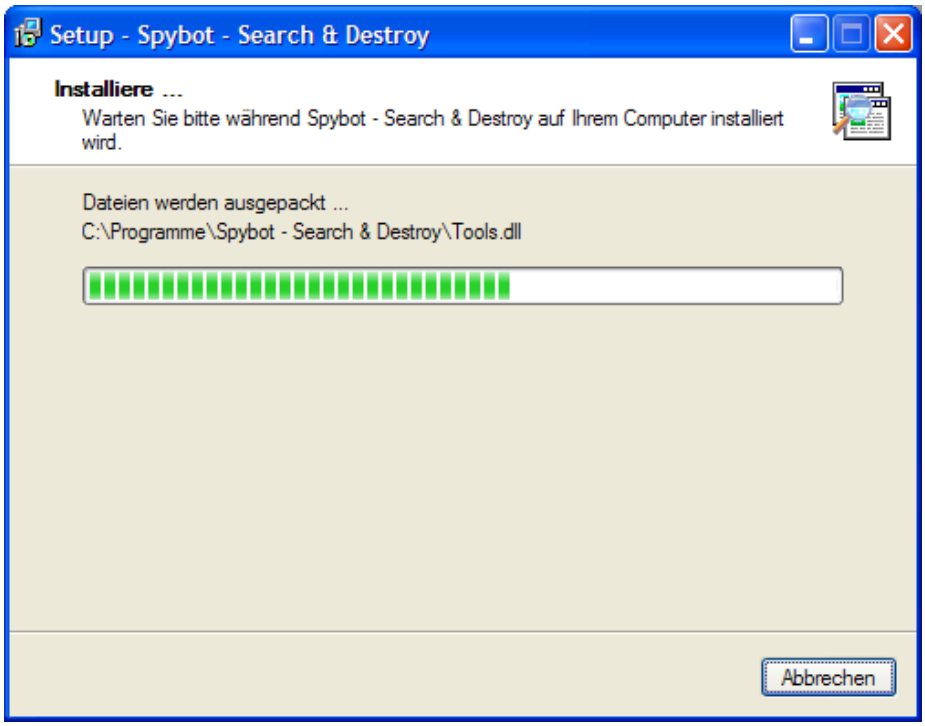
Vor der eigentlichen Installation erhältst du noch eine Liste mit den von dir gewählten Installationsoptionen:



Drücke den Button „Installieren“.

Zurück zum Inhalt dieses Kapitels

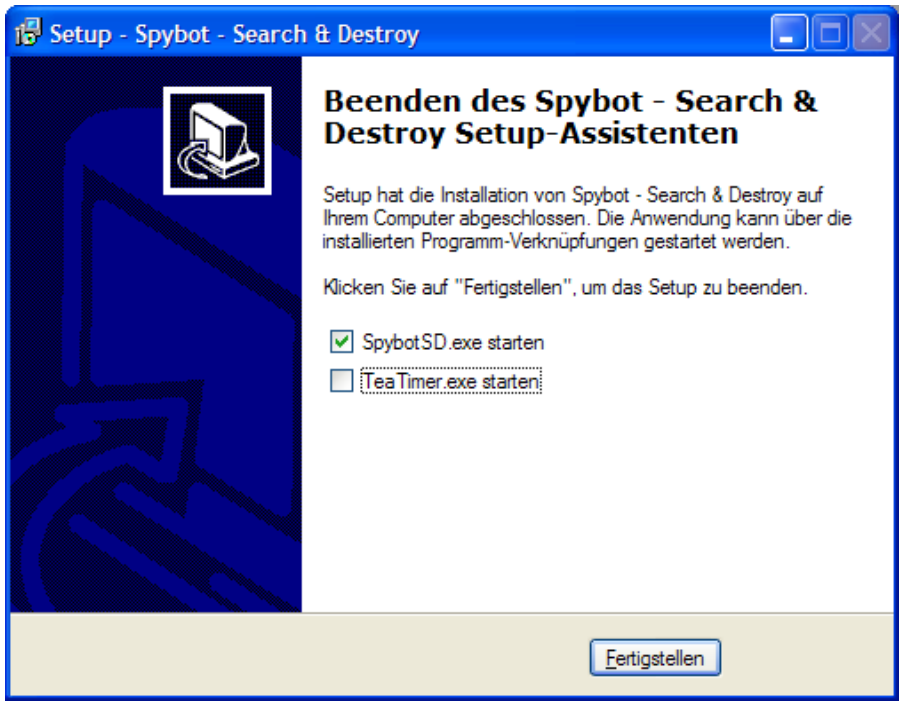
Die Installation beginnt jetzt:



Die Installation ist sehr rasch fertig, du bekommst den Fortschritt angezeigt.

Zurück zum Inhalt dieses Kapitels

Nach Beenden der Installation erhältst du einen entsprechenden Hinweis:



Du kannst dir noch aussuchen, ob du Spybot gleich starten willst. Drücke den Button „Fertigstellen“.

Zurück zum Inhalt dieses Kapitels

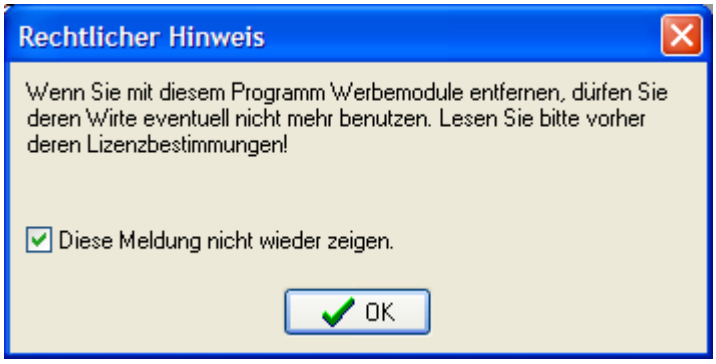
13.2 Die Verwendung von Spybot

Erste Tätigkeiten

Wenn du Spybot das erste Mal startest, wird dir Schritt für Schritt angeboten, die wichtigsten ersten Handgriffe durchzuführen, ohne im Menü des Hauptprogramms herumstöbern zu müssen.

Du kannst aber alle folgenden Tätigkeiten auch aus dem Hauptfenster des Programms ausführen.

Zuerst mal erscheint ein Hinweis:



Hake „Diese Meldung nicht wieder anzeigen“ an und drücke den Button „OK“.

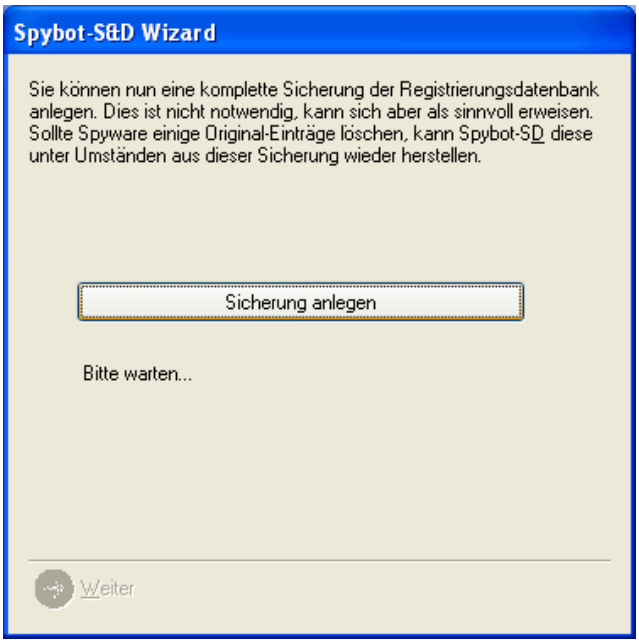
Zurück zum Inhalt dieses Kapitels

Du erhältst gleich die Möglichkeit, deine Windows-Registry zu sichern:

Sehr nett ist ja der Hinweis, dass die Registry auf Wunsch „unter Umständen“ wieder hergestellt werden kann. Drücke den Button „Sicherung anlegen“.

Zurück zum Inhalt dieses Kapitels

Das dauert dann ein bisschen:



Wenn die Sicherung fertig ist, verschwindet das „Bitte warten…“ einfach, du kannst dafür den Button „Weiter“ drücken.

Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

In unserem Fall hat Spybot festgestellt, dass der Microsoft Internet Explorer einen Proxy Server verwendet (siehe JAP):

Drücke einfach den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du eine Aktualisierung des Programms und der Liste von Spyware vornehmen:

Führe diese Aktualisierung unbedingt durch. Das verhält sich wie bei einem Anti-Virenprogramm, eine aktuelle Liste mit den zu eliminierenden Programmen ist sehr wichtig.

Drücke den Button „Nach Updates suchen“.

Zurück zum Inhalt dieses Kapitels

Wenn die Verbindung hergestellt werden konnte, wird der Button „Alle Updates herunterladen“ bedrückbar gemacht:

Drücke den Button „Alle Updates herunterladen“.

Zurück zum Inhalt dieses Kapitels

Das Update beginnt:

Nach der Fertigstellung erscheint wieder das ursprüngliche Fenster, drücke den Button „Weiter“. Es erscheint folgendes Fenster:

Nun kannst du deinen Computer „immunisieren“, d.h. dass Programme, die Spyware enthalten, blockiert werden. Wenn du das willst, drücke den Button „Immunize this system“.

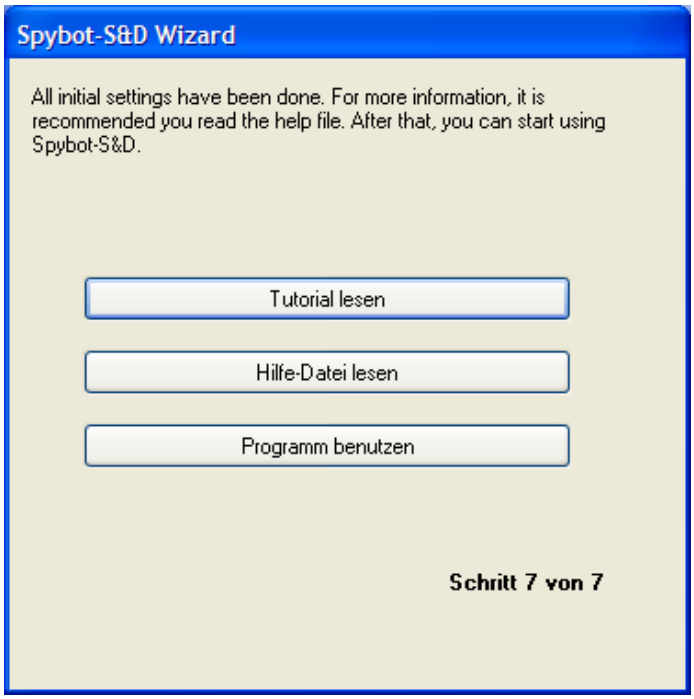
Zurück zum Inhalt dieses Kapitels

Nach der Immunisierung erhältst du folgende Erfolgsmeldung:

Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

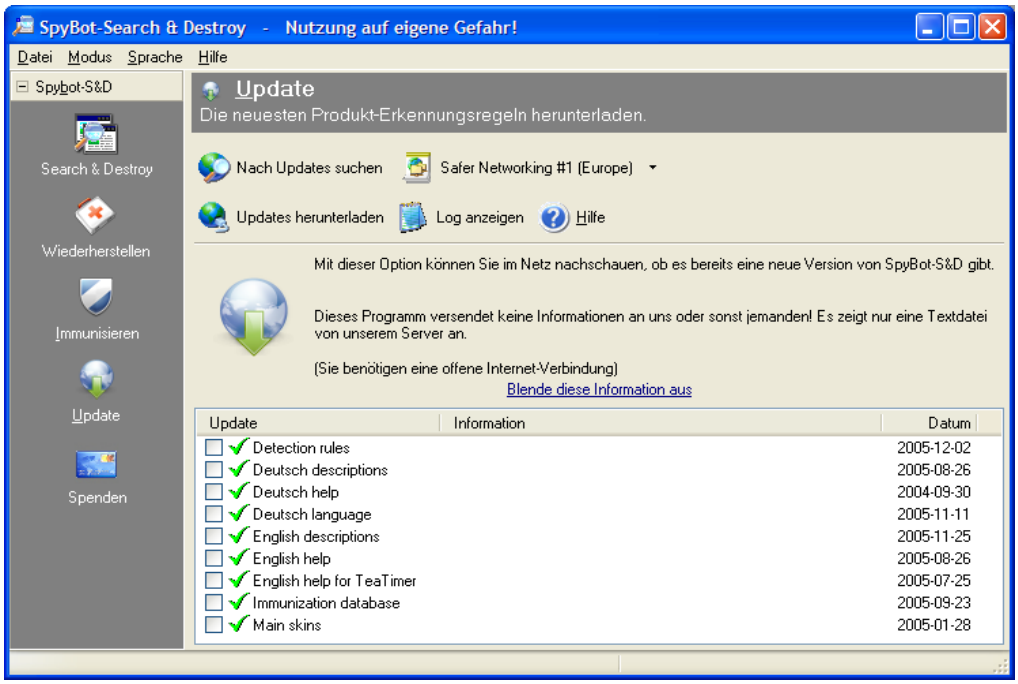
Jetzt hast du noch die Möglichkeit, einiges zu lesen oder einfach das Programm zu verwenden:



Lies, was dich interessiert, und drücke dann den Button „Programm benutzen“.

Zurück zum Inhalt dieses Kapitels

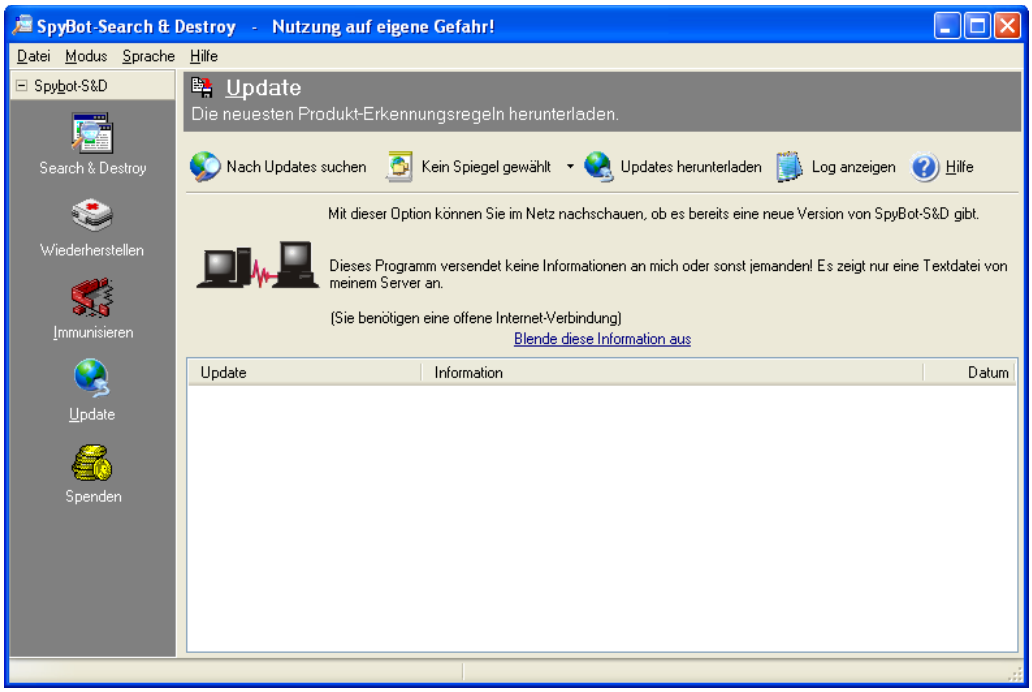
Es erscheint das Hauptfenster von Spybot, das du auch in Zukunft gleich sehen wirst, wenn du Spybot startest:



Zurück zum Inhalt dieses Kapitels

Das Aktualisieren des Programms

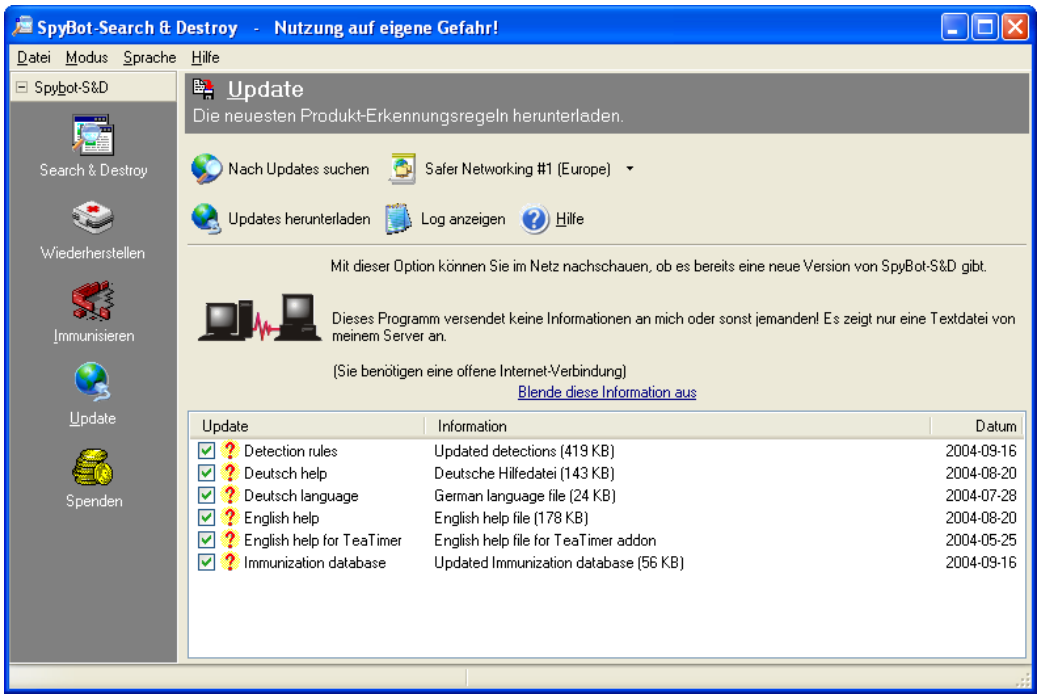
Du kannst das Programm direkt im Hauptfenster aktualisieren, wähle dazu den Menüpunkt „Update“ auf der linken Seite des Fensters:



Drücke auf den Button „Nach Updates suchen“.

Zurück zum Inhalt dieses Kapitels

Es erscheint nach kurzer Zeit eine Liste mit verfügbaren Aktualisierungen:



Kreuze alle Punkte an, die du aktualisieren möchtest (der erste Punkt „Detection rules“ ist unbedingt anzukreuzen) und drücke dann auf den Button „Updates herunterladen“.

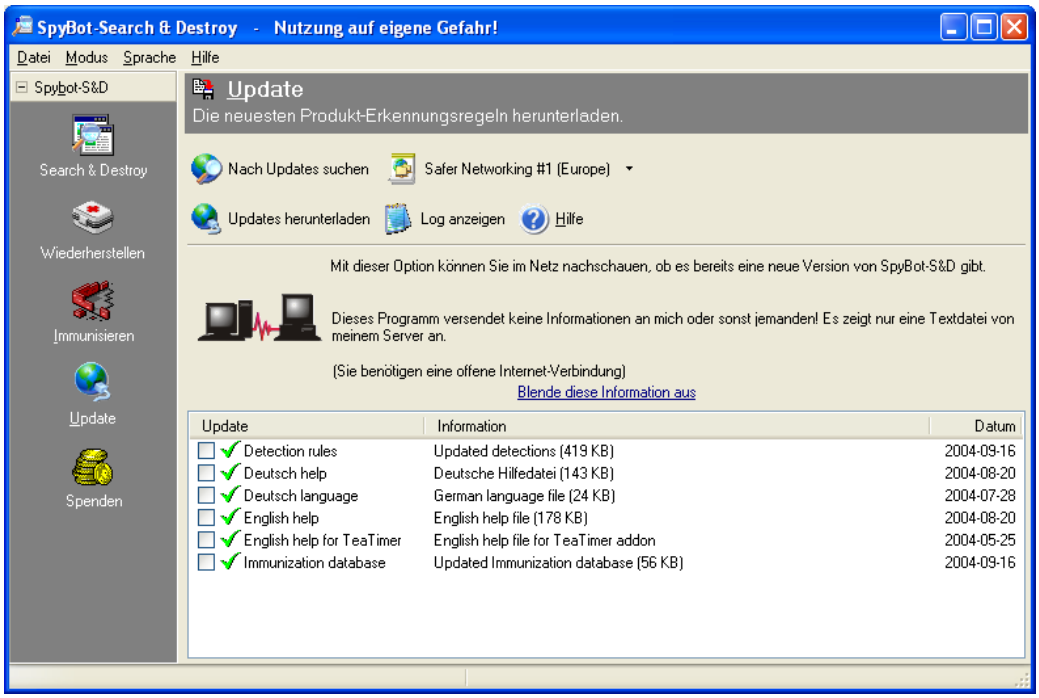
Zurück zum Inhalt dieses Kapitels

Die Aktualisierung wird jetzt vorgenommen:

Du bekommst den Fortschritt der Aktualisierung angezeigt.

Zurück zum Inhalt dieses Kapitels

Wurde die Aktualsierung beendet, erscheint wieder das Hauptfenster:



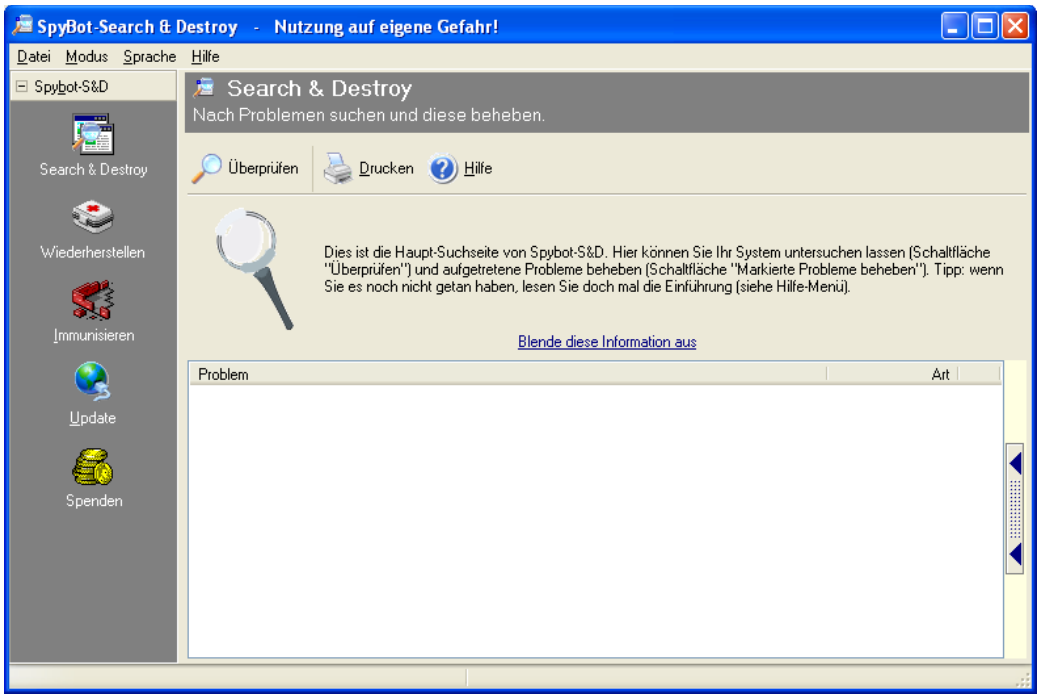
Statt der gelben Fragezeichen siehst du jetzt grüne Häkchen neben den einzelnen Punkten. Fertig, alles ok, dein Programm ist top-aktuell.

Diesen Vorgang solltest du jedes Mal machen, bevor du deinen Computer von Spybot nach Spyware durchsuchen lässt.

Zurück zum Inhalt dieses Kapitels

Das Prüfen des Computers

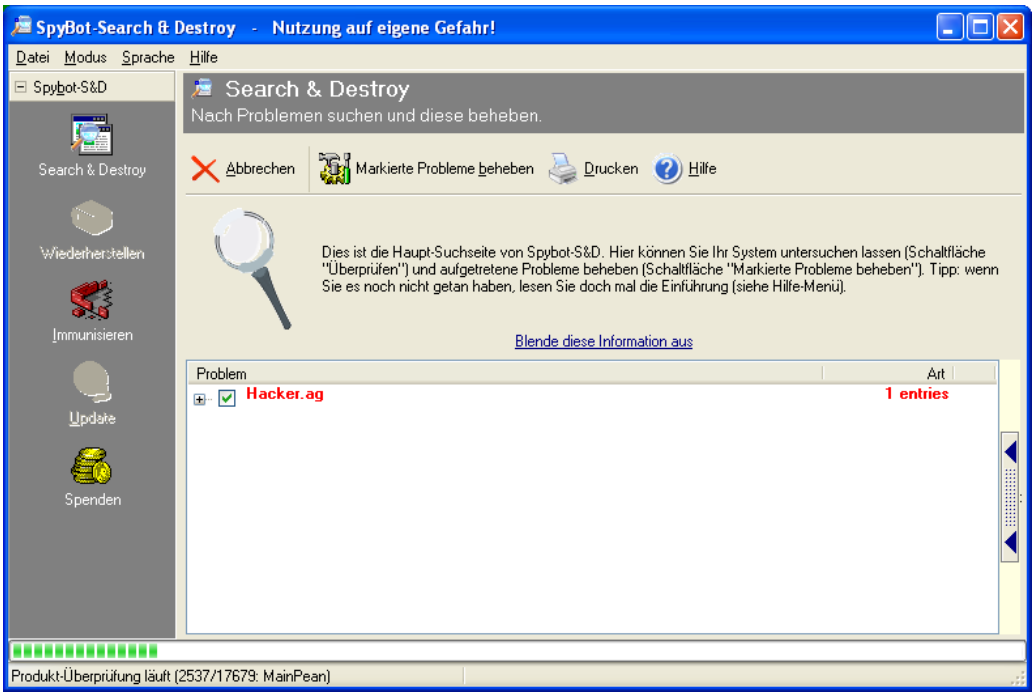
Für die Prüfung des Computers auf Spyware wähle im Hauptmenü des Programms den Punkt „Search & Destroy“ auf der linken Seite:



Drücke den Button „Überprüfen“, die Prüfung beginnt dann gleich.

Zurück zum Inhalt dieses Kapitels

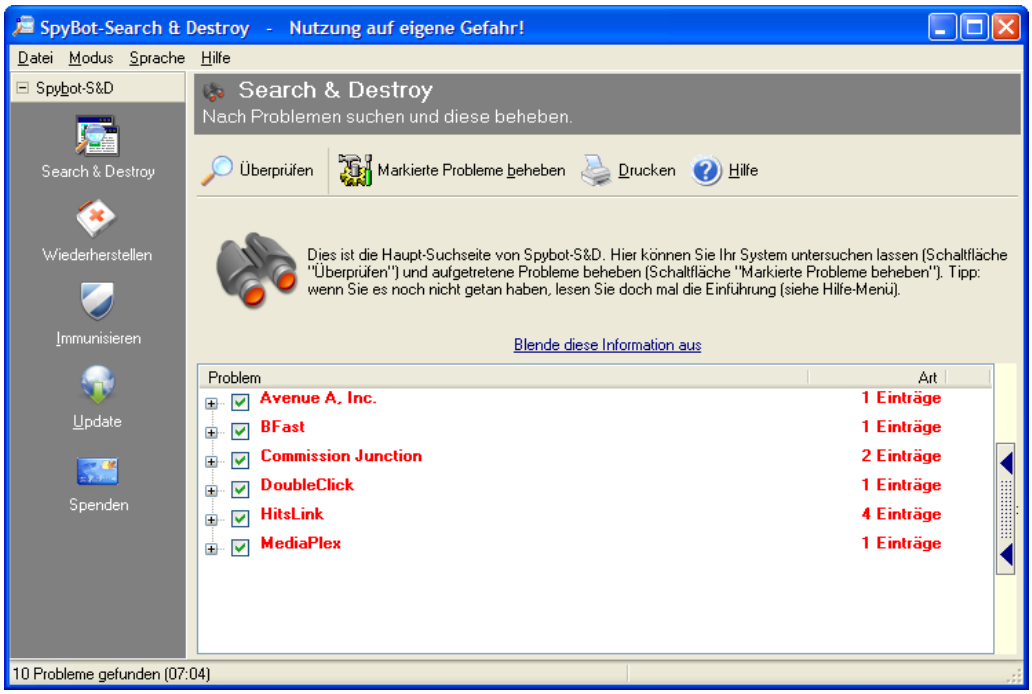
Während der Prüfung bekommst du den Fortschritt und eventuell bereits entdeckte Probleme angezeigt:



Das dauert natürlich ein bisschen – abhängig von der Menge der von dir installierten Programme.

Zurück zum Inhalt dieses Kapitels

Nach Beendigung des Prüfdurchgangs siehst du die ganze Liste gefundener Probleme vor dir:

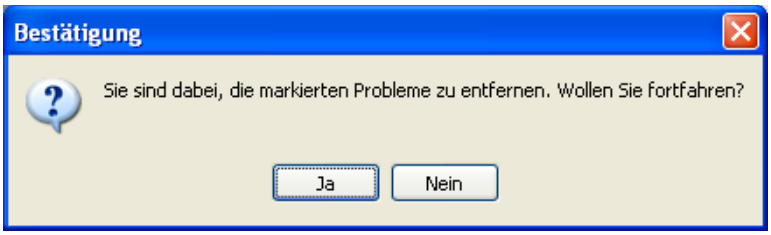


Na, ist ja hier eine ganze Menge…

Kreuze alle Programme an, deren Spyware du entfernen willst (bzw. lasse sie einfach angekreuzt) und drücke dann den Button „Markierte Probleme beheben“.

Zurück zum Inhalt dieses Kapitels

Es folgt eine Sicherheitsabfrage:

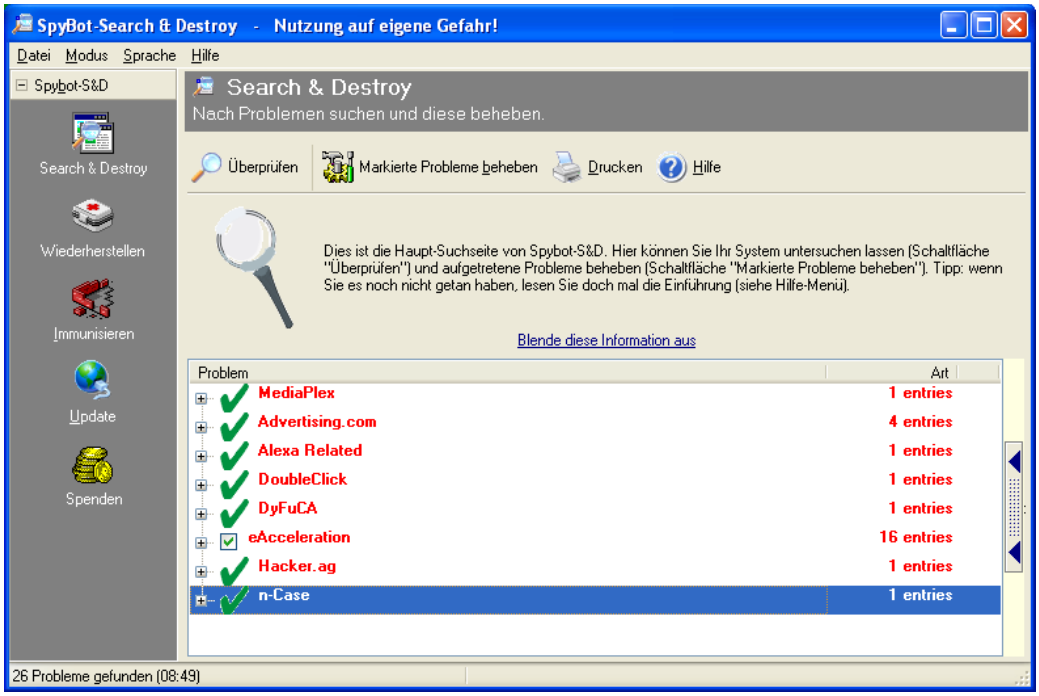


Drücke den Button „Ja“. Das Entfernen der Spyware wird gestartet, Du bekommst den Fortschritt des Vorgangs angezeigt.

Zurück zum Inhalt dieses Kapitels

Nach Beenden des Entfernens folgt eine Bestätigung:

Drücke den Button „OK“, du kehrst dann ins Hauptfenster zurück:



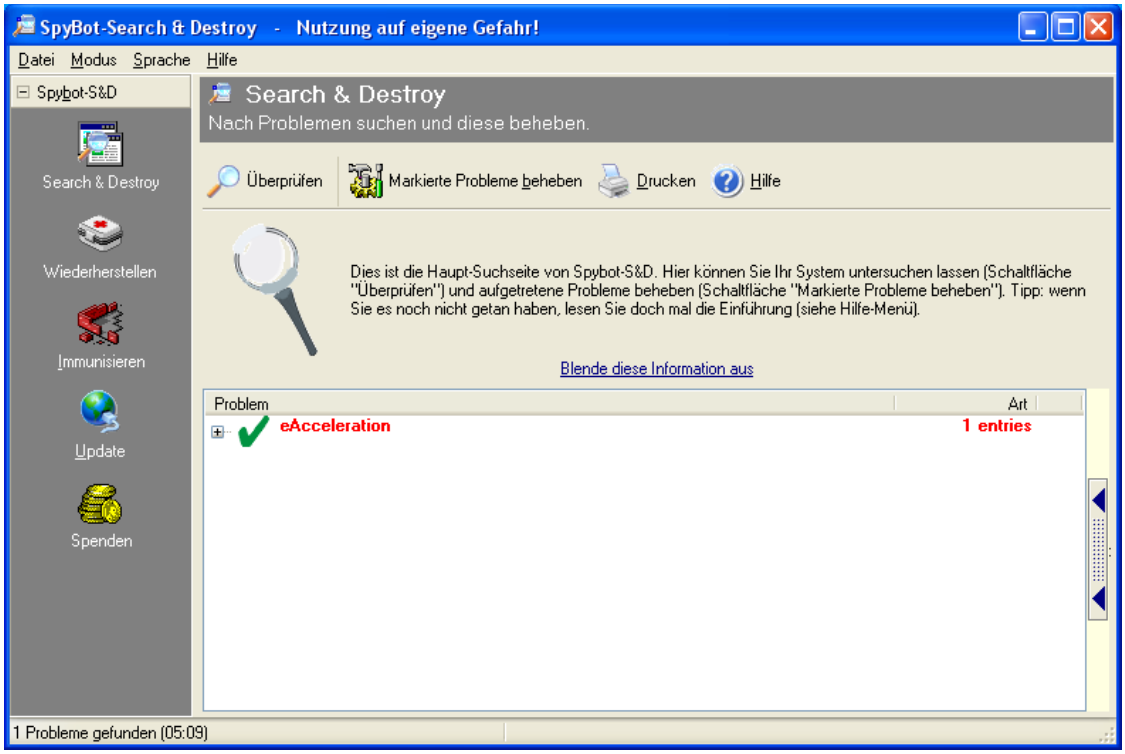
In diesem (anderen) Fall konnte ein Problem nicht behoben werden, vermutlich weil die Entfernung von einem aktiven Programm blockiert wird.

Es erscheint ein Hinweis auf dieses Problem. Bei diesem Hinweis kannst du auch den Vorschlag akzeptieren, dass Spybot beim nächsten Start von Windows automatisch gestartet wird und es versucht, das verbliebene Problem zu beheben. Gestatte dem Programm dies und starte deinen Computer neu.

Zurück zum Inhalt dieses Kapitels

Nach dem Neustart wird dein Computer von Spybot automatisch nochmals komplett durchgecheckt, und zwar vor dem Laden diverser Programme (z.B. deinem Virenscanner, der Firewall etc.).

Wird etwas gefunden, wiederholt sich der Vorgang wie bereits beschrieben. Das Problem kann dann voraussichtlich behoben werden, die Spyware wird entfernt:



Das Problem, das vorher nicht behoben werden konnte, wurde jetzt beseitigt. Alles ok, du kannst jetzt noch vor Begeisterung eine Spende loswerden (Menüpunkt „Spende“ auf der linken Seite) oder gleich das Programm durch Drücken des X ganz rechts oben schließen.

Zurück zum Inhalt dieses Kapitels

14 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.

Die aktuellste Version von XP-Antispy findest du auf der Webseite http://www.xpantispy.org/

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von XP Antispy
- Die Verwendung von XP Antispy

14.1 Die Installation von XP-Antispy

Die Installation von Spybot ist sehr einfach. Starte das Installationsprogramm durch Doppelklick auf das Programm xp-AntiSpy_setup-deutsch.exe im Ordner XP Antispy\Windows auf der CD.

XP Antispy\Windows

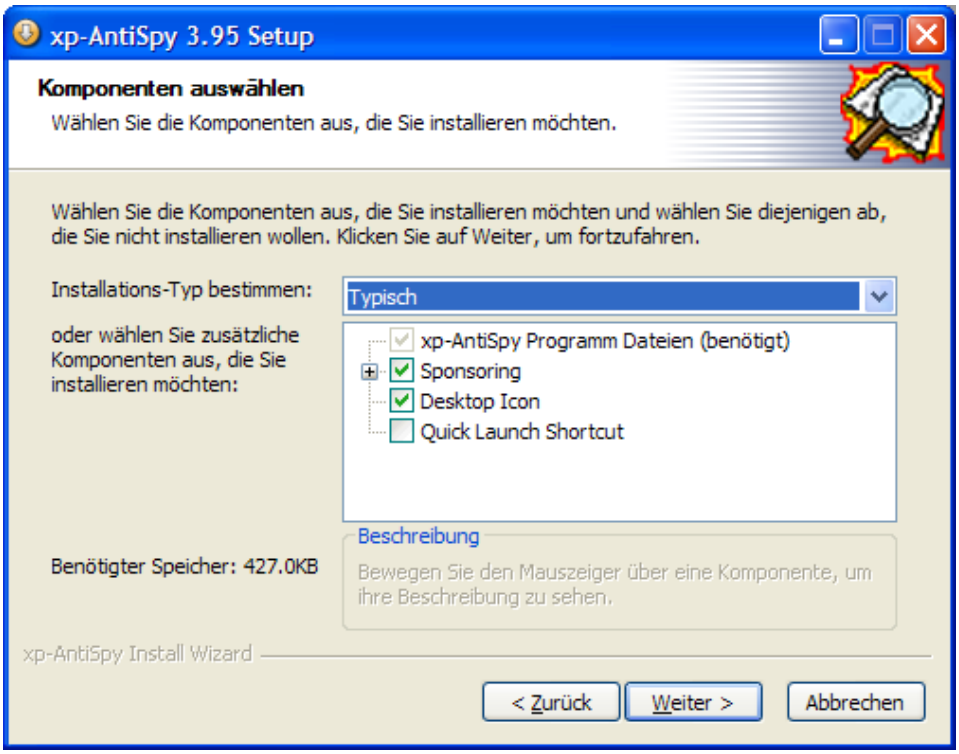
xp-AntiSpy_setup-deutsch.exe

Nach einem Doppelklick auf die angegebene Datei wird das Installationsprogramm gestartet:

Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

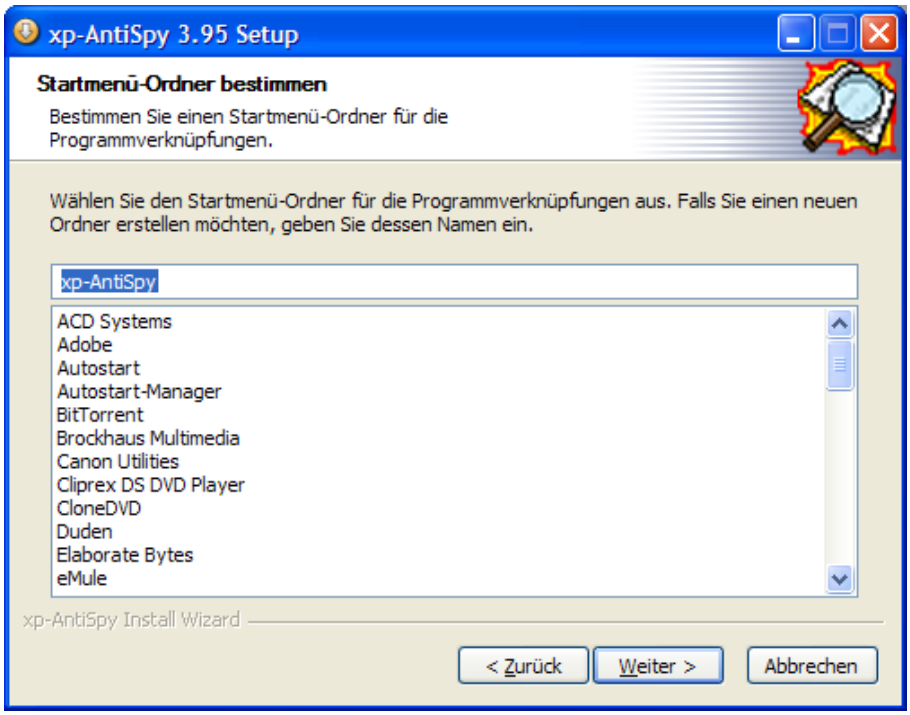
Nun kannst du dir die Programmteile aussuchen, die du installieren möchtest:



Nimm einfach den Vorschlag an oder wähle das von dir Gewünschte aus. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

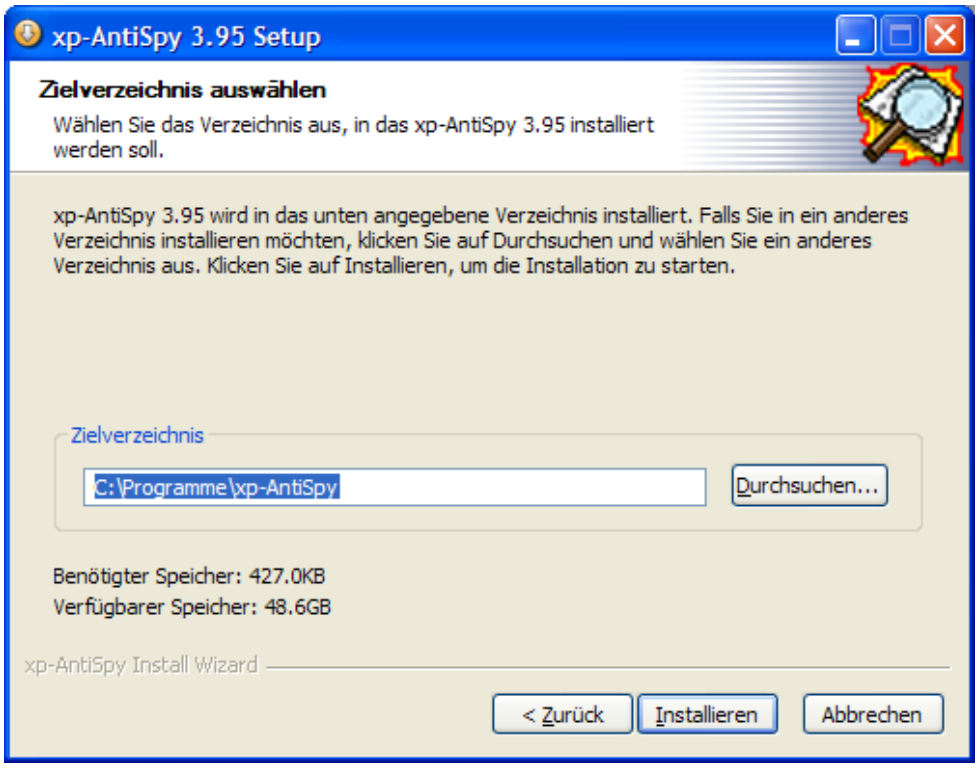
Jetzt kannst du dir aussuchen, wie das Programm in deinem Start-Ordner heißen soll:



Nimm einfach den Vorschlag an oder gib einen anderen Namen an. Drücke dann den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du dir noch aussuchen, in welchem Ordner das Programm installiert werden soll:



Nimm einfach den vorgeschlagenen Ordner oder wähle einen anderen. Drücke dann den Button „Installieren“.

Zurück zum Inhalt dieses Kapitels

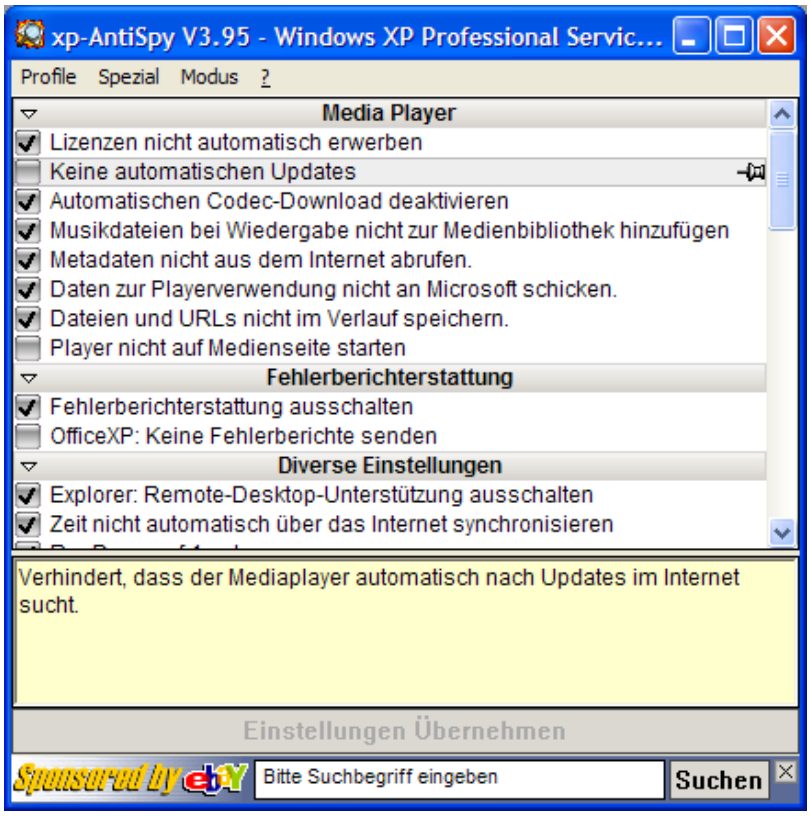
Die Installation ist nach sehr kurzer Zeit fertig:

Hake den Punkt „xp-Antispy 3.95 ausführen“ an und drücke den Button „Fertig stellen“.

Zurück zum Inhalt dieses Kapitels

14.2 Die Verwendung von XP Antispy

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



Du kannst jetzt auswählen, welche Punkte du durchführen willst und welche nicht bzw. nicht mehr.

Du musst nicht alles ausführen, es sind nur Vorschläge. Wenn du z.B. das empfohlene automatische Windows-Update ausführen lässt, ist das natürlich eine Vertrauenssache: nämlich dass das Aktualisierungsprogramm keine vertraulichen Daten an die Firma Microsoft sendet (z.B. eine Liste mit installierten Microsoft-Programmen). Zum Zeitpunkt der Erstellung dieses Handbuchs werden auch definitiv keine solche Daten an Microsoft gesendet.

Zurück zum Inhalt dieses Kapitels

Wenn du mit dem Mauszeiger über die einzelnen Zeilen fährst, erscheinen im unteren Teil des Fensters kurze Erklärungen zum jeweiligen Punkt.

Wenn du alles ausgewählt hast, was du ausführen lassen bzw. rückgängig machen willst, drücke den Button „Einstellungen übernehmen“. Fertig, durch Drücken des x am rechten oberen Rand schließt du das Programm.

Zurück zum Inhalt dieses Kapitels

15 Firefox

Überblick

Dieses Kapitel enthält eine Beschreibung, wie mensch den kostenlosen Internet-Browser Firefox installiert und verwendet.

Wie schon in Kapiteln am Beginn dieses Handbuchs angeführt, raten wir dringend von der Verwendung des Microsoft Internet Explorers und auch von Outlook als Mailprogramm ab. Bei diesen beiden Programmen tauchen dauernd schwerwiegende Sicherheitslücken auf, die großen Schaden anrichten können.

Es gibt zahlreiche kostenlose Internet-Browser, vielleicht hast du einen Internet-Browser, der dir besser gefällt. Wir haben hier als Beispiel Firefox genommen, weil es ein sehr guter, schlanker, schneller und sehr sicherer Browser ist. Dass er einem Open Source-Projekt entstammt, erhöht außerdem unser Vertrauen noch beträchtlich.

Wir können hier nicht alle Funktionalitäten von Firefox vorstellen und beschreiben. Wenn du dich näher dafür interessierst, wirst du auf viele weitere Funktionalitäten stoßen, so z.B. auf zahlreiche Erweiterungsmöglichkeiten („Extensions“). Auch zur Erstellung von Webseiten bietet er reichhaltige Hilfestellungen.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Firefox
- Die Verwendung von Firefox

Die aktuellste Version von Firefox findest du immer auf der Webseite http://www.mozilla.com/firefox/.

Informationen zu weiteren Mozilla Projekten findest du unter http://www.mozilla.org.

Auch ein Internet Browser wie Firefox kann Sicherheitlücken haben. Und Internet Browser müssen auch auf Sicherheitslücken im Betriebssystem selbst (z.B. in Windows) reagieren. Aber diese Sicherheitsprobleme werden nach Bekanntgabe erfahrungsgemäß sehr rasch behoben.

Es ist daher äußerst wichtig, immer auf dem aktuellsten Versionsstand zu sein. Seit der letzten hier vorgestellten Version bietet Firefox eine sehr komfortable Aktualisierungsmöglichkeit, ein Online Update.

Wie du Firefox immer am aktuellen Stand hältst, erfährst du im Kapitel „Aktualisieren von Firefox“.

15.1 Die Installation von Firefox

Auf der CD im Verzeichnis Firefox\Windows findest du das Installationsprogramm von Firefox.

Für Windows öffne den Windows Explorer, wechsle auf der CD ins richtige Verzeichnis.


Firefox\Windows

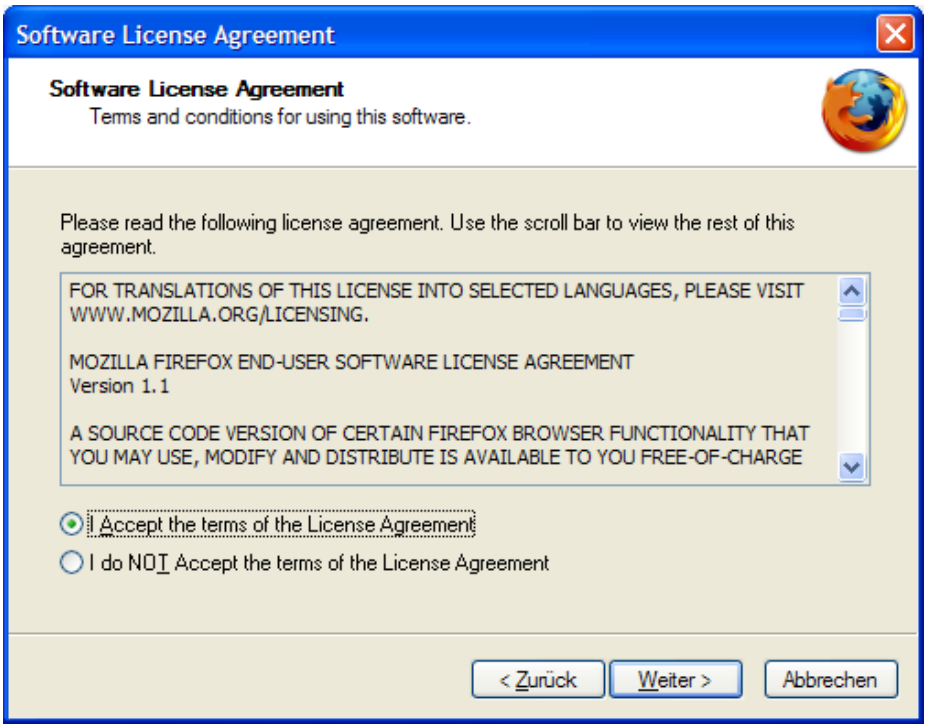
Firefox Setup 1.5.exe

Doppelklicke auf der CD auf die Datei Firefox Setup 1.5.exe, dann erscheint gleich mal das Willkommensfenster:

Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

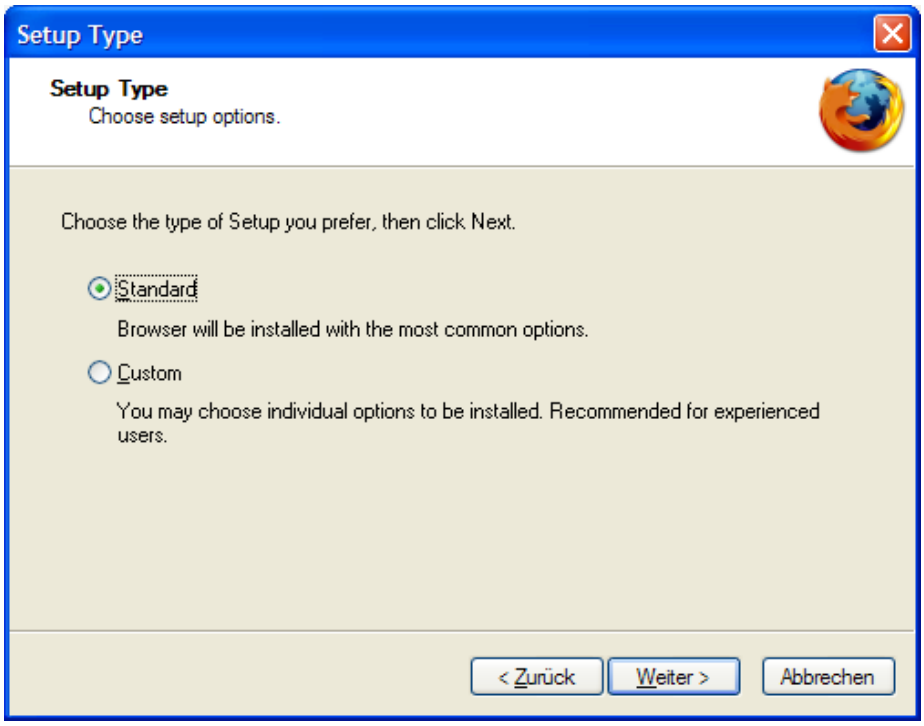
Nun folgt die Lizenzvereinbarung:



Markiere den Punkt „I Accept the terms" und drücke den Button „Weiter".

Zurück zum Inhalt dieses Kapitels

Nun kannst du dir die Einzelheiten der Installation aussuchen:

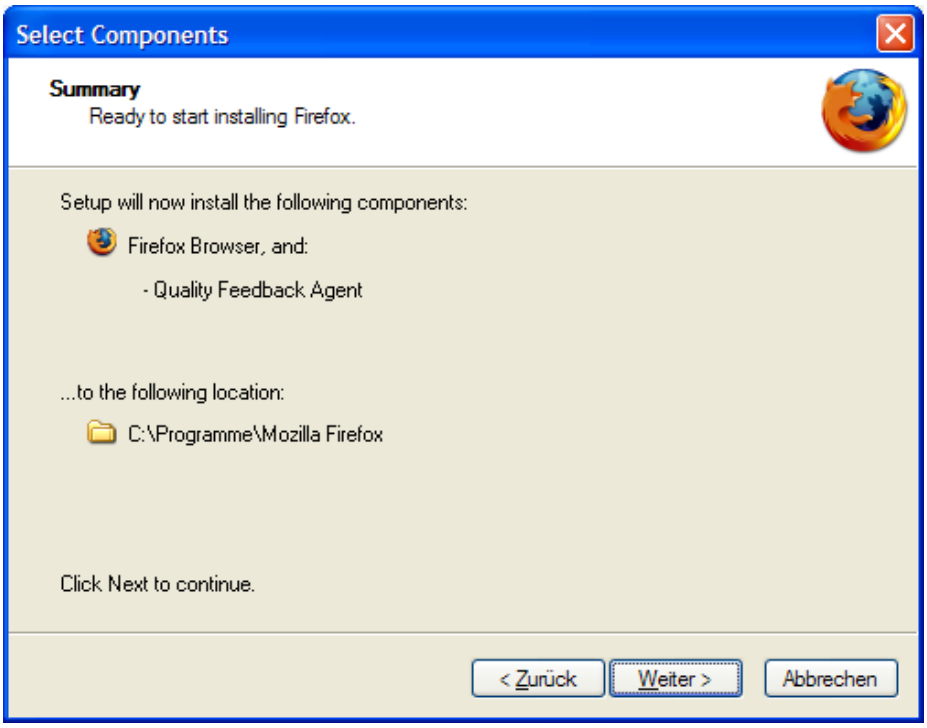


Falls du das Programm in ein anderes als das Mozilla-Standardverzeichnis installieren willst, musst du die „Custom“-Installation wählen. Hier kannst du dir auch aussuchen, ob du ein Firefox-Icon auf dem Desktop haben willst oder nicht und ein paar andere Dinge.

Falls du mit den Standard-Einstellungen leben kannst, wähle die „Standard“-Installation und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

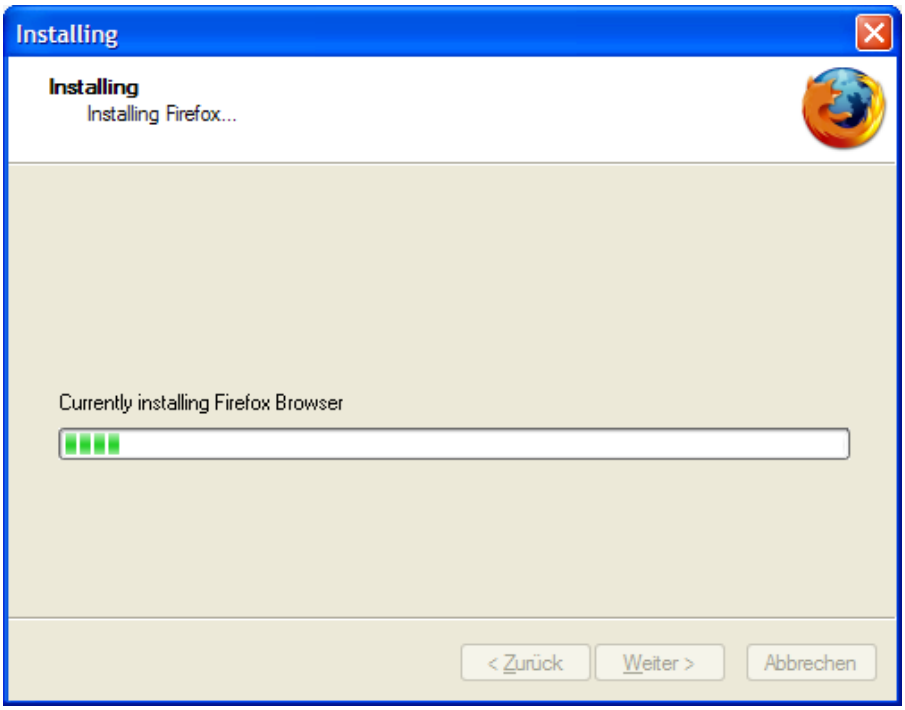
Es folgt noch die Information, was wohin installiert wird (hier die Standard-Installation):



Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

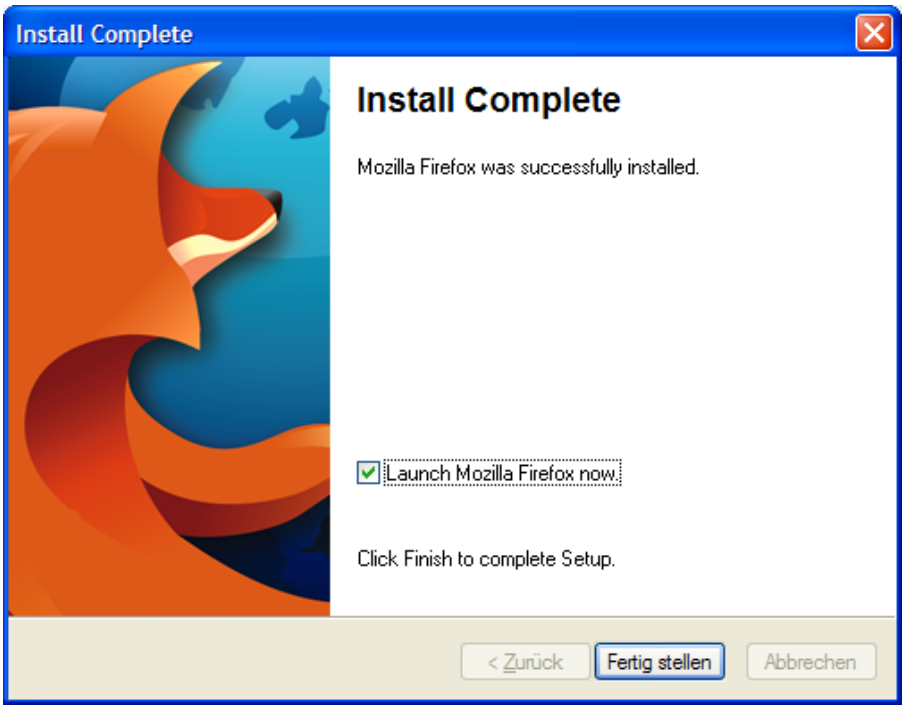
Nun beginnt die eigentliche Installation:



Du bekommst den Fortschritt der Installation angezeigt.

Zurück zum Inhalt dieses Kapitels

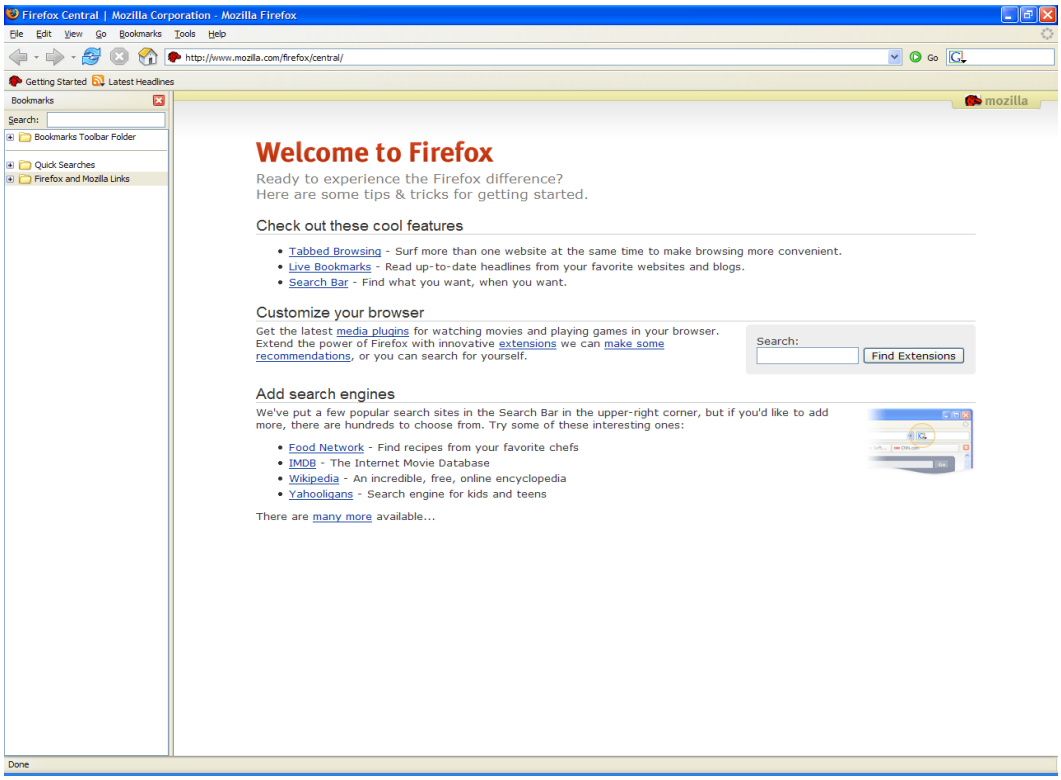
Wenn die Installation beendet wurde, erhältst du einen entsprechenden Hinweis:



Du wirst noch gefragt, ob du Firefox gleich starten willst (Launch Firefox) oder nicht. Drücke den Button „Fertig stellen“

Zurück zum Inhalt dieses Kapitels

Der Internet-Browser wird gleich gestartet:



Du siehst vor dir eine schöne, aufgeräumte Programmoberfläche.

Falls du die Bookmarks (Lesezeichen) auf der linken Seite nicht siehst – keine Panik. Wie du die hervorzauberst, erfährst du im nächsten Kapitel.

Zurück zum Inhalt dieses Kapitels

15.2 Die Verwendung von Firefox

In diesem Kapitel findest du einige wichtige Informationen zur Verwendung von Firefox. Es gibt Kapitel zu

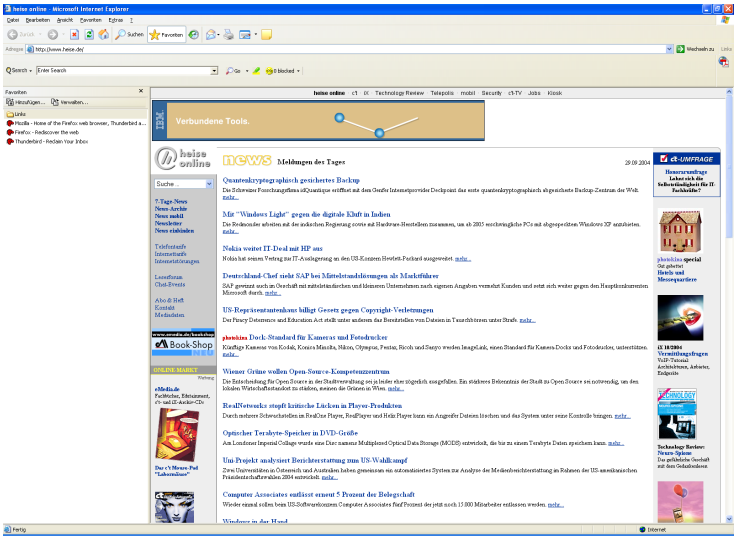
- Import von Daten aus anderen Internet Browsern (z.B. Bookmarks)
- Optionen in Firefox
- Die Anzeige der Bookmarks
- Das Löschen von privaten Daten im Internet Browsser
- Das Aktualisieren von Firefox

Der Import von Daten aus anderen Internet Browsern

Wahrscheinlich hast du in deinem bisher verwendeten Browser bereits Bookmarks (Lesezeichen) angelegt und Optionen ausgewählt. Firefox bietet dir eine komfortable Möglichkeit, diese Daten aus folgenden Browsern zu übernehmen (zu importieren):

- Microsoft Internet Explorer
- Opera

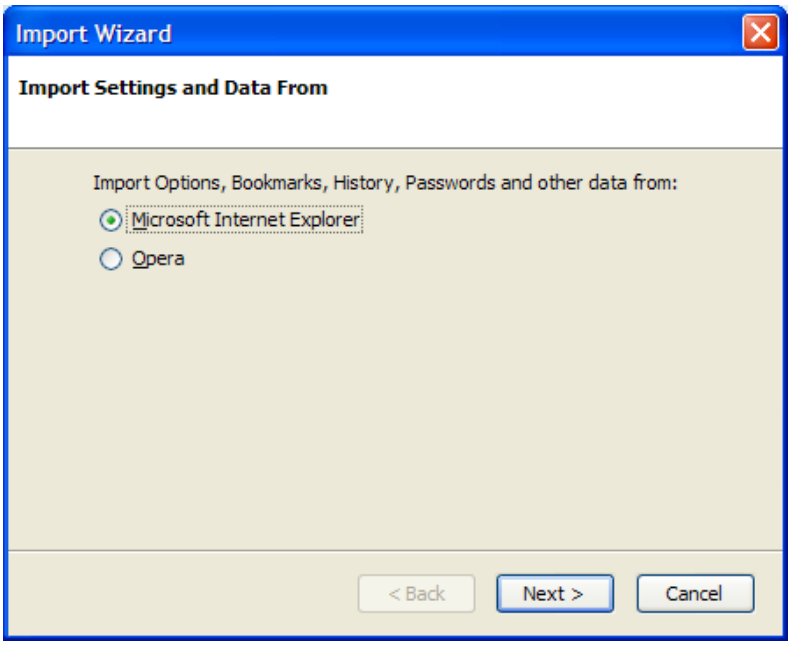
Wir zeigen hier, wie z.B. Einstellungen aus Microsoft Internet Explorer übernommen werden können. Hier das Beispiel des Microsoft Internet Explorer-Fensters:



Zum Ausprobieren haben wir drei Bookmarks (Lesezeichen, Favoriten) angelegt.

Zurück zum Inhalt dieses Kapitels

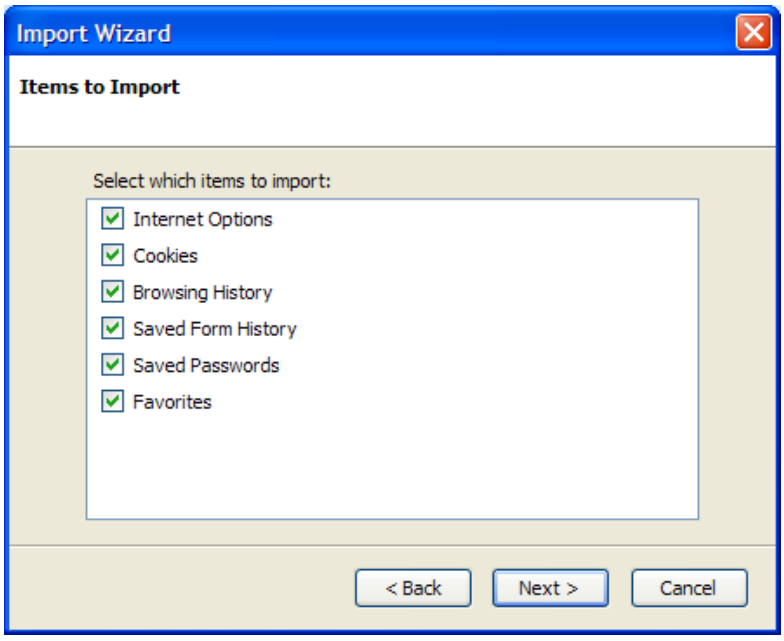
Wähle im Firefox-Browser den Menüpunkt File ⇨ Import. Ein kleines Fenster öffnet sich:



Hier kannst du angeben, von welchem Browser du die Daten importieren willst. In unserem Beispiel markieren wir „Microsoft Internet Explorer“. Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Dann wirst du gefragt, was du alles importieren willst:

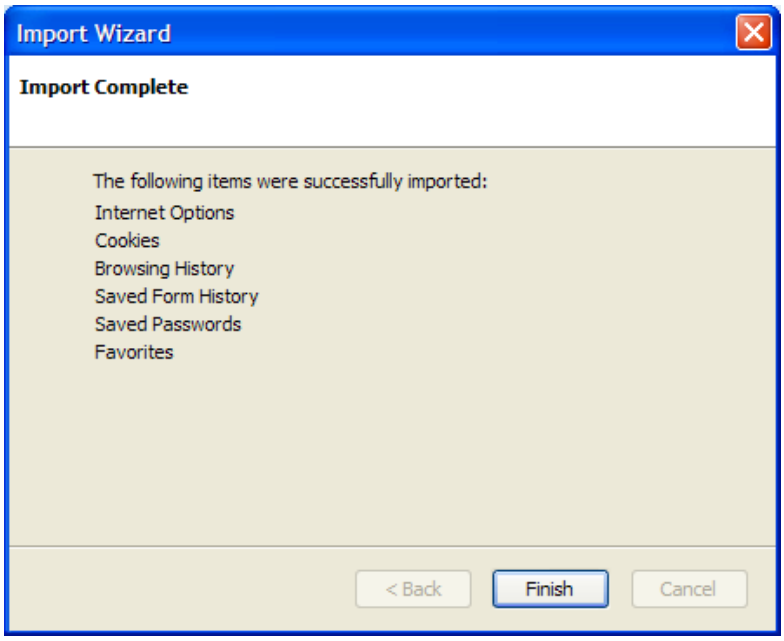


Wie du siehst, kannst du dir sogar gespeicherte Cookies, Passwörter (die solltest du aber nicht im Internet Browser speichern!), die Liste mit besuchten Webseiten u.a. importieren lassen.

Such dir die gewünschten Inhalte aus und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

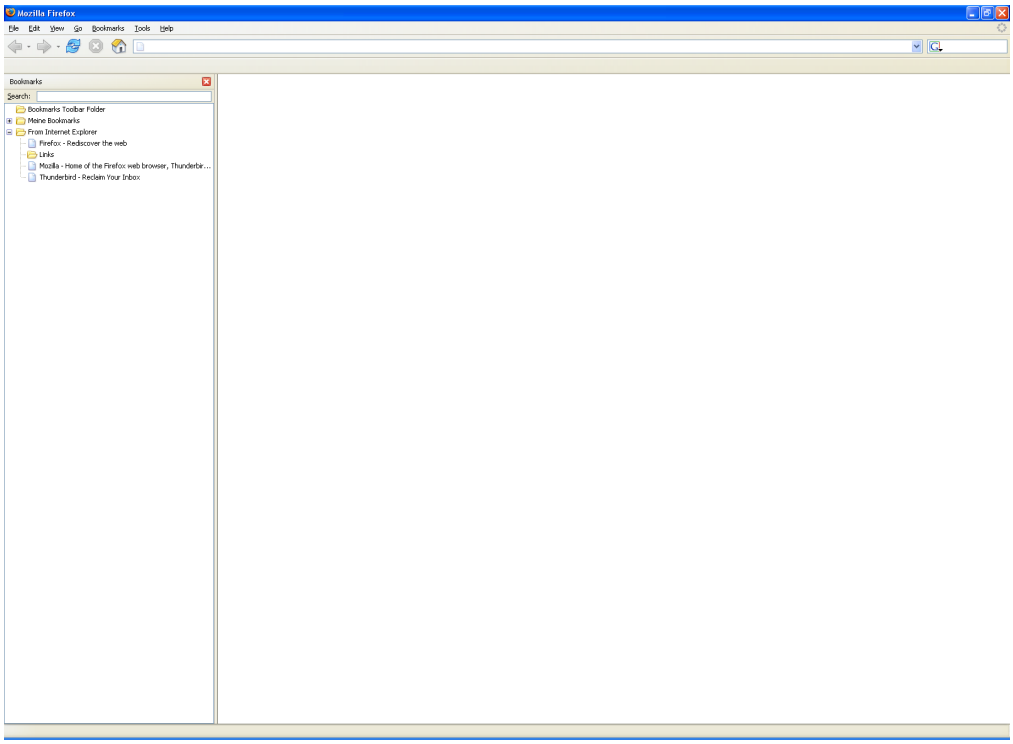
Fertig, du erhältst noch eine Liste mit allen importierten Inhalten:



Schließe die Übernahme durch Drücken des Buttons „Finish“ ab.

Zurück zum Inhalt dieses Kapitels

Du siehst nun im Firefox-Browser die übernommenen Bookmarks (Lesezeichen, Favoriten) auf der linken Seite im Ordner „From Internet Explorer“.

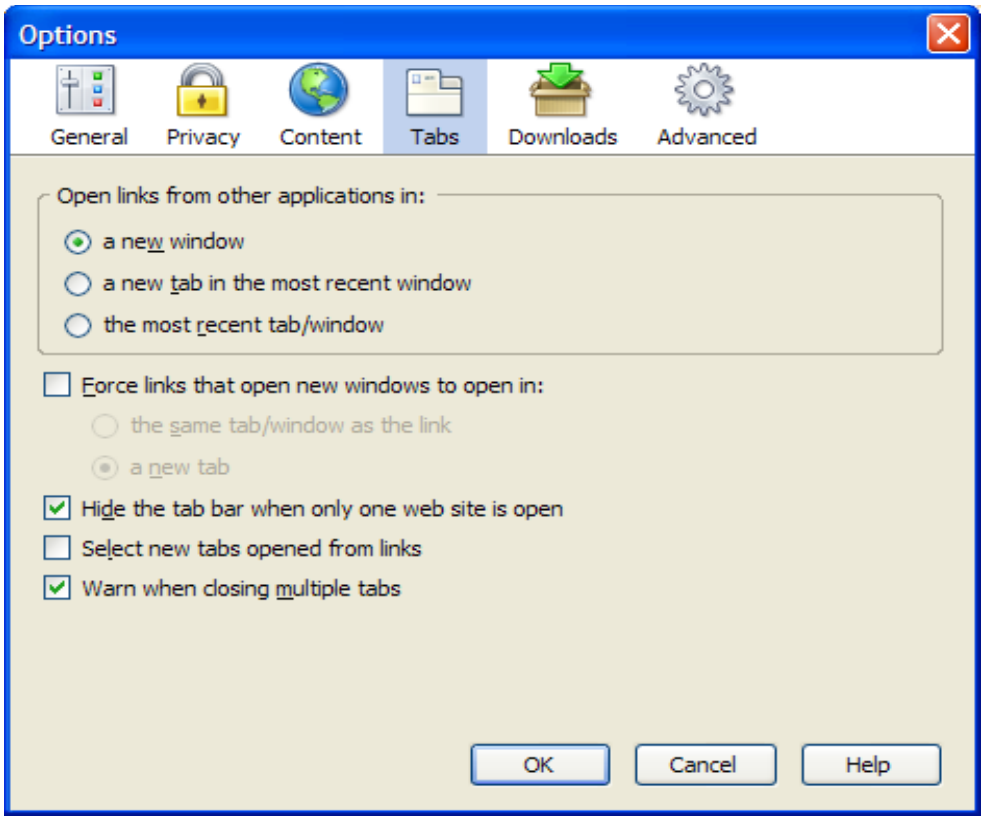


Wie du siehst, ist die Übernahme wirklich sehr einfach. Du kannst nun natürlich die Bookmarks nach Belieben verschieben, z.B. sie aus dem Ordner „From Internet Explorer“ herausholen o.ä.

Zurück zum Inhalt dieses Kapitels

Optionen in Firefox

Wenn du im Menü den Punkt Tools ⇨ Options auswählst, wird das Optionenfenster mit einer Vielzahl von Einstellungsmöglichkeiten geöffnet:



Klicke dich einfach mal durch die verschiedenen Fenster durch. Die einzelnen Punkte sind nicht allzu schwer verständlich.

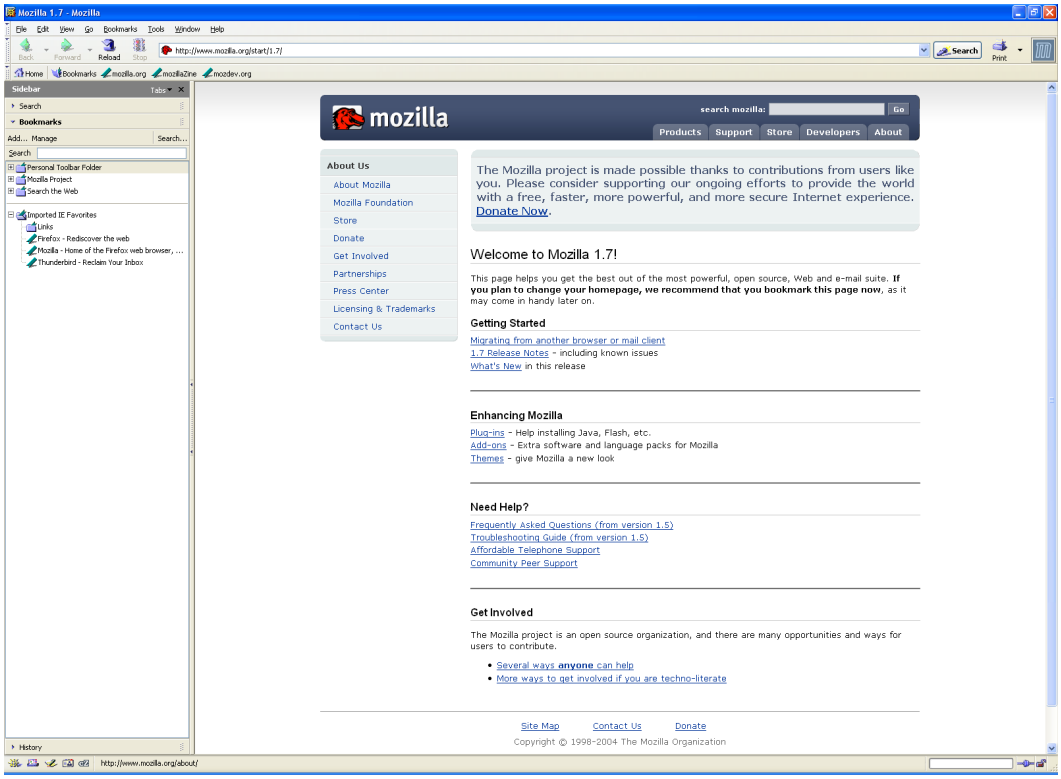
So kannst du z.B. unter „Downloads“ den Standard-Ordner angeben, in den Dateien, die du aus dem Internet ladest, gespeichert werden sollen.

Unter „General“ siehst du auch den Punkt „Connection“ mit dem Button „Connection Settings“. Hier kannst du bei Verwendung von JAP zum anonymen Surfen oder von Webwasher die entsprechenden Port-Nummern angeben, an denen der Browser mit den Programmen kommuniziert.

Zurück zum Inhalt dieses Kapitels

Die Anzeige der Bookmarks

Wenn du willst, dass deine Bookmarks (Lesezeichen, Favoriten) auf der linken Seite angezeigt werden, drücke einfach die Tasten Ctrl+B oder wähle im Menü den Punkt View ⇨ Sidebar ⇨ Bookmars.



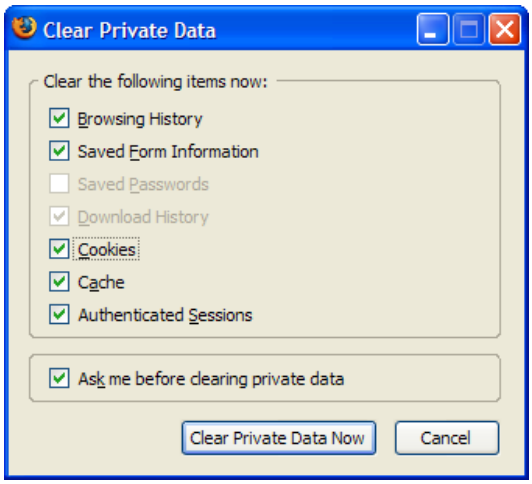
Es erscheint dann auf der linken Seite die sogenannte „Sidebar“ mit deinen Bookmarks. Du kannst dir aber auch durch Drücken von Ctrl+H oder wählen des Menüpunkts View ⇨ Sidebar ⇨ History die letzten Webseiten anzeigen lassen, die du besucht hast (den „Verlauf“).

Zurück zum Inhalt dieses Kapitels

Das Löschen von privaten Daten im Internet Browser

Auch Firefox merkt sich z.B. die Internet-Seiten, die du besucht hast, legt Cookies ab und einiges mehr. Alles natürlich nur, wenn du das in den Optionen von Firefox erlaubt hast.

Wenn du diese privaten Informationen wieder los werden möchtest, wähle einfach im Menü „Tools ⇨ Clear Private Data“. Folgendes Fenster erscheint:



Du kannst dir aussuchen, was du löschen möchtest. Wähle das Gewünschte aus und drücke den Button „Clear Private Data Now“.

Und keine Sorge, es kann nichts passieren. Deine Bookmarks, Einstellungen und andere wichtige Dinge bleiben natürlich immer erhalten.

Es ist gar keine gute Idee, Passwörter und/oder Formulardaten vom Internet Browser speichern zu lassen. Wenn eine andere neugierige Person Zugang zu deinem Computer hat, kann diese Person natürlich diese Informationen ausnutzen.

Unter „Tools ⇨ Options“ findest du dann im Optionenfenster beim Menüpunkt „Privacy“ die entsprechenden Einstellungen.

Zurück zum Inhalt dieses Kapitels

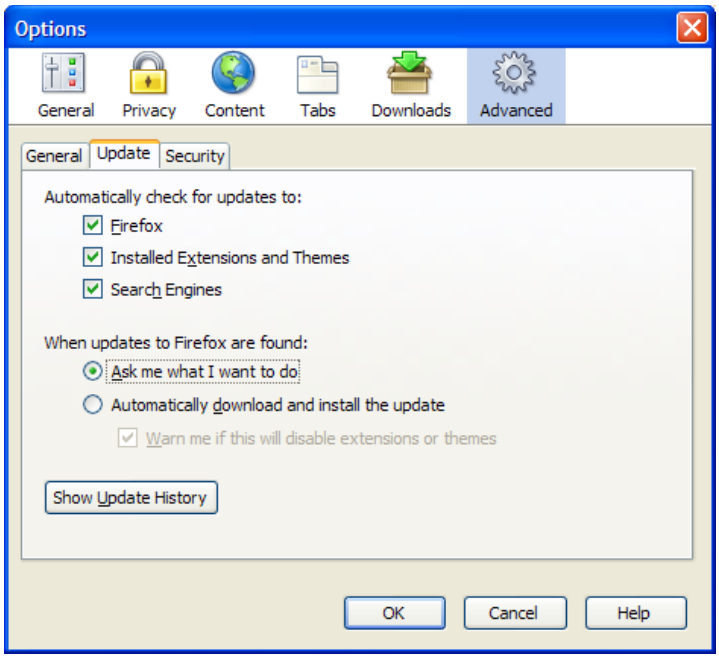
Das Aktualisieren von Firefox

Wie bereits erwähnt, ist es bei allen sicherheitsrelevanten Programmen äußerst wichtig, immer die neueste Version zu verwenden.

Seit der in diesem Handbuch vorgestellten Version 1.5 von Firefox ist das Aktualisieren besonders komfortabel.

Wähle einfach im Menü „Help ⇨ Check for Updates“, es wird sofort geprüft, ob eine neuere Version verfügbar ist.

Du kannst bei den Optionen auch angeben, dass Firefox selbständig prüft, ob es neue Versionen gibt. Wähle dazu den Menüpunkt „Tools ⇨ Options“ und dann den Menüpunkt „Advanced ⇨ Update“:



Hier wurde z.B. eingestellt, dass Firefox selbständig auf Neuerungen prüfen soll und gegebenenfalls nachfragen soll, ob die Änderungen installiert werden sollen.

Zurück zum Inhalt dieses Kapitels

16 Thunderbird

Überblick

Dieses Kapitel enthält eine Beschreibung, wie mensch das kostenlose Mailprogramm Thunderbird installiert und verwendet.

Wie schon in Kapiteln am Beginn dieses Handbuchs angeführt, raten wir dringend von der Verwendung von Microsoft Outlook als Mailprogramm ab. Auch bei Outlook tauchen dauernd schwerwiegende Sicherheitslücken auf, die großen Schaden anrichten können.

Mit Thunderbird erhältst du ein gutes Mailprogramm mit einem sehr wirkungsvollen integrierten Spamfilter. Es gibt aber natürlich auch andere gute Mailprogramme.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Thunderbird
- Die Verwendung von Thunderbird

Die aktuellste Version von Thunderbird findest du immer auf der Webseite http://www.mozilla.com/thunderbird/.

Informationen zu weiteren Mozilla Projekten findest du unter http://www.mozilla.org.

Es wird in Kürze die neue Version 1.5 verfügbar sein, zum Zeitpunkt der Erstellung dieses Handbuchs gibt es davon nur eine noch nicht freigegebene sog. Beta-Version.

Checke von Zeit zu Zeit die Webseite von Thunderbird und installiere diese Version, sobald sie verfügbar ist.

16.1 Die Installation von Thunderbird

Du findest das Installationsprogramm auf der CD im Ordner Thunderbird\Windows.

Für Windows öffne den Windows Explorer, wechsle auf der CD ins richtige Verzeichnis.



Thunderbird\Windows


Thunderbird Setup 1.0.7.exe

Doppelklicke auf der CD auf die Datei Thunderbird Setup 1.0.7.exe, dann erscheint gleich mal das Willkommensfenster:

Drücke den Button „Weiter“.

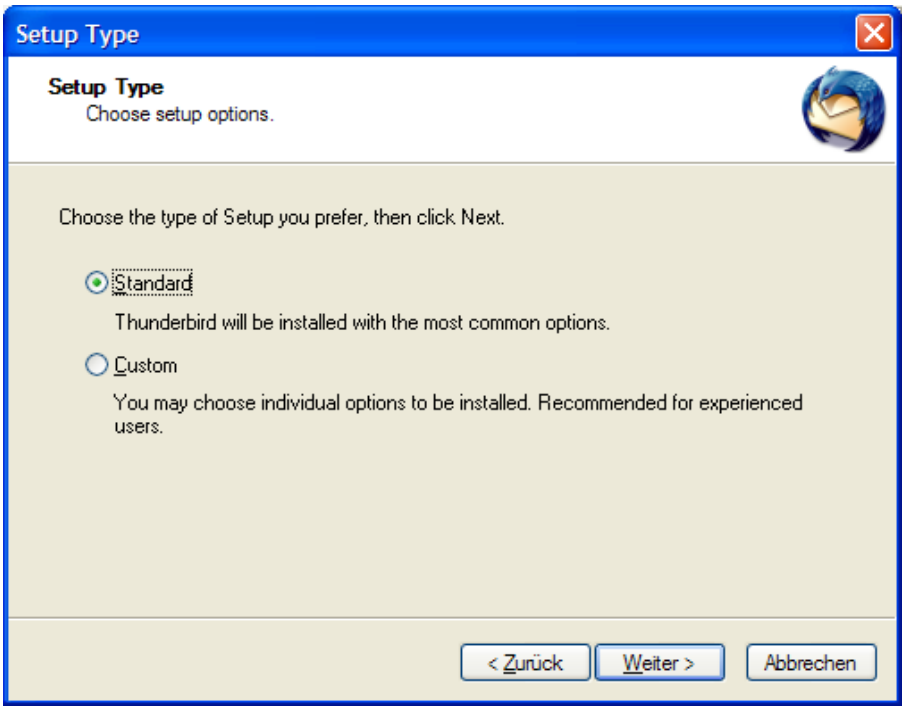
Zurück zum Inhalt dieses Kapitels

Es folgt die Lizenzvereinbarung:

Markiere „I Accept the terms” und drücke den Button “Weiter”.

Zurück zum Inhalt dieses Kapitels

Du kannst dir nun die Art der Installation aussuchen:

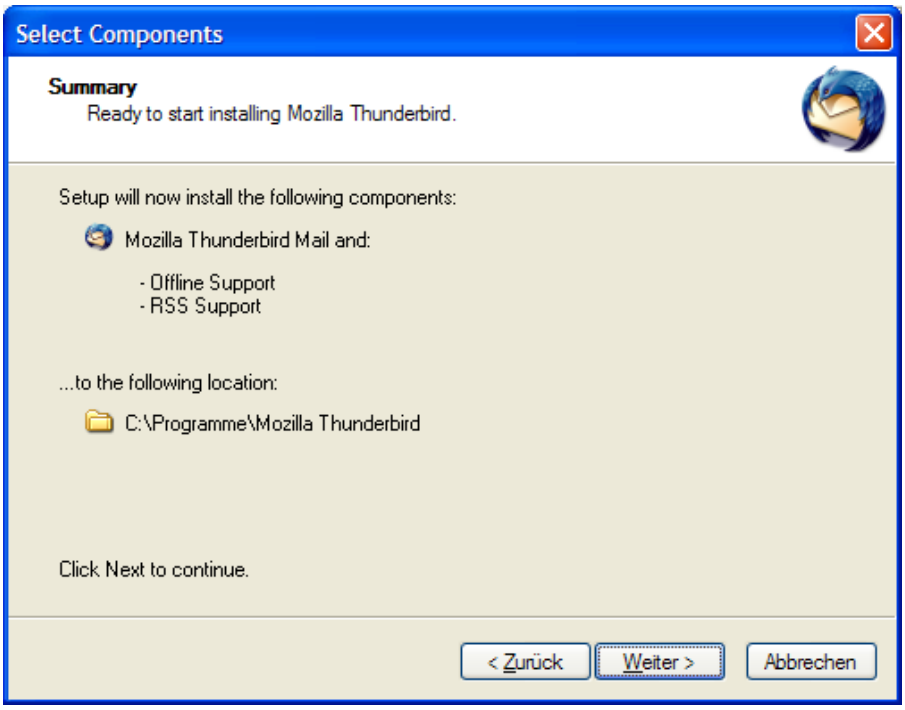


Falls du das Programm in ein anderes als das Mozilla-Standardverzeichnis installieren willst, musst du die „Custom“-Installation wählen. Hier kannst du dir auch aussuchen, ob du ein Thunderbird-Icon auf dem Desktop haben willst oder nicht und ein paar andere Dinge.

Falls du mit den Standard-Einstellungen leben kannst, wähle die „Standard“-Installation und drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

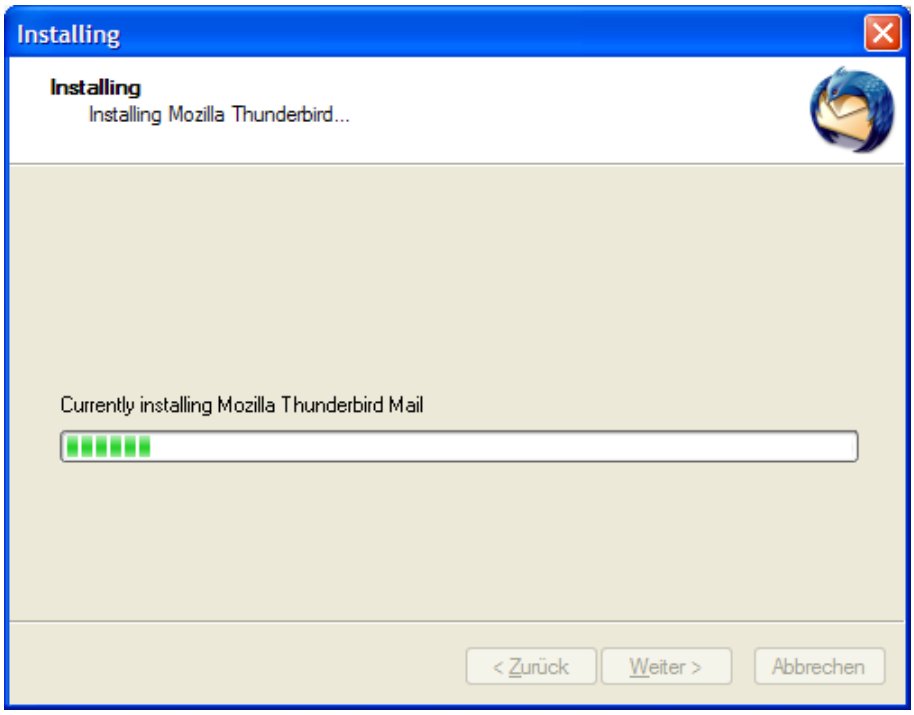
Es folgt noch die Information, was wohin installiert wird (hier die Standard-Installation):



Drücke den Button „Weiter“.

Zurück zum Inhalt dieses Kapitels

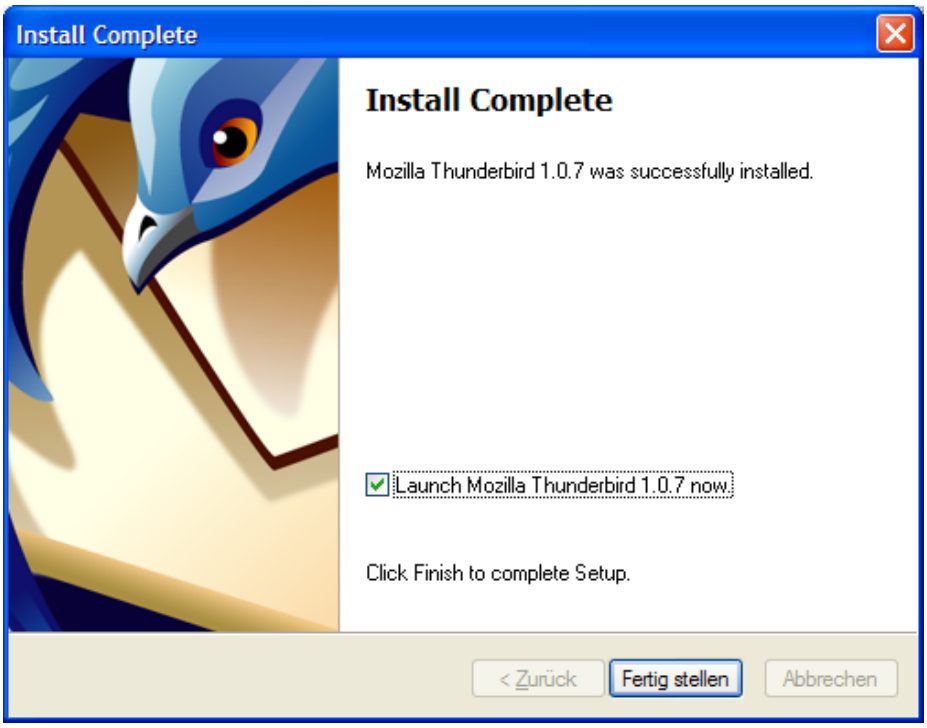
Nun beginnt die eigentliche Installation:



Der Fortschritt der Installation wird angezeigt.

Zurück zum Inhalt dieses Kapitels

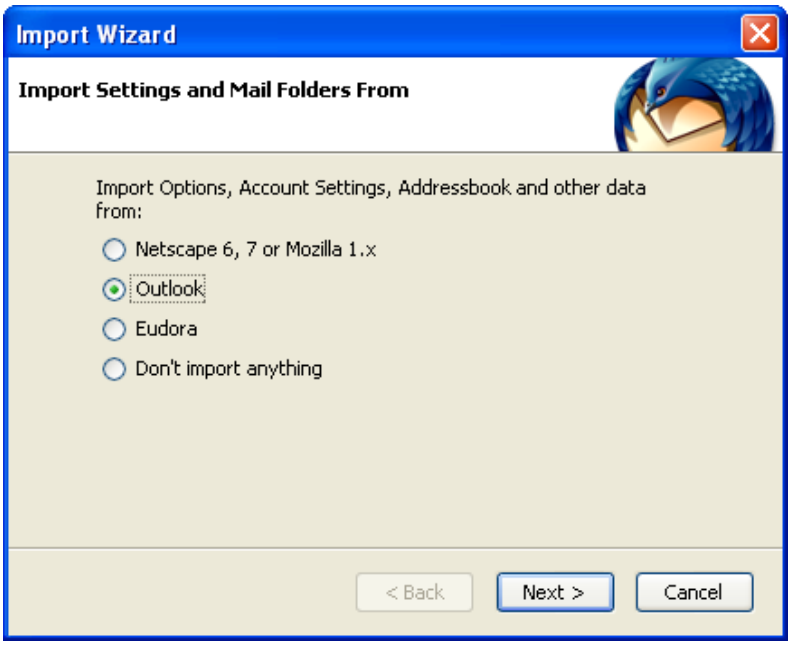
Nach Beenden der Installation wird die entsprechende Information angezeigt:



Du kannst dir noch aussuchen, ob Thunderbird gleich gestartet werden soll (Launch Thunderbird) oder nicht. Drücke den Button „Fertig stellen“.

Zurück zum Inhalt dieses Kapitels

Nach dem ersten Start von Thunderbird wirst du gleich gefragt, ob du Daten (z.B. Mails) gleich von einem anderen vorher verwendeten Mailprogramm übernehmen (importieren) willst:



Wenn du das willst, markiere das entsprechende Mailprogramm. Wenn nicht, markiere „Don't import anything". Du kannst diesen Import auch später jederzeit durchführen. Drücke den Button „Next".

Wie dieser Import von Daten aus einem anderen Mailprogramm durchgeführt wird, erfährst du im nächsten Kapitel.

Wenn du hier (oder später) die Einstellungen (Settings) und Mails aus einem anderen Mailprogramm übernimmst, ersparst du dir das Anlegen eines Accounts mit den Informationen zu deinem Internetprovider.

Zurück zum Inhalt dieses Kapitels

16.2 Die Verwendung von Thunderbird

In diesem Kapitel werden einige wichtige Punkte zur Verwendung von Thunderbird angeführt. Du findest Informationen zu

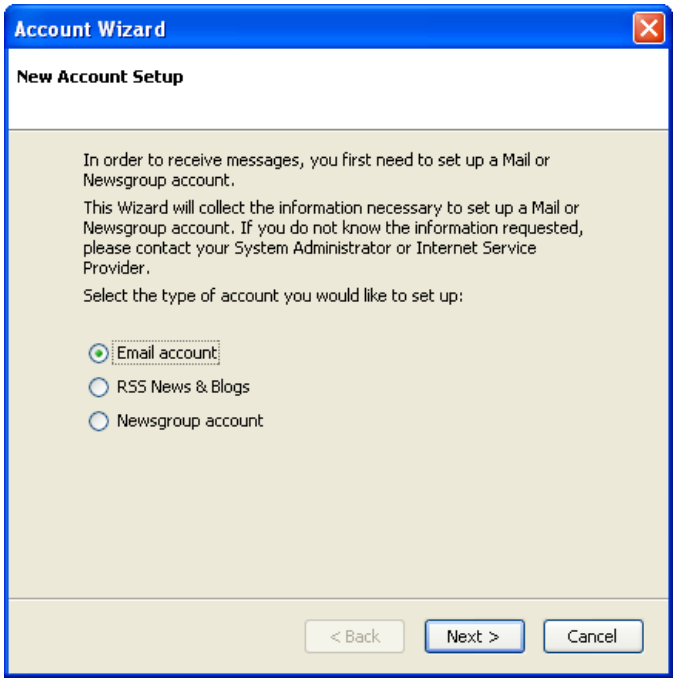
- Das Anlegen eines neuen Accounts
- Der Import von Daten aus anderen Internet Browsern (z.B. Bookmarks)
- Das Ändern der Ordner mit den Mails
- Die Einstellung des Spam-Filters

Zurück zum Inhalt dieses Kapitels

Das Anlegen eines neuen Accounts

Bei der erstmaligen Verwendung von Thunderbird musst du einen neuen Mail-Account für dich anlegen. Du erhältst gleich nach dem Start des Programms die Möglichkeit dazu.

Du kannst einen Account auch durch Wahl des Menüpunktes Tools ⇨ Account Settings im Programm Thunderbird anlegen, wähle in diesem Fall dann den Button „Add Account…



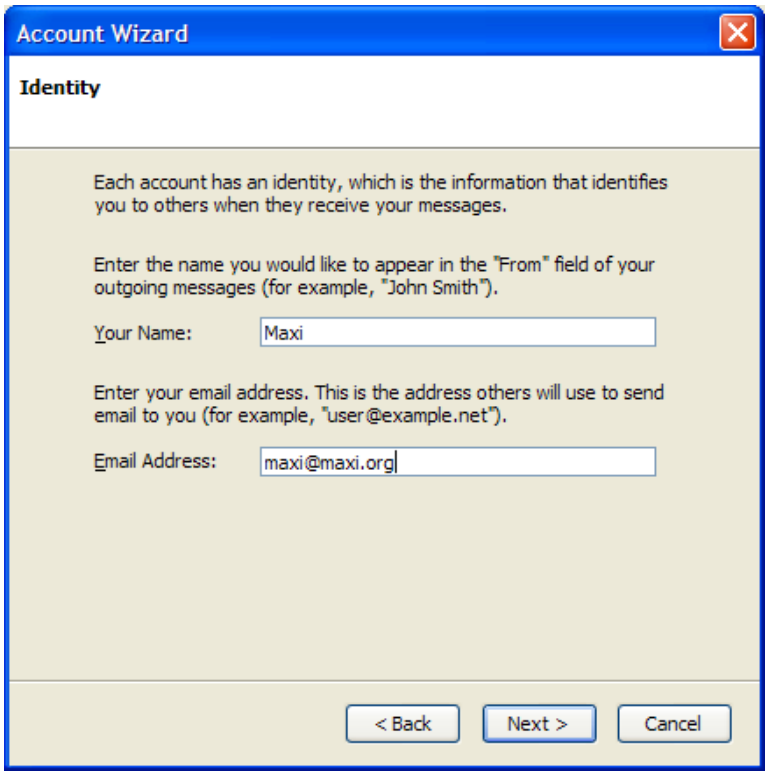
Lege mal einen E-Mail Account an. Markiere den entsprechenden Punkt und drücke den Button „Next“.

Wenn du die Einstellungen (Settings) aus einem anderen Mailprogramm übernimmst (importierst), ersparst du dir das Anlegen eines Accounts mit den Informationen zu deinem Internetprovider.

Wie du diese Informationen nachträglich übernehmen kannst, erfährst du im Kapitel Das Importieren von Daten aus anderen Mailprogrammen.

Zurück zum Inhalt dieses Kapitels

Du kannst jetzt deinen Namen (wie er in deinen E-Mails als AbsenderIn aufscheinen soll) und deine E-Mail-Adresse angeben:



Gib deinen E-Mail-Namen und deine E-Mail-Adresse an, drücke dann den Button „Next“.

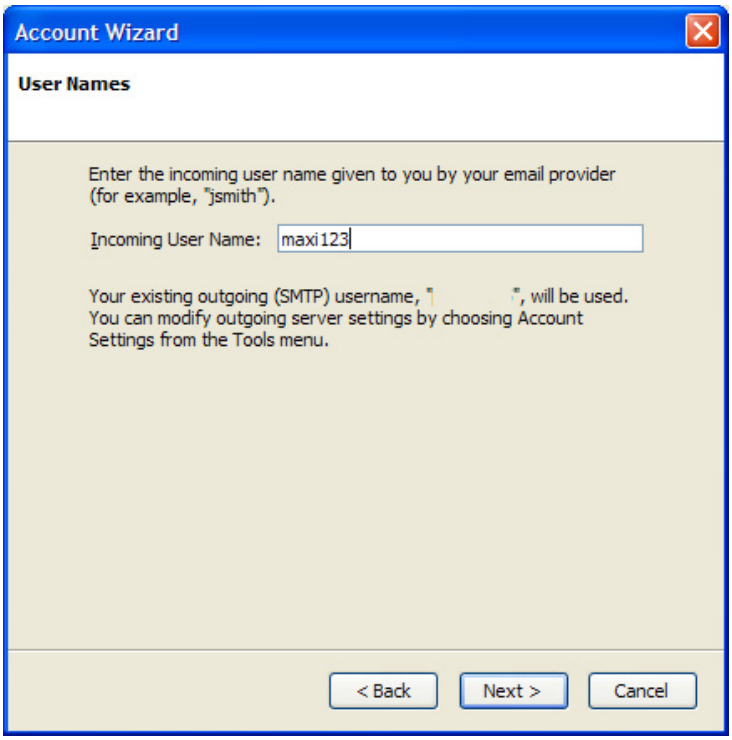
Zurück zum Inhalt dieses Kapitels

Nun musst du Informationen dazu angeben, wo deine Mails zu holen sind:

Näheres zum „Incoming Server“ muss dir dein Internet-Provider zur Verfügung stellen (z.B. hier die Adresse des POP3-Server). Trage die Information ein und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

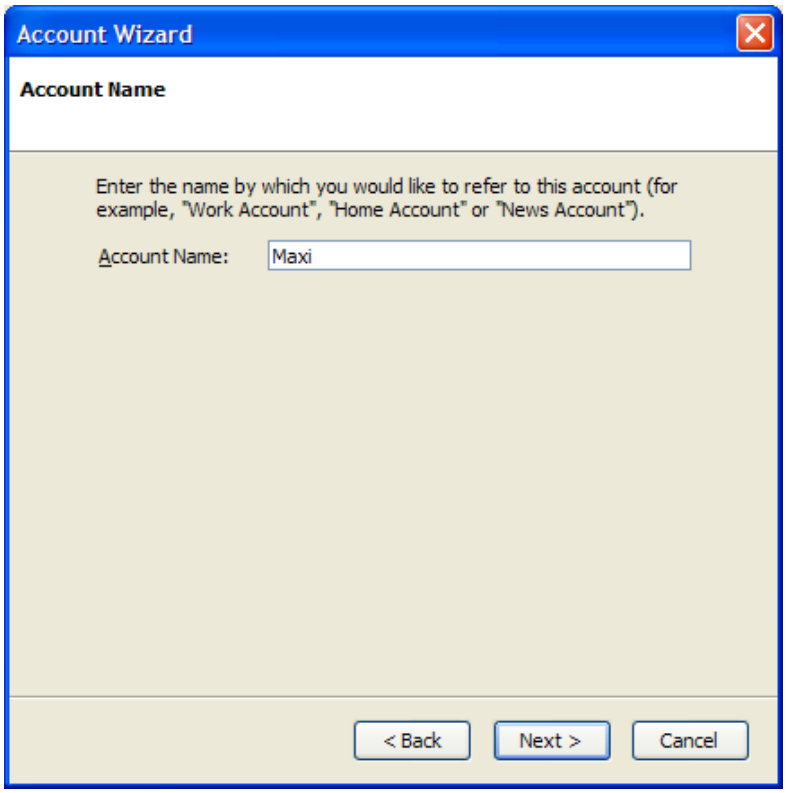
Nun musst du noch den BenutzerInnennamen angeben, den du bei der Verbindung zum Mailserver deines Internet-Providers verwendest:



Gib deinen BenutzerInnen-Namen an und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

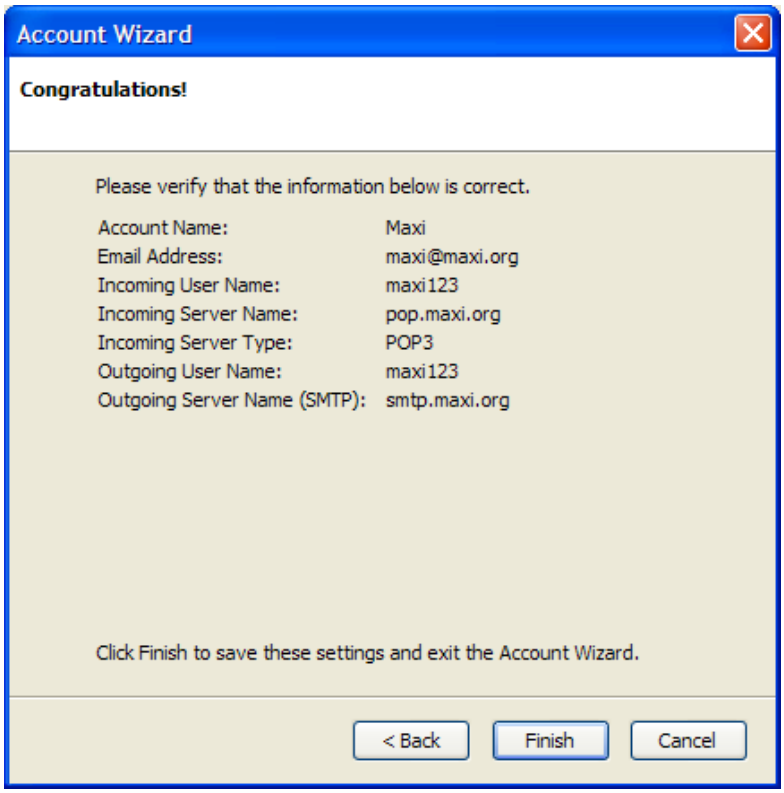
Jetzt kannst du diesem Account noch einen hübschen Namen geben:



Trage den von dir gewünschten Namen ein, diesen Namen siehst du nur in deinem Thunderbird-Programm. Drücke dann den Button „Next“.

Zurück zum Inhalt dieses Kapitels

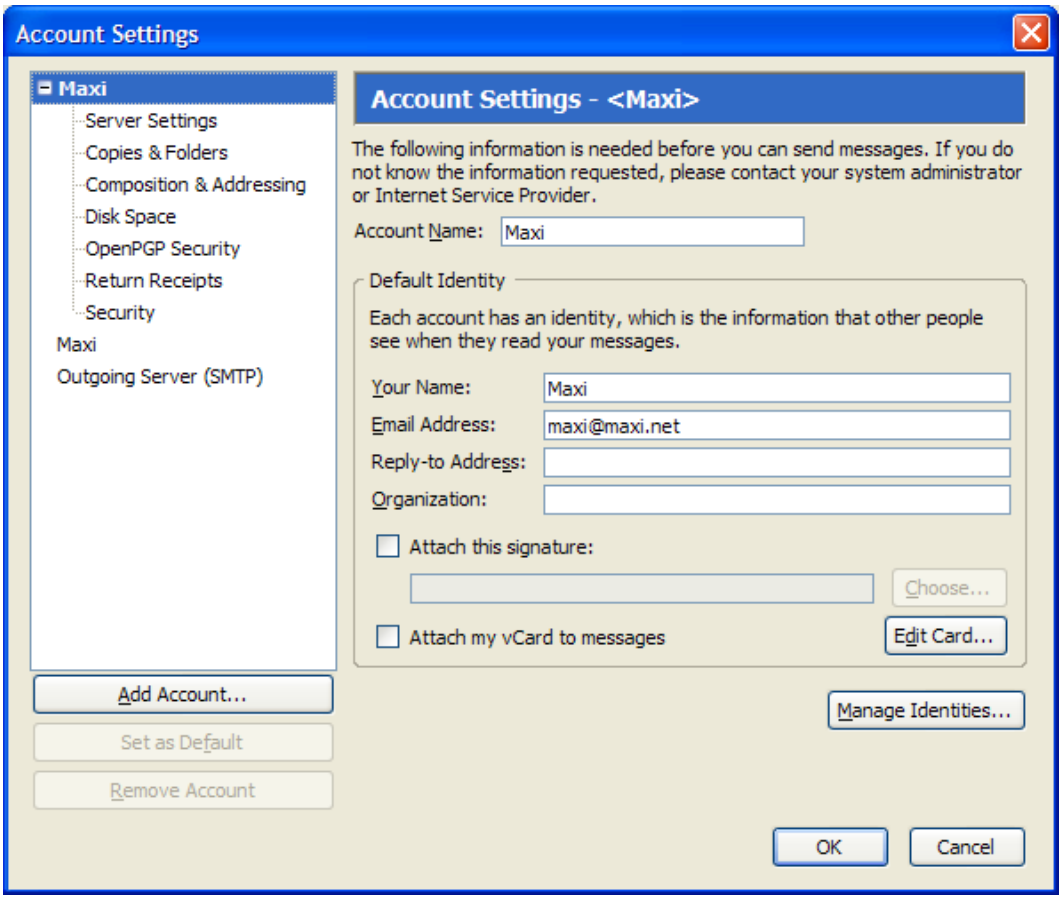
Du erhältst noch eine Zusammenstellung aller von dir zur Verfügung gestellten Angaben:



Bestätige die Angaben durch Drücken des Buttons „Finish“.

Zurück zum Inhalt dieses Kapitels

Wenn du das Anlegen des Accounts über das Thunderbird-Menü gestartet hast, siehst du jetzt im Account-Settings-Fenster den Account. Du kannst das nachfolgende Fenster auch durch Wahl des Menüpunktes „Tools ⇨ Account Settings“ öffnen.



Hier kannst du auch die Einstellungen zu einem Account ändern, weitere Einstellungen vornehmen oder einen Account löschen (Remove Account).

So, das war’s schon, du hast jetzt ein ausgezeichnetes, sicheres und sehr komfortables E-Mail-Programm vor dir. Und so nebenbei: es hat einen sehr wirkungsvollen Spam-Filter zum Aussortieren von Mail-Müll integriert – mehr dazu in Kapitel Die Einstellungen des Spam-Filters.

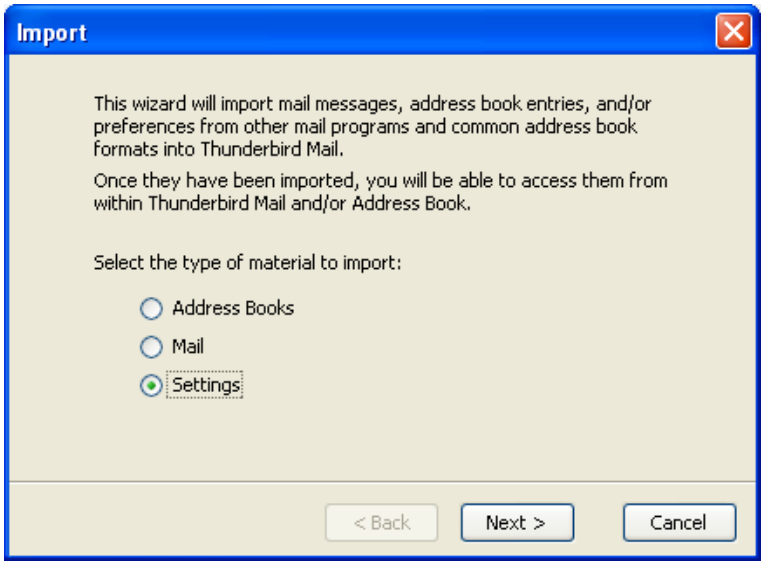
Zurück zum Inhalt dieses Kapitels

Der Import von Daten aus anderen Mailprogrammen

Wenn du Einstellungen und Daten (Mails) aus deinem bisher verwendeten E-Mail-Programm übernehmen (importieren) willst, so geht das bei Thunderbird ganz einfach. So ersparst du dir auch das manuelle Anlegen von Accounts und ihren Einstellungen.

Das Übernehmen von Einstellungen und Account-Informationen

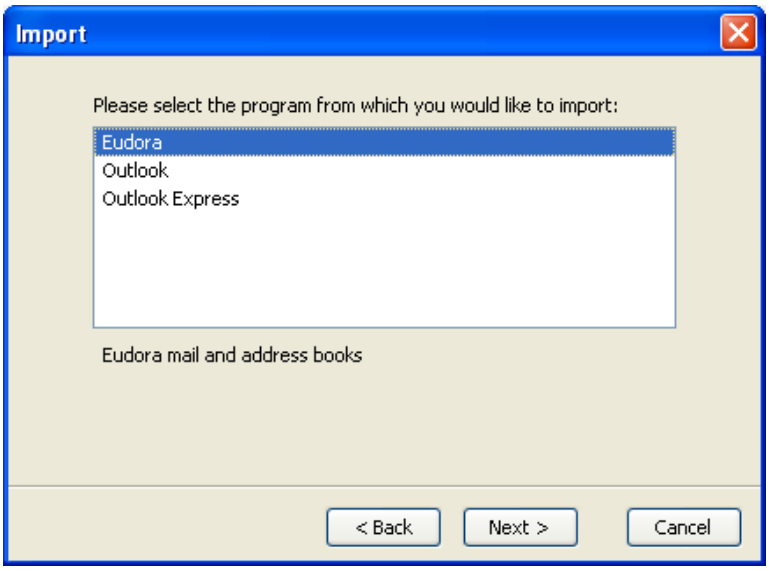
Wähle nach dem Starten des Programms den Menüpunkt Tools ⇨ Import: Im ersten Fenster wirst du gefragt, was du importieren willst:



In unserem Beispiel wählen wir als ersten Schritt das Importieren der Einstellungen (Account-, Serverinformationen). Drücke nach der Auswahl den Button „Next“.

Zurück zum Inhalt dieses Kapitels

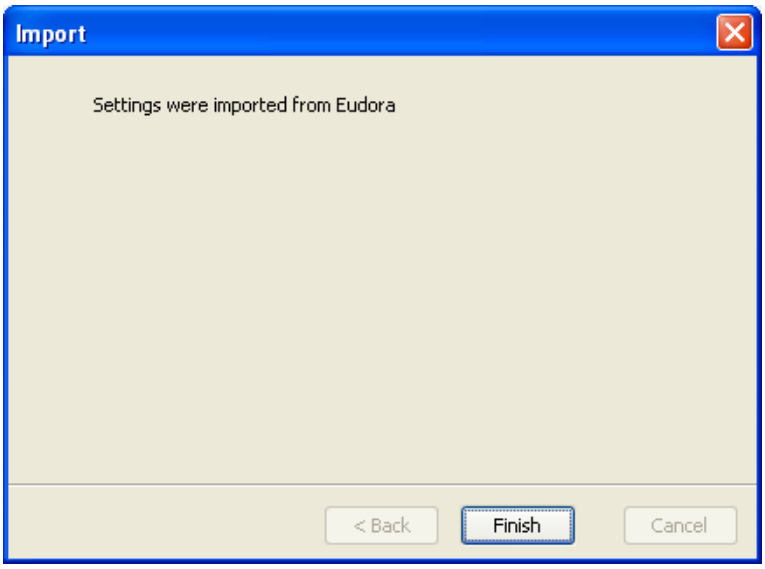
Nun musst du angeben, aus welchem Programm du die Einstellungen übernehmen willst:



Markiere das entsprechende Programm und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

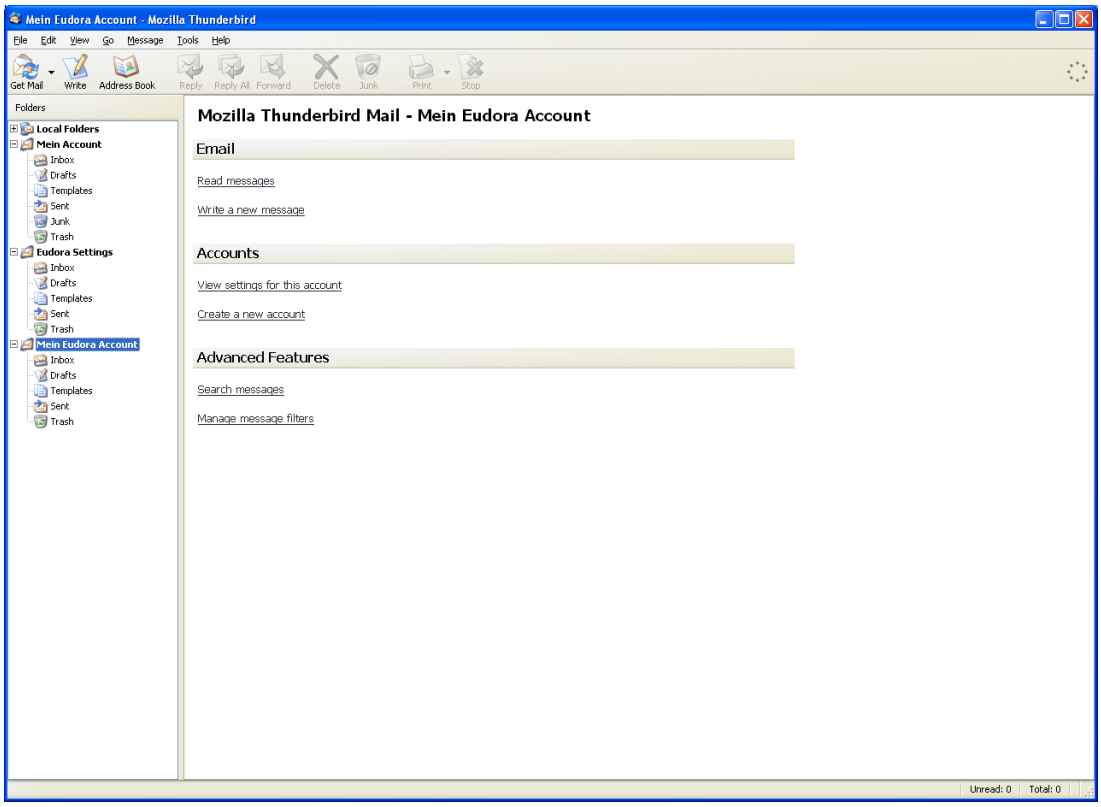
Du erhältst nun die Erfolgsmeldung, dass die Einstellungen importiert wurden:



Bestätige die Information durch Drücken des Buttons „Finish“.

Zurück zum Inhalt dieses Kapitels

Du siehst nun die übernommenen Informationen im Hauptfenster von Thunderbird auf der linken Seite:

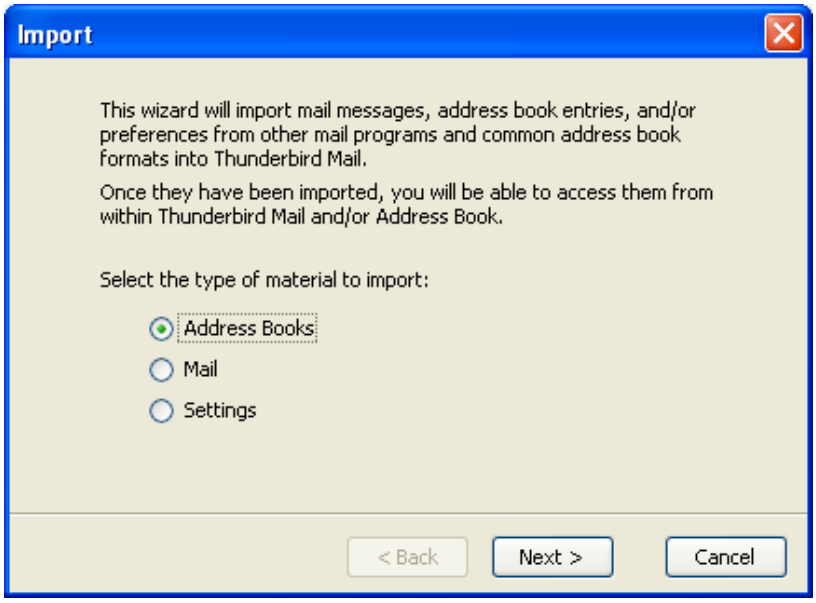


Sowohl die Einstellungen (Eudora Settings) als auch die Account-Informationen (Mein Eudora Account) wurden übernommen. Jetzt fehlen noch die Adressbücher und die Mails selbst.

Zurück zum Inhalt dieses Kapitels

Das Übernehmen von Adressbüchern

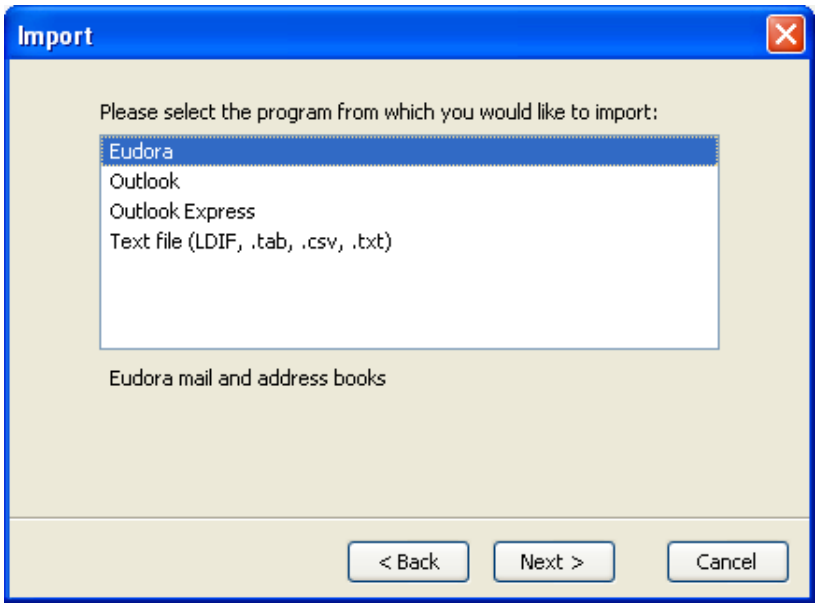
Wähle zur Übernahme (zum Import) deines Adressbuches aus einem anderen Mailprogramm den Menüpunkt „Tools ⇨ Import“. Im ersten Fenster wirst du gefragt, was du importieren willst.



Wähle den Punkt „Address Books“ und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

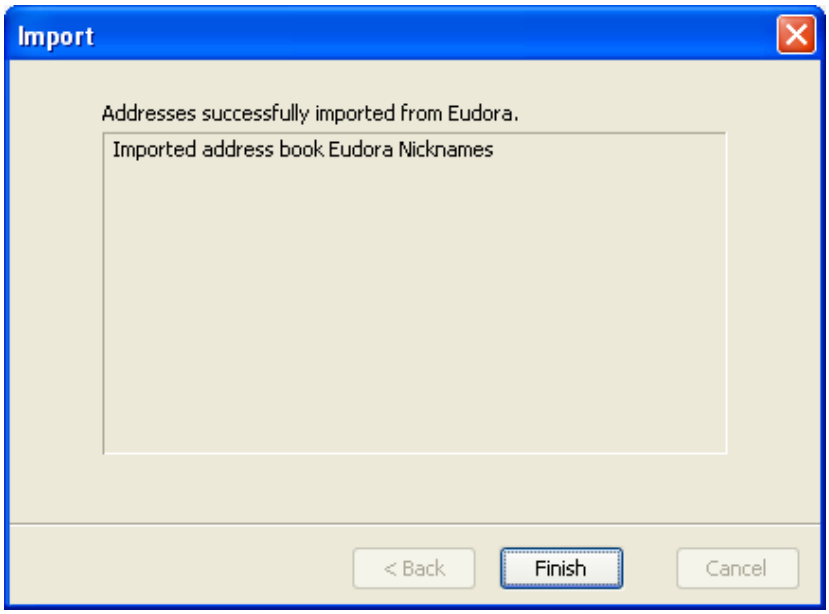
Nun musst du angeben, aus welchem Programm bzw. welcher Datei du die Einstellungen übernehmen willst:



Wähle das entsprechende Programm oder die entsprechende Datei aus und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Nun beginnt die Übernahme des Adressbuchs. Nach kurzer Zeit erhältst du die Meldung über das Beenden des Imports:



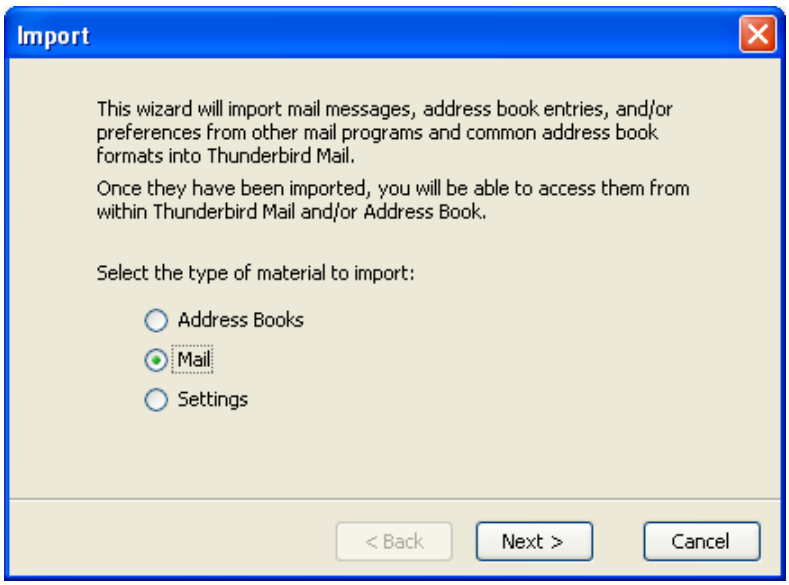
Fertig, das Adressbuch wurde vollständig importiert. Drücke den Button „Finish“.

Du kannst die korrekte Übernahme prüfen, wenn du auf das Icon „Address Book“ in der Menüleiste von Thunderbird drückst. Dort siehst du eine Liste mit allen vorhandenen Einträgen und den zugehörigen Nicknames.

Zurück zum Inhalt dieses Kapitels

Das Übernehmen von Mails

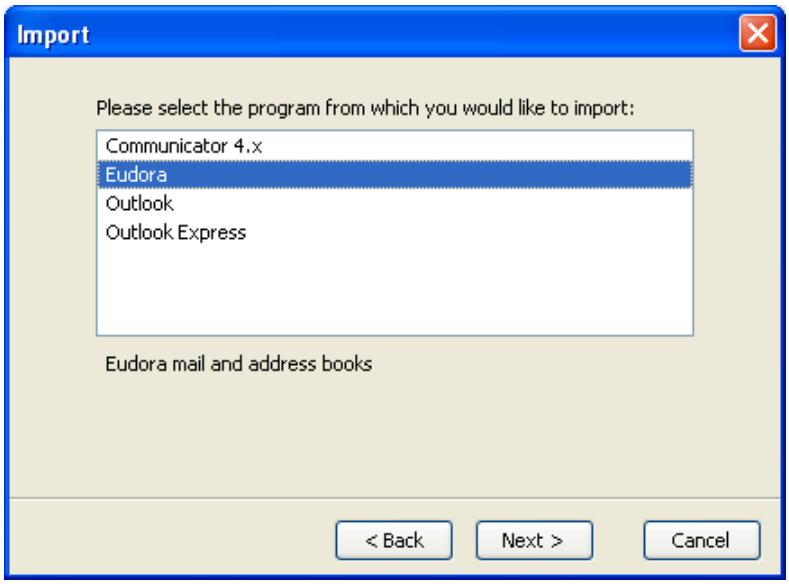
Wähle nach dem Starten des Programms den Menüpunkt „Tools ⇨ Import“: Im ersten Fenster wirst du gefragt, was du importieren willst.



Wähle das Importieren von Mails. Drücke nach der Auswahl den Button „Next“.

Zurück zum Inhalt dieses Kapitels

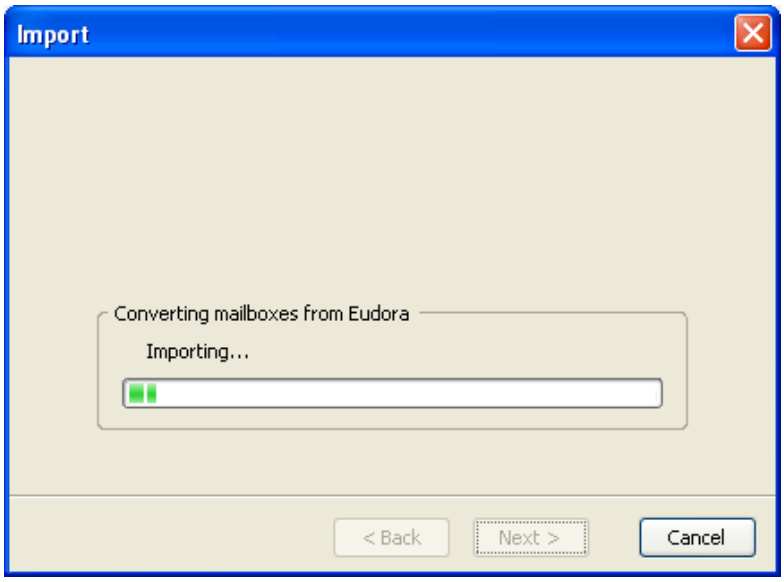
Nun musst du angeben, aus welchem Programm du die Einstellungen übernehmen willst:



Markiere das entsprechende Programm und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Der Import beginnt nun:

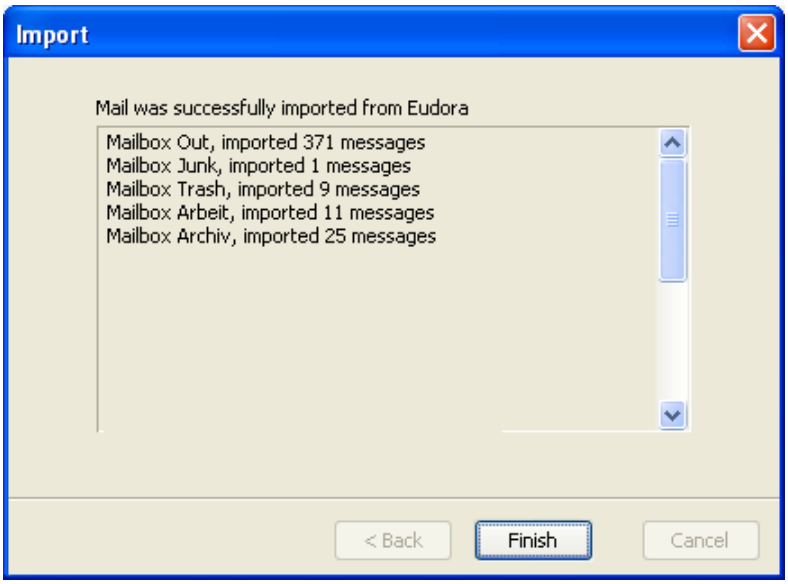


Du siehst in einem Fenster den Fortschritt des Vorgangs.

Dieser Import dauert - abhängig von der Menge deiner bisher gesammelten Mails – ein bisschen länger als die bisherigen Schritte. Ist aber nicht sehr schlimm, hab ein bisschen Geduld.

Zurück zum Inhalt dieses Kapitels

Nach Fertigstellung des Imports erhältst du die entsprechende Erfolgsmeldung:



Alle Mails wurden importiert. Bestätige die Information durch Drücken des Buttons „Finish“.

Du findest die importierten Mails nun im Thunderbird-Fenster im Mail-Ordner „Local Folders ⇨ Eudora Mail“.

Zurück zum Inhalt dieses Kapitels

Ändern der Ordner mit den Mails

Nach der Installation wurde ein Ordner angelegt, in dem sich deine Mails befinden. Willst du dein Mails aber an einem anderen Ort speichern (z.B. in einem verschlüsselten Bereich), musst du folgendes tun:

- Lege einen Ordner an, in dem alles gespeichert werden soll, in unserem Beispiel ist das der Ordner „Mail“ auf der verschlüsselten Partition mit dem Laufwerksbuchstaben „X“ (zu verschlüsselten Partitionen siehe auch das Kapitel über das Speichern von Thunderbird-Daten auf einem verschlüsselten Laufwerk)
- Suche das Thunderbird-Standardverzeichnis und verschiebe alle Ordner und Dateien in den vorher erstellten Ordner.

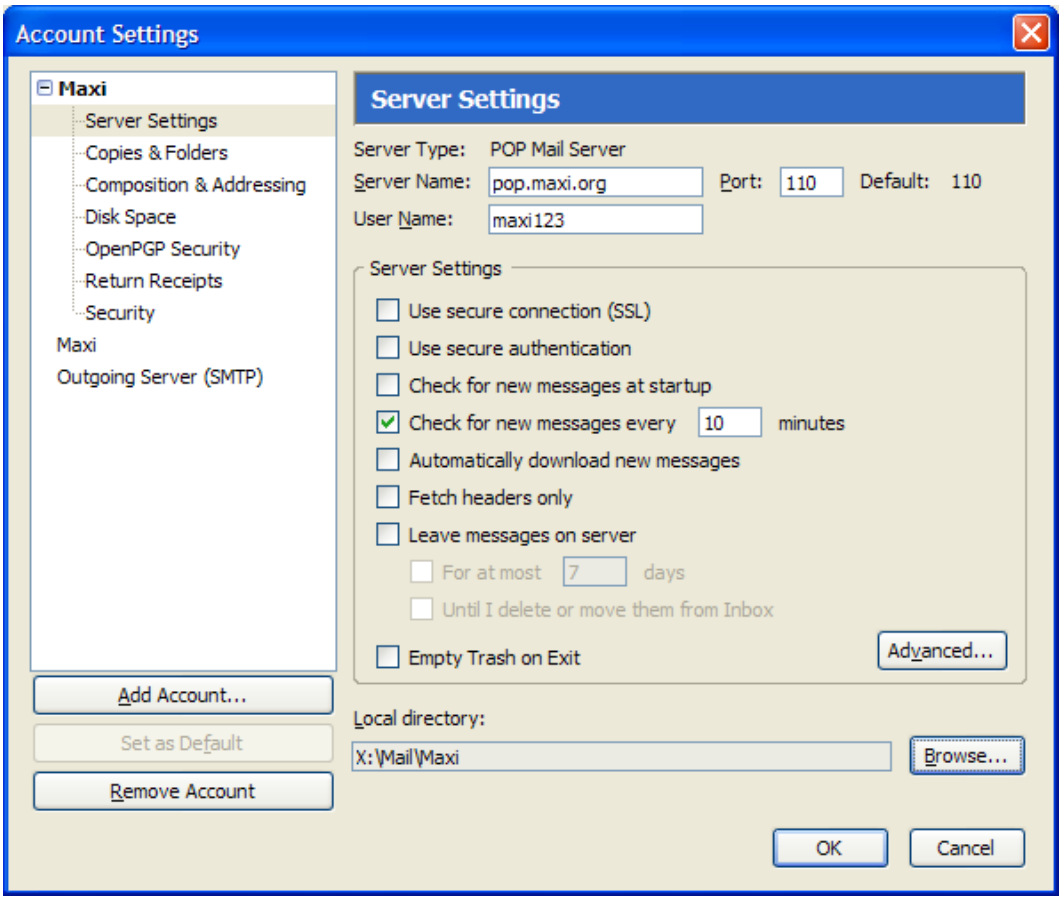
Du findest die Angabe zu diesem Ordner durch Wählen des Menüpunkts Tools ⇨ Account Settings im Thunderbird-Fenster.

Bei deinem Account findest du beim Menüpunkt „Server Settings“ unter „Local Directory“ den Pfad zum Ordner des auf der linken Seite gewählten Accounts.

- Trage den neuen Ordner ein. Wähle dazu im Menü von Firefox Tools ⇨ Account Settings. Wähle „Server Settings“ bei dem Account, dessen Mails du am neuen Ort speichern willst. Trage den Ordner unter „Local Directory“ ein, du musst dazu den Button „Browse“ drücken und den Ordner suchen.

Zurück zum Inhalt dieses Kapitels

Nachfolgend siehst du, dass unter „Local directory“ ein anderer Ordner eingetragen wurde:



Bestätige die Angaben durch Drücken des Buttons „OK“. Ab sofort werden die Mails dieses Accounts im neuen Ordner abgelegt.

Diesen Vorgang musst du gegebenenfalls für alle Accounts ausführen, deren Mails in diesem Ordner gespeichert werden sollen.

Zurück zum Inhalt dieses Kapitels

Die Einstellungen des Spam-Filters

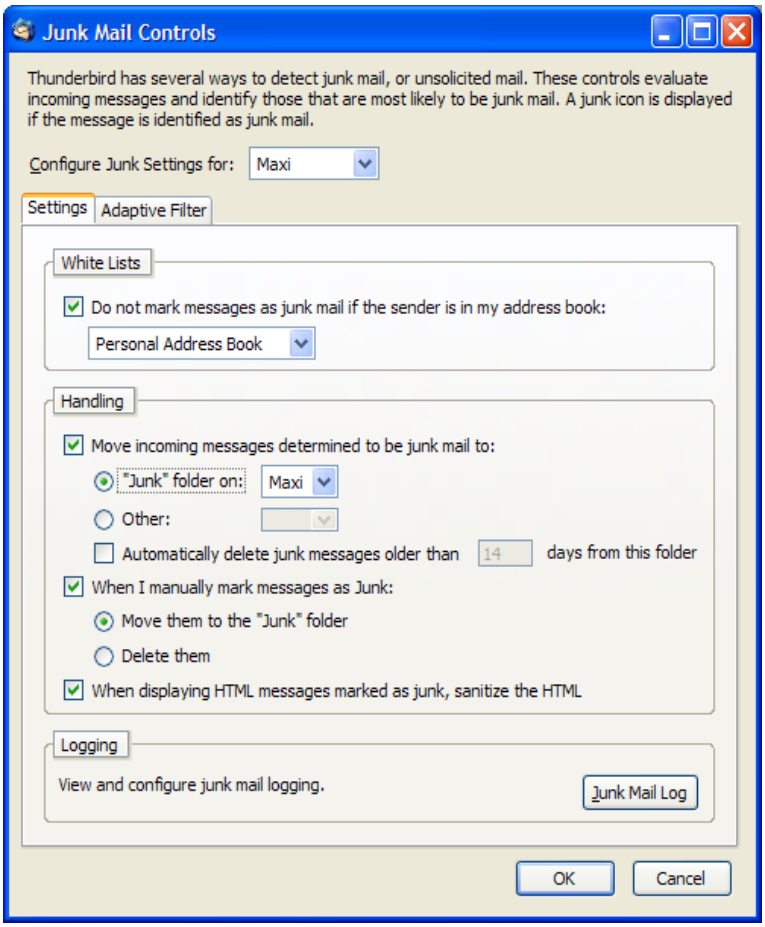
Wie schon erwähnt: mit dem Programm Thunderbird kommt gleich einer der wirkungsvollsten derzeit erhältlichen Spam-Filter mit.

Dieser Filter lernt mit, d.h. zu Beginn wird er Fehler machen (Mails als Mist klassifizieren, die kein Mist sind und umgekehrt). Wenn du vermeintliche Müll-Mails als Nicht-Müll markierst bzw. durchgeschlüpfte Müll-Mails als solche markierst, merkt sich das der Spam-Filter für die Zukunft. So stellt er sich mit der Zeit selbst Regeln zusammen, nach denen er recht zuverlässig Mist und Nicht-Mist auseinanderhalten kann.

Trotzdem musst du immer auch den Ordner mit diesen Spam-Mails prüfen, es kann immer wieder mal passieren, dass eine korrekte Mail als Junk klassifiziert worden ist. Das kommt aber laut Tests nach einer gewissen Lernphase des Filters bei Thunderbird sehr selten vor, seltener jedenfalls als bei den meisten anderen erhältlichen Spam-Filtern.

Zurück zum Inhalt dieses Kapitels

Die Aktivierung und die Einstellungen des Spam-Filters kannst du nach Auswahl des Menüpunktes Tools ⇨ Junk Mail Controls vornehmen:

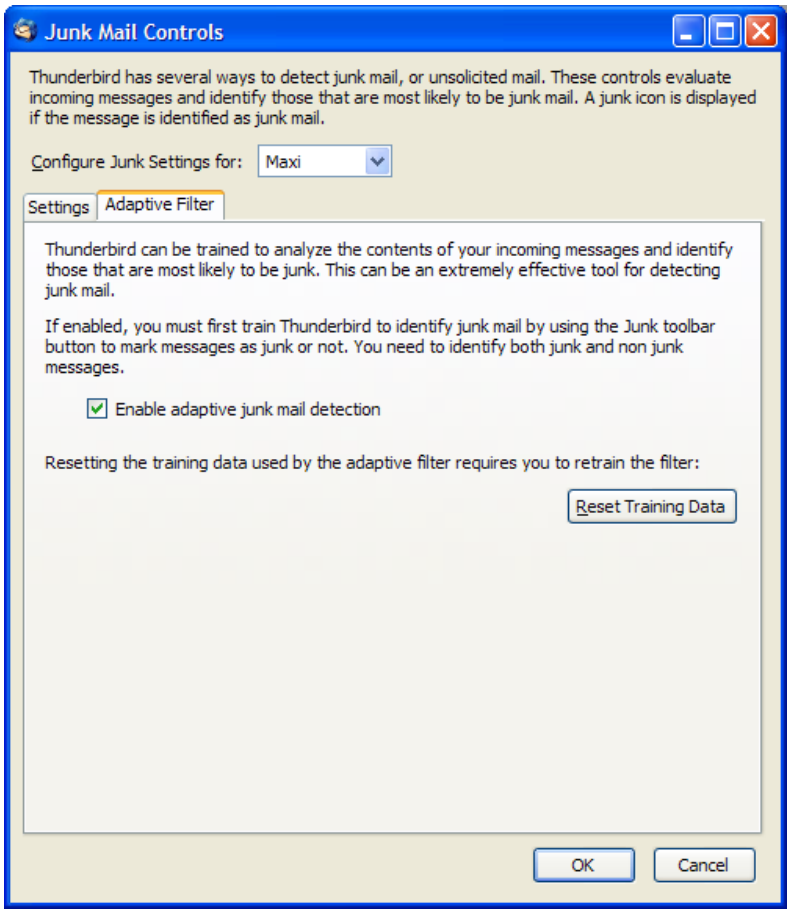


Du kannst hier angeben:

- Den Account, für den diese Einstellungen gelten sollen (hier Maxi)
- White Lists: ob Mails von AbsenderInnen, die in deinem Mail-Adressbuch gefunden werden, automatisch als Nicht-Müll klassifiziert werden sollen
- Handling: in welchen Mail-Ordner als Müll (Junk) erkannte Mails verschoben werden sollen (hier der Ordner „Junk“ des Accounts „Maxi“
- Wo von dir manuell als Junk markierte Mails hinverschoben werden sollen (hier ebenfalls in den Junk-Ordner)

Zurück zum Inhalt dieses Kapitels

Weiters kannst du unter „Adaptive Filter“ angeben, dass der Filter lernen soll, Spam und Nicht-Spam auseinanderzuhalten:



Wenn du „Enable adaptive junk mail detection“ anhakst, lernt der Filter mit, was natürlich sehr sinnvoll ist.

Zurück zum Inhalt dieses Kapitels

17 Window Washer

Überblick

In diesem Kapitel erfährst du Näheres zum Programm Window Washer, einem kostenpflichtigen Programm zum Aufräumen von Datenschrott in Windows.

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 nur für das Betriebssystem Windows.

Du findest Beschreibungen zu folgenden Bereichen:

- Die Installation von Window Washer
- Die Verwendung von Window Washer

Die aktuellste Version von Window Washer findest du immer auf der Webseite http://www.webroot.com/de/downloads/.

17.1 Die Installation von Window Washer

Du findest das Installationsprogramm einer 30-Tage-Testversion von Window Washer auf der zugehörigen CD im Verzeichnis „Window Washer Testversion\Windows“. Dieses Programm gibt es nur für Windows.

Window Washer Testversion\Windows

wwisetup1_1836575495.exe

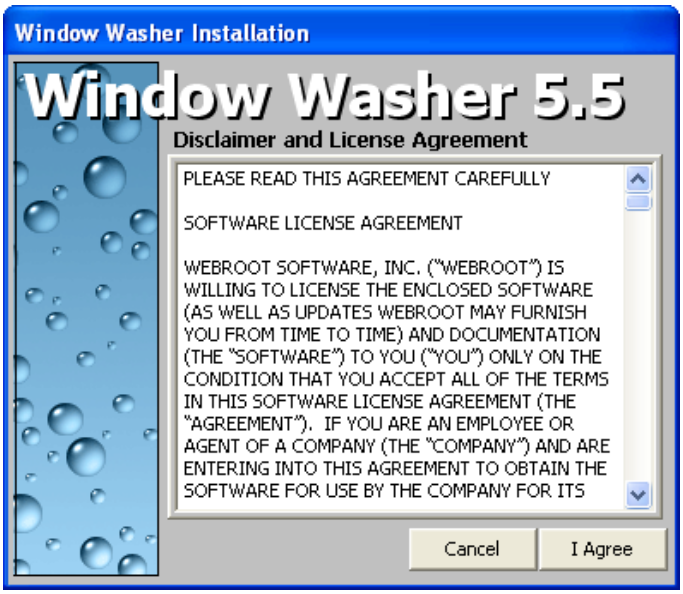
Auf der CD befindet sich nur eine 30-Tage-Testversion. Nach Ablauf der 30 Tage müsstest du das Programm bezahlen. Window Washer kostet ca. EUR 30,-.

Auf der CD befindet sich nicht die allerletzte zu bezahlende Vollversion 6.0, die gibt es derzeit (noch?) nicht als Testversion.

Zum Ausprobieren ist aber auch diese ältere Version 5.5 völlig ausreichend.

Zurück zum Inhalt dieses Kapitels

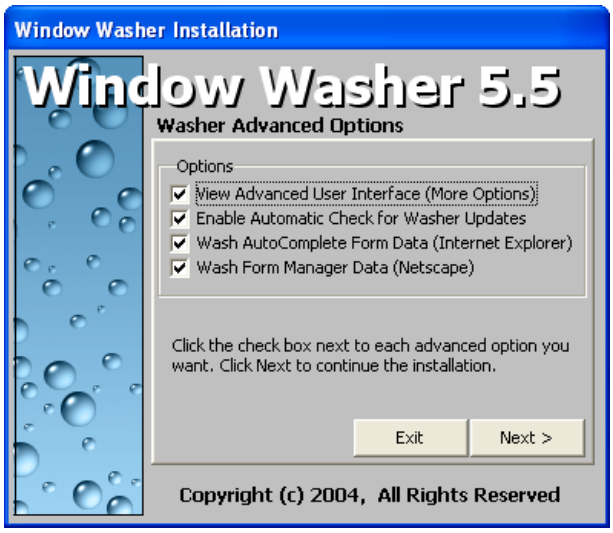
Doppelklicke auf der CD auf die Datei wwisetup1_1836575495.exe. dann erscheint gleich mal das Lizenzvereinbarungsfenster:



Drücke den Button „I Agree“.

Zurück zum Inhalt dieses Kapitels

Jetzt kannst du dir die Bestandteile aussuchen, die installiert werden sollen:



In diesem Fall wird alles installiert inkl. automatischer Aktualisierungen des Programms und erweiterten Einstellungsmöglichkeiten.

Drücke nach der Auswahl den Button „Next“.

Zurück zum Inhalt dieses Kapitels

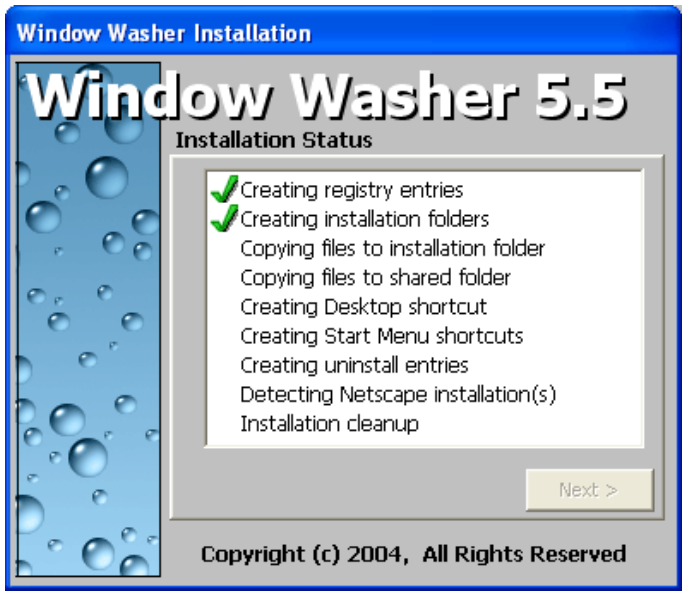
Dann kannst du dir das Verzeichnis aussuchen, in welches das Programm installiert wird. Weiters kannst du dir aussuchen, ob ein Icon am Desktop angelegt werden soll und einiges mehr:

Nimm einfach das vorgeschlagene Verzeichnis und drücke nur den Button „Install“, oder wähle ein eigenes Installationsverzeichnis (z.B. C:\Programme statt C:\Program Files.

Drücken dann den Button „Install“.

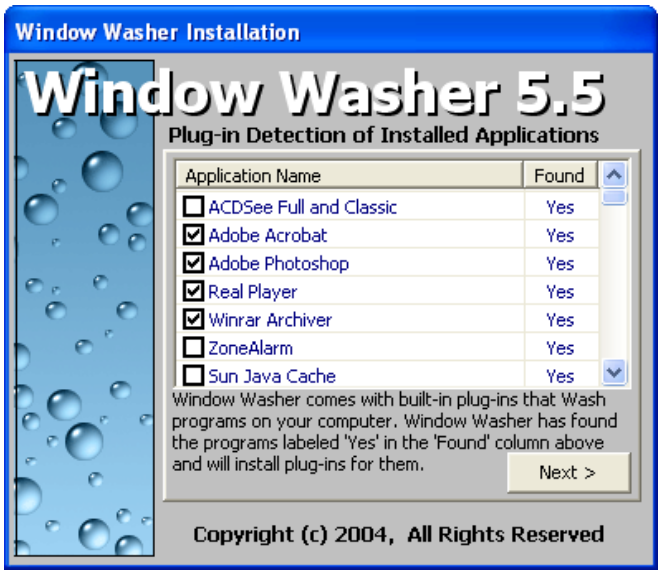
Zurück zum Inhalt dieses Kapitels

Nun startet die Installation, der Fortschritt der Installation wird angezeigt:



Zurück zum Inhalt dieses Kapitels

Nun versucht Window Washer gleich, auf deinem Computer installierte Programme zu entdecken, deren angelegte Information – falls von dir gewünscht – aufgeräumt werden können:



Du kannst zusätzliche Programme ankreuzen. Diesen Vorgang kannst du aber auch später nach der Installation nachholen. Drücke den Button „Next“.

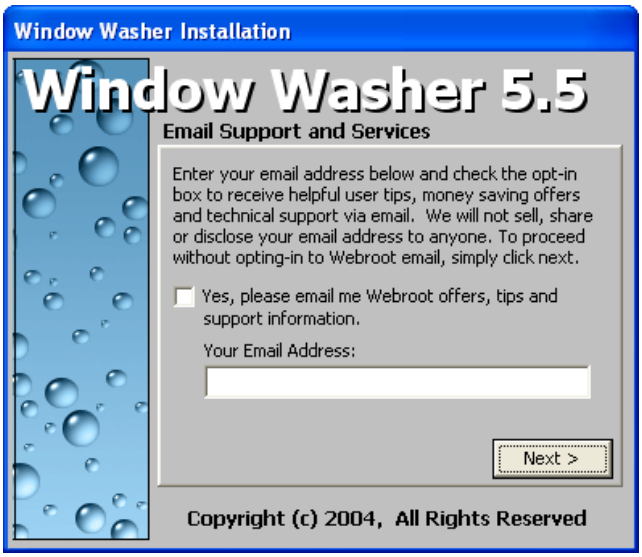
Zurück zum Inhalt dieses Kapitels

Nach dem Beenden der Installation erhältst du folgende Erfolgsmeldung:

Drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Du kannst nun noch angeben, ob du per E-Mail Tipps und Infos zugeschickt bekommen willst:



Das willst du voraussichtlich nicht, drücke einfach den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Und das war's auch schon, Window Washer ist jetzt installiert und einsatzbereit:

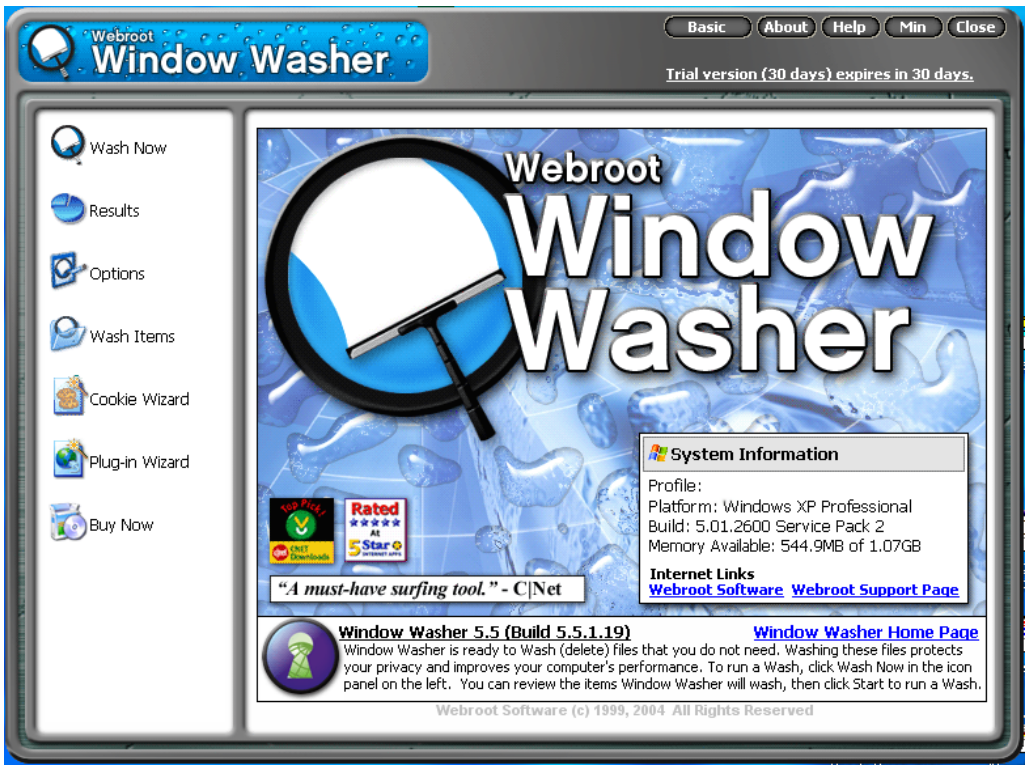
Drücke den Button „Finished". Falls du bereits eine Firewall installiert hast (z.B. ZoneAlarm) und Window Washer gleich versucht, mit der HerstellerInnenfirma Webroot Kontakt aufzunehmen, kannst du das ruhig mal ablehnen.

Zurück zum Inhalt dieses Kapitels

17.2 Die Verwendung von Window Washer

Einstellungen und Plug-ins

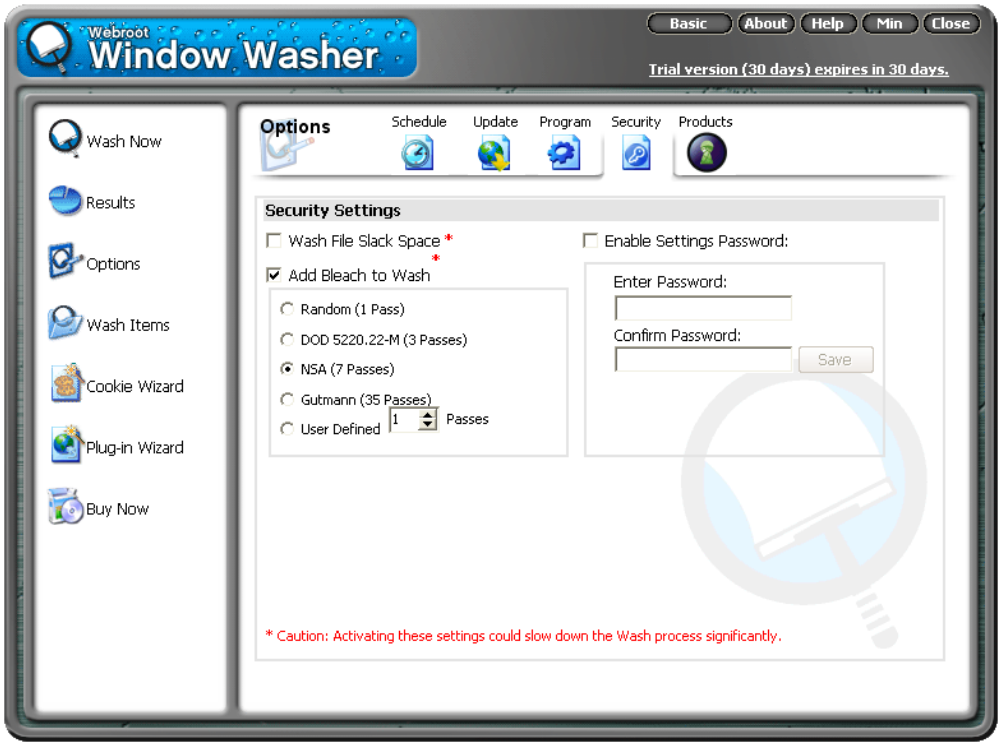
Nach der Installation wird Window Washer gleich gestartet. Du kannst das Programm aber auch jederzeit mittels Doppelklick auf das Icon am Desktop oder durch Auswahl im Start-Menü Start -> Programme -> Window Washer -> Window Washer 5 starten.



An der Information rechts oben „Trial version (30 days) expires in 30 days“ kannst du erkennen, dass es nur eine Version zum Ausprobieren ist.

Zurück zum Inhalt dieses Kapitels

Wenn du im linken Hauptmenü den Punkt „Options“ und im Untermenü oben den Punkt „Security“ wählst, siehst du folgenden Dialog:

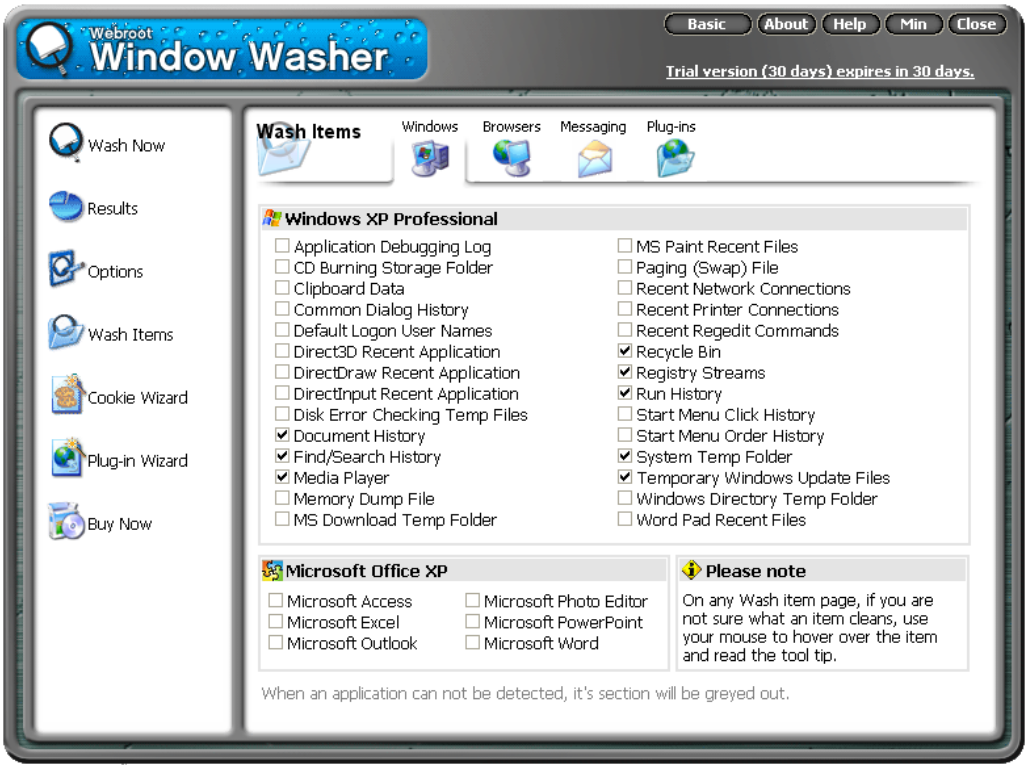


Eine wichtige Einstellung ist, was mit den gelöschten Informationen passieren soll. Was in WinPT „Wipe“ heißt, heißt hier „Bleach“, nämlich das mehrmalige Überschreiben der gelöschten Bereiche, damit sie auch mit dem vorhandenen Restmagnetismus auf der Festplatte nicht mehr wiederhergestellt werden können.

Der voreingestellte Wert von 7 Durchgängen ist hier ausreichend, besonders vorsichtige Menschen können aber auch einen höheren Wert angeben, dafür dauert das Aufräumen dann halt auch länger.

Zurück zum Inhalt dieses Kapitels

Sehr wichtige Einstellungen kannst du durch Anklicken des Menüpunkts „Wash Items“ auf der linken Seite vornehmen:



Hier kannst du angeben, was alles gelöscht werden soll. So z.B. für Microsoft Office-Programme, ob die Liste der zuletzt geöffneten Dateien gelöscht werden soll oder nicht.

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 „Microsoft Word“, usw.

Wenn du nicht willst, dass Window Washer nach jedem Start von Windows geladen wird, entmarkiere den Punkt „Load Washer at Windows Startup“ unter dem Menüpunkt „Program“. 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.

Schau dir einfach alles durch.

Zurück zum Inhalt dieses Kapitels

Wichtig ist noch der Untermenüpunkt „Plug-ins“ am oberen Rand. Wähle diesen Menüpunkt aus:

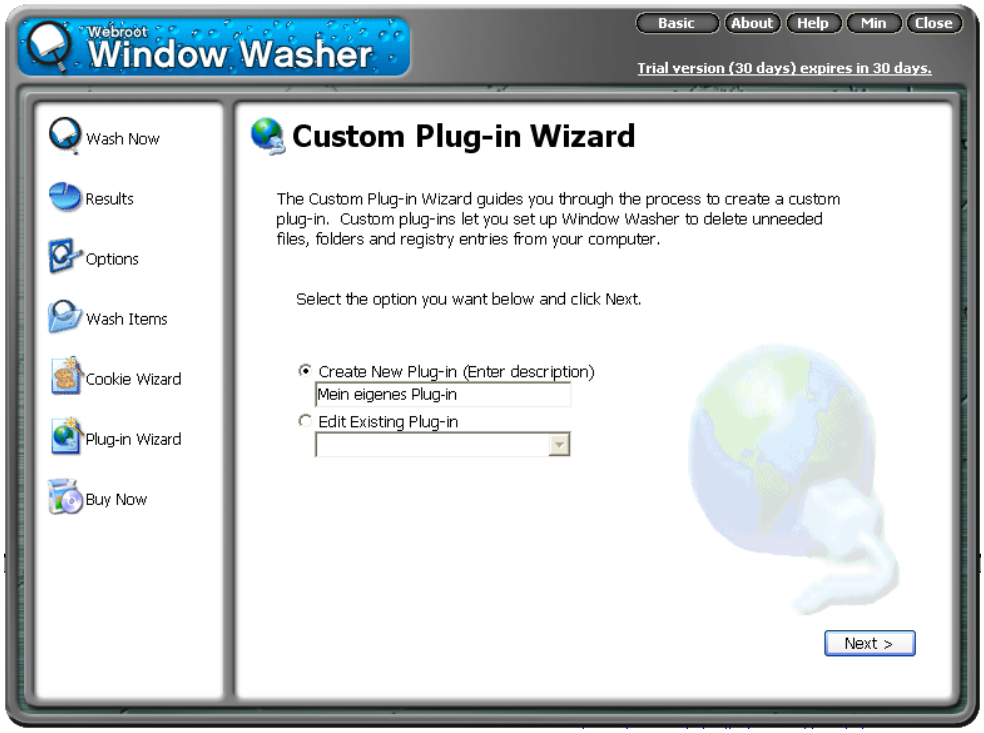
Hier kannst du sogenannte „Plug-ins“ (Zusätze) für weitere Programme automatisch dazuinstallieren.

Drücke den Button „Plug-in Detection“, das Programm sucht dann nach den angeführten Programmen und wählt sie gleich aus.

Wenn du ein bestimmtes Programm vom Aufräumvorgang ausnehmen willst, entmarkiere es einfach.

Zurück zum Inhalt dieses Kapitels

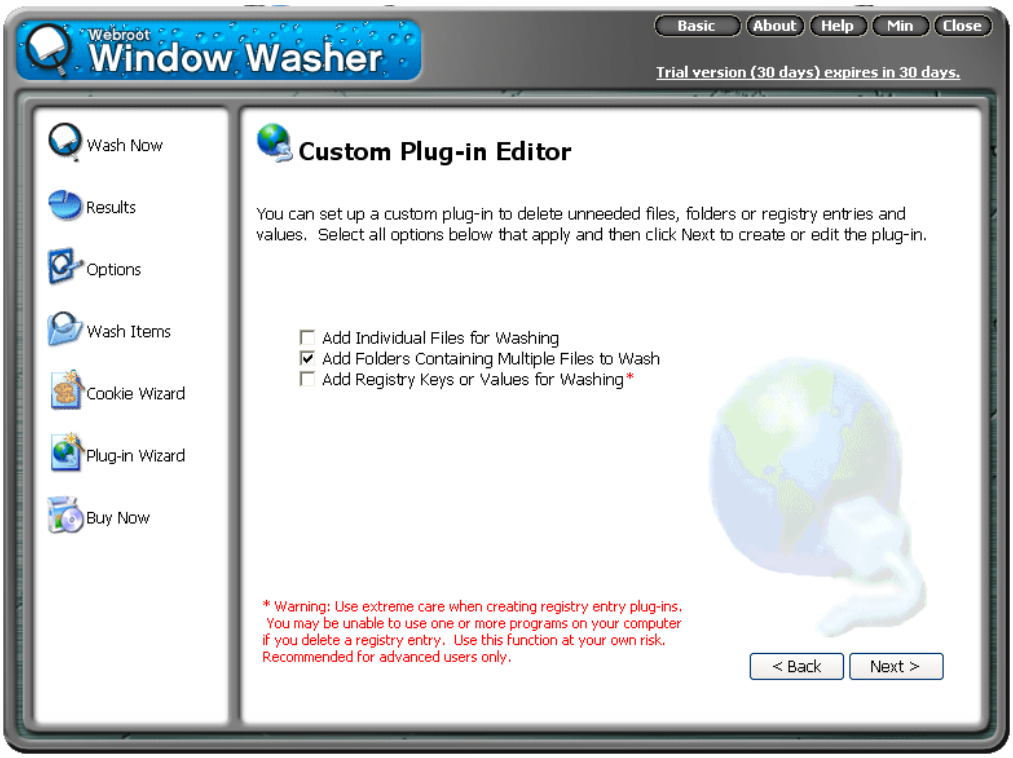
Du musst dich aber nicht mit den automatisch erkannten Programmen begnügen. Wenn du eigene Ordner und Dateien angeben willst, die gelöscht werden sollen, kannst du sie nach Auswählen des Hauptmenüpunkts „Plug-in Wizard“ angeben:



Gib einen Namen (eine Beschreibung) für das Plug-in an und drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Nun kannst du angeben, was du löschen willst:

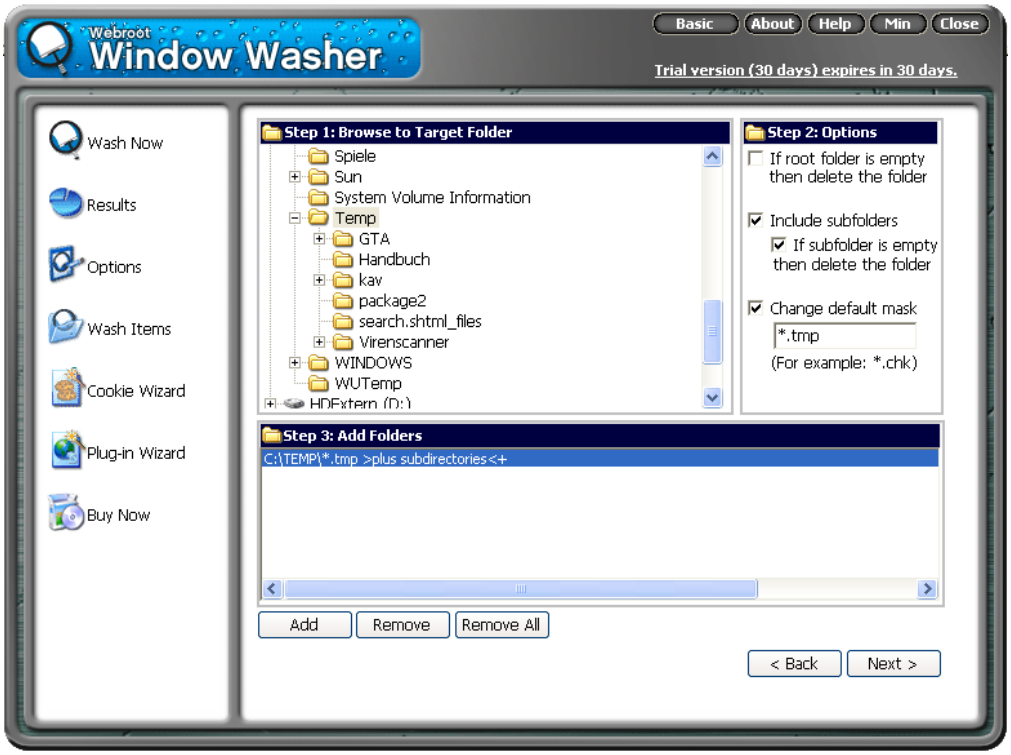


- Individual Files (einzelne Dateien)
- Folders (ganze Ordner)
- Registry Keys (Registry-Einträge)

Nachdem du eine oder mehrere Möglichkeiten ausgewählt hast (hier „Folders“), drücke den Button „Next“.

Zurück zum Inhalt dieses Kapitels

Hier kannst du genau angeben, was gelöscht werden soll:

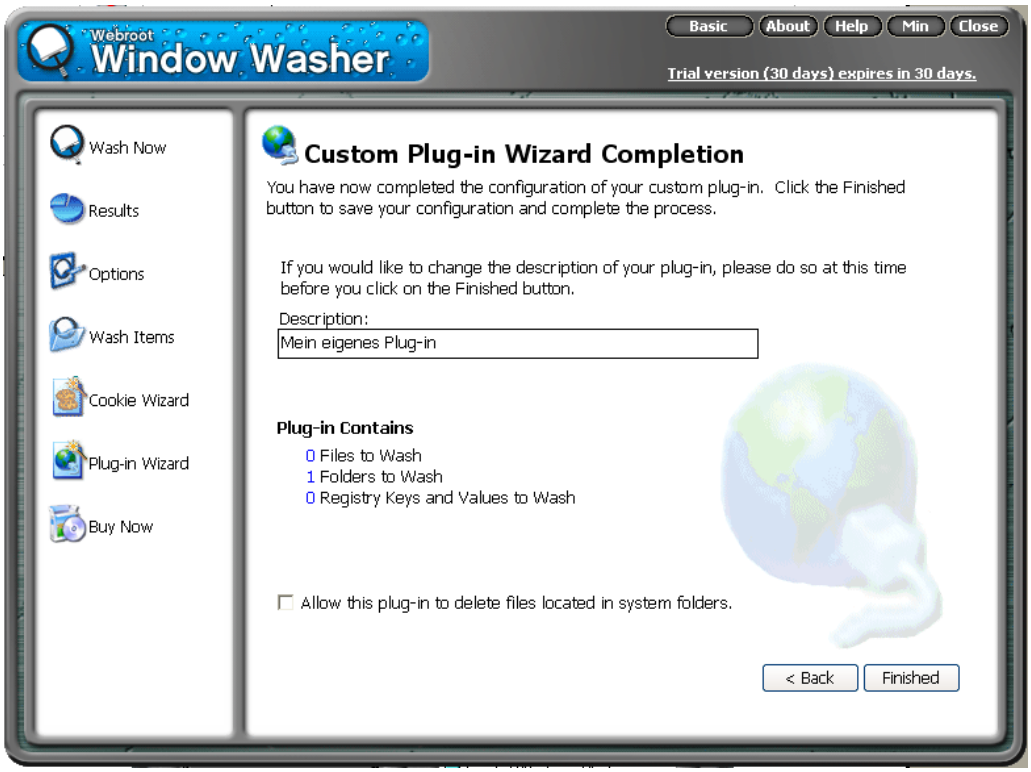


- Step 1: Wähle einen oder mehrere Ordner aus
- Step 2: Du kannst dir aussuchen, ob Unterordner auch geleert werden sollen, ob diese Unterordner selbst gelöscht werden sollen, wenn sie leer sind und Suchmuster für Dateinamen (hier z.B. werden nur alle Dateien gelöscht, die auf .tmp enden).
- Step 3: Übernehme die Angaben durch Drücken des Buttons „Add“

Wenn du fertig bist, drücke den Button „Next“, es erscheint noch ein Bestätigungsfenster.

Zurück zum Inhalt dieses Kapitels

Eine Zusammenfassung deiner Angaben wird angezeigt:



Drücke den Button „Finished“. Die soeben angegebenen Ordner und Dateien werden beim nächsten Waschvorgang gelöscht.

Zurück zum Inhalt dieses Kapitels

Das kannst du auch an der Liste erkennen, die nach Auswahl des Hauptmenüpunkts „Wash Items“ auf der linken Seite erscheint:

In der Liste auf der rechten Seite siehst du jetzt ganz oben das in diesem Beispiel soeben erstellte Plug-in („Mein eigenes Plug-in“), es hat den Typ „Custom“, ist also ein selbst erstelltes Plug-in.

Du kannst es im Unterschied zu den vorgegebenen Plug-ins auch wieder löschen (vorher den Namen anklicken) und so wie alle Plug-ins kannst du es durch Entmarkieren deaktivieren.

Zurück zum Inhalt dieses Kapitels

Das Durchführen des Waschvorgangs

Wähle nach dem Starten von Window Washer den Hauptmenüpunkt „Wash Now“ auf der linken Seite:

Du siehst noch eine Liste mit allen Punkten, die deinen Angaben bei den Einstellungen entsprechend bereinigt werden.

Starte dann den Waschvorgang durch Drücken des Buttons „Start“.

Zurück zum Inhalt dieses Kapitels

Der Fortschritt des Waschvorgangs wird angezeigt:

Dauert dir das Ganze gerade zu lange, kannst du den Vorgang durch Drücken des Buttons „Stop“ abbrechen.

Zurück zum Inhalt dieses Kapitels

Nach dem Beenden des Waschvorgangs erhältst du die Meldung „Washing completed“:

Drücke den Button „Finished“. Es erscheint dann noch eine Statistik zu deinen Waschvorgängen. Ist ganz nett, wenn mensch sieht, wie viel vergeudeten Festplattenplatz mensch mit der Zeit wieder zurückgewonnen hat.

Durch Drücken des Buttons „Close“ ganz rechts oben kannst du das Programm beenden.

Zurück zum Inhalt dieses Kapitels

18 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 gute Passwörter

18.1 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 Lexika 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 gute 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 das ausgeklügelte 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.
- Wenn du wie z.B. bei WinPT die Möglichkeit hast, ganze Sätze anzugeben, kannst du diese Möglichkeit nutzen, beachte aber trotzdem den Tipp im ersten Punkt.
- Je länger und (lexikalisch gesehen) wirrer ein Passwort ist, desto schwieriger ist es zu knacken. Es sollte daher mindestens acht Zeichen haben, ab ca. 14 Zeichen ist ein gutes Passwort durch reines Ausprobieren derzeit nicht knackbar.

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

Ein Vorschlag ist daher, zwei oder drei Gruppen von Passwörtern zu bilden: kürzere, einfachere (aber trotzdem ohne lexikalische Begriffe!) für Dinge, die nicht ganz so wichtig sind bis lange, ausgeklügelte für Dinge, die sehr wichtig sind (z.B. mit TrueCrypt verschlüsselte Daten).

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

Zurück zum Inhalt dieses Kapitels

19 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-AdministratorInnen 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".

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.

Keyserver

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.

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

20 Quellen/Verweise/Weitere Infos

Software

http://www.gnupg.org	GnuPG
http://winpt.sourceforge.net/de/download.php	Windows Privacy Tools
http://www.truecrypt.org/downloads.php	TrueCrypt
http://www.zonelabs.de	Zone Alarm
http://www.free-av.de/	AntiVir
http://www.kaspersky.com/	Kaspersky Anti-Virus
http://www.mozilla.org/firefox	Firefox
http://www.mozilla.org/thunderbird	Thunderbird
http://www.eudora.com/	Eudora
http://anon.inf.tu-dresden.de/	JAP
http://www.lavasoft.de/	Ad-Aware
http://www.safer-networking.org/de/spybotsd	Spybot Search & Destroy
http://www.xpantispy.org	XP AntiSpy
http://www.webroot.com/de/	Window Washer
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.heise.de	Internet-Portal des Heise-Verlags, mit zahlreichen interessanten allgemeinen Informationen, aber auch zu Viren, Verschlüsselung u.v.m. (z.B. bei den Zeitschriften c't und Telepolis)
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/	“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	Info- und Diskussions-Forum 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.
Http://www.macuser.de http://www.macosxhints.com/	Foren für Mac OS-BenutzerInnen
http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html http://macgpg.sourceforge.net/	GnuPG für Mac OS

Online-Zeitungen

http://www.heise.de/tp/	Telepolis, sehr informative und nette Online-Zeitung, in der viel zu Überwachung und Internet berichtet wird (große Empfehlung)

Allgemeines

http://www.n3tw0rk.org	Politisches Diskussionsforum mit vielen Themenbereichen, u.a. auch zu Computersicherheit
http://www.glossar.de/	Alle möglichen Begriffe aus der Computerwelt erklärt, nach Anfangsbuchstaben sortiert
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://www.schulzki-haddouti.de/	Homepage von Christiane Schulzki-Haddouti, die u.a. einige sehr empfehlenswerte Bücher geschrieben hat, so z.B. „Vom Ende der Anonymität, die Globalisierung der Überwachung“und „Datenjagd im Internet, eine Anleitung zur Selbstverteidigung“
http://www.heise.de/tp/r4/buch/buch_3.html	„Netzpiraten – Die Kultur des elektronischen Verbrechens“ aus dem Heise-Verlag