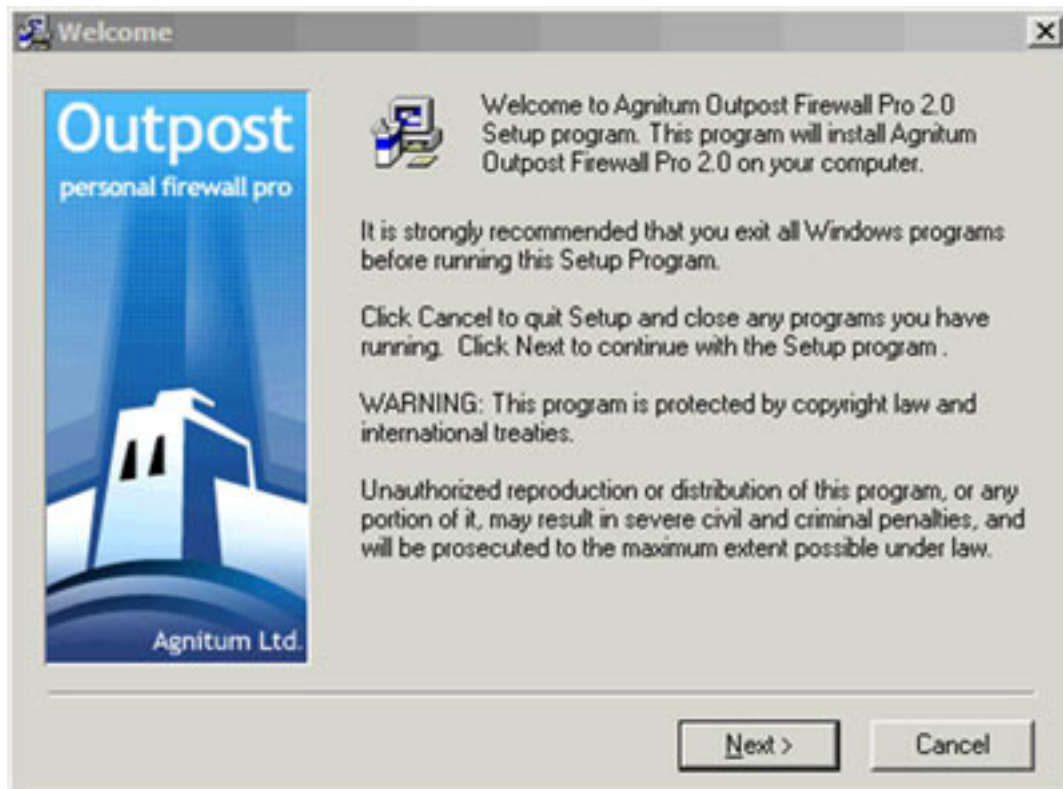
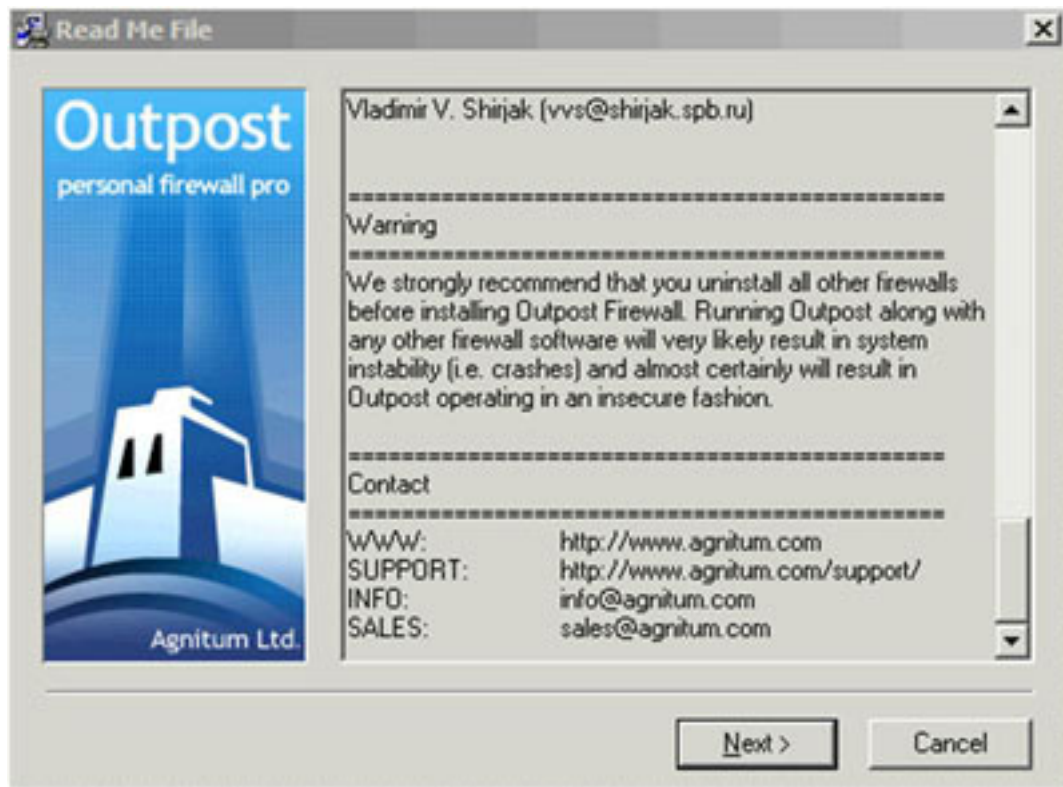


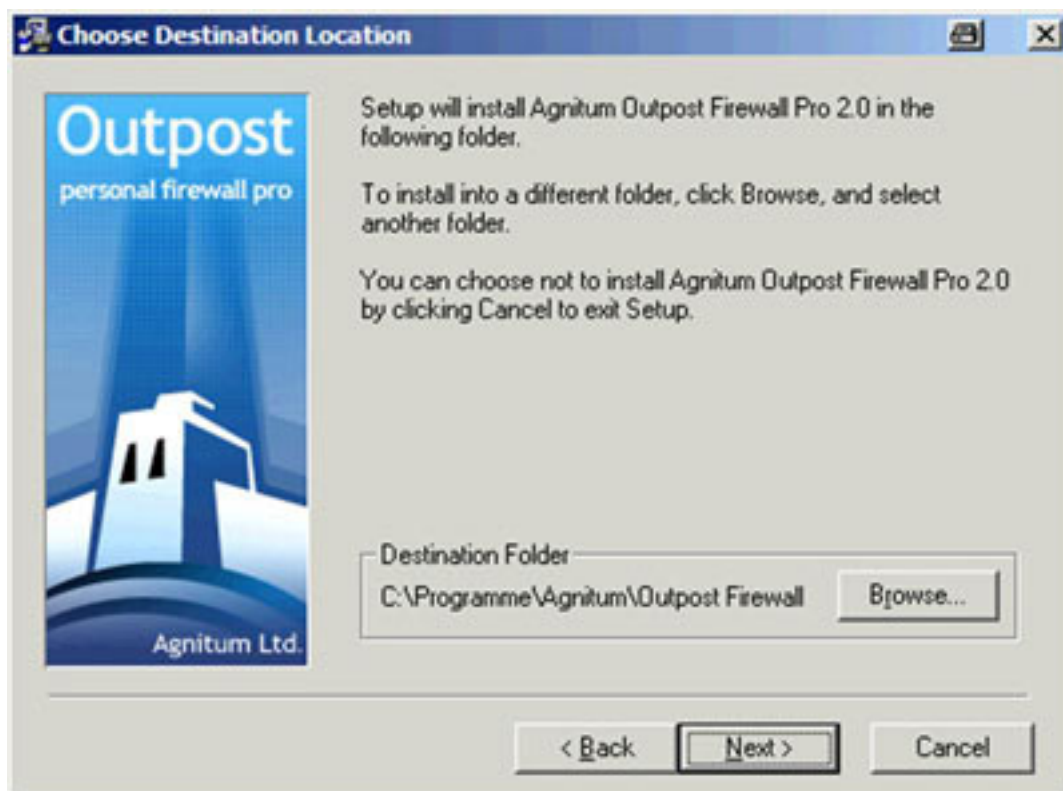
Outpost Firewall Pro Version 2 :: Deutscher Einstieg - Installation, erste Schritte und weitere Hilfen -



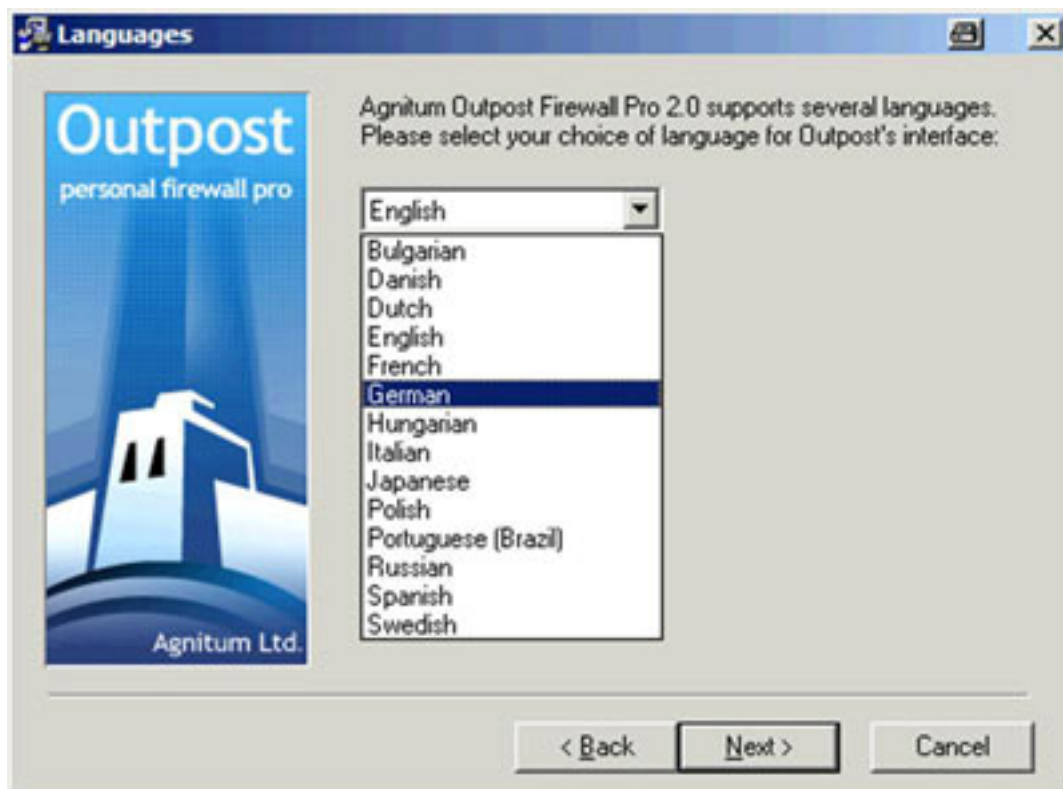
Anklicken der SETUP.EXE Datei und Setup startet



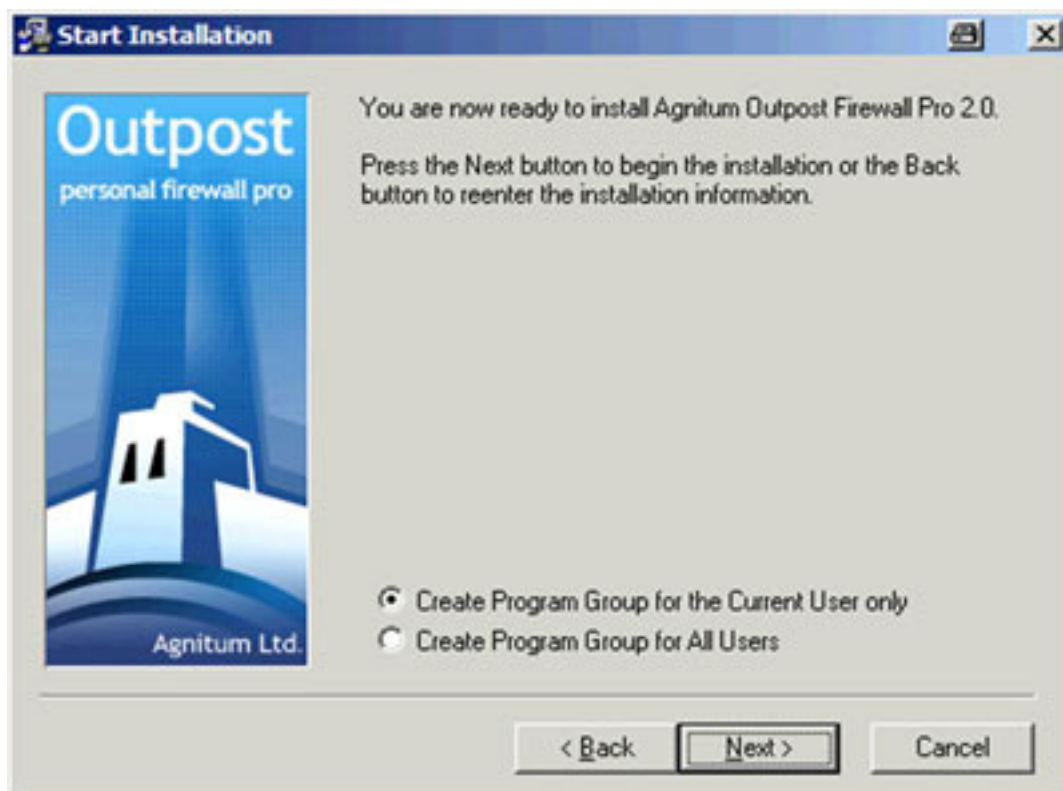
Anschliessend muss man die Software vom Inhalt bestätigen



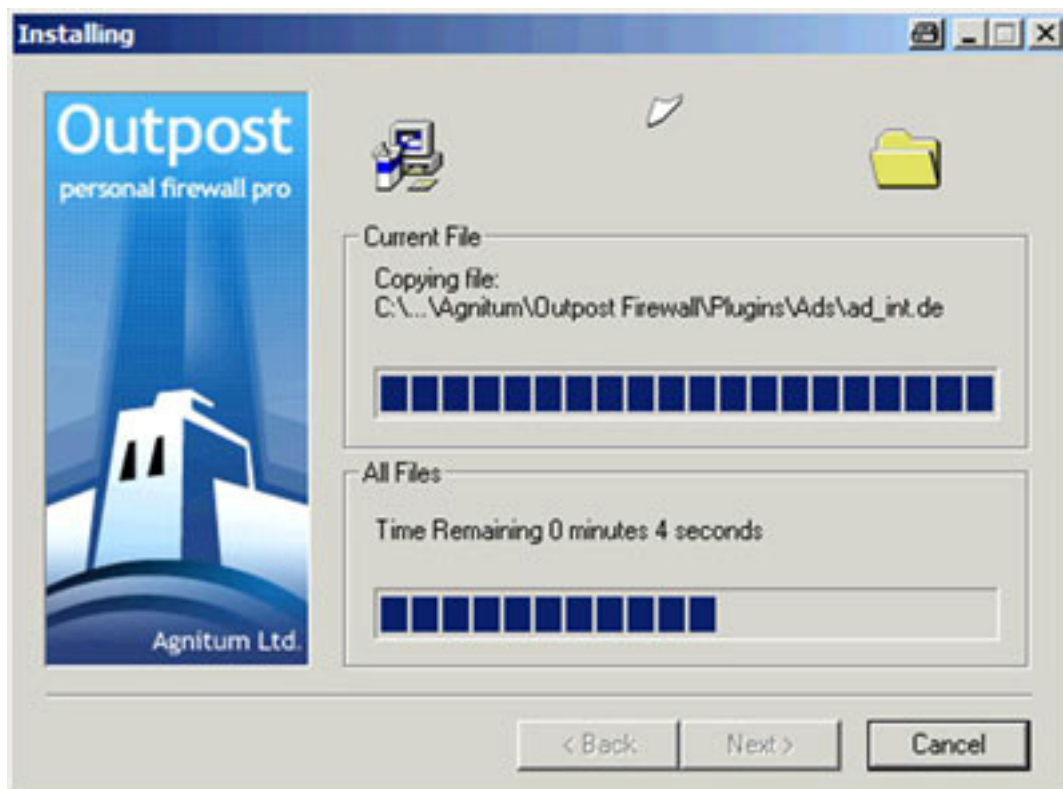
Nun hat man die Auswahl, in welchem Ordner man Outpost installieren möchte. Vorgegeben (wie hier im Bild) ist natürlich der Standardordner.



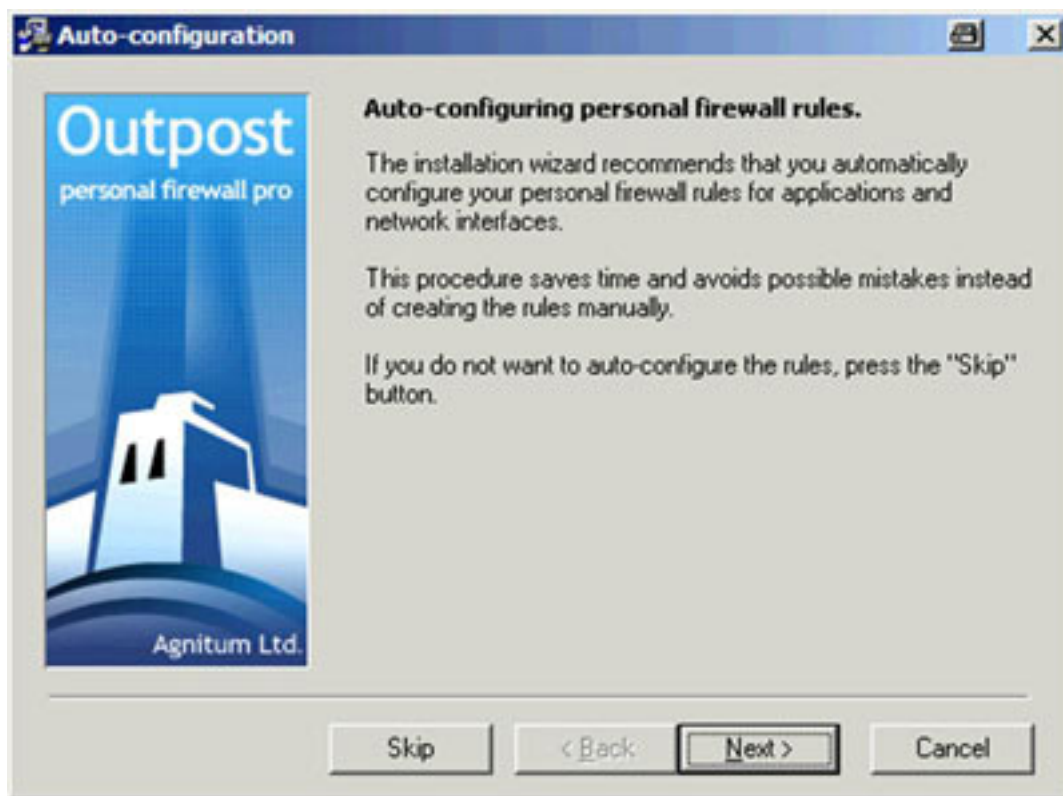
Jetzt wird die Sprache des Programms auf Deutsch gewählt und man kann mit der Installation fortfahren.



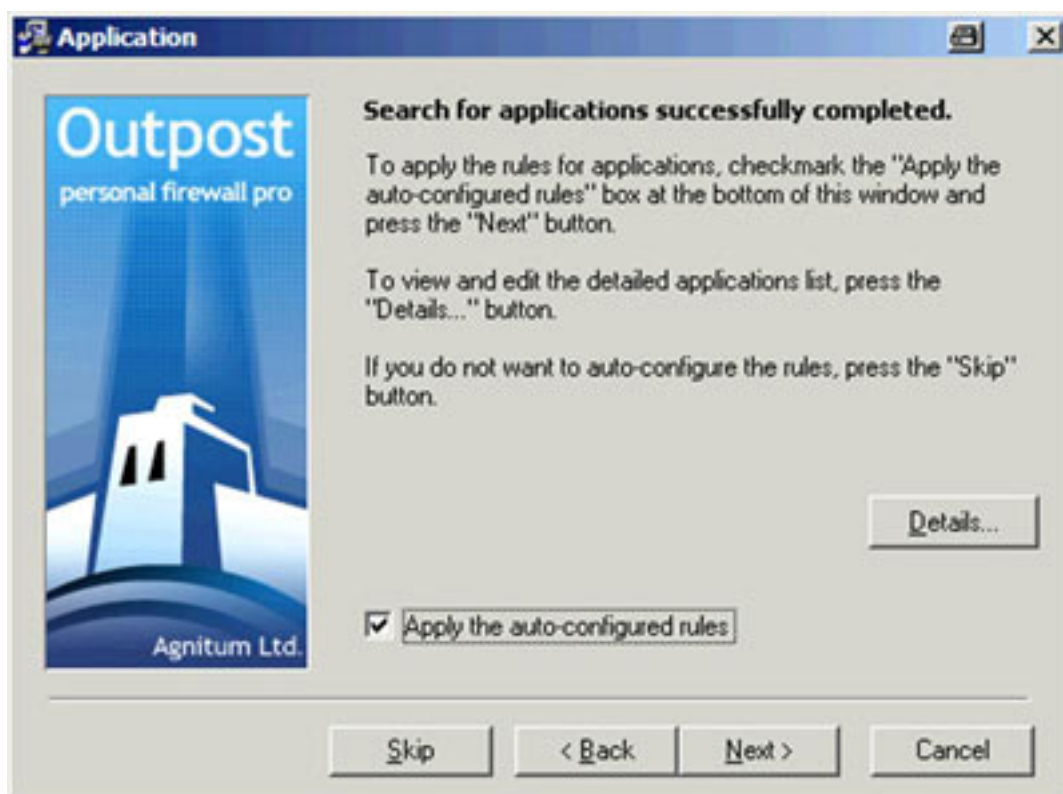
Hier wird erfragt, ob Outpost für alle Benutzer des Computers installiert werden soll, oder nur für den Benutzer, der gerade bei der Installation angemeldet ist.



Der Installationsverlauf zeigt welche Details gerade kopiert werden.



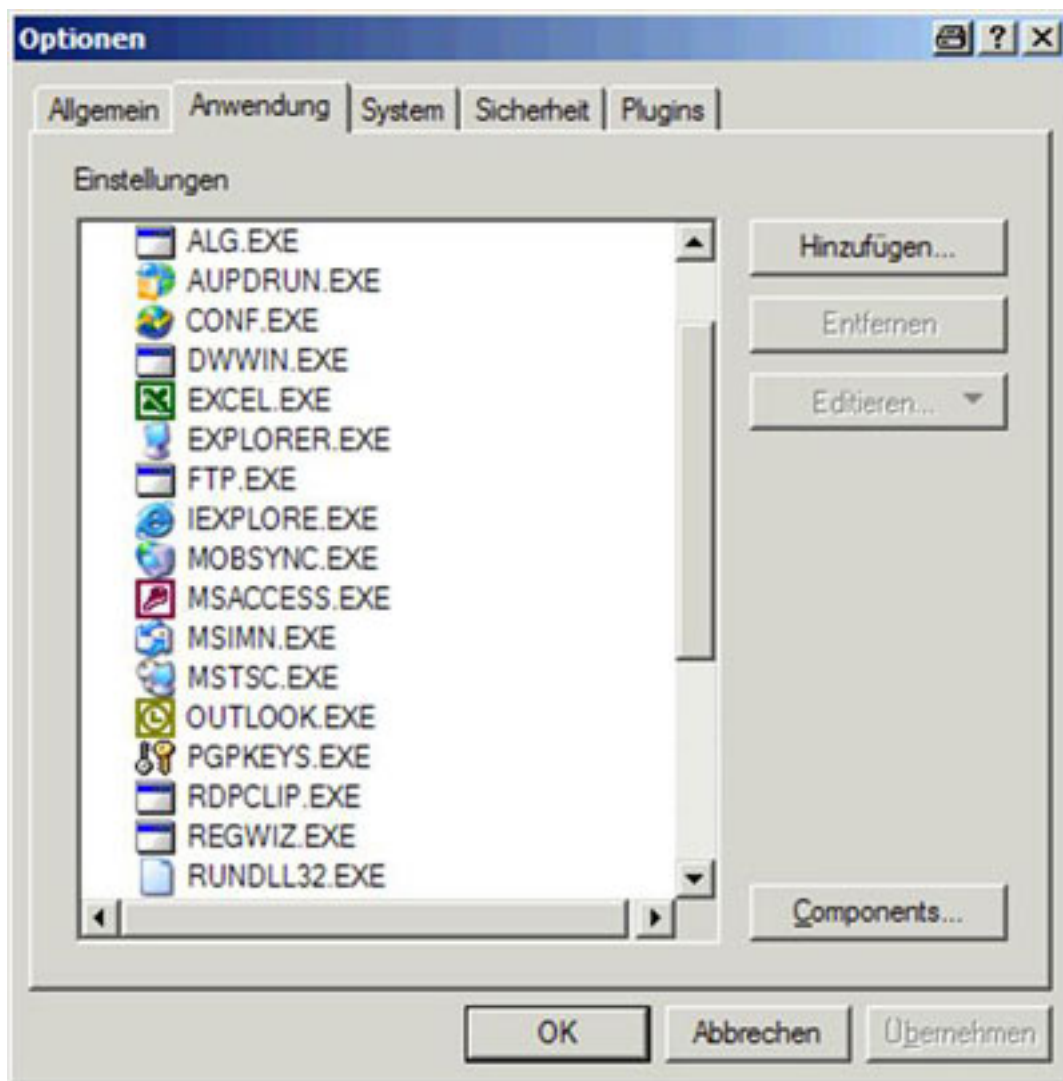
Während der Installation kann man bereits erste Einstellungen vornehmen, dazu klickt man hier auf NEXT und wenn man dies nicht möchte, dann klickt man einfach auf SKIP.



Geht man in diesem Schritt in die DETAILS, so kann man bereits die Anwendungen konfigurieren, die Outpost als aktiv gefunden hat.

Sollten Sie dies zunächst nicht wünschen, so kann man einen Haken bei "Apply the auto-configured rules" setzen und die Anwendungen werden zunächst in einem halbsicheren Modus geladen.

Anschliessend bestätigt man die Installation mit ok und startet den Computer neu.



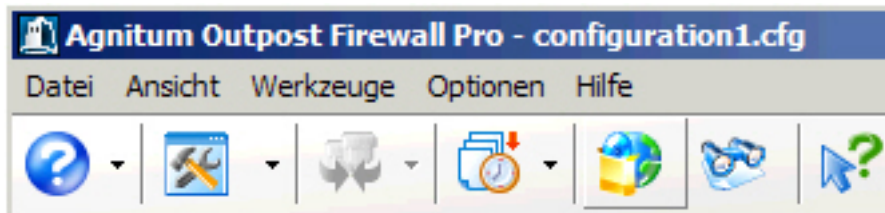
Dieses Bild zeigt alle die Anwendungen, die unter WindowsXP Professional installiert sind und entsprechend in den halb-sicheren Modus geladen werden. Wie man erkennen kann, sind dies 99% aller Anwendungen die auf einem Computer installiert sind.



Beim Start von Outpost Firewall Pro 2 wird dann nach der Evaluationslegitimierung gefragt, sprich: Man sollte hier den Registrierungsschlüssel eintragen den man von Agnitum bekommt wenn man die Firewall käuflich erwirbt.

Die weiteren Instruktionen erfolgen dann bereits in deutscher Sprache.

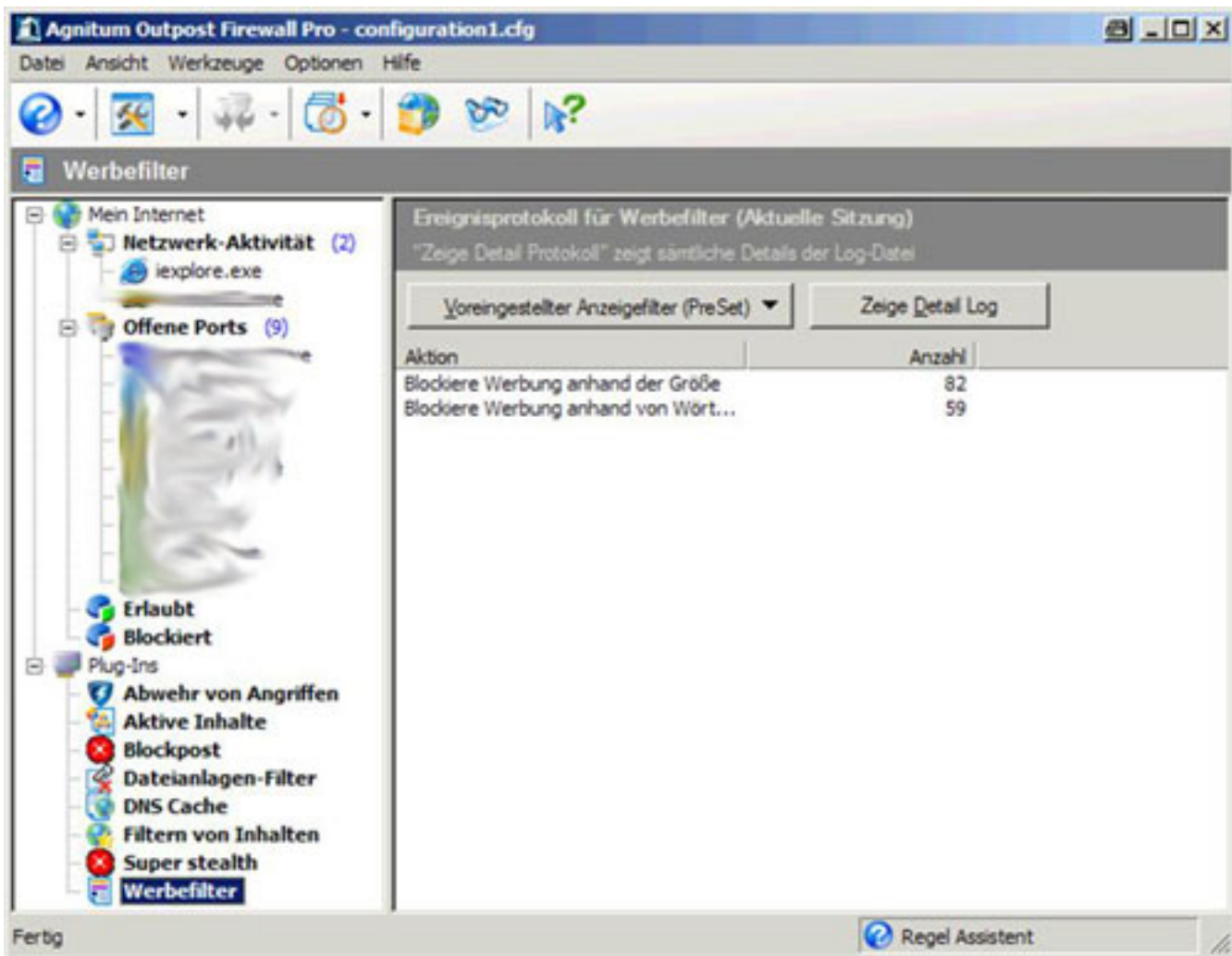
Ist die Outpost Firewall erst einmal gestartet, so finden Sie ein Menüleiste die wie folgt aussieht:



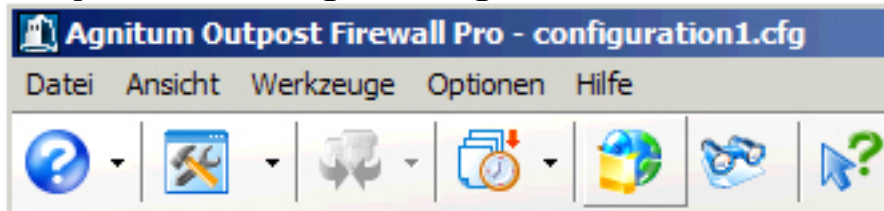
Nach der ersten Installation sollte man auf die Weltkugel klicken, sich mit dem Internet verbinden und das erste Outpost Update herunterladen, da man so auf dem aktuellsten Stand der Software ist. (Weltkugel mit der CD)



Updates verfügbar und der Download läuft bereits. Nach dem Update wird es gleich installiert und ein Neustart der Firewall ist erforderlich.
Gehen Sie dazu offline.

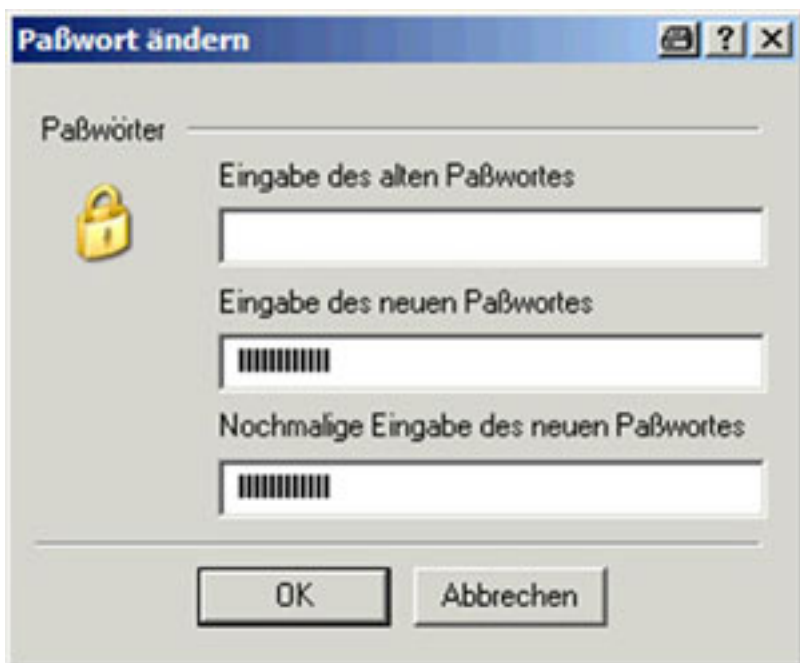


Das Hauptfenster der Outpost Firewall zeigt nun alle Verbindungen an sowie die entsprechenden Plug Ins die geladen wurden.



Wieder über die Menüleiste klickt man auf das Werkzeugsymbol (Hammer und Schraubenschlüssel) um die Optionen festzulegen.

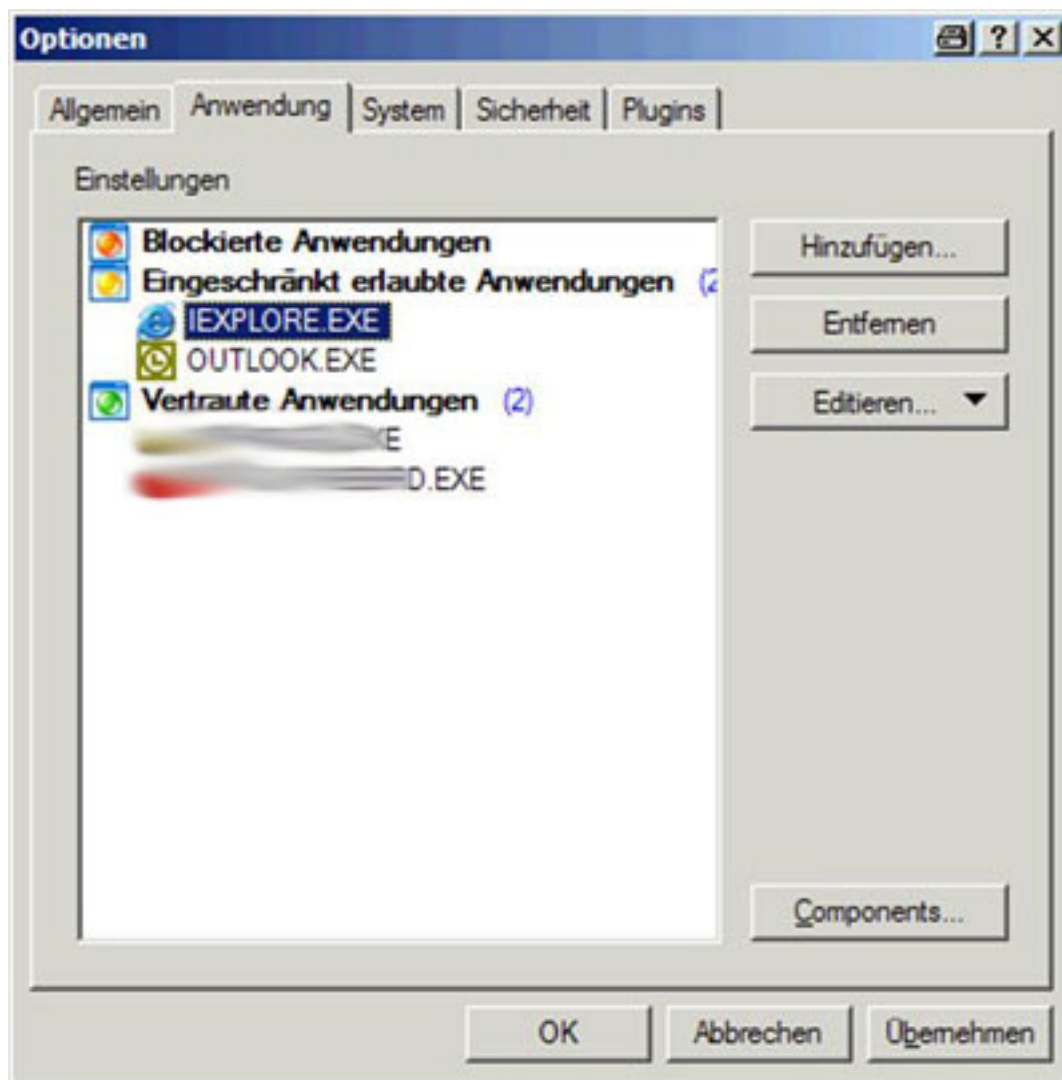
Als erstes würde ich aus dem OPTIONEN Dialog heraus ein Passwort festlegen, damit nur Sie die Einstellungen der Outpost festlegen können und auch die Outpost somit nicht beendet werden kann ohne Passwortheingabe.



Da es ja kein altes Passwort gibt, kann man direkt in neues Passwort eingeben und nochmals bestätigen.

Der Passwortschutz befindet sich gleich beim öffnen des Werkzeugregisters Einstellungen. Passwortschutz aktivieren und Passwort eingeben und schon ist man ein Stück sicherer.





Im Register Anwendungen sollte man dann die Anwendungen wieder entfernen, die durch Outpost während der Installation als halbsicher zugelassen wurden. Anschliessend sollten entsprechend nur die Anwendungen übrig bleiben, die auch das Internet nutzen und die durch entsprechende Regeln dann verändert und spezifiziert werden.



Bei den Systemoptionen kann man dann entsprechend den Stealth Modus einstellen, der standart aber bereits eingestellt ist.

Als weitere Einstellungen ist hier die Netzwerkkennung möglich sowie die globalen Systemregeln.

Für erste Schritte mit der Firewall ins Internet sind diese Einstellungen ausreichend.



Die Sicherheit kann entsprechend dem Register dann der jeweiligen Situation angepasst werden, hier ist es sinnvoll den Regelassistenten zu wählen, da hierbei alle Einstellungen von Ihnen selbst geändert werden.

Ebenfalls kann man hier das System nach außen hin komplett blockieren oder die Firewall deaktivieren.

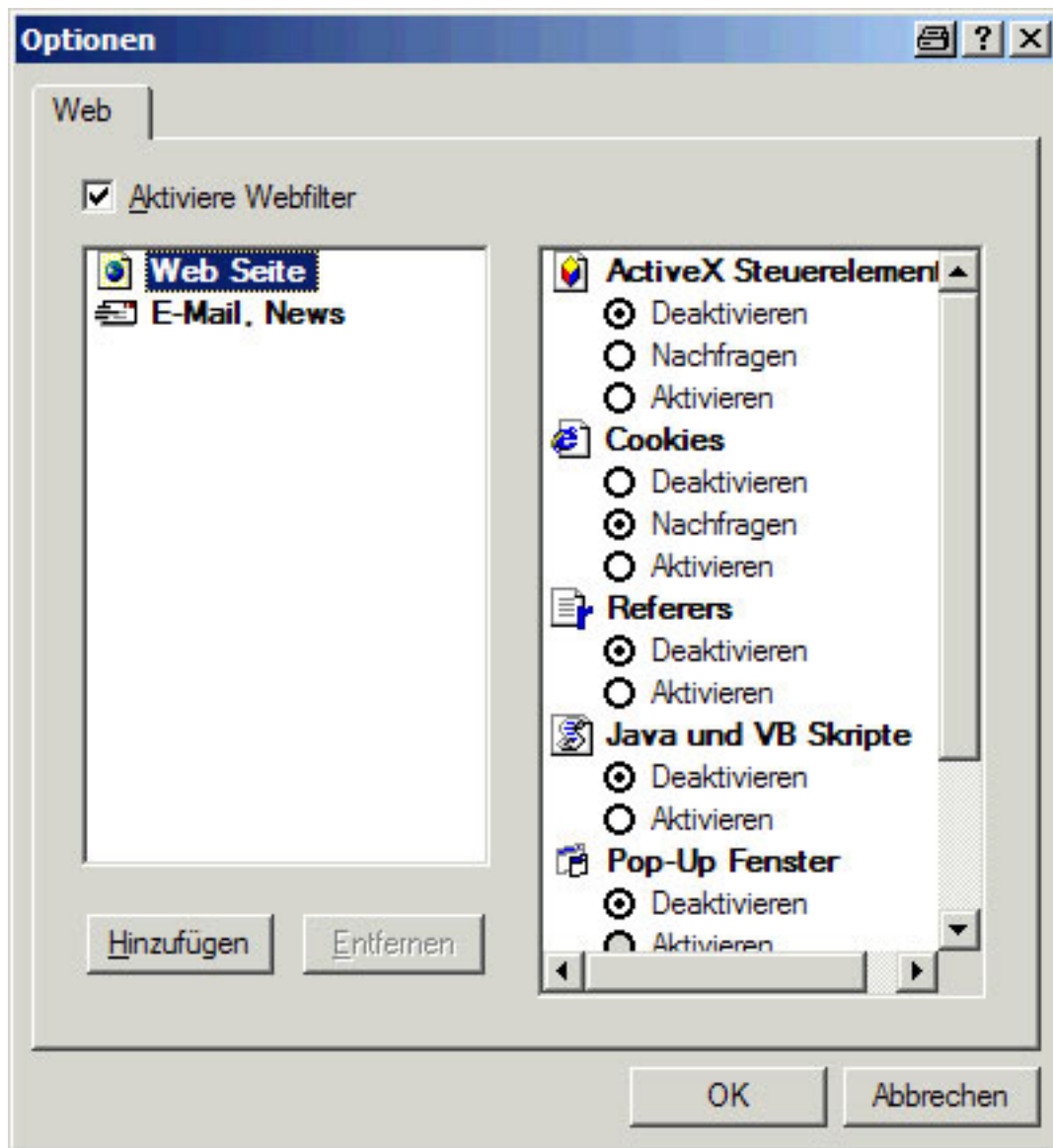
Klickt man nun auf den Register Plug Ins, so kann man hier die verschiedenen Filter setzen, die man für sicheres surfen benötigt oder wünscht.

Diese führe ich hier nur kurz mit an, da diese etwas ausführlicher in der Anleitung beschrieben sind, die bereits veröffentlicht wurde.

Der Active Content Filter:

Dieser beinhaltet das Filtern von Internetseiten- und E-Mail Inhalten wie ActiveX, Cookies, Java etc.

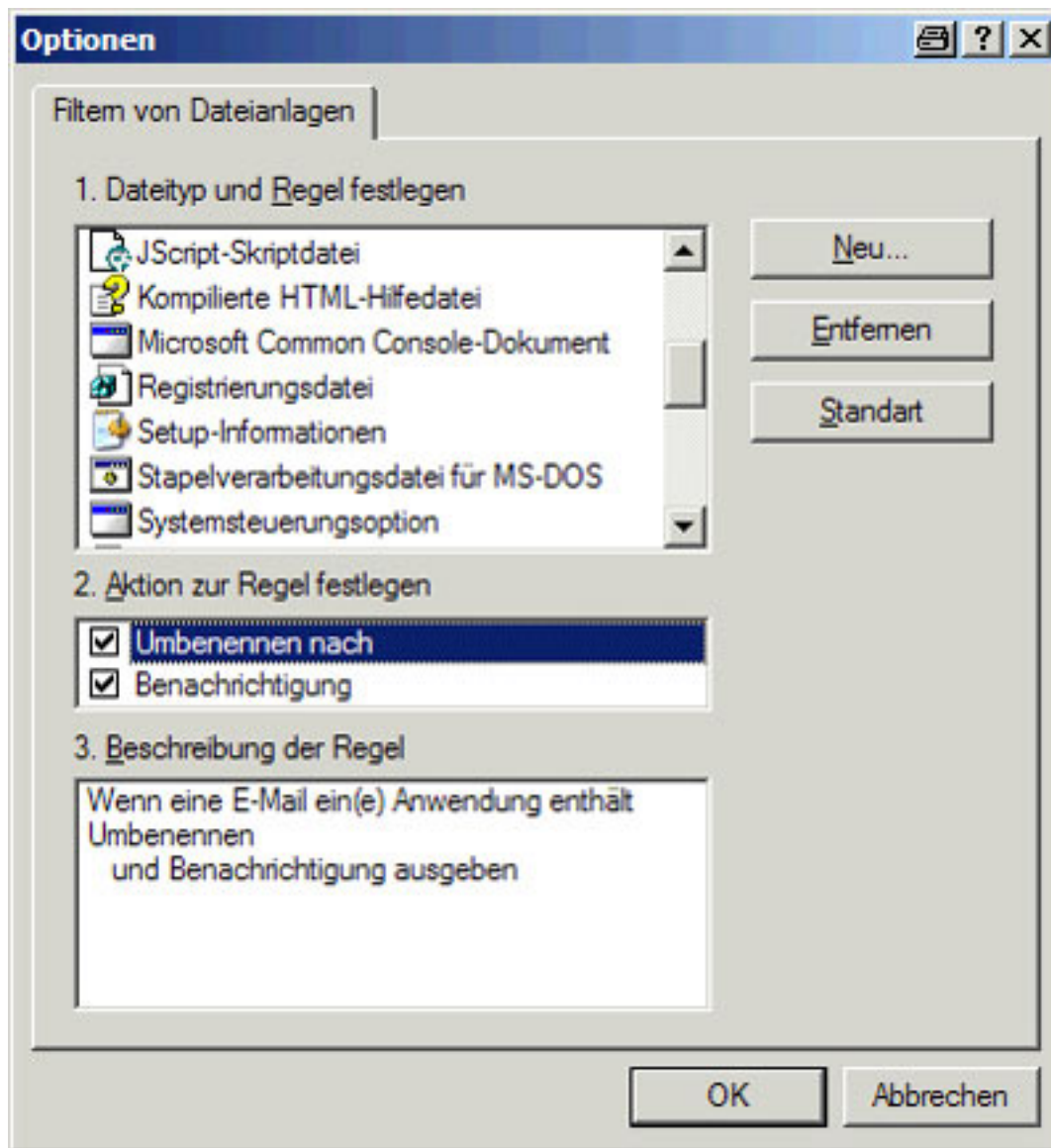
Je nach Bedürfnis können hier die Einstellungen vorgenommen werden.



Der Dateianlagefilter: (Attachmentsfilter)

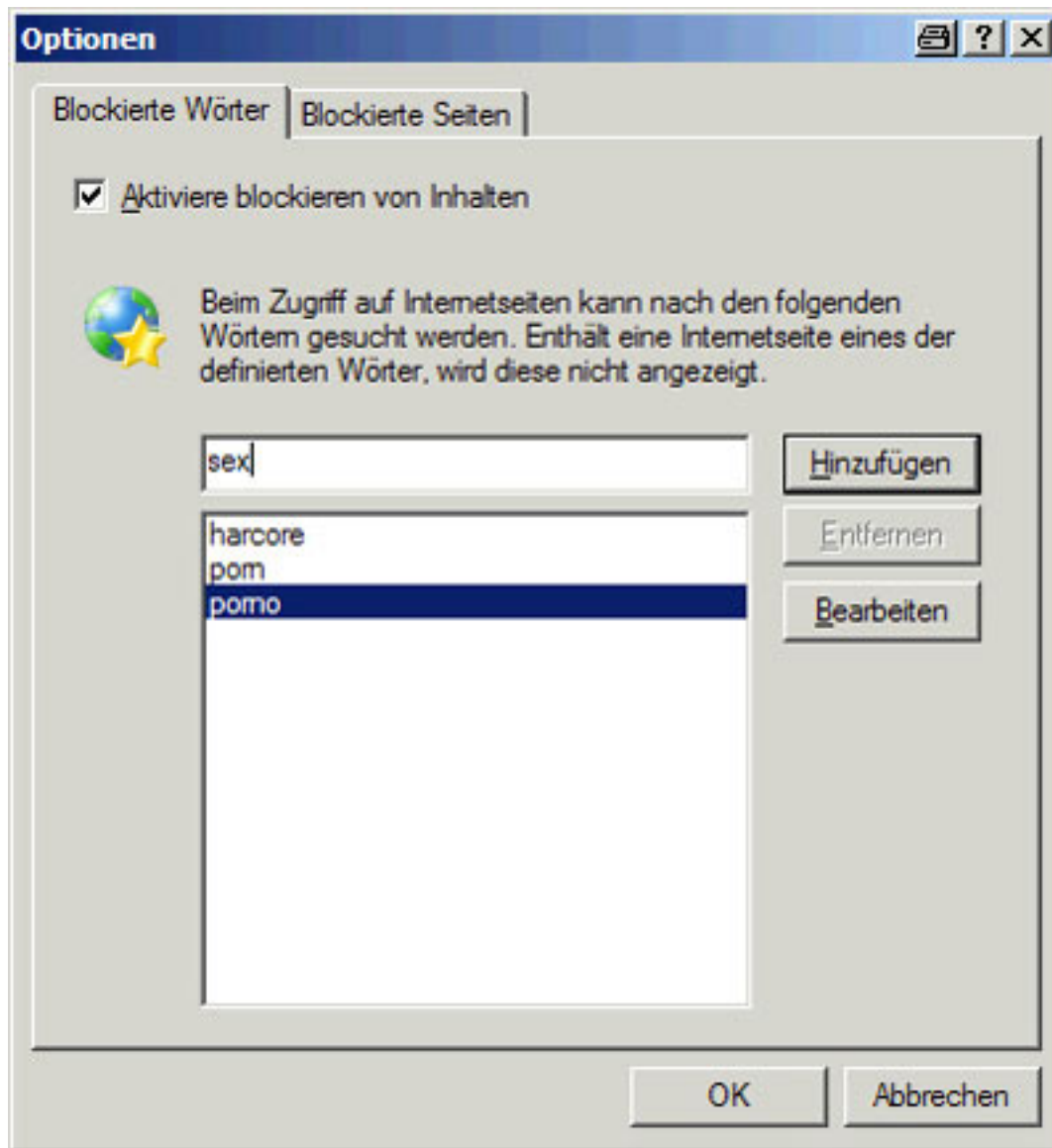
Hierbei kann man jegliche Inhalte von E-Mails die als Anhang kommen filtern oder unberücksichtigt lassen.

Sie können im Beispiel sehen, dass eine Datei als Stapelverarbeitung für MS-DOS umbenannt wird und eine Nachricht auf dem Bildschirm erscheint, wenn eine solche Datei per E-Mail den Computer erreicht.

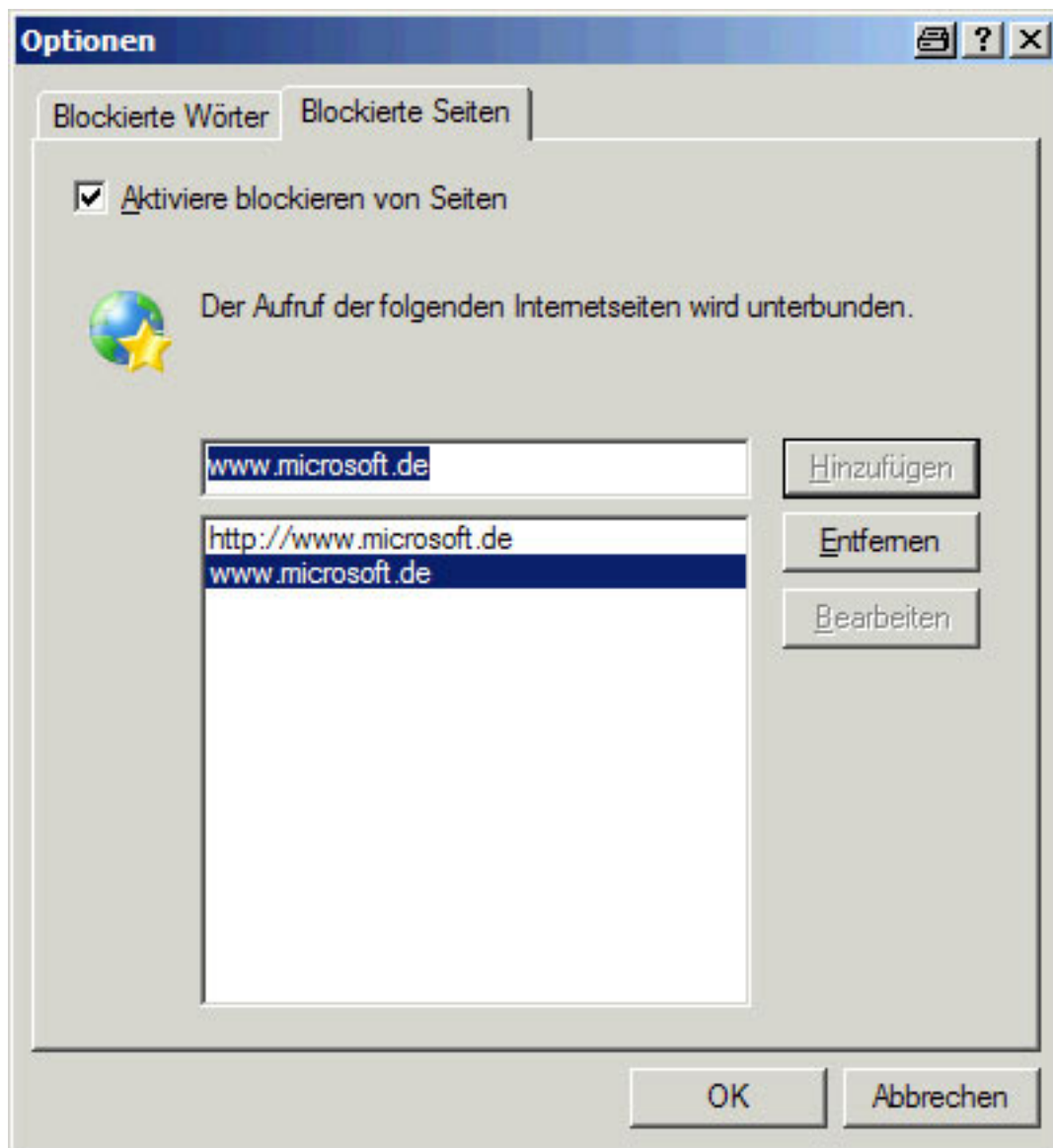


Das Contentfiltering:

Im ersten Bereich des Contentfiltering kann man Internetseiten durch die Outpost Firewall blockieren lassen, sofern hier eine Wortauswahl getroffen wurde die auf Ihrem Computer nicht angezeigt werden soll.



Im weiteren Verlauf kann man gesamte Seiten nach der Benennung blockieren lassen:



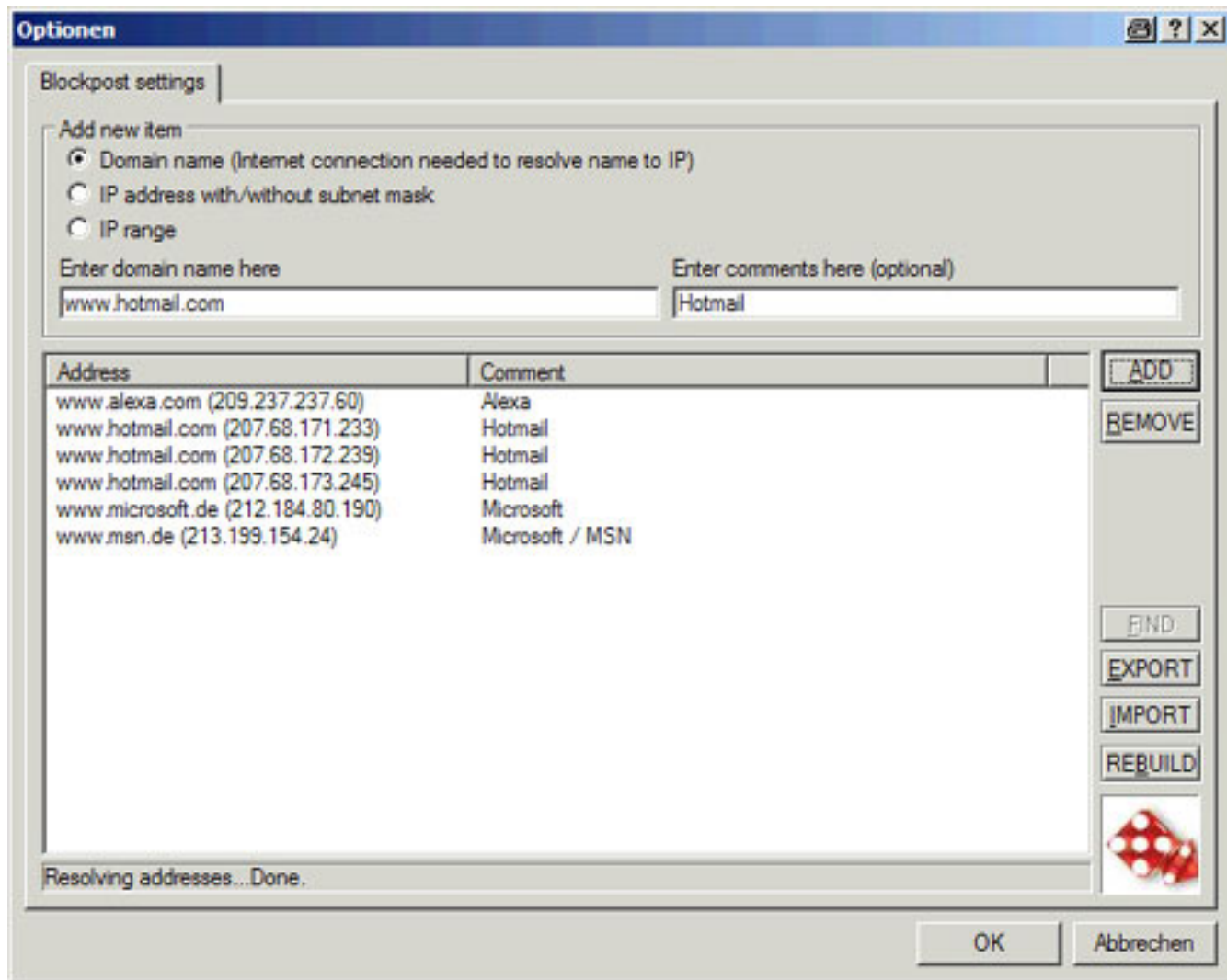
Der Advertisement Filter:

Anhand dieses Filters haben Sie die Möglichkeit, Werbebanner und Werbeeinblendungen dezent zu unterdrücken und Sie werden damit nicht weiter belästigt.

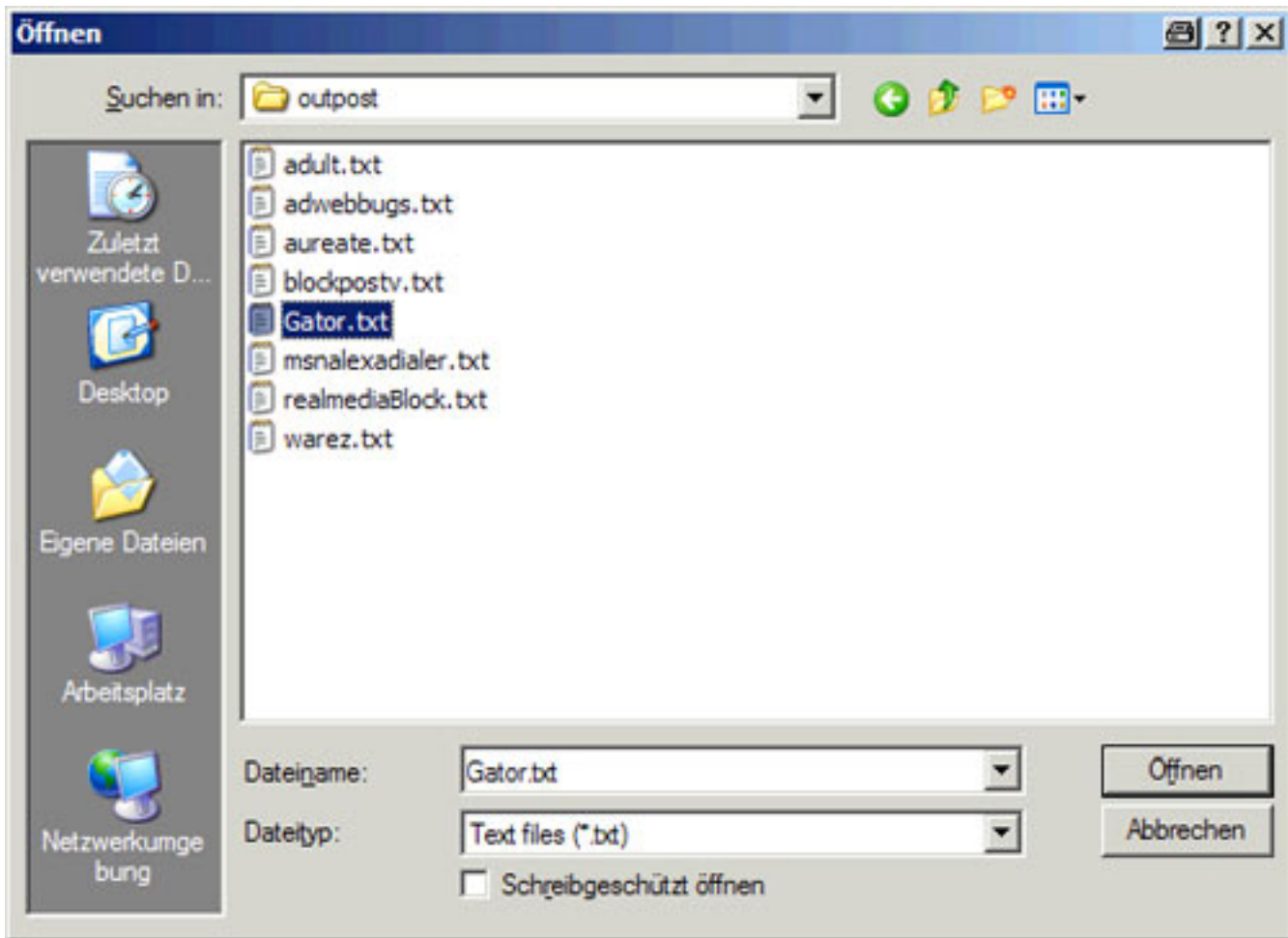
Es erscheint jeweils ein Hinweis auf der Homepage, der einen Platzhalter zeigt.

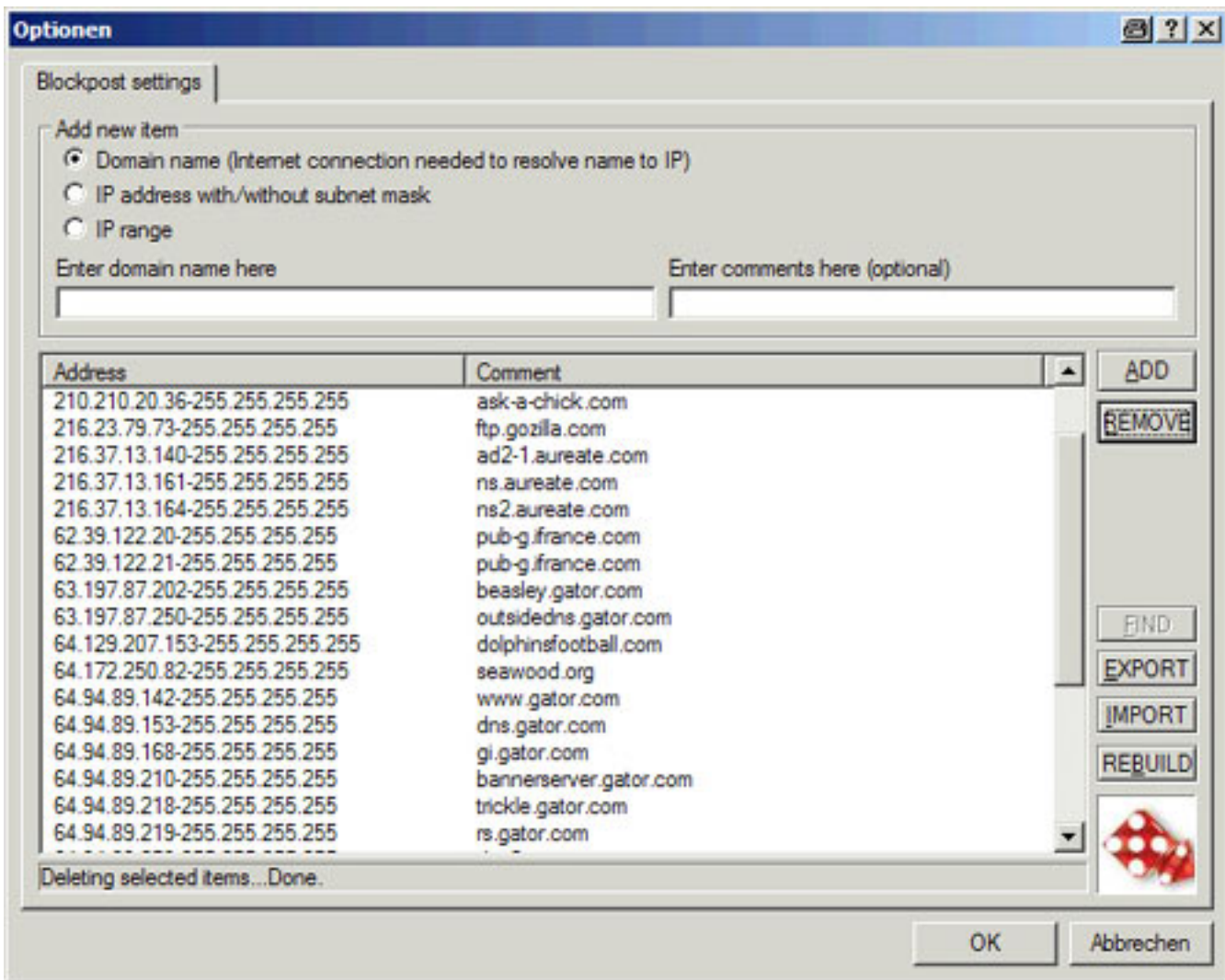
Im nachfolgenden sehen Sie Einstellungen, die durch Plug In Erweiterungen getätigt werden können, die zusätzlich installiert werden müssen.

Blockpost kann ganze Adressbereiche als IP / IP-Range oder anhand des Domain Namens blockieren:

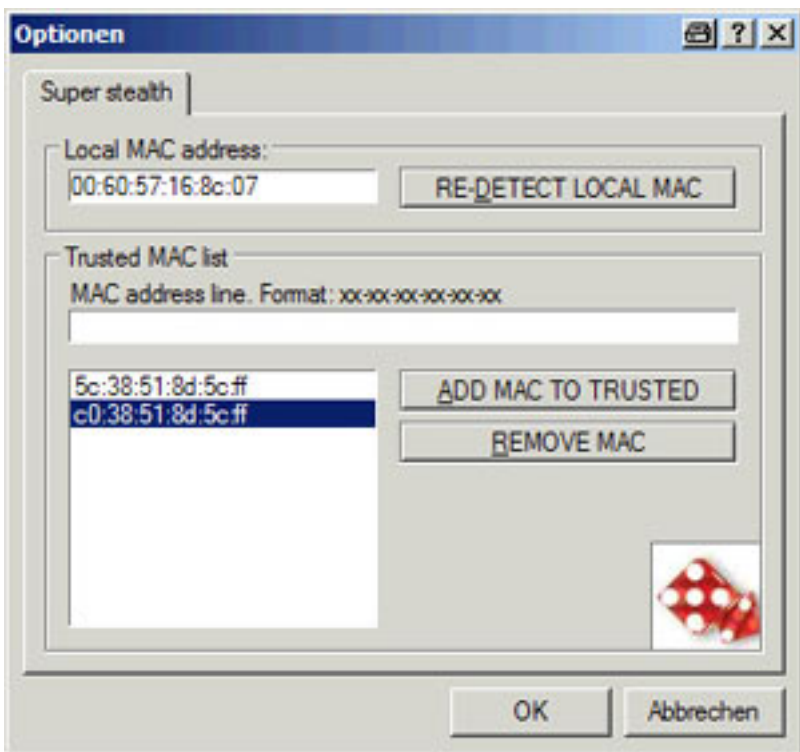


Der Import funktioniert sehr einfach über Text Dateien, die Sie auch bei Brain-Pro Security als Download finden.





Gator und Aureate (Spyware) wurden hier importiert und werden in Zukunft blockiert.



Mit dem Stealth Plug In haben Sie die Möglichkeit, dann entsprechend einen zusätzlichen Schutz für die jeweilige MAC Adresse aufzubauen.

Weitere interessante Features, Hilfen sowie Anleitungen zur Outpost Firewall:

Outpost Spezialseite von Brain-Pro Security: <http://www.brain-pro.de/outpostspezial.htm>
Homepage von Agnitum, Hersteller: <http://www.agnitum.com>
Verschiedene Regeln für die Outpost: <http://www.brain-pro.de/outpost/rules.htm>
Penetrationstest der Outpost 2: <http://www.brain-pro.de/outpost/pentest.htm>
Hacking Intern: Kapitel 11, ab Seite 707: [Firewalls & Co, Schutz vor Angreifern.](#)
Outpost Forum: <http://www.outpostfirewall.com/>

Respektvolle & Beste Grüße

Marko Rogge :: IT-Security Consultant

Brain-Pro Security Coburg

E-Mail: mr@brain-pro.de

<http://www.brain-pro.de>

Tel.: +49 (0) 162-1964818

11.09.2003

Dieser Artikel:

<http://www.brain-pro.de/anleitung/index.htm>