

Benutzer-Handbuch

Referenz

Outpost Firewall

Personal Firewall Software

von

Agnitum

1.1 Zweck des Handbuchs

Dieses Handbuch ist die komplette und ausführliche offizielle Referenz des Firewallsystems Outpost Firewall Pro 1.0. Das Quick-Start Manual finden Sie online unter: [Quick Start manual](#).

Benutzer der Freeware-Version sollten sich möglichst an das Quick-Start Manual halten, da das Handbuch zur Pro-Version sich in einigen Dialogen und Einstellungen unterscheidet.

Copyright © 2002 **Agnitum**, Ltd. Alle Rechte vorbehalten.



Copyright © 2002 **Network-Secure** für das deutsche Handbuch.



Inhaltsverzeichnis

1.1	ZWECK DES HANDBUCHS	2
1.2	WILLKOMMEN	5
Part 1:	Für alle Anwender	6
2	BASICS	7
2.1	NETZWERK BASICS	7
2.2	WIE ARBEITET DAS INTERNET	8
2.3	GEFAHREN IM INTERNET	9
2.4	WINDOWS TERMINOLOGIE	10
3	OUTPOST FIREWALL	12
3.1	SYSTEM-VORAUSSETZUNGEN	12
3.2	OUTPOST FIREWALL FÄHIGKEITEN	12
3.3	TECHNISCHER SUPPORT	13
4	OUTPOST FIREWALL IN DER PRAXIS	14
4.1	OUTPOST FIREWALL INSTALLIEREN	14
4.2	OUTPOST FIREWALL DEINSTALLIEREN	19
4.3	OUTPOST FIREWALL STARTEN	21
4.4	OUTPOST FIREWALL STOPPEN	21
4.5	AUTOMATISCHES UPDATE	22
5	ORIENTIERUNGSHILFEN.....	27
5.1	DAS SYSTEM TRAY-ICON.....	27
5.2	DAS OUTPOST FIREWALL HAUPTFENSTER.....	29
5.3	DIE OUTPOST PANELS	30
5.4	DIE ICON-LEISTE	34
6	OUTPOST FIREWALL EINSTELLEN	36
6.1	BASIS-INFORMATIONEN	36
6.2	INITIALE EINSTELLUNGEN.....	38
6.3	AUSWAHL DES SECURITY-LEVELS	40
6.4	REGEL-EINSTELLUNG FÜR ANWENDUNGEN.....	43
7	PLUGINS	46
7.1	EINFÜHRUNG	46
7.2	WERBEFILTER	48
7.3	BLOCKIEREN VON AKTIVEN ELEMENTEN	51
7.4	ABWEHR VON ANGRIFFEN	53
7.5	DATEIANLAGEN FILTER	55
7.6	DOMAIN NAME CACHE	57
7.7	FILTERN VON INHALTEN	59
Part 2:	für erfahrene Anwender.....	61
8	ERWEITERTE EINSTELLUNGEN	62
8.1	EINFÜHRUNG	62
8.2	SPEICHERN UND LADEN VON KONFIGURATIONEN.....	63
8.3	PASSWORT SETZEN.....	64
8.4	FILTER ERSTELLEN FÜR ANWENDUNGEN	65
8.5	SYSTEM-LEVEL FILTER.....	67

8.6	EINSTELLUNGEN FÜR EIN HOME- ODER OFFICE-NETZWERK	70
9	DAS ANZEIGE-MENÜ	72
9.1	LAYOUT	72
9.2	FILTER	74
9.3	SPALTEN	76
9.4	GRUPPIEREN NACH.....	79
10	APPENDIX	80
10.1	ICMP-NACHRICHTEN-TYPEN	80
10.2	DAS OUTPOST FIREWALL MENÜSYSTEM	82
10.3	GLOSSAR.....	84
11	ZUR DEUTSCHEN ÜBERSETZUNG	90
11.1	REFERENZ OUTPOST FIREWALL	90

1.2 Willkommen

Herzlichen Glückwunsch! Sie haben das sicherste und trotzdem anwenderfreundlichste Firewallsystem der Welt entdeckt.

Das Benutzer-Handbuch gliedert sich in zwei Teile:

- Der erste Teil umfasst die Beschreibung und Anleitung für alle Benutzer.
- Der zweite Teil eignet sich für den technisch fortgeschrittenen Benutzer.

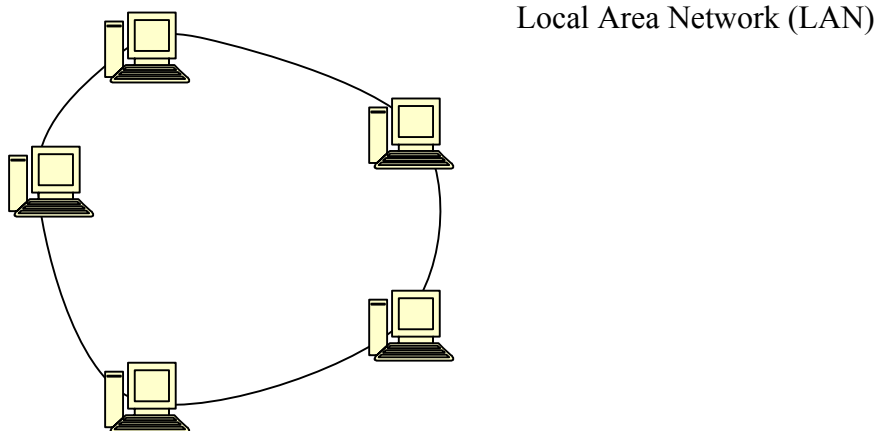
Wir beginnen damit, einige Grundlagen über Netzwerke und dem Internet zu erklären. Danach werden wir Schritt für Schritt auch die technischen Details erläutern. Überspringen Sie Kapitel einfach, wenn Ihnen die Informationen bereits bekannt sind.

Part 1: Für alle Anwender

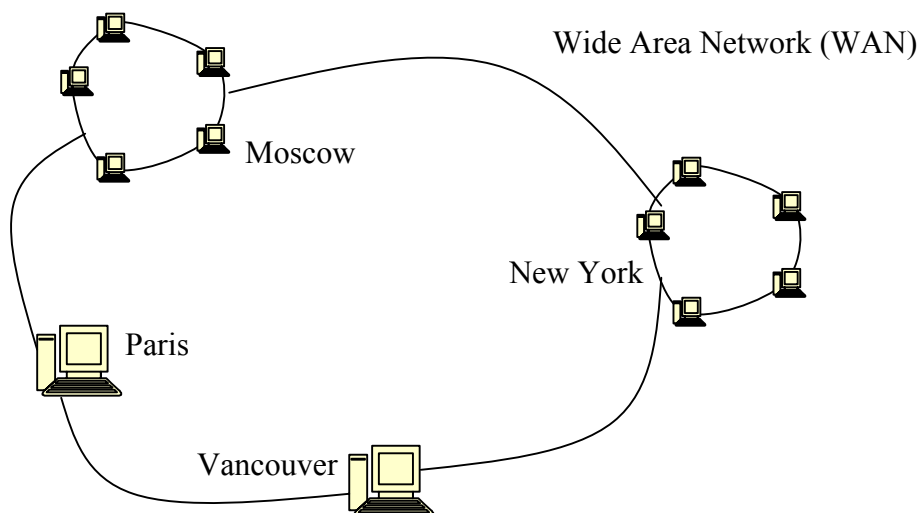
2 Basics

2.1 Netzwerk Basics

Ein Netzwerk ist eine simple Methode, zwei oder mehr Computer miteinander zu verbinden. Auf die Weise können Ressourcen wie zum Beispiel Drucker oder Verzeichnisse und Dateien gemeinsam genutzt werden. Das einfachste Netz ist ein LAN (Lokal Area Network). Diese Computer sind im gleichen Büro oder Gebäude. Ein LAN kann aus praktisch unzähligen Computern bestehen, die typische Größe ist aber ein Netzwerk aus 2 bis 80 Rechnern:



Wenn Computer in unterschiedlichen Gebäuden oder Städten zu einem Netzwerk zusammengeschlossen werden, so nennt sich das Netzwerk WAN (Wide Area Network):



2.2 Wie arbeitet das Internet

Das Internet ist ein Netz der Netze. Es gibt zwei unterschiedliche Arten Computer an das Internet anzuschließen, als [Client](#) oder als [Server](#).

Ein Server stellt seine darauf gespeicherten Dateien zur Verfügung, entweder zur Ansicht oder zum Download. Das können zum Beispiel Webseiten sein, ein Programm, Videos, Musik oder andere Dateien. Ein Client kann die angebotenen Daten dann abrufen.

Ein Client ist irgendein Computer, der an das Internet angeschlossen ist. Das kann ein Desktop-PC sein, ein Laptop, Handheld-PC, Zellentelefon usw.

Zum Abruf eines solchen Dokuments gibt der Benutzer des Clients eine Adresse in den Web-Browser ein und kann dann in der Regel auf die gewünschten Informationen zugreifen. Eine andere Möglichkeit ist die, Daten über eine eMail zu empfangen oder zu versenden.

Grundsätzlich kann jeder Computer sowohl als Server wie auch als Client an das Internet angeschlossen werden. Ohne korrekten Schutz kann allerdings jedermann sowohl auf den Server wie auch auf Clients zugreifen.

Aus dem Grund kann ein Firewallsystem zwischen dem lokalen Computer und dem Internet gesetzt werden. Zugriffe erfolgen dann nicht mehr ohne Ihre Erlaubnis und auch nicht unbemerkt.

Es gibt viele unterschiedliche Arten von Firewalls, die mehr oder weniger einfach zu bedienen sind. In der Regel sind sehr sichere Firewalls aber auch gleichzeitig schwierig zu bedienen.

Eine Ausnahme macht **Outpost Firewall**. Das System ist von Anfang an so entwickelt worden, um extrem leistungsfähig zu sein und trotzdem einfach bedienbar.

2.3 Gefahren im Internet



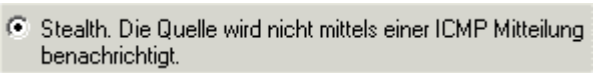

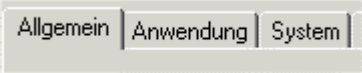

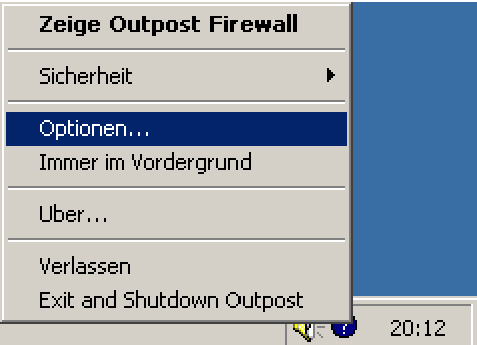
Wir haben alle schon von den Gefahren im Internet gehört. Einige von diesen Gefahren sind sehr groß und es ändert nichts daran, wenn derjenige verantwortlich ist, der seinen Rechner an das Internet anschließt. Es gibt leider psychisch Gestörte und Verbrecher im Netz, die das Leben anderer gern schwer machen. Einige dieser Verbrecher kennen sich sehr gut mit Computern aus und sie wissen, wie man erfolgreich in Rechnern einbrechen kann. Diese Gruppe wird [Cracker](#) genannt. Um sie aus unseren Systemen heraus zu halten, benötigen wir ein starkes Firewallsystem.

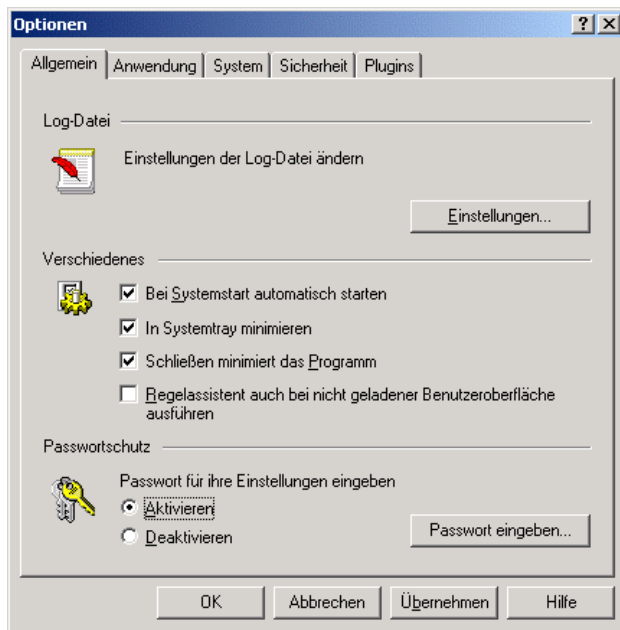
Die größten Gefahren sind:

- Nicht autorisierte Anwendungen können an Ihren Computer geschickt und ohne Ihr Wissen ausgeführt werden (z.B. [ActiveX](#) oder [JAVA-Applets](#), die in Webseiten oder HTML-eMails eingebettet sind). Diese Anwendungen können Befehle auf Ihrem Computer ausführen, um private Informationen zu spionieren oder um Daten zu verändern oder zu löschen.
- Ist Ihr Rechner falsch eingestellt (z.B. unter Windows sind [NetBIOS](#) oder Remote-Procedure-Call per Default eingestellt), können andere Nutzer im Internet unbemerkt auf die freigegebenen Ressourcen wie Ordner und Dateien zugreifen, ohne spezielle Software dafür einsetzen zu müssen.
- Einige Informationen wie zum Beispiel [Cookies](#) oder [Referrers](#) können auf Ihrem Rechner kopiert und später ausgelesen werden. So können mögliche Angreifer eventuell persönliche Informationen von Ihnen spionieren.
- Es können trojanische Pferde ([Trojaner](#)) auf Ihrem Computer installiert werden, die eine Tür zu Ihren persönlichen Informationen öffnet. Auf die Weise können Angreifer in Besitz Ihrer Bankdaten oder Kreditkarteninformationen kommen. Einer der grundlegenden Unterschiede zwischen einem Virus und einem Trojaner ist der, dass ein Virus eigenständig schädliche Funktionen ausführt, während ein Trojaner so programmiert wurde, um vom Eindringling gezielt benutzt zu werden. Auf die Weise spioniert er Daten und sendet sich die Daten zu seinem Rechner zu.
- Nicht unbedingt notwendige Daten in Form von [Bannern](#) und anderen Advertisements gefährden nicht direkt Ihre Daten, beeinträchtigen aber die Bandbreite Ihrer Internet-Verbindung, was den Rechner langsamer macht.
- Spyware sind Programme, die Informationen über Sie erfassen und Ihre Interessen. Einige Anbieter von Software und insbesondere freier Software setzen Spyware ein, um ihre Software damit zu finanzieren.

2.4 Windows Terminologie

Es gibt einige unterschiedliche Objekte im Windows-Environment, die mitunter unverständlich oder missverständlich sind. Wir erklären daher hier einige Objekte, die im weiteren Verlauf dieses Handbuchs genannt werden:

Objekt	Name
	Check-Box ist aktiviert.
	Check-Box ist deaktiviert.
	Optionsfeld ist aktiviert.
	Optionsfeld ist deaktiviert.
	Registerfeld
	Button
	Kontext-Menü. Ein solches Kontext-Menü wird ausgewählt, wenn zum Beispiel das Tray-Icon mit der rechten Maustaste angeklickt wird.



Dialogfeld

3 Outpost Firewall

3.1 System-Voraussetzungen

Die angegebenen Werte sind Mindest-Voraussetzungen für den Betrieb von **Outpost Firewall**:

- 166 MHz Prozessor
- 16 MB Arbeitsspeicher
- Windows 95, 98, NT 4, 2000 oder XP
- 4 MB Festplattenspeicher

Anmerkung: Es ist kein spezielles Modem oder eine spezielle Netzwerkkarte notwendig.

3.2 Outpost Firewall Fähigkeiten

Outpost Firewall ist das weltweit am weitesten entwickelte Firewallsystem mit außergewöhnlichen Eigenschaften und leichter Bedienbarkeit. Um **Outpost Firewall** zu benutzen, benötigen Sie keine tiefgreifenden Kenntnisse über Netzwerktechnik. Die Outpost-Entwickler haben bereits eine Standard Konfiguration erstellt, die bei der Installation Anwendung findet. Natürlich können die Standard-Einstellungen jederzeit manuell verändert werden. Wie Sie Einstellungen verändern, erläutern wir im späteren Verlauf dieses Handbuchs.

Eine enorme Stärke des **Outpost Firewall**system ist seine modulare Organisation. Die Outpost-Funktionen sind in Modulen in Form von DLLs (dynamische Bibliotheken) untergebracht. Auf die Weise können neue und bessere Funktionen jederzeit nachgerüstet werden, um **Outpost Firewall** stets auf dem neuesten Stand zu halten.

Outpost Firewall bietet folgende Eigenschaften:

- Sie kann sofort nach der Installation ohne Schwierigkeiten benutzt werden.
- Sie ermöglicht eine einfache Konfiguration in Kombination mit bereits vordefinierten Regeln.
- Die Oberfläche ermöglicht selbst schwierigste Regeln mit einem simplen Mausklick auf einen Button.

- Sie besitzt viele Einstellungen, um den Netzzugang für den Rechner sicherer zu machen.
- Erfahrene Benutzer können Service-[Protokolle](#) sehr fein justieren und individuell anpassen.
- Der „Stealth-Modus“ macht den Rechner für andere Benutzer im Netz völlig unsichtbar.
- Das modulare System ermöglicht einfachste Erweiterbarkeit.
- Das System ist mit allen Windows-Versionen kompatibel.
- Es ist sehr kompakt und verbraucht wenige Ressourcen.
- Es ermöglicht die gezielte Einschränkung von Anwendungen, die Zugang zum Netz haben dürfen.
- Alle ankommenden und abgehenden [Protokolle](#) und [Ports](#) werden überwacht und geschützt.
- Blockieren oder Einschränken von Informationen, die über den Rechner angefordert werden.
- Blockieren oder Einschränken von [JAVA](#), [ActiveX](#) und Scripten.
- Einrichten einer sicheren Zone für das interne Netzwerk (LAN).
- Einschränken der Benutzung von [Cookies](#).
- **Outpost Firewall** warnt mit einer Anzeige vor jeglichen Zugriffen auf den Rechner und blockiert sie.

3.3 Technischer Support

Benötigen Sie Hilfe und Unterstützung, besuchen Sie bitte folgende unserer Webseiten:

<http://www.agnitum.com/support/>

Sie finden dort unsere FAQ, Dokumentationen, Tipps und Tricks und Hilfe bei der Fehlersuche.

Benutzen Sie die Freeware-Version, können wir Ihnen leider keinen persönlichen Support anbieten. Falls Sie Informationen auf unserer Webseite nicht finden, können Sie sich an das **Outpost Firewall**-Forum wenden unter:

[Outpost Firewall Forum](#)

4 Outpost Firewall in der Praxis

4.1 Outpost Firewall installieren

Die Installation von **Outpost Firewall** ist einfach und orientiert sich am Standard-Installationsvorgang der meisten Anwendungen unter Windows.

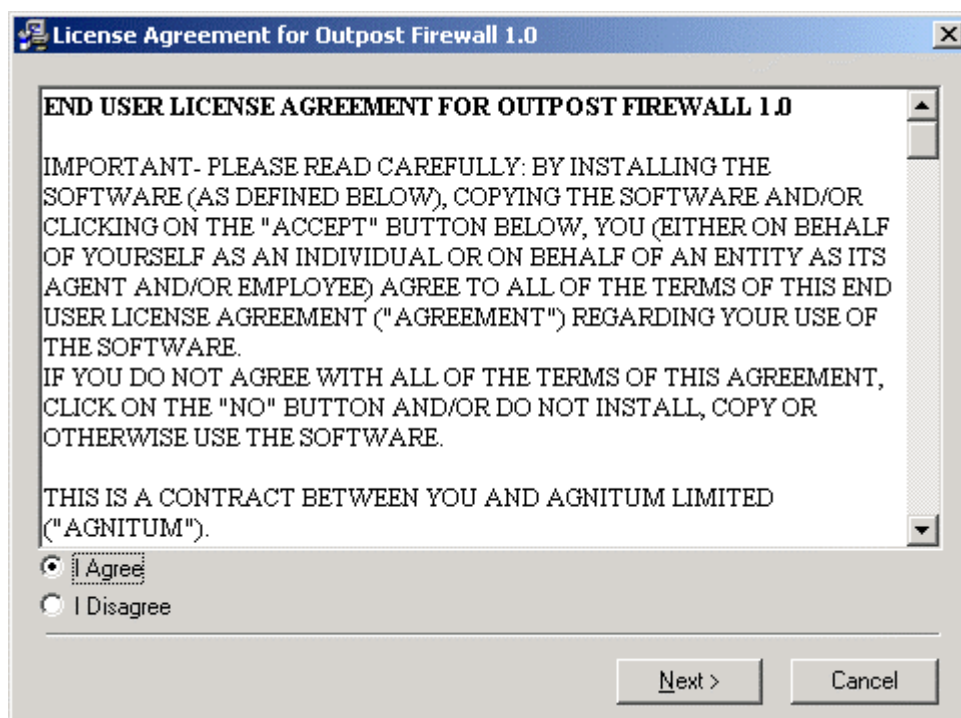
Bitte beachten: Wenn Sie eine neue Version installieren möchten, muss die alte Version zunächst deinstalliert und der Rechner neu gestartet werden. Erst danach darf die neue Version installiert werden. Das ist ein wichtiger Schritt, um die Funktionen sicherzustellen. Weiteres hierzu erfahren Sie im Abschnitt „[Deinstallation](#)“

Ebenso sollte kein weiteres Firewallsystem neben **Outpost Firewall** installiert sein. Beide Firewallssysteme würden sich sonst wechselseitig behindern und sie würden unter Umständen sogar eine erfolgreiche Verbindung zum Netz verhindern.

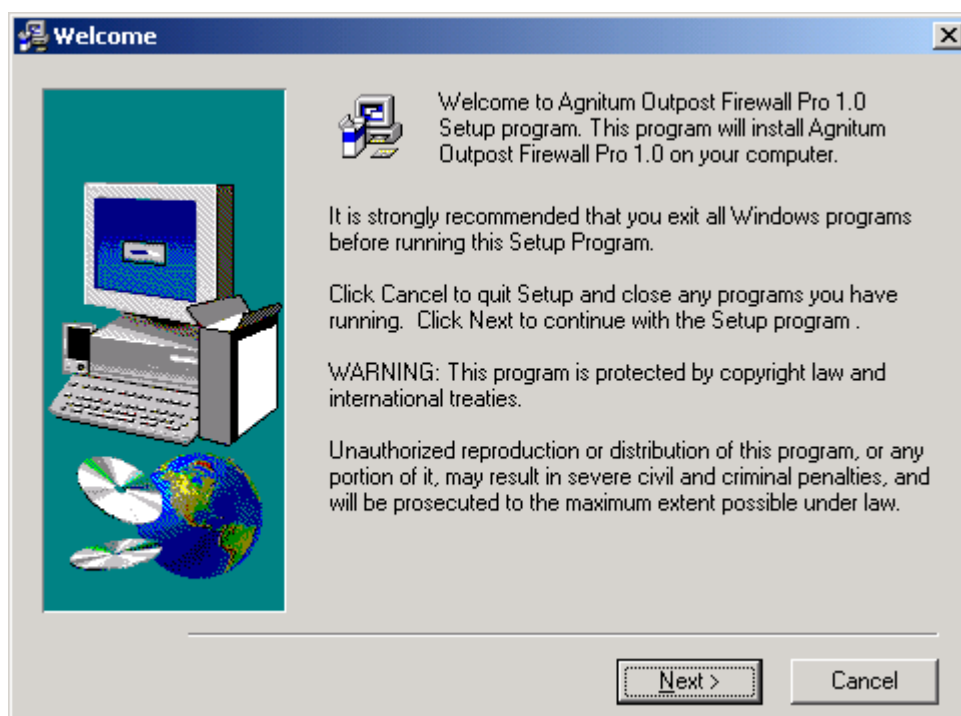
Outpost Firewall installieren:

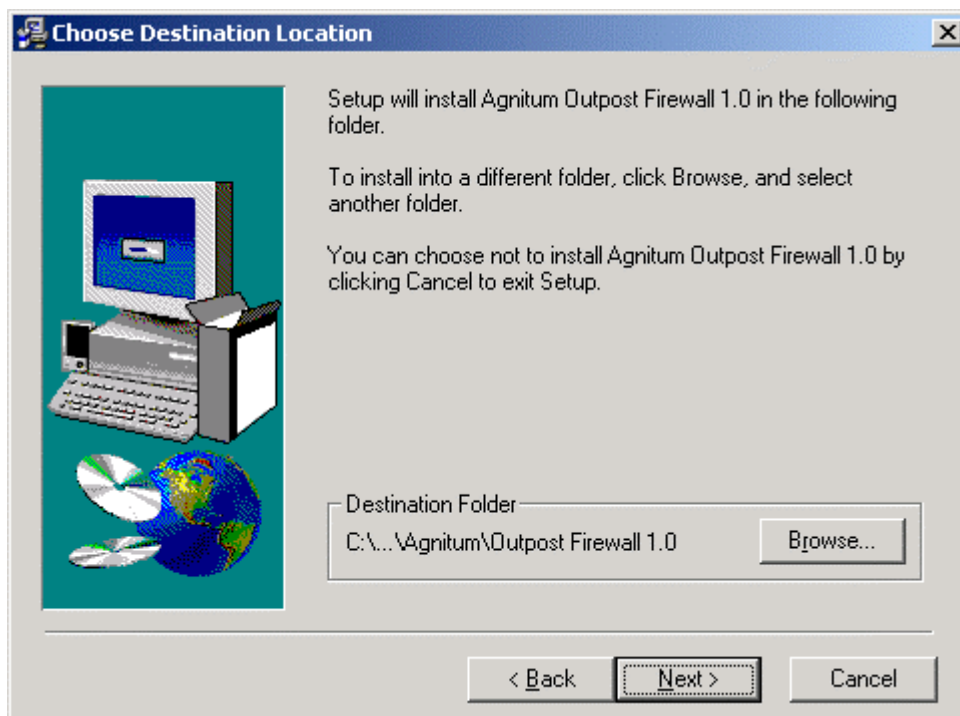
1. **Sehr wichtig!** Bevor Sie **Outpost Firewall** installieren, muss ein anderes Firewallsystem deinstalliert werden. Ebenso muss vorher eine ältere Version von **Outpost Firewall** deinstalliert werden. Danach muss der Rechner zunächst neu gestartet werden.
2. Klicken Sie mit der Maustaste auf den **Start-Button**.
3. Wählen Sie „**Ausführen...**“ aus.
4. Wählen Sie die Outpost-Installationsdatei `OutpostInstall.exe` aus.
5. Klicken Sie auf den Button „**OK**“.

Das Installationsprogramm starten. Es werden zunächst die Lizenzvereinbarungen angezeigt, die Sie sich bitte aufmerksam durchlesen. Erst nach der Annahme der Lizenzvereinbarungen wird die Installation fortgesetzt. Im folgenden Dialog wählen Sie entweder den Standard-Vorschlag zur Installation oder geben selbst ein Verzeichnis Ihrer Wahl zur Installation an.

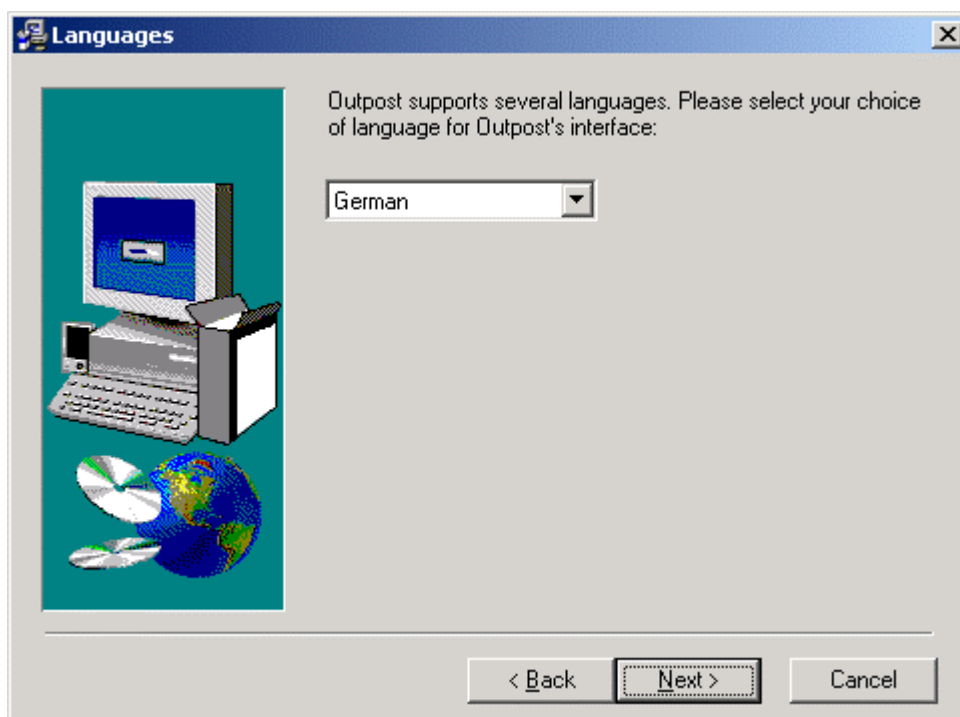


Wenn Sie die Lizenzvereinbarungen angenommen haben und den Options-Knopf auf „I Agree“ (angenommen) gesetzt haben, öffnet sich der weitere Dialog:

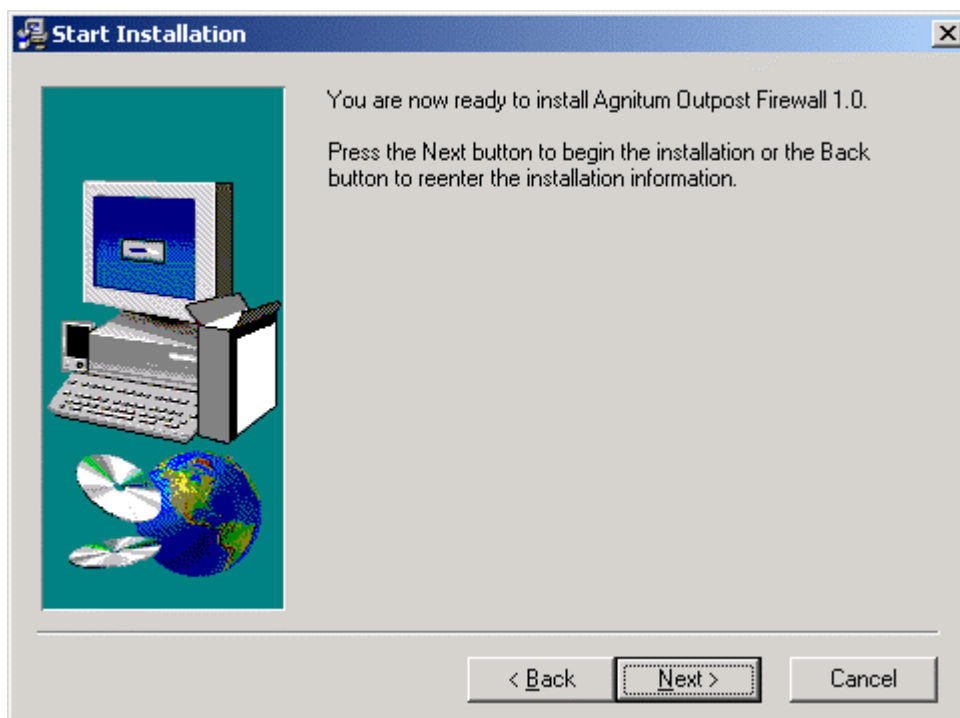




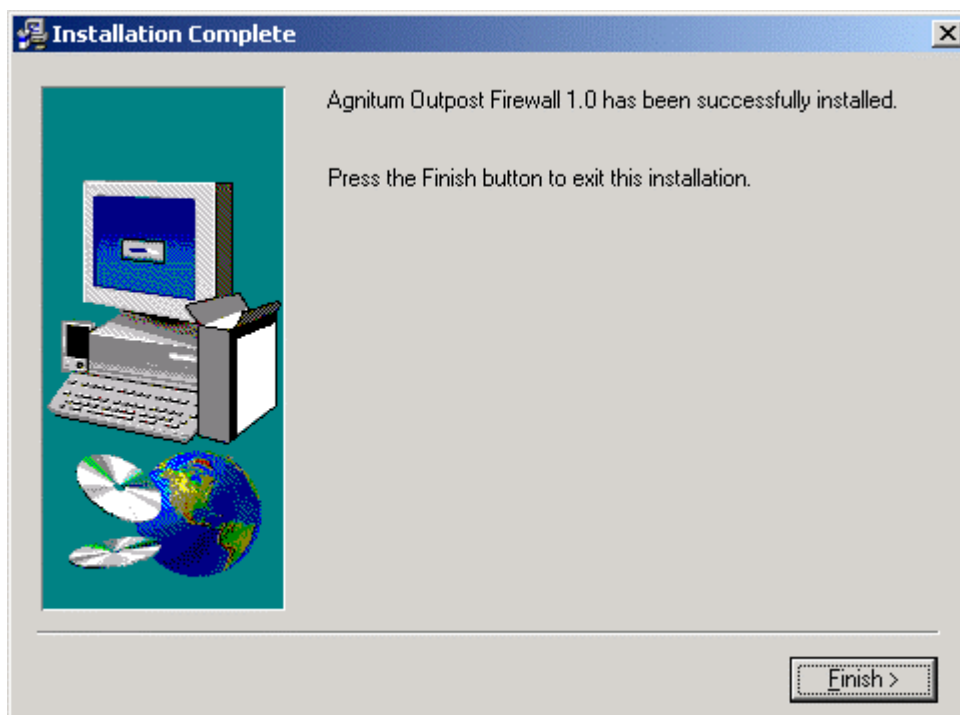
Nehmen Sie entweder den vorgeschlagenen Installationspfad an oder wählen ein eigenes Verzeichnis Ihrer Wahl zur Installation. Ein Klick auf den Button „**Next**“ öffnet den nächsten Installations-Dialog zur Auswahl der Sprache:



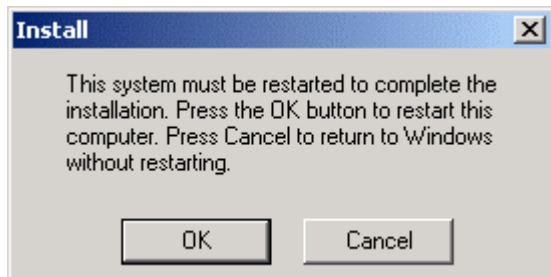
Der nächste Dialog startet den eigentlichen Installationsvorgang. Klicken Sie auf den Button „**Next**“, dann startet die Installation:



Nach der Installation wird ein weiterer Dialog angezeigt, der Sie darüber informiert, ob die Installation erfolgreich war:



Zuletzt erscheint der Dialog zum Neustart des Rechners. Der Neustart ist sehr wichtig für die korrekte Funktion des Firewallsystems. Starten Sie also **Outpost Firewall** bitte nicht vor einem Neustart:

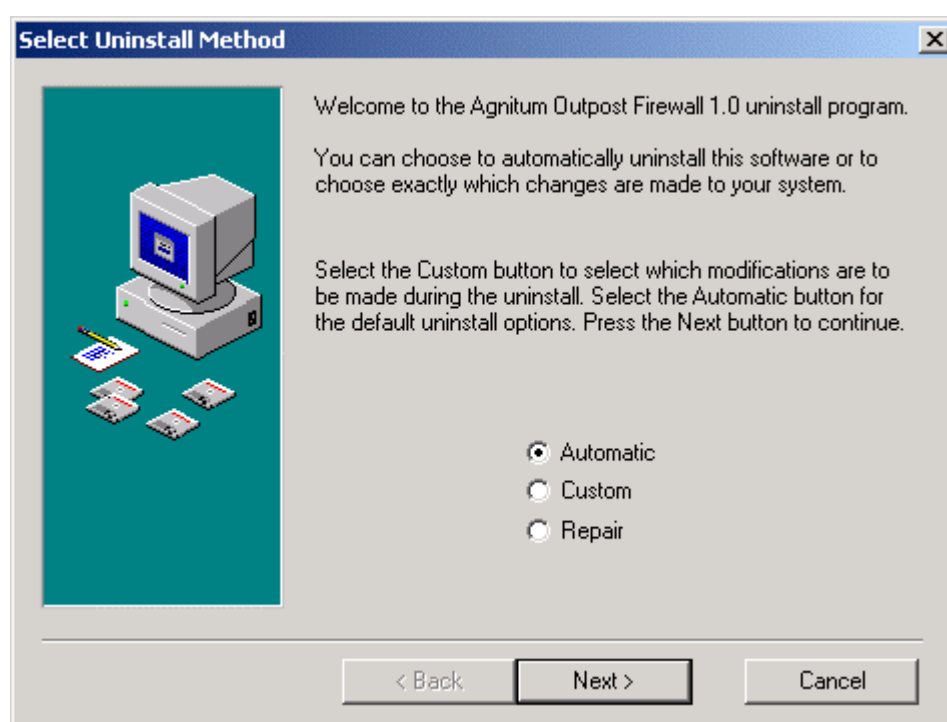


4.2 Outpost Firewall deinstallieren

Sehr wichtig! Bevor Sie eine neuere Outpost Version installieren, müssen Sie die alte Version deinstallieren. Folgen Sie also bitte den nachfolgenden Schritten:

Outpost Firewall deinstallieren:

1. Klicken Sie mit der Maus auf den „Start-Button“.
2. Wählen Sie das Verzeichnis „**Agnitum**“ aus und dort den Eintrag „**Outpost Firewall 1.0**“
3. Wählen Sie dort den Eintrag „**Uninstall Outpost Firewall**“
4. Folgen Sie den weiteren Dialogen:

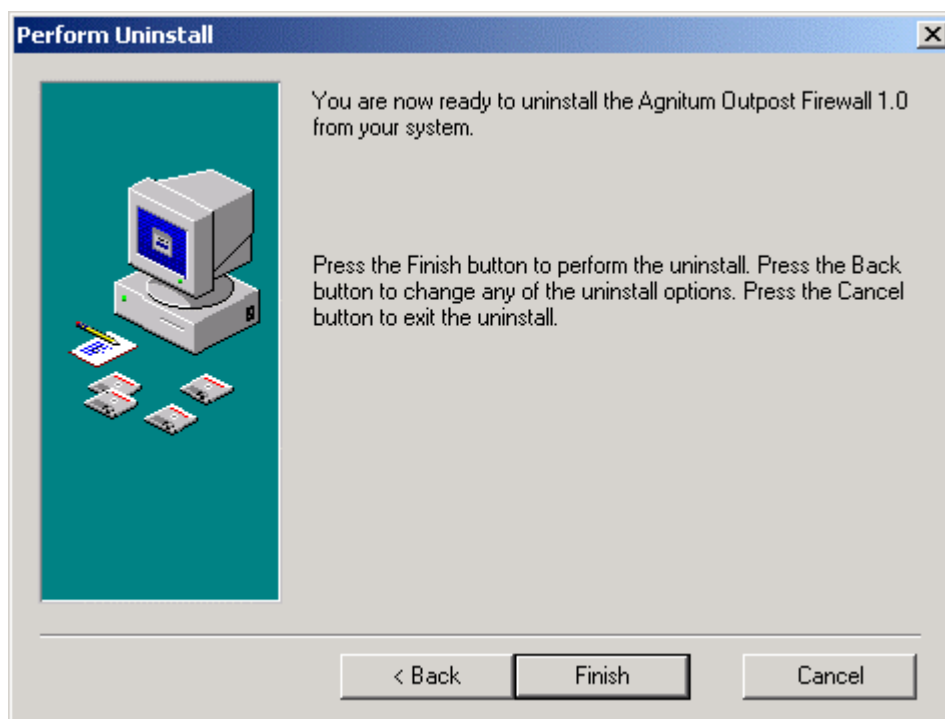


Sind Sie unerfahren mit Windows-Anwendungen, wählen Sie bitte die automatische Deinstallation und bestätigen Sie die Auswahl mit dem Button „**Next**“.

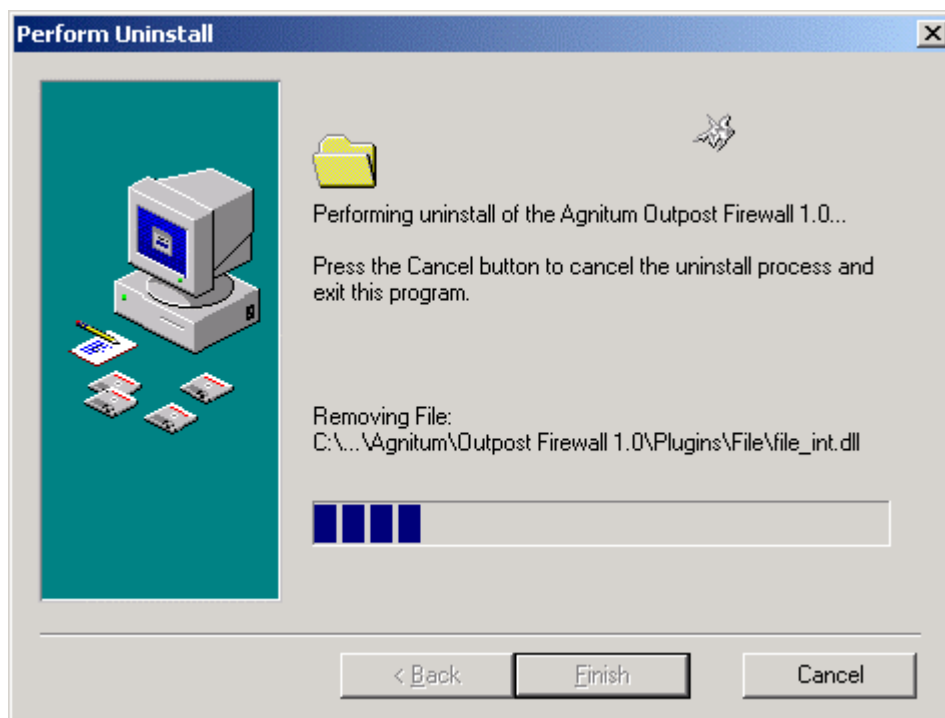
Als erfahrener Anwender können Sie auch die Option „**Custom**“ zur selektiven Deinstallation wählen und die Auswahl dann wieder mit dem Button „**Next**“ bestätigen.

Die Auswahl „**Repair**“ ermöglicht eine Reparatur eines eventuell beschädigten **Outpost Firewalls**. Nach dem Durchlauf der „**Repair-Funktion**“ steht Ihnen **Outpost Firewall** wieder mit gewohntem Umfang zur Verfügung.

Anschließend zeigt sich der nächste Dialog:



Klicken Sie auf den Button „**Finish**“, zeigt sich ein weiterer Dialog:



Anmerkung: Starten Sie nach dem Deinstallationsvorgang den Rechner bitte neu.

4.3 Outpost Firewall starten

Nach der Installation und dem Neustart des Rechners wird **Outpost Firewall** automatisch gestartet und schützt Ihren Computer.

Wenn **Outpost Firewall** startet, zeigt sich rechts unten im „Tray“ der Startleiste neben der Uhr ein kleines Icon. Wenn aus irgendeinem Grund **Outpost Firewall** nicht gestartet wird, gehen Sie bitte folgend vor:

1. Klicken Sie mit der Maus auf den „**Start-Button**“.
2. Wählen Sie den Eintrag „**Agnitum**“ aus.
3. Wählen Sie dort den Eintrag „**Outpost Firewall 1.0**“ aus.

Startet **Outpost Firewall**, zeigt sich rechts unten im „Tray“ der Startleiste neben der Uhr ein kleines Icon (blauer Punkt mit einem Fragezeichen, um Ihnen zu zeigen, dass Ihr Computer geschützt wird, es sei denn, Sie haben in den Einstellungen eingestellt, die Regeln auch zu verwenden, wenn die Oberfläche nicht sichtbar ist.

4.4 Outpost Firewall stoppen

Um **Outpost Firewall** zu beenden reicht es nicht, die Oberfläche zu schließen. Die Firewall-Engine bleibt trotzdem aktiv. Es gibt zwei Möglichkeiten, **Outpost Firewall** zu beenden:

- Klicken Sie mit der rechten Maustaste auf das Outpost-Icon im Tray und wählen im sich öffnenden Kontextmenü den Punkt „**Exit and shutdown Outpost**“. Dies stoppt die Schnittstelle und beendet **Outpost**. Ihr Rechner ist danach nicht mehr geschützt.
- Die zweite Möglichkeit finden Sie in der Benutzer-Schnittstelle des Programms. Wählen Sie dort das Menü „**Datei**“ und dort den Menüpunkt „**Beenden**“. **Outpost** wird dann komplett beendet und der Rechner ist nicht mehr geschützt.

4.5 Automatisches Update

Outpost Firewall besitzt eine automatische **Update-Funktion**, die Sie regelmäßig vor den neuen Gefahren im Internet schützt.

Dieser Vorgang geschieht automatisch in dem Moment, wo Sie eine Verbindung zum Internet aufnehmen. Bitte unterbrechen Sie diesen Vorgang nicht, er ist wichtig für die Funktionalität des Systems. Bei der Übertragung von Programmdateien werden keine persönlichen Informationen übermittelt.

Wenn Sie aus irgendeinem Grund manuell nach **Updates** schauen möchten, finden Sie in der Icon-Leiste der Benutzer-Schnittstelle ein Icon, mit dem Sie manuell Kontakt zum **Agnitum-Updateserver** aufnehmen können:



Alternativ können Sie die **Update-Funktion** auch im **Programm-Eintrag** des **Start-Menüs** aufrufen. Gehen Sie dabei bitte wie folgt vor:

1. Klicken Sie auf den „**Start-Button**“.
2. Wählen Sie den Eintrag „**Agnitum**“ aus.
3. Wählen Sie dort den Eintrag „**Outpost Firewall 1.0**“ aus.
4. Wählen Sie dort den Eintrag „**Agnitum Update**“.

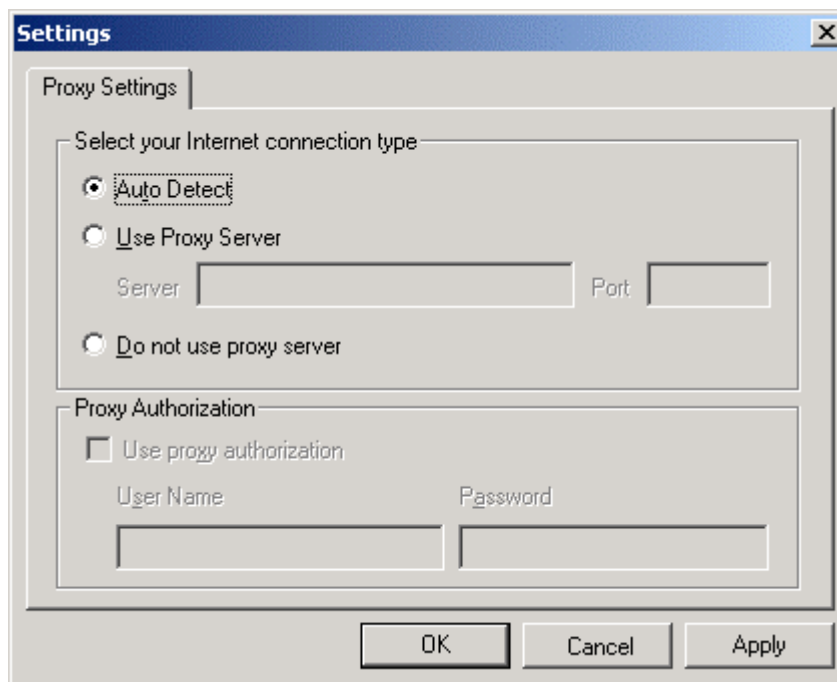
Es zeigt sich in beiden Fällen der erste von zwei Dialogen:



Sie können hier wählen zwischen automatischem **Update** und einem selektierten **Update**:

- Das **automatische** Update installiert alle verfügbaren Programmteile.
- Das **erweiterte** Update ermöglicht eine selektive Auswahl einzelne angebotener Module.

Wählen Sie eine der Möglichkeiten, öffnet sich der nächste Dialog:

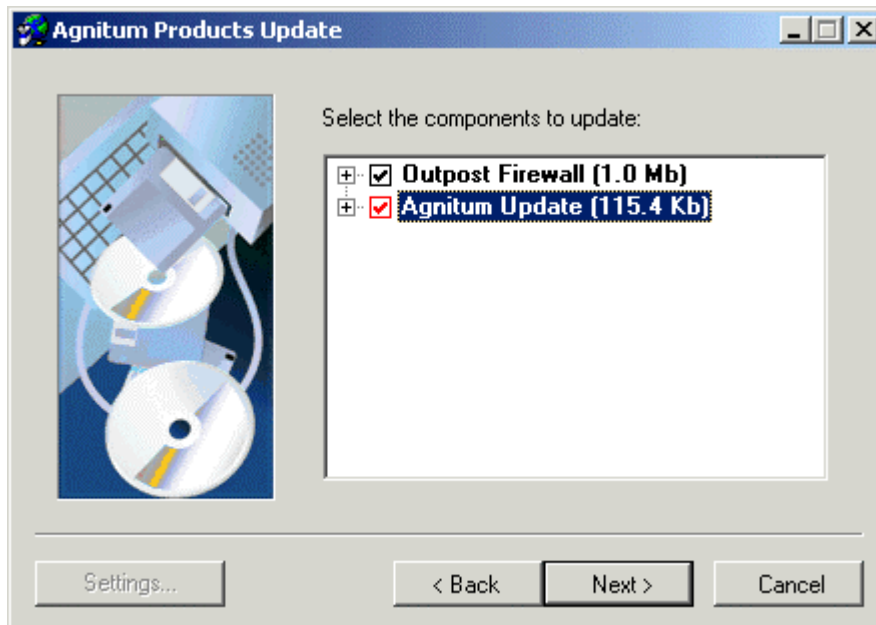


Hier wählen Sie aus, ob und wie Ihr Rechner Verbindung zum Internet aufnimmt und ob Sie einen [Proxy-Server](#) benutzen.

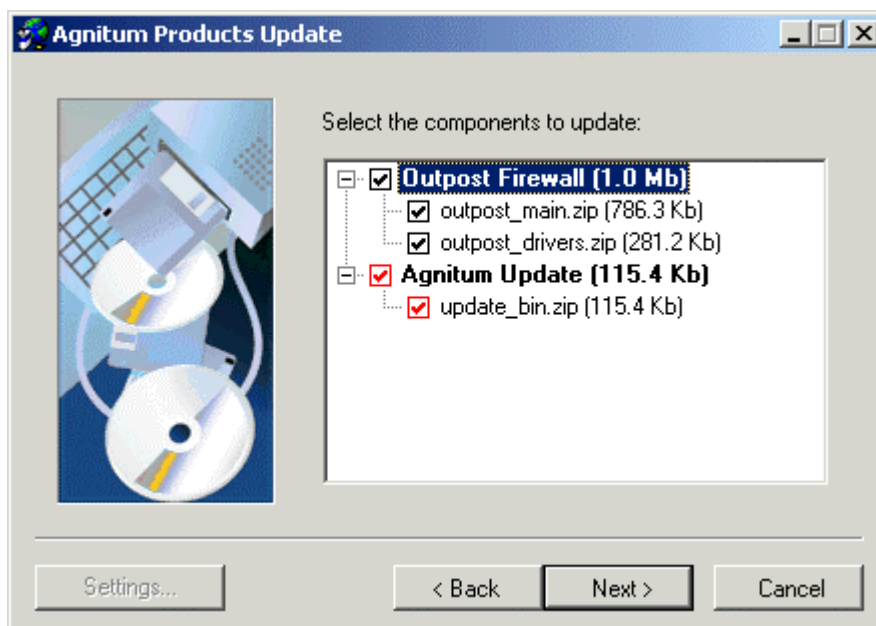
Hier gibt es die Möglichkeit, die Verbindung automatisch vornehmen zu lassen. In dem Fall werden die Einstellungen Ihres Web-Browsers automatisch übernommen und Sie müssen keine weiteren Angaben machen.

Benutzen Sie einen Proxy-Server und möchten die Daten hierfür manuell eingeben, wählen Sie bitte die zweite Möglichkeit zur Verbindungsaufnahme, geben die Daten Ihres Proxy-Servers ein und eventuell auch den Benutzernamen und das Passwort zur Proxy-Autorisation.

Benutzen Sie die selektive **Update**-Funktion, zeigt sich folgender Dialog:



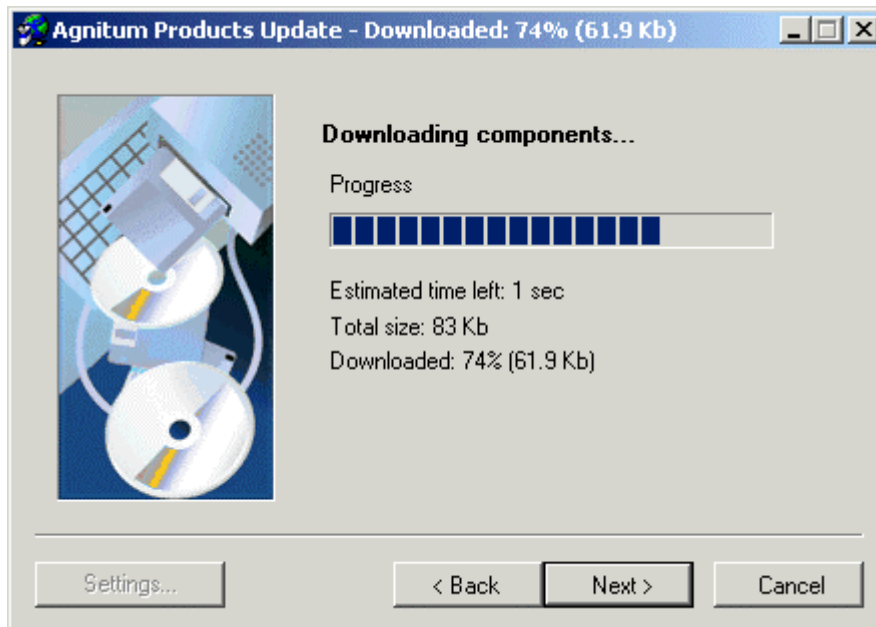
Einige der Einträge im Dialog haben ein + vorangestellt. Wenn Sie das + anklicken, öffnet sich ein Baum mit erweiterten Informationen zu den angebotenen **Updates**:



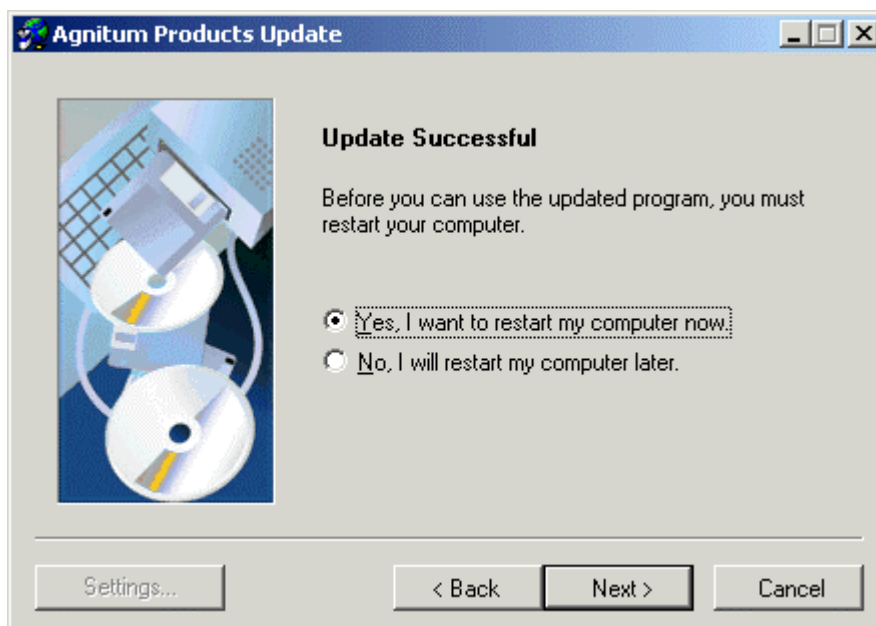
Update-Dateien mit einem roten Häkchen voran müssen installiert werden, um die Kompatibilität mit den Modulen und anderen Programmteilen zu halten.

Update-Dateien mit einem schwarzen Häkchen voran können, müssen aber nicht installiert werden.

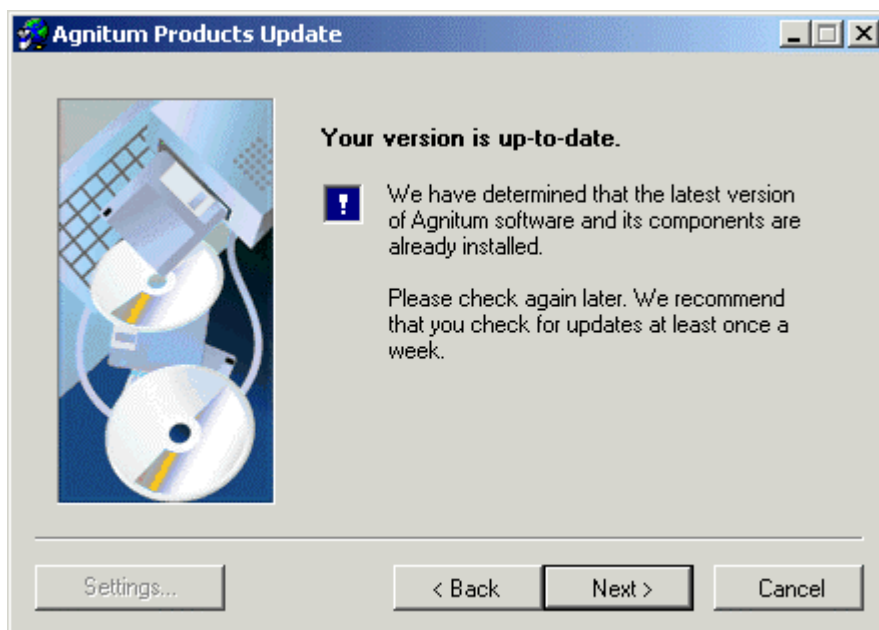
Wählen Sie die gewünschten Komponenten aus und bestätigen den Dialog mit einem Klick auf den Button „Next“, dann öffnet sich der Download-Dialog:



Nach erfolgreichem Download bestätigen Sie den Dialog mit einem Klick auf den Button „Next“. Es öffnet sich dann der letzte Dialog zum Neustart des Rechners. Nach Installationen oder Updates von **Outpost Firewall** muss immer der Rechner erst neu gestartet werden. Das ist wichtig für die Funktionalität des Firewallsystems:



Steht kein aktuelles **Update** zur Verfügung oder benutzen Sie bereits die aktuellste Version, zeigt sich beim Aufruf der Update-Funktion folgender Dialog:








5 Orientierungshilfen

5.1 Das System Tray-Icon

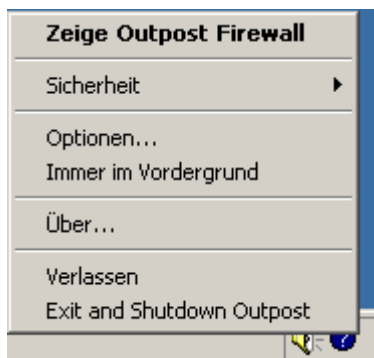
Wurde **Outpost Firewall** gestartet, zeigt sich rechts unten im System-Tray neben der Uhr ein Icon:



Je nach Einstellung von **Outpost Firewall** werden verschiedene Icons angezeigt, die eine spezielle Bedeutung haben:

Icon	Mode	Beschreibung
	Alles blockieren	Alle Verbindungen sind geblockt.
	Blockiere alles außer	Verbindungen sind geblockt, die nicht explizit erlaubt wurden.
	Rules Assistent	Der Regel Assistent hilft bei der Regel-Erstellung und meldet sich immer dann, wenn eine unbekannte Verbindung bemerkt wird.
	Erlaube alles außer	Verbindungen sind erlaubt, die nicht explizit verboten wurden.
	Deaktiviert	Alle Verbindungen sind erlaubt.

Klicken Sie mit der rechten Maustaste auf das Tray-Icon, öffnet sich ein Kontext-Menü:

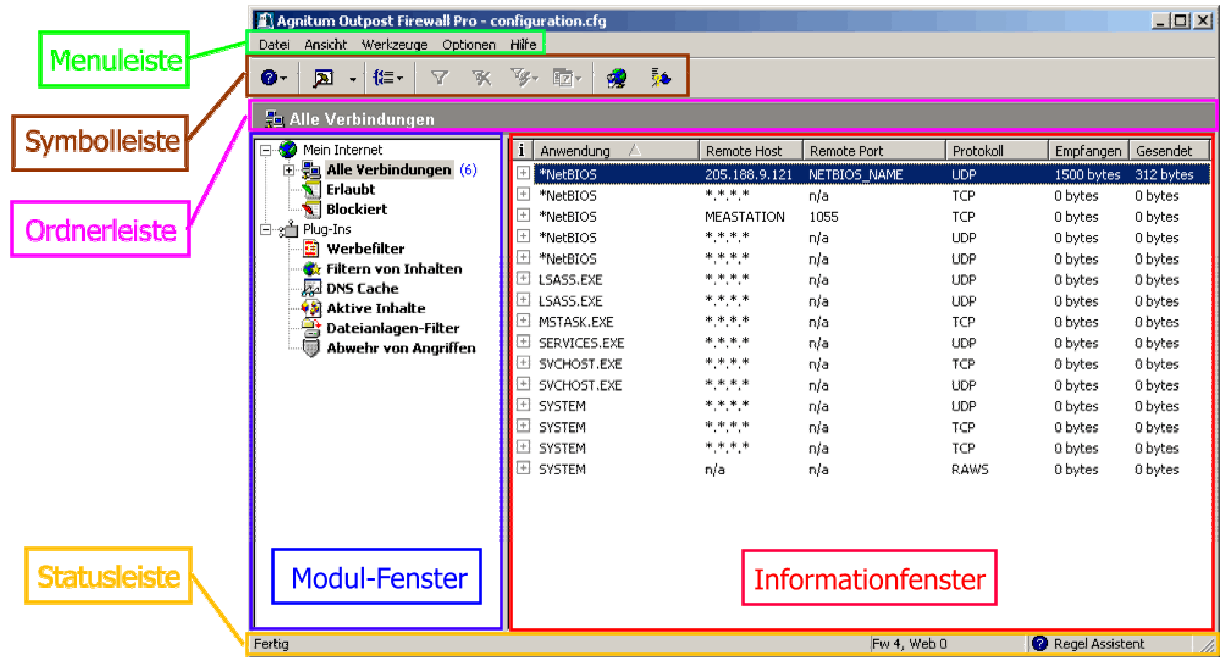


- „**Zeige Outpost Firewall**“ zeigt die Benutzer-Schnittstelle des Programms, über die sämtliche Einstellungen vorgenommen werden sowie Filter-Regeln erstellt werden können.

- „**Sicherheit**“ zeigt ein weiteres Auswahlmenü, um den Security-Level festzulegen, der bereits [weiter](#) oben beschrieben wurde. So können Sie den Regel-Assistenten einstellen, alle Verbindungen stoppen freigeben, die meisten Verbindungen stoppen oder freigeben oder alle Verbindungen freigeben.
- „**Immer im Vordergrund**“ setzt das Fenster der Benutzer-Schnittstelle als „Top-Fenster“. Es wird dann immer als erstes Fenster angezeigt, egal wie viele und welche anderen Programme gestartet wurden.
- „**Über...**“ zeigt Informationen zum Programm und zur Version an.
- „**Verlassen**“ schließt die Benutzer-Schnittstelle, lässt **Outpost Firewall** aber weiter aktiv.
- „**Exit and Shutdown Outpost**“ schließt die Benutzerschnittstelle und beendet **Outpost**.

5.2 Das Outpost Firewall Hauptfenster

Das **Outpost Firewall** Hauptfenster ist die zentrale Schnittstelle zum Firewall. Hier können Sie Verbindungen überwachen, neue Regeln erstellen und die Module konfigurieren. Sie rufen das Hauptfenster auf, wenn Sie mit der rechten Maustaste auf das Tray-Icon klicken und im Kontextmenü den Eintrag „**Zeige Outpost Firewall**“ auswählen. Es zeigt sich dann folgendes Fenster:



5.3 Die Outpost Panels

Das **Outpost Firewall** Hauptfenster ist in verschiedene Bereiche unterteilt, die verschiedene Funktionen besitzen.

Sie setzen sich zusammen aus:

- Menüleiste
- Symbolleiste
- Ordnerleiste
- Modul-Fenster
- Informationsfenster
- Statusleiste

Die beiden Fenster „Module“ und „Informationen“ verhalten sich ähnlich wie der Windows-Explorer. Das Modul-Fenster zeigt die installierten Module von **Outpost Firewall**, das Informationsfenster zeigt die Informationen, die das ausgewählte Modul zur Verfügung stellen kann.

Das **Modul-Fenster**:



Das **Modul-Fenster** stellt folgende Informationen zur Verfügung:

- **Alle Verbindungen:** Hier werden alle Verbindungen, Anwendungen und offenen [Ports](#) angezeigt, die aktuell eine Verbindung zum Internet oder zum LAN besitzen.

- **Erlaubt:** Hier werden alle Verbindungen und Anwendungen angezeigt, die **Outpost Firewall** erlaubt.
- **Blockiert:** Hier werden alle Verbindungen und Anwendungen angezeigt, die von **Outpost Firewall** am Zugang zum Netz gehindert werden.
- **Meldet:** Hier werden alle „Logs“ über Verbindungen und Anwendungen angezeigt, die von Outpost protokolliert wurden.

Obgleich die Details der Log-Dateien für fortgeschrittene Benutzer gedacht sind, sind die oben genannten protokollierten Details wichtig, wenn Sie ermitteln wollen, welche Anwendungen Zugriff auf das Netz genommen haben oder welche Verbindungsversuche stattgefunden haben. Sie können die Details auch benutzen um festzustellen, ob **Outpost Firewall** und die Module entsprechend Ihrer Wünsche arbeiten.

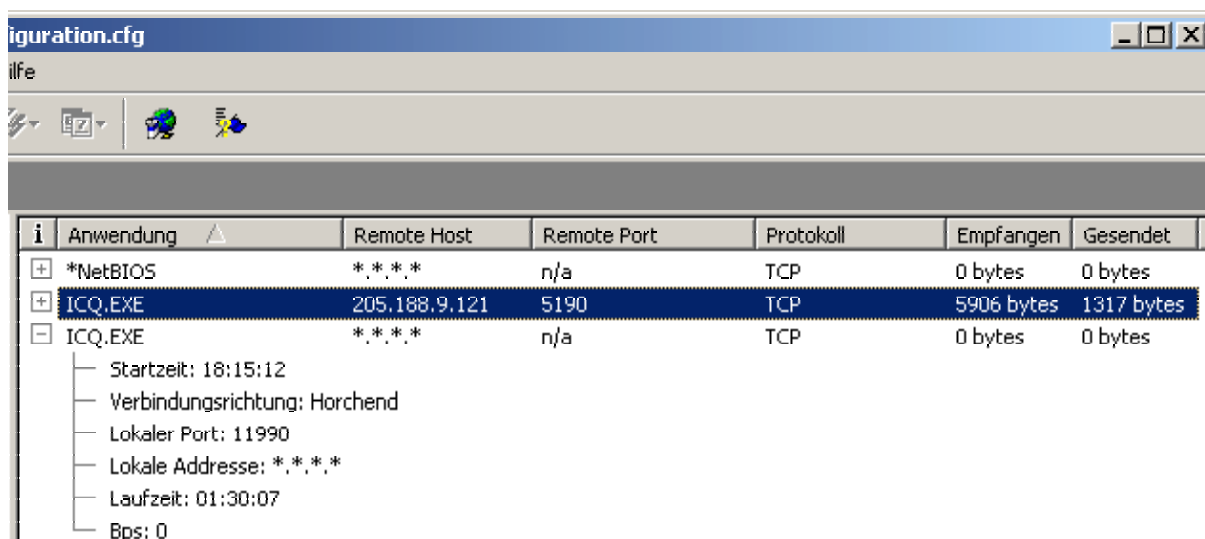
- **PlugIns:** Einige der Module (PlugIns) sind bereits im Installationsprogramm enthalten. Sie können aber auch PlugIns von Drittanwendern in das System einsetzen. Die installierten PlugIns werden Ihnen ebenfalls im linken Modul-Fenster angezeigt, während die Aktivitäten der PlugIns im rechten Modul-Fenster angezeigt werden.

Direkt nach der ersten Installation von **Outpost Firewall** sind folgende **PlugIns** bereits installiert:

- **Werbefilter:** Zeigt alle geblockten [Banner](#) und andere „Werbe-Effekte“.
- **Filtern von Inhalten:** Zeigt alle Webseiten, die über dieses PlugIn geblockt werden sollten.
- **DNS Cache:** Zeigt alle von Outpost gespeicherten Adressen an. Die Speicherung der Adressen beschleunigt zukünftige Aufrufe dieser Adressen oder Seiten.
- **Active Inhalte:** Zeigt alle aktiven Inhalte wie [Cookies](#), [JAVA-Scripte](#) und [Applets](#) sowie [ActiveX-Controls](#) an, die auf besuchten Seiten vorhanden waren, entsprechend der Einstellungen aber geblockt wurden.
- **Dateianlagen-Filter:** Zeigt alle eMail-Anhänge, die entsprechend der Einstellungen neutralisiert, umbenannt und in ein Quarantäne-Verzeichnis abgelegt wurden.

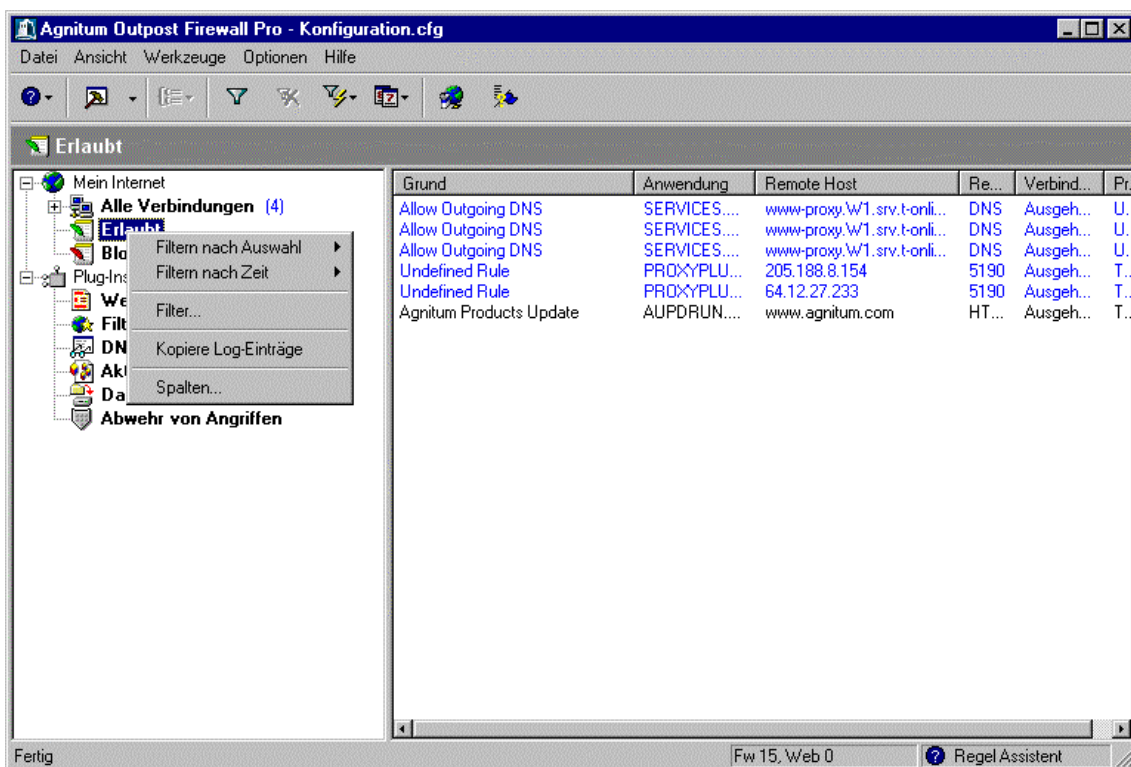
- **Abwehr von Angriffen:** Zeigt alle suspekten Zugriffe auf Ihren Rechner, gescannte [Ports](#) und die Adresse, von der die Zugriffe erfolgten. Je nach Einstellung werden auch einzelne Port-Scans angezeigt.

Wie in allen Explorer ähnlichen Fenstern können auch hier die eventuell vor dem Eintrag stehenden Pluszeichen (+) „angeklickt“ werden, um den Baum mit weiteren Details zu öffnen. Auf dem folgenden Bild sehen Sie ein Beispiel, was damit gemeint ist:



i	Anwendung	Remote Host	Remote Port	Protokoll	Empfangen	Gesendet
+	*NetBIOS	*.*.*.*	n/a	TCP	0 bytes	0 bytes
+	ICQ.EXE	205.188.9.121	5190	TCP	5906 bytes	1317 bytes
-	ICQ.EXE	*.*.*.*	n/a	TCP	0 bytes	0 bytes
	— Startzeit: 18:15:12					
	— Verbindungsrichtung: Horchend					
	— Lokaler Port: 11990					
	— Lokale Adresse: *.*.*.*					
	— Laufzeit: 01:30:07					
	— Bps: 0					

Wie bei fast allen Elementen von **Outpost Firewall** können auch hier mit einem Klick der rechten Maustaste Kontext-Menüs aufgerufen werden, über die weitere Funktionen abgerufen werden können. Im folgenden Beispiel sehen Sie die Filtermöglichkeiten, die über ein Kontext-Menü aufgerufen werden können:



Das Menü oben zeigt, wie angezeigte Daten sortiert werden können, um mit einem Blick eine bestimmte Aussage über die Aktivitäten machen zu können. Diese Möglichkeit ist besonders für Fachleute wie Systemverwalter interessant und wichtig, wenn sie einen bestimmten Bezugspunkt schnell aufspüren müssen. Obwohl **Outpost Firewall** einfach genug ist für Anwender ohne spezielle Kenntnisse, erfüllt sie auch die Bedürfnisse von Anwendern mit Hintergrundwissen.

Die oben gezeigte Auswahl im Menü zeigt, wie Informationen sortiert, gruppiert und gefiltert werden können. **Outpost Firewall** macht sehr regen Gebrauch von Kontext sensitiven Menüs. Ein bisschen experimentieren wird Ihnen schnell helfen, sich mit den Funktionen dieser Menüs vertraut zu machen. Benötigen Sie mehr Informationen über die Filtermöglichkeiten, lesen Sie sich bitte das Kapitel [Filter](#) durch.

5.4 Die Icon-Leiste

Die Icon-Leiste im oberen Teil des Hauptfensters stellt diverse Funktionen zur Verfügung, die Sie mit einem Klick auf eines der Icons schnell aufrufen können:



Über das erste Icon von links (blauer Kreis mit Fragezeichen) können Sie den Security-Level einstellen:



Hier sehen Sie alle verfügbaren Informationen, die über die Icons abrufbar sind:

Button	Function
	Einstellen des Security-Levels von Outpost Firewall . Korrespondierendes Menü ist „ Optionen/Sicherheit “.
	Öffnet den Dialog „Optionen“. Korrespondierendes Menü ist „ Optionen “.
	Öffnet die Auswahl „Gruppieren nach“. Korrespondierendes Menü ist „ Anzeige/Gruppieren nach “.
	Öffnet den Dialog zur Auswahl eines Filters nach Ihren Wünschen. Korrespondierendes Menü ist „ Anzeige/Filter “.
	Löscht den ausgewählten Filter und zeigt wieder alle Details an. Korrespondierendes Menü ist „ Anzeige/Filter/Alles anzeigen “.
	Öffnet eine Auswahlmöglichkeit für eine Filterung der Daten nach Ihren Wünschen. Korrespondierendes Menü ist „Kontextmenü mit Auswahl nach „ Erlaubt “, „ Blockiert “ oder „ Meldet “ bei der Auswahl „ Sortieren nach selektierter Anwendung “.
	Öffnet eine Auswahlmöglichkeit für eine Filterung der Daten nach Ihren Wünschen. Korrespondierendes Menü ist „Kontextmenü mit Auswahl nach „ Erlaubt “, „ Blockiert “ oder „ Meldet “ bei der Auswahl „ Sortieren nach Zeit “.
	Überprüft auf Updates von Outpost Firewall . Kein Korrespondierendes Menü.
	Öffnet den Dialog „Über Outpost Firewall“. Korrespondierendes Menü ist „ Hilfe/Über Outpost Firewall “.

6 Outpost Firewall einstellen

6.1 Basis-Informationen

Ein Firewallsystem für Ihren Computer ist wie die Verriegelung einer Tür Ihres Hauses. In den meisten Städten wird die Eingangstür unserer Häuser verschlossen, wenn wir sie verlassen. Dies geschieht nicht, weil wir potentielle Verbrecher befürchten oder den Nachbarn nicht trauen sondern um uns einzig um unsere eigenen Geschäfte zu kümmern. Wir verschließen die Türen aber auch, um Schnüffeleien, Diebstahl oder Beschädigungen an unserem Eigentum zu verhindern.

Das Internet ist ähnlich. Die meisten Webseiten sind gutartig. Nur ein kleiner Prozentsatz stellt eine Bedrohung dar. Weil jedoch die Zahl der Internet-Nutzer so groß ist, stellt sogar ein kleiner Teil bössartiger Zugriffe eine mögliche Bedrohung unseres Privatlebens dar.

Aus diesem Grund ist es nicht gerade besonnen, Ihren Computer ungeschützt zu lassen.

Outpost Firewall wurde entwickelt, um unberechtigte Zugriffe zu ermitteln. Für den täglichen Gebrauch wird empfohlen, die meisten Verbindungen zu blockieren oder den Regel-Assistenten zu benutzen, wenn Sie nicht so erfahren im Umgang mit Firewalls sind.

Anmerkung: Wenn Sie irgendeinen Zweifel daran haben, Einstellungen zu ändern, sollten Sie das auch nicht machen. Aber auch wenn Sie erfahren sind im Umgang mit Firewalls und wenn Sie verstehen, warum welche Einstellung verändert werden soll, ist es ratsam, die vorherigen Einstellungen zu notieren.

Wenn Outpost Ihnen eine neue Verbindung anzeigt und Sie auffordert, eine Regel für diese Anwendung zu erstellen, erhalten Sie Informationen über diese Verbindung. So können Sie erkennen, welche Adresse die Gegenstelle der Verbindung hat sowie andere Informationen, die Ihnen bei der Entscheidungsfindung helfen. Im Zweifelsfall sollten Sie eine solche Verbindung zunächst blockieren und abwarten, ob im weiteren Verlauf Störungen bei der Kommunikation mit dem Internet entstehen. Auf die Weise können Sie lernen, was Ihre Anwendungen tun. Sie lernen dabei sogar, wenn ein [Trojaner](#) auf Ihr System zugreift oder ein bereits installierter Trojaner Verbindung zum Internet aufnimmt.

Anmerkung: Eine gute Richtlinie für die Entscheidungsfindung ist der Vorschlag, der Ihnen von Outpost angezeigt wird, wenn Sie nicht das nötige Wissen oder die Erfahrung haben, zielgerichtet eine Regel für die Verbindung selbst zu erstellen.

Outpost Firewall besitzt bereits nach der Installation eine Zugangseinstellung, die regelt, wie viele Informationen über Ihren Rechner an andere Rechner im Internet übermittelt werden.

Outpost Firewall benutzt verschiedene Sicherheitseinstellungen, um Ihren Computer vor der unerwünschten Weitergabe von Informationen zu anderen Computern zu schützen. Diese Einstellungen schränken auch den Fluss der Informationen ein, wie viele Informationen von Ihrem Computer gesendet werden dürfen und welche Informationen empfangen werden dürfen.

Einige Anwendungen, Webseiten oder Computer müssen nicht ständig überwacht und eingeschränkt werden. Aus diesem Grund können Sie mit **Outpost Firewall** vertraute Zonen einrichten, in denen einzelne Computer ohne Einschränkungen miteinander kommunizieren können. Das kann zum Beispiel das interne LAN sein, bekannte und vertrauenswürdige Webseiten oder auch Anwendungen. Auf diese Weise lässt sich ein Netzwerk in vertraute Zonen einteilen und in Zonen, in denen Webseiten, Anwendungen und Computer nur eingeschränkt miteinander kommunizieren dürfen.

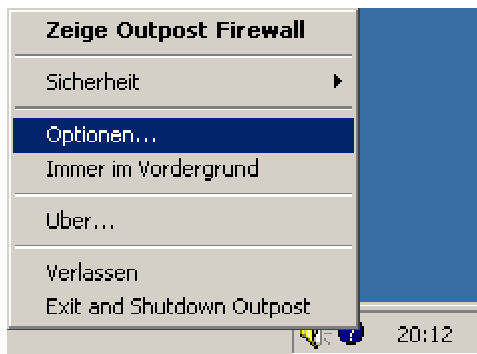
Anmerkung: Es ist sehr wichtig, dass Sie Anwendungen oder Webseiten nicht unreflektiert in die vertraute Zone aufnehmen, wenn Sie nicht ganz sicher sind.

6.2 Initiale Einstellungen

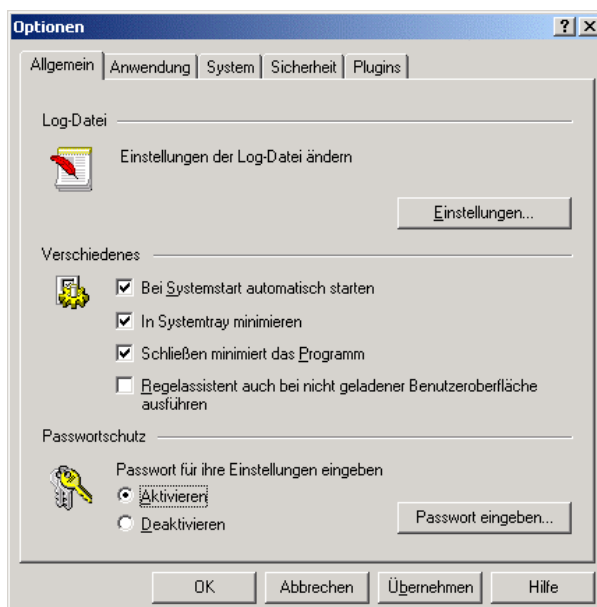
Outpost Firewall ist betriebsbereit, sowie das Firewallsystem installiert ist. Seine Standard-Regeln sind mehr als ausreichend für die meisten Verwendungszwecke. Es wird deshalb empfohlen, erst dann Einstellungen zu verändern, wenn Sie die Funktionsweise von **Outpost Firewall** genau kennen.

Sobald Sie mit **Outpost Firewall** vertraut sind, können Sie das Firewallsystem individuell auf Ihre Arbeitsgewohnheiten einstellen. Der Abschnitt hier gibt Ihnen einen Überblick, wie **Outpost Firewall** individuell eingestellt werden kann.

Den Dialog zur individuellen Einstellung von **Outpost Firewall** sehen Sie, wenn Sie das Icon rechts unten im System-Tray mit der rechten Maustaste anklicken und im Kontext-Menü den Punkt „Optionen“ auswählen:



Es öffnet sich dann folgender Dialog:



Der erste Abschnitt des Dialog-Reiters „**Allgemein**“ betrifft das Format der **Log-Dateien**. Klicken Sie mit der linken Maustaste auf den Button „**Einstellungen**“, können Sie die maximale Größe der Log-Dateien festlegen und wie lange Sie die Einträge in den Log-Dateien speichern wollen. Neue Eintragungen überschreiben dann ältere Eintragungen. Diese Möglichkeit ist interessant für Computer mit begrenzten Speichermöglichkeiten.






Der Abschnitt „**Verschiedenes**“ ermöglicht Ihnen Einstellungen, ob **Outpost Firewall** automatisch beim Start des Systems geladen werden soll, ob die Benutzerschnittstelle im System-Tray minimiert werden soll, ob das Schließen der Benutzerschnittstelle das Programm im Systemtray minimieren oder das komplette Programm beenden soll und ob der Regel-Assistent auch ausgeführt werden soll, wenn die Benutzerschnittstelle nicht angezeigt wird.

Der Abschnitt „**Passwortschutz**“ definiert, ob die Benutzung der Benutzerschnittstelle mit einem Passwort gesichert werden soll. Benutzen mehrere Personen den Computer und sollen nicht alle Benutzer **Outpost Firewall** einstellen dürfen, macht die Vergabe eines Passwortes außerordentlichen Sinn.

6.3 Auswahl des Security-Levels

Eine der nützlichsten und wichtigsten Eigenschaften ist die Einstellung des Security-Levels. Die verschiedenen Security-Level legen fest, mit welcher grundlegenden Haltung **Outpost Firewall** auf Ereignisse reagieren soll:

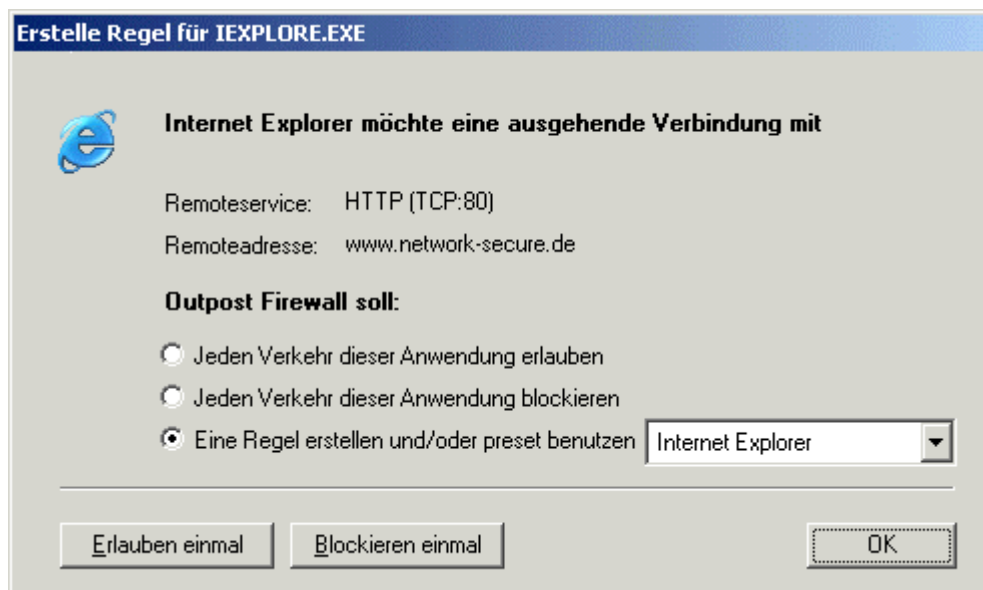
Die verschiedenen Security-Level in der Auflistung:

Icon	Mode	Beschreibung
	Alles blockieren	Alle Verbindungen sind geblockt.
	Blockiere alles außer	Verbindungen sind geblockt, die nicht explizit erlaubt wurden.
	Rules Assistent	Der Regel Assistent hilft bei der Regel-Erstellung und meldet sich immer dann, wenn eine unbekannte Verbindung bemerkt wird.
	Erlaube alles außer	Verbindungen sind erlaubt, die nicht explizit verboten wurden.
	Deaktiviert	Alle Verbindungen sind erlaubt.

Der hier eingestellte Security-Level wird als Icon im System-Tray fortlaufend angezeigt. So wissen Sie mit einem Blick, in welchem Security-Level **Outpost Firewall** aktuell betrieben wird.

Wenn **Outpost Firewall** gerade frisch installiert ist, steht der Security-Level auf „**Regel-Assistent**“, der Ihnen eine Entscheidungshilfe bei unbekanntem und noch nicht erfassten Verbindungen gibt.

Dieser Regel-Assistent erleichtert das Spezifizieren der anwendbaren Netzmerkmalen für jede Art von Anwendung. Der „**Regel-Assistent-Modus**“ erleichtert Ihr Netzleben ungemein, denn anstatt der zeitaufwendigen Erstellung von mitunter komplizierten manuellen Regeln schlägt Ihnen der Assistent eine Standard-Regel vor, die Sie nur akzeptieren müssen. Die Entwickler von **Outpost Firewall** haben in der Entwicklungszeitzeit eine große Anzahl von Standard-Anwendungen erfasst und optimale Regeln hierfür erstellt. So können Sie sich meistens auf die Vorschläge verlassen, es sei denn, Sie wissen was Sie tun und möchten eine individuelle Regel erstellen. So zeigt sich zum Beispiel beim ersten Aufruf des Internet Explorers folgender Vorschlag des Regel-Assistenten:



Die von den Entwicklungsingenieuren in die Datenbank aufgenommen Regeln für Anwendungen werden in drei Gruppen eingeteilt:

- Anwendungen, die grundsätzlich blockiert werden.
- Anwendungen, die eine eingeschränkte Erlaubnis erhalten.
- Vertrauenswürdige Anwendungen, die eine uneingeschränkte Erlaubnis erhalten.

Im oben gezeigten Beispiel wird gezeigt, wie der Regel-Assistent auf neue Verbindungsversuche reagiert. Erscheint ein solcher Dialog, haben Sie folgende Möglichkeiten:

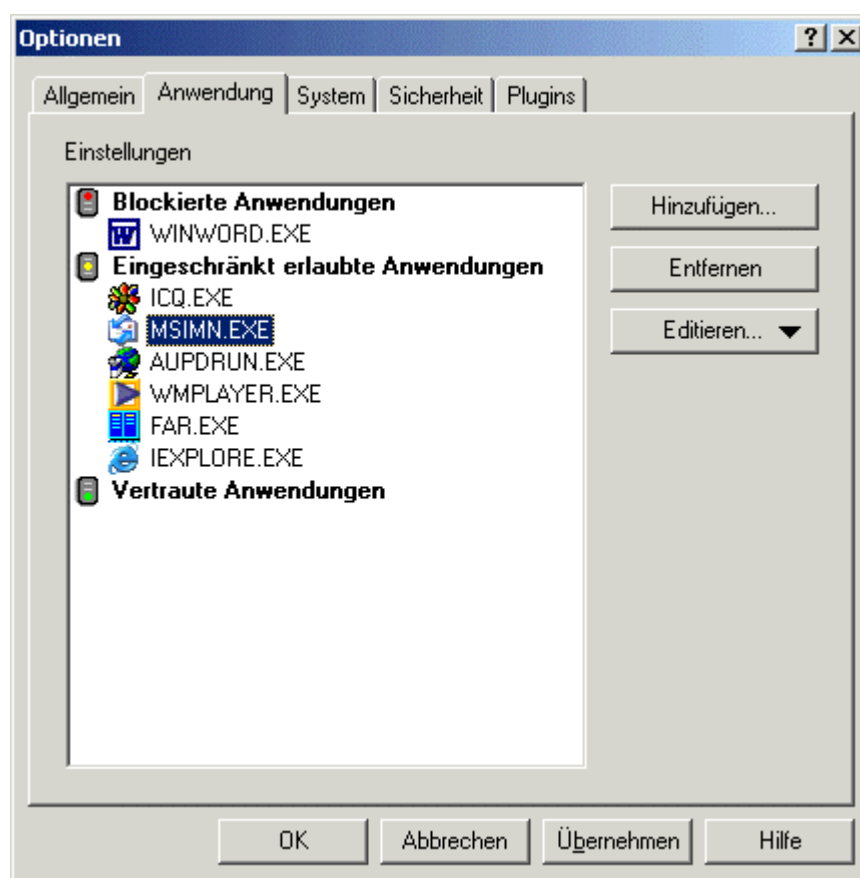
Auswahl	Zweck	Resultat
Jeden Verkehr dieser Anwendung erlauben	Für Anwendungen, die freien Zugriff erhalten sollen.	Mit dieser Einstellung geben Sie der Anwendung den Status der vertrauenswürdigen Anwendung. Die Anwendung darf dauerhaft und ohne Einschränkungen frei auf das Internet zugreifen.
Jeden Verkehr dieser Anwendung blockieren	Für Anwendungen, die keinen Netzzugriff erhalten sollen.	Mit dieser Einstellung blockieren Sie den gesamten Verkehr einer Anwendung dauerhaft.
Eine Regel erstellen und/oder preset benutzen	Für Anwendungen, die Netzzugriff über ein genau definiertes Protokoll, Port, etc. erhalten sollen.	Hier können Sie entweder eine Regel erstellen, bei der die Anwendung unter genau definierten Punkten die Erlaubnis zur Netzverbindung erhält (Lokaler Port, entfernte Adresse, entfernter Port usw.) oder sie können auf eine der vorgefertigten Regeln zugreifen, die von den Entwicklungsingenieuren bereits in der Datenbank erfasst und mit einer optimalen Regel versorgt wurden.
Einmal Zugriff erlauben.	Für Anwendungen, die Ihnen noch skeptisch vorkommen, trotzdem aber bei Netzzugriff kontrolliert werden sollen.	Diese Anwendung erhält nur einmalig die Freigabe für den Netzzugriff. Beim nächsten Zugriff erscheint wieder zuerst das Dialogfenster.
Zugriff einmal blockieren.	Für Anwendungen, die einmalig keinen Netzzugriff erhalten sollen.	Der Netzzugriff für diese Anwendung wird einmalig blockiert. Beim nächsten Zugriff erscheint wieder zuerst das Dialogfenster.

Outpost Firewall ermittelt sehr schnell die Anwendungen, die für die tägliche Arbeit im Internet benutzt werden. Auf die Weise kann der Security-Level ebenso schnell auf die Einstellung „**Blockiere alles außer...**“ gesetzt werden. So werden Sie weniger häufig vom Firewall gestört und können produktiv Ihrer Arbeit nachgehen.

6.4 Regel-Einstellung für Anwendungen

Eine der wichtigsten Einstellungen von **Outpost Firewall** ist die Regel-Einstellung für Anwendungen. Hier können Sie entscheiden, ob und wie Anwendungen Verbindungen zum Internet aufnehmen dürfen.

Den Dialog zur Einstellung rufen Sie auf, wenn Sie das Icon rechts unten im Systemtray mit der rechten Maustaste anklicken, die Optionen auswählen und „**Anwendungen**“. Es zeigt sich dann folgendes Bild:



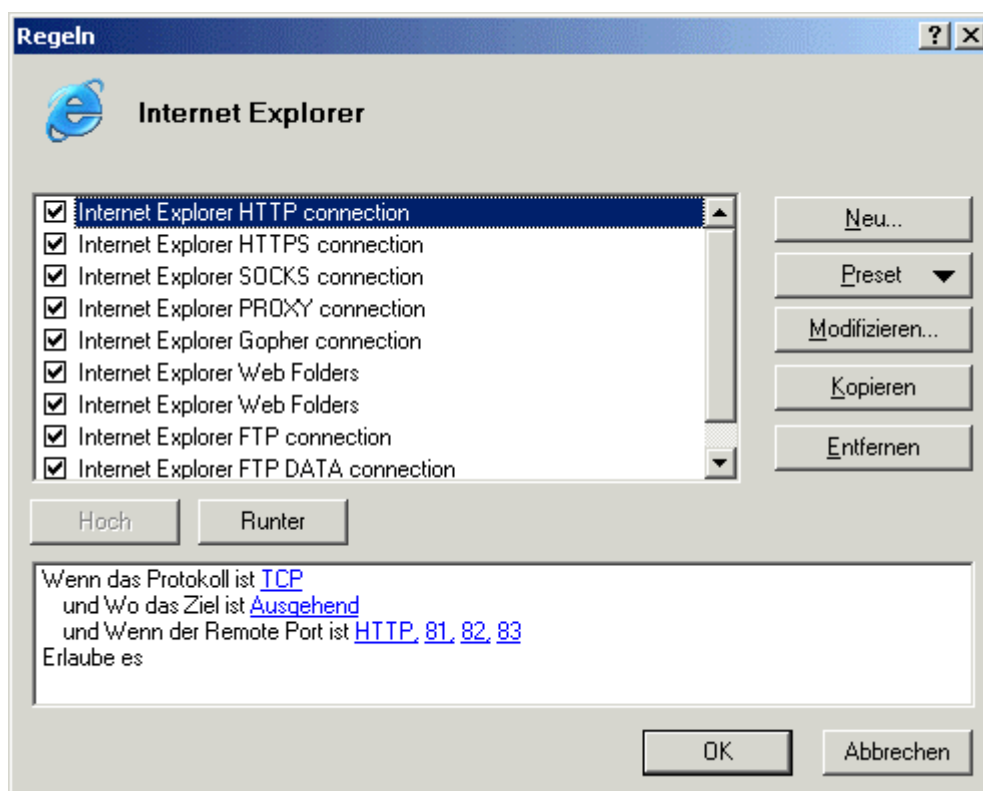
Der Dialog zeigt drei Bereiche, in die Anwendungen aufgenommen wurden oder aufgenommen werden können:

- **Blockierte Anwendungen:** Hier sind alle Anwendungen erfasst, die unter keinen Umständen Zugriff auf das Internet nehmen sollen oder dürfen. Das kann zum Beispiel der Windows-Editor sein oder der Windows-Taschenrechner.
- **Eingeschränkt erlaubte Anwendungen:** Hier sind alle Anwendungen erfasst, die nur unter genau definierten Punkten Verbindungen zum Netz aufnehmen dürfen. Die Einschränkungen können mit einer individuellen Regel erstellt werden oder mit vordefinierten Regeln aus der Datenbank.

- **Vertraute Anwendungen:** Hier sind und werden alle Anwendungen erfasst, die den Status „vertraute Anwendungen“ erhalten oder erhalten haben. Diese Anwendungen besitzen eine vollständige Freigabe für Verbindungen.

Sie können die aufgeführten Anwendungen durch einfaches „Ziehen“ (anklicken und bewegen bei gedrückter linker Maustaste) zwischen den einzelnen Bereichen bewegen, neue Anwendungen über einen Klick auf den Button „**Hinzufügen**“ einfügen, ebenso Anwendungen über einen Klick auf den Button „**Entfernen**“ aus der Liste entfernen oder nachträglich über einen Klick auf den Button „**Editieren**“ mit einer anderen vordefinierten Regel verändern oder eine individuelle Regel für diese Anwendung erstellen.

Wenn Sie also zum Beispiel eine Regel für den Internet-Explorer verändern möchten, klicken Sie auf den Button „**Editieren**“ und wählen dort aus „**Modifiziere Regel...**“. Es zeigt sich dann folgendes Bild:



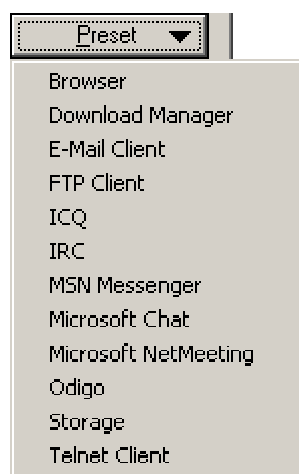
Mit diesem Dialog haben fortgeschrittene Benutzer die volle Kontrolle über die unterschiedlichen Protokolleinstellungen, indem Sie die Häkchen an den Vorgaben setzen oder entfernen und sowohl eingehende wie ausgehende Verbindungen, [Protokolle](#) und [Ports](#) gezielt einschränken und definieren.

Die einfachste Möglichkeit ist immer die Akzeptanz der vorgeschlagenen Regel. Diese Regel wurde von den Entwicklungsingenieuren erarbeitet und erfüllt mehr als nur gut ihren Zweck. Einzig fortgeschrittene Anwender können und sollen für spezielle Verbindungsfälle die Regel nach ihren eigenen Bedürfnissen verändern.

Werden in diesen Dialog-Feldern leere oder grau unterlegte Check-Boxen angezeigt so heißt das, hierfür stehen keine Einstellmöglichkeiten zur Verfügung.

Anmerkung: Es ist grundsätzlich möglich, einige unterschiedliche Regeln für die gleiche Anwendung zu erstellen. **Outpost Firewall** verwendet grundsätzlich die Regel der ersten Instanz zur Verbindungsaufnahme und ignoriert zunächst alle weiteren Instanzen. Erst wenn keine Verbindungsaufnahme erfolgt, werden die nachfolgenden Instanzen beachtet. Durch Schieben der einzelnen Instanzen dieser Regeln nach oben oder unten können Sie die Wertigkeit einer Instanz verändern. Merken Sie sich aber bitte, die oberste Instanz einer Regel wird als erste beachtet.

Wählen Sie zur Erstellung oder Veränderung einer Regel den Button „Preset“, erscheint folgender Dialog:



Die Liste der vordefinierten Anwendungen und erarbeiteten Regeln wird ständig erweitert und in jedem neuen Update von **Outpost Firewall** zur Verfügung gestellt.

7 PlugIns

7.1 Einführung

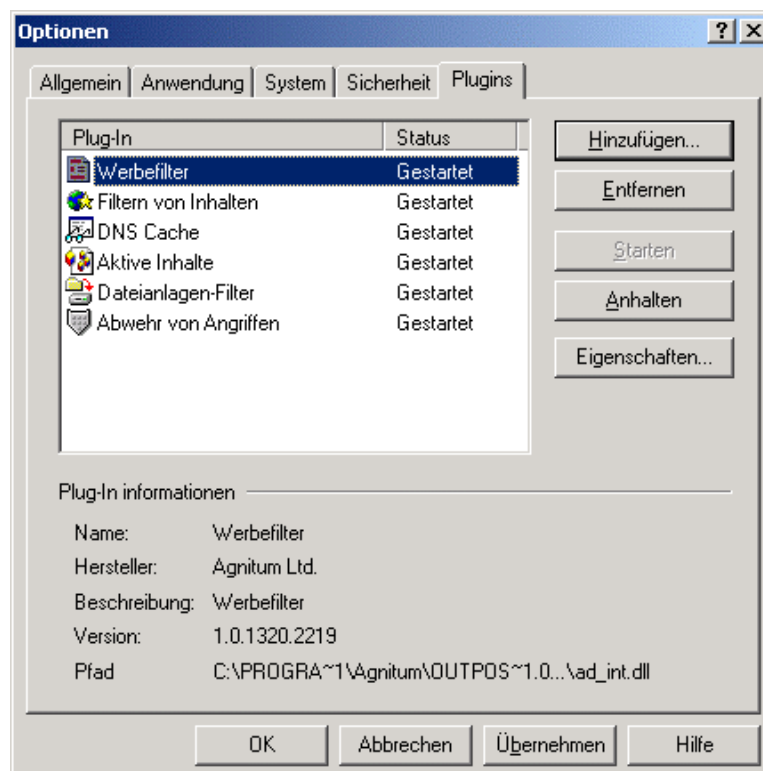
Eine der nützlichsten und wirkungsvollsten Designstrategien von **Outpost Firewall** ist der Einsatz von auswechselbaren PlugIns. Diese Module können durch Entwickler von anderen Firmen hergestellt und leicht hinzugefügt werden. Auf die Weise lässt sich **Outpost Firewall** auch an die außergewöhnlichsten Arbeitsumgebungen anpassen, um die Funktionalität von **Outpost Firewall** zu erhöhen.

Wenn Sie die Entwicklung der auswechselbaren PlugIns interessiert, besuchen Sie unser Forum unter <http://agnitum.com/products/outpost/developers.html>.

Dies ist das Forum für Entwickler, die hier über PlugIns diskutieren, Testversionen zur Verfügung stellen sowie Anleitungen und Erklärungen.

Bitte merken Sie sich, dass die auswechselbaren PlugIns völlig unabhängig voneinander und vom Programm **Outpost Firewall** sind. Sie stehen in keiner Verbindung zu den Sicherheitsrichtlinien, die bereits vordefiniert sind oder von Ihnen erstellt wurden.

Den Dialog zur Anzeige der PlugIns rufen Sie auf, indem Sie mit der rechten Maustaste auf das Icon im Systemtray klicken, im Kontext-Menü den Punkt „**Optionen**“ auswählen und dort den Reiter „**PlugIns**“. Es zeigt sich dann folgendes Bild:



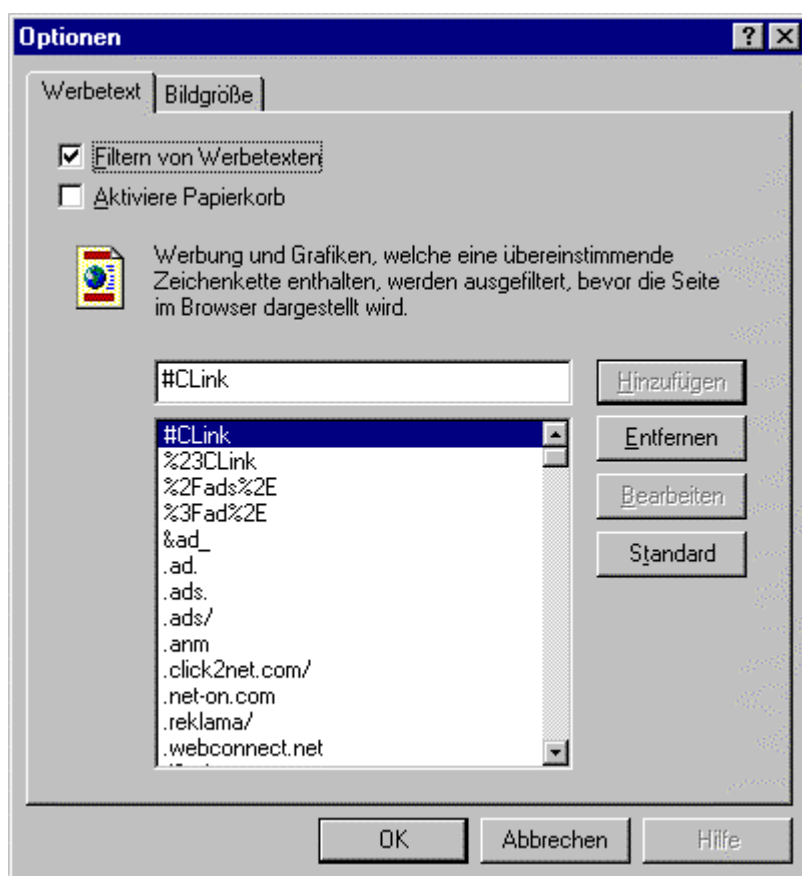
Die Button-Leiste am rechten Rand des Dialogs besitzt folgende Funktionen:

- **Hinzufügen...:** Über diesen Button können Sie neue PlugIns hinzufügen.
- **Entfernen:** Über diesen Button entfernen Sie ein markiertes PlugIn.
- **Starten:** Über diesen Button starten Sie ein beendetes PlugIn wieder neu.
- **Anhalten:** Über diesen Button halten Sie ein markiertes PlugIn an.
- **Eigenschaften...:** Über diesen Button verändern Sie die spezifischen Eigenschaften des markierten PlugIns. Entsprechend der Auswahl des PlugIns verändert sich der Inhalt der Eigenschaften. Die Eigenschaften können Sie übrigens nur für ein gestartetes PlugIn verändern.

7.2 Werbefilter

Mehr und mehr Webseiten sind mit [Werbe-Bannern](#) und anderen Werbeformen ausgestattet. Die Anzeige dieser Werbung kostet Bandbreite und verlangsamt die Aufrufe der gewünschten Webseite.

Sie können **Outpost Firewall** so einstellen, dass alle oder bestimmte Werbung nicht mehr angezeigt wird. Sie öffnen den Dialog zur Einstellung, indem Sie das PlugIn „**Werbefilter**“ markieren und den Button „**Eigenschaften**“ anklicken. Es öffnet sich dann folgender Dialog:



Outpost Firewall kann die Anzeige der Banner von bestimmten Inserenten blockieren. Dazu besitzt **Outpost Firewall** bereits eine große Datenbank mit Anbietern, die besonders aggressive Werbung benutzen. Sie sehen in der Liste einzelne Wörter. Jedes dieser Worte kommt in einer bestimmten [URL](#) vor und kann somit blockiert werden. Wird eine Webseite aufgerufen, die über eine URL mit einem dieser Schlüsselworte [Banner](#) abrufen, so wird der Banner blockiert und es wird statt dessen ein Vermerk angezeigt [**AD-IMG**].

Natürlich haben Sie hier auch die Möglichkeit, einzelne „Strings“ zu löschen, neue „Strings“ hinzuzufügen oder bestehende „Strings“ zu verändern.

Als weiteres Highlight besitzt der Dialog zur Einstellung von Werbung einen Papierkorb. Aktivieren Sie den Papierkorb, erscheint auf dem Desktop ein kleines Fenster mit einem Papierkorb, der immer sichtbar bleibt:



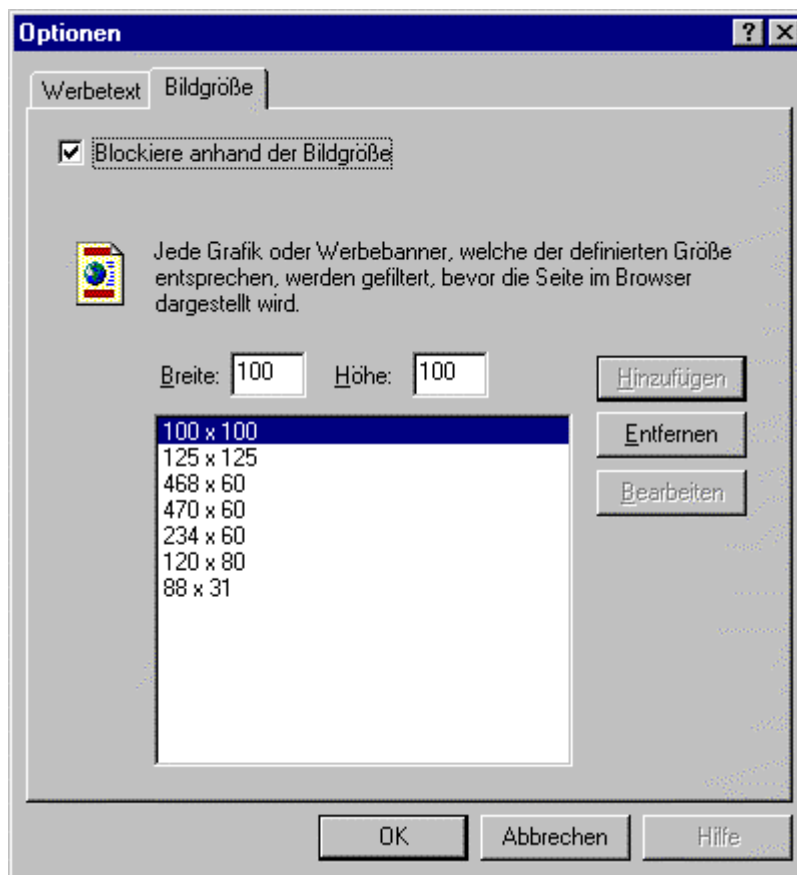
Mit Hilfe dieses kleinen Papierkorbs können Sie Werbung auf besuchten Webseiten durch einfaches „Ziehen“ (anklicken und bewegen des Objekts bei gedrückter linker Maustaste) den Banner in den Papierkorb befördern, er wird dann auf der Webseite nicht mehr angezeigt.

Ziehen Sie einen Banner auf den Papierkorb, öffnet sich folgender Dialog:



Sie können hier die gesamte URL in die Liste der nicht erwünschten Werbung aufnehmen oder auch nur einen Teil der URL.

Outpost Firewall ist auch in der Lage, Werbung anhand der Größe des Banners zu blockieren. Wechseln Sie dazu im Eigenschafts-Dialog von [HTML](#) auf Größe, dann zeigt sich folgender Dialog:



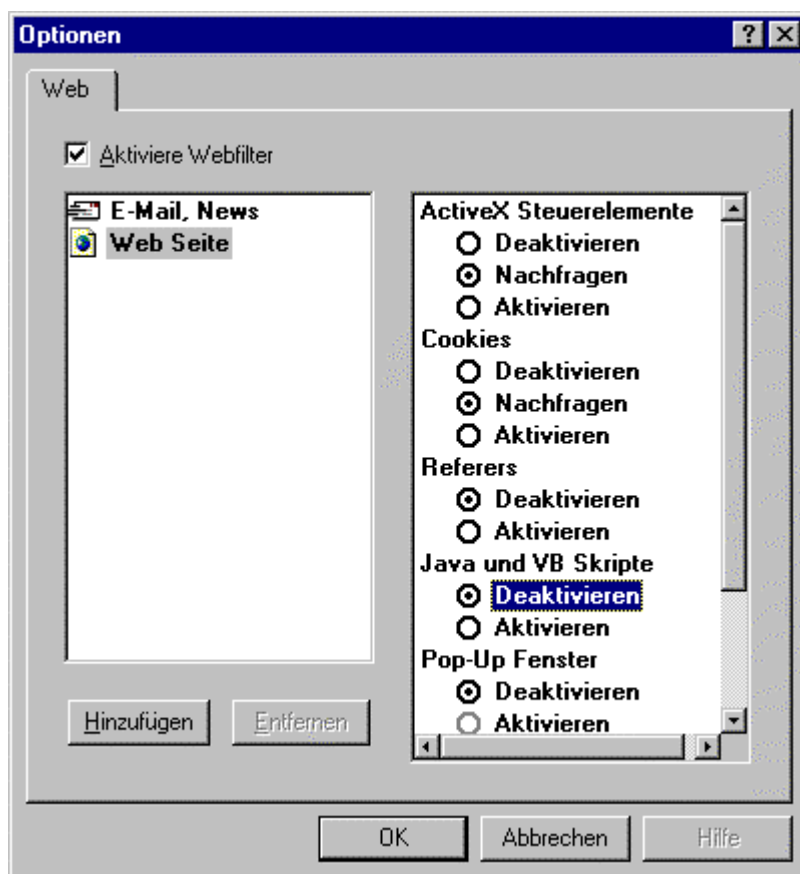
Hier können Sie verschiedene Banner-Formate eingeben, bestehende Formate verändern oder auch löschen. Ist diese Funktion aktiviert, werden Banner in der eingetragenen Größe nicht mehr angezeigt.

7.3 Blockieren von aktiven Elementen

Das PlugIn „Aktive Inhalte“ überwacht die folgenden Elemente:

- [ActiveX](#)
- [Java-Applets](#)
- Programme, die auf [Java-Script](#) oder [VB-Script](#) basieren
- [Cookies](#)
- PopUp Fenster
- [Referrers](#)

Rufen Sie die Eigenschaften dieses PlugIns auf, sehen Sie folgenden Dialog:

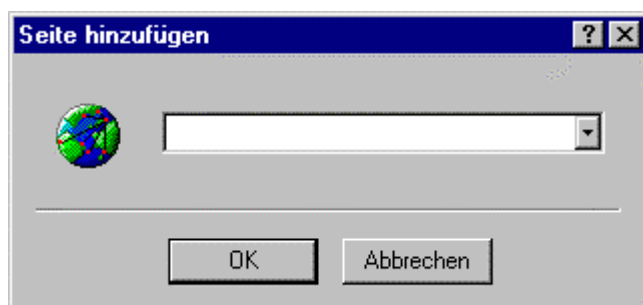


Sie können hier für **Webseiten** und **eMail/News** individuelle Einstellungen zum Verhalten von **Outpost Firewall** vornehmen. So haben Sie die Möglichkeit, grundsätzlich folgende Funktionen zu wählen, wenn **Outpost Firewall** auf das entsprechende Element trifft:

- **Deaktivieren:** Das Element wird blockiert, nicht angezeigt oder ausgeführt.

- **Aktivieren:** Das Element wird angezeigt oder ausgeführt.
- **Nachfragen:** Trifft **Outpost Firewall** auf das entsprechende Element, erscheint eine Abfrage, in der Sie individuell entscheiden können, ob das Element blockiert oder freigegeben wird.

Im Bereich Webseiten haben Sie zusätzlich die Möglichkeit, einzelne Webseiten individuell einzustellen. Wählen Sie diese Möglichkeit, erscheint ein Dialog mit einem Textfeld zur Eingabe der Adresse:



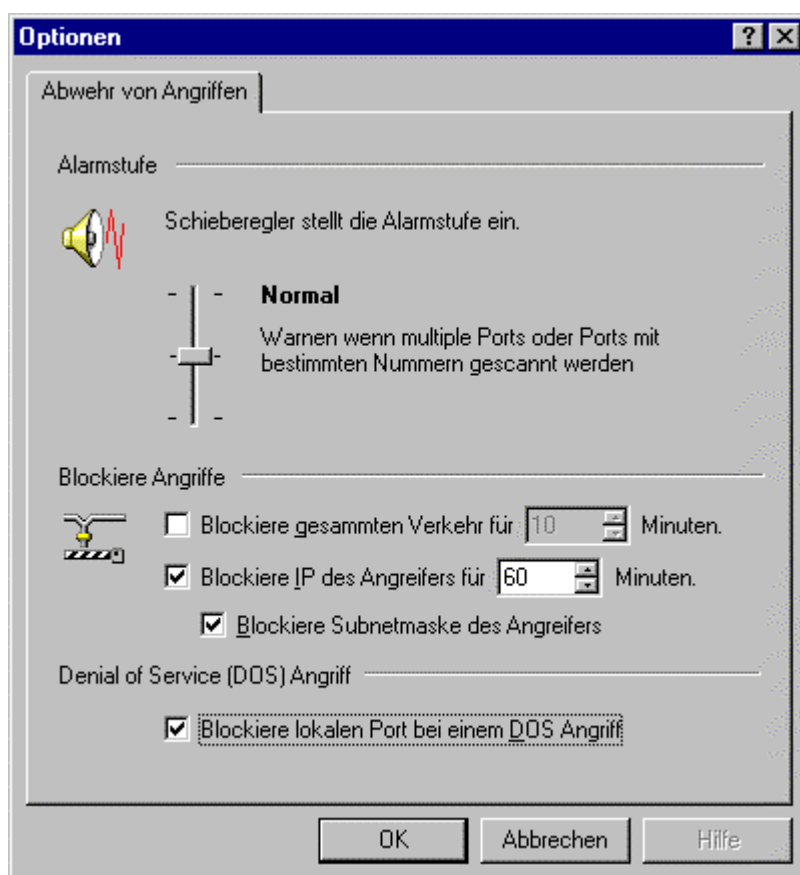
Bedenken Sie aber bitte, dass einige Webseiten die Freigabe aller Elemente benötigen, um korrekt angezeigt zu werden. Im anderen Fall können einzelne aber eventuell wichtige Elemente wie zum Beispiel die Suchfunktion auf einer Webseite funktionsuntüchtig werden.

7.4 Abwehr von Angriffen

Dieses PlugIn informiert Sie über einen möglichen Angriff auf Ihrem Computer vom Internet aus oder von einem Computer im internen Netzwerk.

Sie können über die Eigenschaften dieses PlugIns sehr fein einstellen, wie Outpost mit eventuellen Angriffen dieser Form umgehen soll. So können Sie zum Beispiel eine Wartezeit einstellen, in der die angreifende Stelle nicht auf Ihren Computer zugreifen darf.

Rufen Sie die Eigenschaften dieses PlugIns auf, zeigt sich folgender Dialog:



Im Abschnitt „**Alarmstufe**“ können Sie den Schieberegler auf ein höheres oder niedrigeres Niveau der Sicherheit einstellen. Die Abstufung zeigt sich wie folgt:

- **Maximal:** Es erfolgt eine Meldung und die Aktivierung der Einstellungen bereits, wenn ein einzelner [Port](#) gescannt wird.
- **Normal:** Es erfolgt eine Meldung und die Aktivierung der Einstellungen, wenn mehrere Ports oder Ports einer bestimmten Nummer gescannt werden.
- **Minimal:** Es erfolgt eine Meldung und die Aktivierung der Einstellungen, wenn ein Angriff identifiziert wurde.

Im unteren Teil des Dialogs können Sie die Einstellungen vornehmen, in welcher Art **Outpost Firewall** auf eventuelle Angriffe reagieren soll. Hier stehen mehrere Optionen zur Auswahl:

- Blockiere gesamten Verkehr für x Minuten. Die Blockadezeit kann hier frei eingestellt werden.
- Blockiere die [IP](#)-Nummer des Angreifers für x Minuten. Die Blockadezeit kann frei eingestellt werden.
- Blockiere Subnetmaske des Angreifers.
- Blockiere lokalen Port bei einem [Denial of Service](#) Angriff.

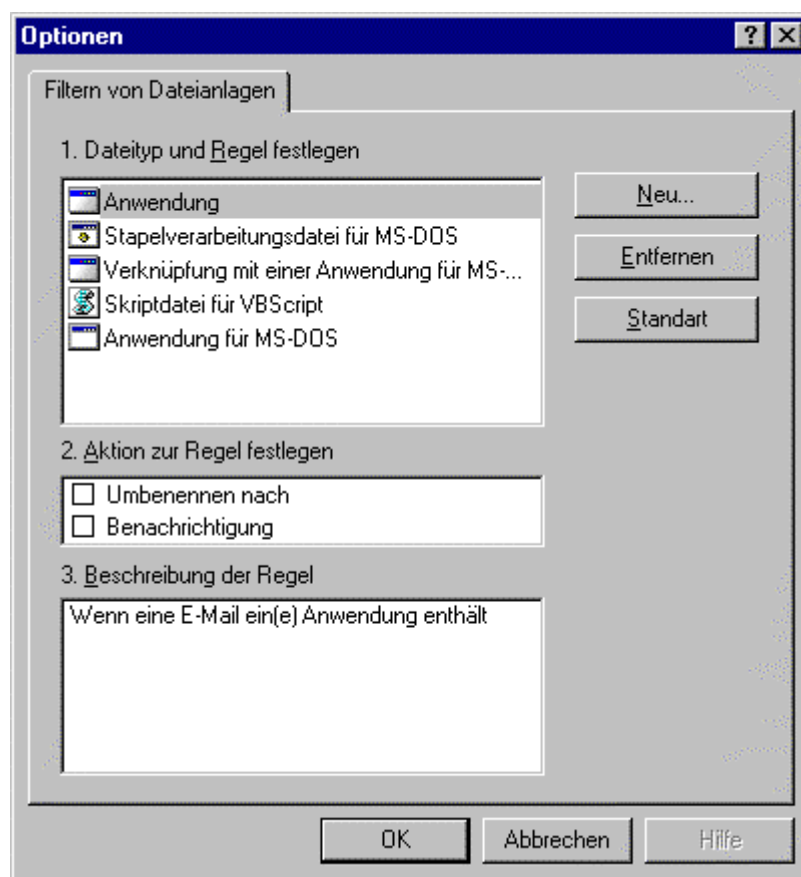
Es ist allerdings dringend zu empfehlen, nicht sämtlichen Verkehr nach einem harmlosen einzelnen Portscan zu blocken. Anderenfalls ist die Gefahr zu groß, überhaupt nicht mehr mit dem Internet arbeiten zu können. Mehr Informationen über das „Feintuning“ dieses PlugIns finden Sie in der Datei „**protect.lst**“ im Outpost-Verzeichnis.

7.5 Dateianlagen Filter

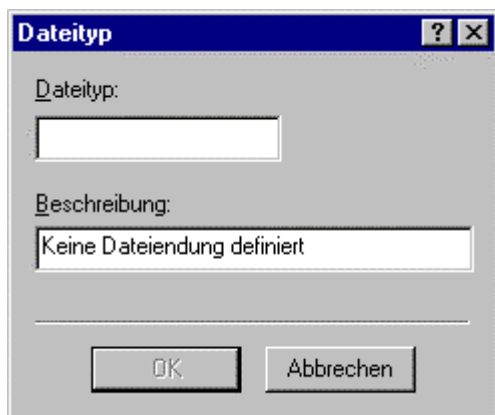
Dieses PlugIn überprüft die Dateianhänge Ihrer eingehenden elektronischen Post. Mit diesem PlugIn können Sie einstellen, welche Dateianhänge umbenannt werden sollen, damit Sie keine zerstörerischen Funktionen in Ihrem Computer ausführen können.

Der Dateianlagen Filter ist vielseitig einsetzbar und konfigurierbar. So können Sie frei entscheiden, welche Dateianhänge grundsätzlich überwacht werden sollen und in welcher Weise **Outpost Firewall** damit umgehen soll, wenn Ihnen eine der überwachten Anhänge zugeschickt wird. Sie können die Datei dann automatisch mit einer anderen harmlosen Dateieindung umbenennen und/oder sich eine Meldung anzeigen lassen.

Wenn Sie die Einstellungen dieses PlugIns aufrufen, zeigt sich folgendes Bild:



Der Dialog ist bereits mit den populärsten Dateiartern ausgestattet, die von den Entwicklungsingenieuren erarbeitet wurden. Wenn Sie eine andere Dateiart überwachen lassen möchten, können Sie nach einem Klick auf den Button „Neu“ eine neue Dateiart eingeben. Nach Aufruf der Funktion zeigt sich folgendes Bild:



Geben Sie im oberen Textfeld die Dateiendung der neuen Datei ohne Zusatz ein (z.B. shs) und im unteren Textfeld eine Beschreibung (z.B. Scrap Objekt) ein und bestätigen den neuen Dateityp mit einem Klick auf den Button „**OK**“.

7.6 Domain Name Cache

Das Internet arbeitet, indem es eine Reihe von Zahlen jedem Computer zuweist, der am Internet angeschlossen wird. Diese so genannte [IP-Adresse](#) besteht aus einer 32bittigen Zahl, die der leichten Lesbarkeit wegen mit einzelnen Punkten unterbrochen wird (z.B. die lokale IP: 192.168.0.1).

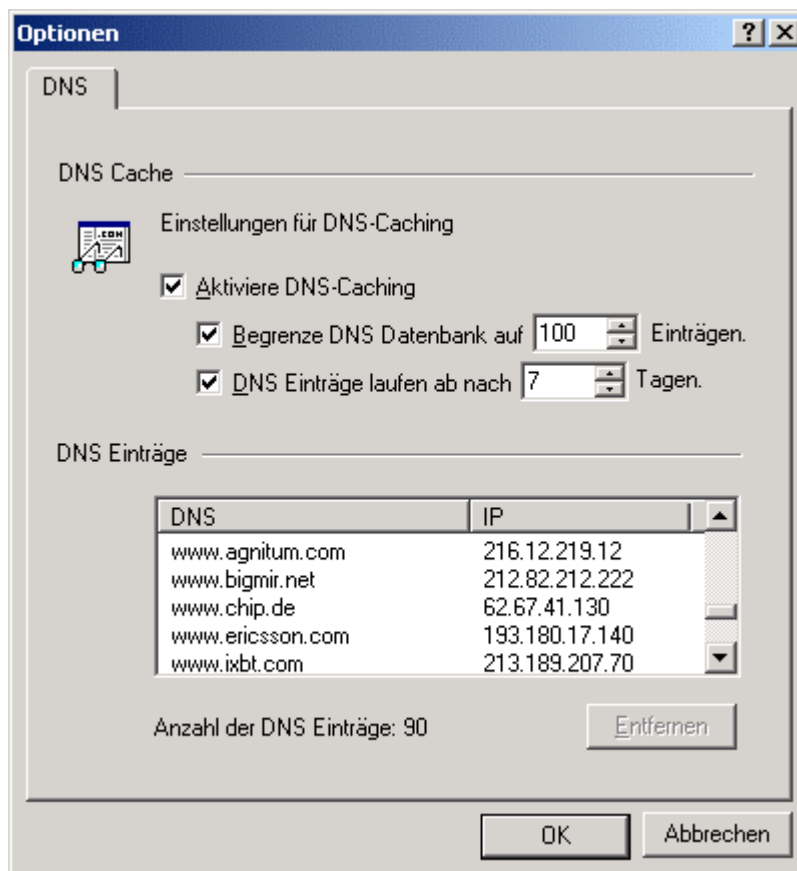
Geben Sie diese Zahl in die Adressleiste Ihres Browsers ein, würde Ihnen zur Zeit die Webseite unserer Domain <http://www.network-secure.de/> angezeigt.

Obwohl diese numerischen IP-Adressen einfach für einen Computer zu verwenden sind, sind sie für Menschen schwierig zu merken. So wurde ein Adressensystem erfunden, das Wörter oder Buchstaben benutzt und was als Domain-Name-System bezeichnet wird. Diese [DNS-Namen](#) sind leichter zu merken. Aus diesem Grund gibt es im Internet Systeme bzw. [Server](#), die Angaben über die IP-Adresse gespeichert haben, während andere Systeme bzw. Server den DNS-Namen gespeichert haben. Um eine Adresse aufzurufen, werden die IP-Adresse und der DNS-Name miteinander verglichen. Hierzu werden riesige Tabellen eingelesen, bis die Daten übereinstimmen.

Um den Vergleich zu beschleunigen, besitzt **Outpost Firewall** eine personalisierte DNS-Tabelle, die auf Ihrem Computer gespeichert ist und dynamisch aktualisiert wird. Dieser Mechanismus wird DNS Pufferspeicher genannt. Auf die Weise lassen sich kürzlich besuchte Webseiten schneller wieder aufrufen.

Der Domain-Name-Cache von **Outpost Firewall** ist individuell einstellbar, was heißt, Sie können selbst entscheiden und einstellen, ob, wie viele und wie lange DNS-Namen gespeichert werden.

Rufen Sie die Einstellungen dieses PlugIns auf, zeigt sich folgendes Bild:



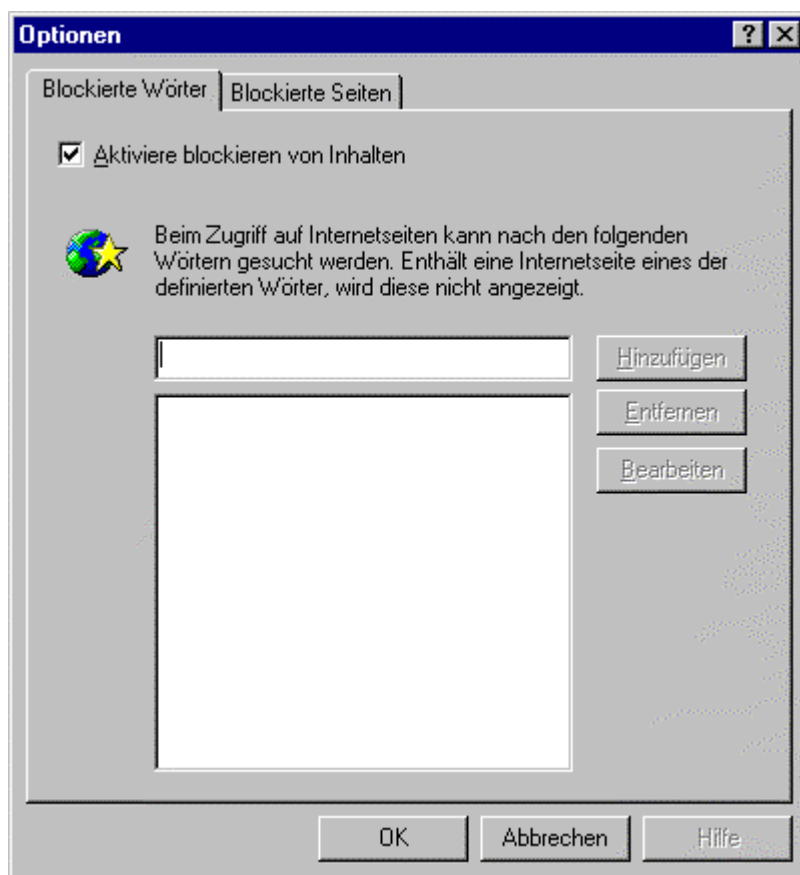
Hier können Sie einstellen:

- DNS-Caching aktivieren
- Die Anzahl der Einträge in die DNS-Datenbank
- Wann die Einträge abgelaufen sind und überschrieben werden können

7.7 Filtern von Inhalten

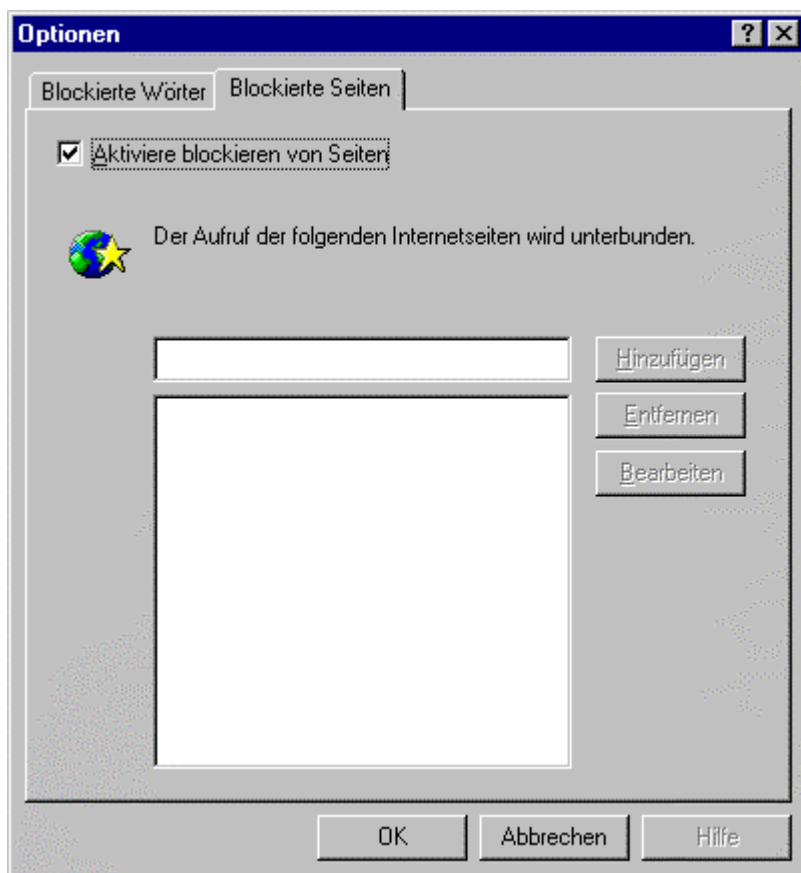
Outpost Firewall stellt Ihnen mit diesem PlugIn eine Möglichkeit zur Verfügung, mit der Sie ausgewählte Webseiten filtern können, sie werden dann nicht angezeigt. Zudem können Sie aufgerufene Webseiten nach bestimmten Wörtern durchsuchen lassen. Stimmt eines der Worte auf der besuchten Webseite mit einem zuvor eingegebenen Wort überein, wird die Webseite ebenfalls nicht angezeigt.

Rufen Sie die Einstellungen dieses PlugIns auf, zeigt sich folgendes Bild:



Geben Sie hierzu die gewünschten Worte der Webseite ein und bestätigen Ihre Eingabe mit einem Klick auf den Button „**Hinzufügen**“. Wird zukünftig eine Webseite aufgerufen, die eines der eingegebenen Worte enthält, wird sie nicht mehr angezeigt.

Alternativ können Sie auch ganze Webseiten eingeben, die nicht mehr angezeigt werden sollen. Wechseln Sie hierzu den Reiter nach „**Blockierte Seiten**“:



Part 2: für erfahrene Anwender

8 Erweiterte Einstellungen

8.1 Einführung

Die Entwicklungsingenieure bauten Standardannahmen für **Outpost Firewall** zusammen, um Computersystemen und Netzen optimalen Schutz zu geben. **Outpost Firewall** wurde von Anfang an so entworfen, um auch Computeranfängern einen effektiven Schutz zur Verfügung zu stellen. Sie brauchen sich nicht mit Vermittlungsprotokollen auszukennen und sind doch wirksam gegen Angriffe geschützt.

Fortgeschrittene Anwender mit Kenntnissen über Netztechnik sollen jedoch **Outpost Firewall** völlig allein konfigurieren dürfen. Dieses Kapitel wird entsprechend denjenigen Benutzern zur Verfügung gestellt, die **Outpost Firewall** als effektives und leistungsfähigstes System kennen lernen möchten.

Anmerkung: Outpost Firewall wird Ihnen stets gut durchdachte Standardvorschläge machen, wenn Sie nicht das nötige Wissen haben, um Einstellungen manuell einzurichten.

8.2 Speichern und Laden von Konfigurationen

Outpost Firewall besitzt sehr viele Einstellungen. Sie sind grundsätzlich in der Lage, mehrere verschiedene Konfigurationen zu speichern und wieder zu laden, um Outpost Firewall an wechselnde Arbeitsbedingungen optimal anzupassen.

So haben Sie die Möglichkeit:

- Konfigurationen für Ihre Familie oder Kollegen zu erstellen
- Konfigurationen für Ihre Kinder, um sie vor unerwünschten Aktivitäten fernzuhalten
- Um mit einem Mausklick zwischen „Arbeit“, „Rest“, „ich bin unterwegs“ und „Kinder“ umzuschalten
- Spezielle Konfigurationen zu sichern

Die Default-Konfigurationsdatei nennt sich `configuration.cfg`, die sich im Installationsverzeichnis von **Outpost Firewall** befindet. Hier können Sie mehrere Konfigurationsdateien abspeichern, indem Sie der Datei einen anderen Namen geben.

Eine Konfigurationsdatei kann mit einem Passwort gesichert werden, damit auch wirklich nur autorisierte Personen Änderungen an den Einstellungen vornehmen können.

Sie können Konfigurationsdateien ändern, laden, speichern oder neu erstellen, wenn Sie den Menüpunkt „**Datei**“ aufrufen. Hier können Sie auf einfache Weise neue Konfigurationen anlegen, bereits gespeicherte Konfigurationen laden oder die aktuelle Konfiguration unter einem aussagefähigen Namen speichern.

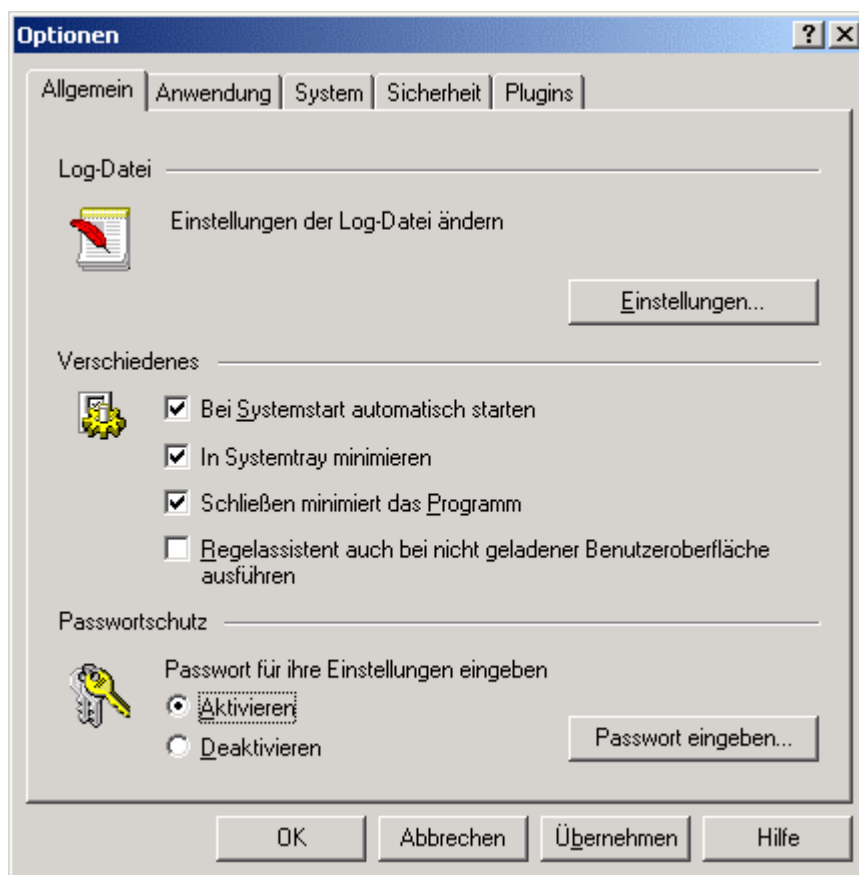
Anmerkung: Speichern Sie Ihre aktuelle Konfiguration immer erst ab, wenn Sie eine neue Konfigurationsdatei anlegen. Es werden bei der Neuanlage oder beim Laden einer bereits gespeicherten Konfiguration alle Einstellungen der aktuellen Konfiguration überschrieben.

Outpost Firewall benutzt automatisch die zuletzt gespeicherte Konfiguration, wenn Outpost wieder neu gestartet wird.

8.3 Passwort setzen

Sie können die Einstellungen von **Outpost Firewall** schützen, indem Sie ein Passwort vergeben. Die Vergabe eines Passwortes verhindert eine Veränderung der Einstellungen von nicht autorisierten Personen wie zum Beispiel Ihren Kindern.

Sie öffnen den Dialog zur Eingabe eines Passwortes, wenn Sie mit der rechten Maustaste auf das Icon im Systemtray der Startleiste klicken und dort die **Optionen** auswählen. Es zeigt sich dann folgender Dialog:



Wenn Sie im unteren Bereich des Dialoges Passwortschutz aktivieren, wird auch der Button zur Eingabe eines Passwortes aktiv. Klicken Sie den Button „**Passwort eingeben...**“ mit der linken Maustaste an, zeigt sich der Dialog zur Eingabe des Passwortes.

8.4 Filter erstellen für Anwendungen

Dieser Abschnitt ist eine Erweiterung der Erklärungen zur Erstellung von Regeln für Anwendungen. Der Gebrauch des Dialogs zur individuellen Erstellung von Regeln wird nur erfahrenen Anwendern empfohlen, die sich mit [Netzprotokollen](#) auskennen und genau wissen, was sie tun.

Gehören Sie zu den erfahrenen Anwendern, können Sie zum Beispiel die Standard-Regeln bereits erfasster Anwendungen individuell verändern oder eigene individuelle Regeln für neu erfasste Verbindungen erstellen.

Sie rufen den Dialog zur Erstellung von erweiterten Regeln auf, wenn Sie mit der linken das Icon rechts unten im Systemtray neben der Uhr anklicken, dort **Optionen** auswählen und im Dialog den Reiter „**Anwendungen**“. Markieren Sie dort eine Anwendung oder fügen Sie eine neue Anwendung ein. Klicken Sie dann auf den Button „**Editieren**“ und im folgenden Dialog auf den Button „**Neu**“.

Es öffnet sich dann folgender Dialog:

Regeln [?] [X]

Wählen Sie erst in (1) aus in welchem Fall die Regel aufgerufen wird. Danach spezifizieren Sie in (2) die Antwort und in (3) die Regel selbst.

1. Wählen Sie den Fall aus, wann die Regel ausgeführt werden soll

- Wo das gewählte Protokoll ist
- Wo das gewählte Ziel ist
- Wo der gewählte Remotehost ist**
- Wo der gewählte Remoteport ist

2. Antwort wenn die Regel ausgeführt wird

- Erlaube es
- Verbiete es
- Lehne es ab
- Berichte es

3. Regelbeschreibung (klicken Sie auf die unterstrichenen Werte um diese zu ändern)

Wo das Protokoll ist TCP
und Wo das Ziel ist Innerhalb
und Wo der host ist 192.168.0.0 - 192.168.0.3 [192.168.0.0 - 255.255.255.252]
Erlaube es

4. Regelname

SVCHOST Rule #1

OK Abbrechen

Grundsätzlich gilt, ein wenig Experimentieren mit den Einstellmöglichkeiten dieses Dialogs zeigt dem erfahrenen Anwender weit mehr als die wenigen Punkte, die hier beschrieben werden können.

Sie können nun eine individuelle Regel erstellen, für die Sie folgende Einstellungen vornehmen können:

- Das entsprechende [Netzprotokoll](#) ([TCP](#), [UDP](#), [ICMP](#) oder unbekanntes Protokoll)
- Das Ziel der Verbindung (eingehende Verbindungen oder abgehende Verbindungen)
- Ziel-Adresse (Domäne, [IP-Adresse](#) (auch Wildcards möglich) oder IP-Adress-Bereich)
- Der Ziel-[Port](#)
- Der lokale Host (wie auch der Remote-Host der Gegenstelle)
- Der lokale Port
- Innerhalb eines bestimmten Zeitintervalls (Immer, stündlich, täglich usw.)

Grau unterlegte Optionen stehen nicht zur Verfügung.

Haben Sie hier alle Einstellungen getroffen, geben Sie an, was **Outpost Firewall** auführen soll, wenn die oben genannten Einstellungen zutreffen. Hier haben Sie wieder mehrere Möglichkeiten:

- Erlaube es
- Verbiete es
- Lehne es ab (es wird eine ablehnende Antwort gegeben)
- Berichte es
- Starte Applikation

Haben Sie auch hier alle Einstellungen für diese Regel getroffen, können Sie der Regel im Textfeld unterhalb der Eingabe-Optionen einen treffenden Namen geben (zum Beispiel eMail-Client senden). Ein Klick auf den Button „**OK**“ übernimmt diese Regel, die fortan Anwendung findet.

8.5 System-Level Filter

Mit dem System-Level Filter können erfahrene Anwender die Systemaktivitäten wie zum Beispiel die Nutzung von [NetBIOS-Kommunikation](#) einstellen, den Umgang mit [ICMP](#)-Nachrichten, das Antwortverhalten von **Outpost Firewall** sowie grundlegende Anwendungs- und System-Regeln.

Sie rufen den Dialog auf, indem Sie mit der rechten Maustaste auf das Icon rechts unten im Systemtray neben der Uhr klicken, im Kontextmenü den Punkt „**Optionen**“ und dort den Reiter „**System**“ auswählen. Es öffnet sich dann folgender Dialog:



NetBIOS ist ein spezielles Protokoll, über das die Benutzung von freigegebenen und gemeinsam genutzten Ordnern oder anderen Ressourcen gesteuert wird.

Sie können hier verschiedene Einstellungen vornehmen, die die Nutzung der [NetBIOS](#)-Funktionen auf einen begrenzten Bereich einschränkt:

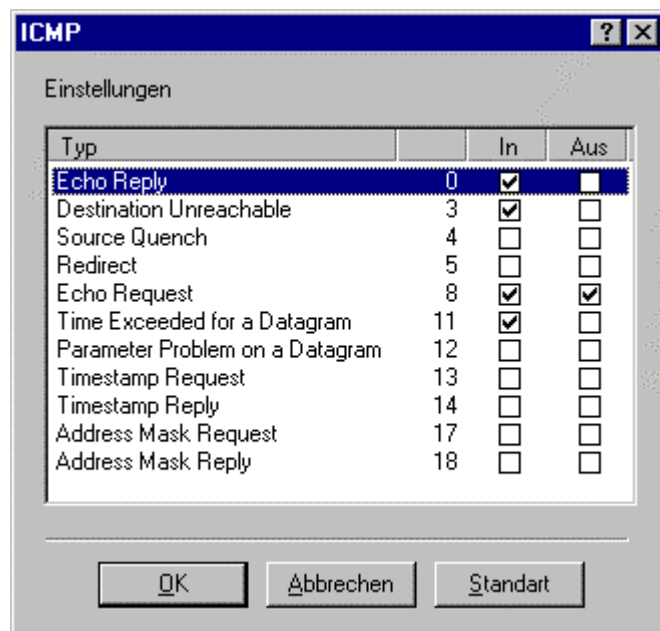
- Domänenname (Internetverbindung notwendig)
- [IP-Adresse](#) (Wildcards möglich)
- IP-Adressbereich

Geben Sie hier die gewünschten Angaben ein und bestätigen die Eingaben mit einem Klick auf den Button „**Hinzufügen**“. Auf die gleiche Weise können Sie bereits bestehende Eingaben modifizieren oder auch wieder entfernen, indem Sie den entsprechenden Button im Dialog auswählen.

Anmerkung: Während die Freigabe für gemeinsam genutzte Ressourcen im internen Netzwerk (LAN) durchaus sinnvoll sein kann, wird die Freigabe im Internet aber gefährlich, weil jeder Internet-Nutzer auf die Weise unbemerkt auf Ihre freigegebenen Ressourcen zugreifen kann.

ICMP, das Internet-Control-Message-Potokoll, mit dem im einfachsten Fall ein PING ausgelöst wird, kann in beiden Richtungen, also ankommend wie abgehend eingestellt, aktiviert oder deaktiviert werden. **Outpost Firewall** bringt bereits eine sinnvolle Einstellung des ICMP mit. Änderungen sollten also nur in Ausnahmefällen sinnvoll und berechtigt sein, weil falsche Einstellungen wie die Deaktivierung zu Störungen der Kommunikation im Internet auslösen können.

Sie rufen den Dialog auf, wenn Sie im Options-Dialog-System den Button „**Einstellungen**“ von **ICMP** anklicken. Es zeigt sich dann folgender Dialog:



Das Antwortverhalten von Outpost Firewall

Über die Option „**Typ der Antwort**“ können Sie einstellen, wie Outpost auf Verbindungsanfragen reagieren soll. Hier stehen zwei Auswahlmöglichkeiten zur Verfügung:

- **Stealth:** Die Quelle der Anfrage wird nicht mittels einer [ICMP](#) Mitteilung benachrichtigt. Normalerweise erfolgt zum Beispiel auf einen PING (Erreichbarkeitsprüfung eines Rechners im Netz) eine entsprechende Antwort. Wird das Antwortverhalten auf „Stealth“ gesetzt, erhält die anfragende Stelle keine Antwort darüber, ob der „angepingte“ Rechner überhaupt existiert. Ebenso erfolgt keine Antwort, ob ein geprüfter [Port](#) offen oder geschlossen ist.
- **Normal:** Die Quelle der Anfrage erhält eine normale ICMP Mitteilung.

Es wird empfohlen, **Outpost Firewall** im „Stealth-Modus“ zu betreiben, es sei denn, besondere Gründe sprechen für ein normales Antwortverhalten.

Über die **globalen Anwendungs- und System-Regeln** spezifizieren Sie globale Richtlinien für folgende Ereignisse:

- Abgehende [DNS](#) (Domain-Name-Server)
- [DHCP](#) (Dynamic Host Control Protokoll – z.B. zur automatischen Vergabe von IPs im LAN)
- Unbekannte Protokolle verweigern
- Inbound-Identifikation
- [Broadcast/Multicast](#) (unspezifische Pakets, die keinem bestimmten Zielhost zugeordnet sind)
- Inbound/Outbound [Loopback](#)

Der erfahrene Anwender kann hier die vorgefertigten Filter-Sets aktivieren und nutzen, einzelne Filter löschen oder neue hinzufügen und als Feintuning auch spezielle Angaben über die Art und Weise der Benutzung eines Filter-Sets einstellen. Hierzu wird der Button „**Editieren**“ angeklickt und es öffnet sich der bereits bekannte Dialog zur Erstellung von individuellen Regeln.

8.6 Einstellungen für ein Home- oder Office-Netzwerk

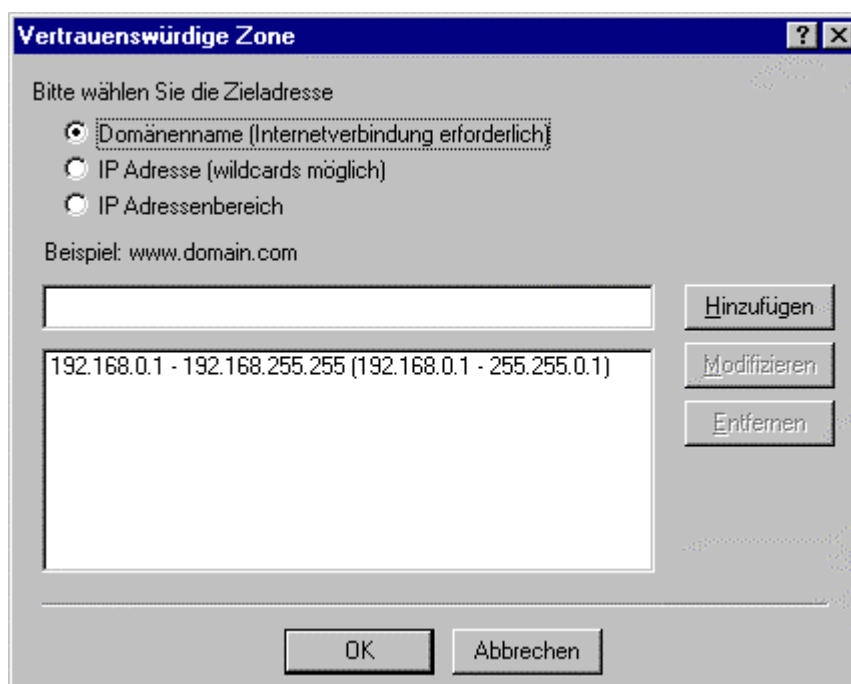
Ein grundlegender Unterschied zwischen einem lokalen Netzwerk (LAN) und dem Internet ist das Niveau des Vertrauens, das grundsätzlich erteilt wird. Ein LAN im Haus oder im Büro wird in der Regel aus freundlich gestimmten Computer-Benutzern bestehen. Entsprechend gehören die Rechner der Familie oder der Kollegen in die vertrauenswürdige Zone.

Anmerkung des Übersetzers: Grundsätzlich mag das stimmen. Im Einzelfall würde ich aber eher gezielt einzelne Computer im LAN die absolute Vertrauenswürdigkeit erteilen. Die Wichtigkeit dieser Entscheidung liegt hier in der Brisanz der Daten begründet. Werden streng vertrauliche Informationen oder Geschäftsunterlagen auf einem bestimmten Rechner im LAN bearbeitet und gespeichert, reicht eine globale Vertrauenswürdigkeit für alle im LAN angeschlossenen Computer nicht aus.

Den Dialog zur Einstellung der vertrauenswürdigen Zone rufen Sie auf, indem Sie mit der rechten Maustaste auf das Icon im Systemtray rechts unten neben der Uhr klicken und im Kontextmenü „**Optionen**“ auswählen und im folgenden Dialog den Reiter „**Sicherheit**“. Es öffnet sich dann folgender Dialog:



Klicken Sie im Bereich „**Vertrauenswürdige Zone**“ auf den Button „**Ändern**“, dann öffnet sich folgender Dialog:



In der Liste der vertrauenswürdigen Zone können Sie folgende Einstellungen vornehmen:

- Domänenname (z.B. www.domänenname.com - Internetverbindung notwendig)
- [IP-Adresse](#) (Wildcards sind möglich)
- IP-Adressenbereich

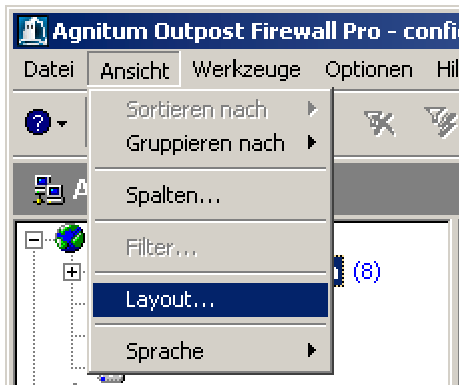
Sie können hier neue Adressen eingeben, bereits vorhandene Adressen modifizieren oder auch löschen. Vergessen Sie dabei aber bitte nicht, dass die Einstellungen der PlugIns unabhängig von der vertrauenswürdigen Zone sind.

Wir raten Ihnen grundsätzlich, nur wirklich vertrauenswürdige Computer in diesen Bereich aufzunehmen und nie zu vergessen, welche Computer vertrauenswürdige eingestuft wurden.

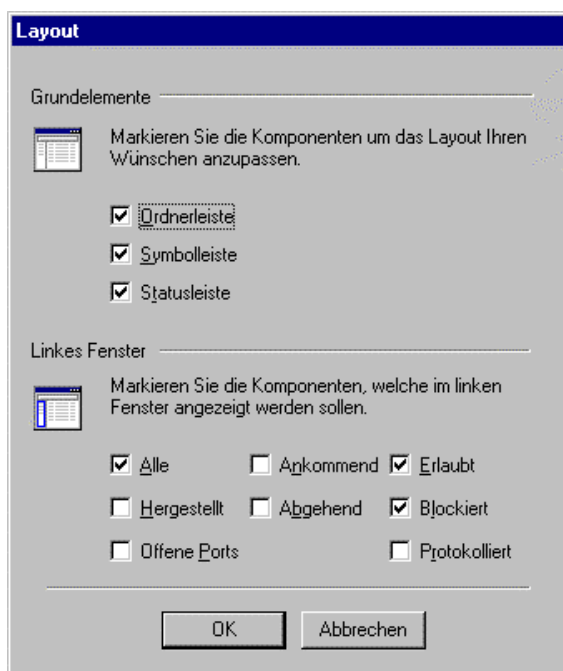
9 Das Anzeige-Menü

9.1 Layout

Sie können die im **Outpost Firewall** Hauptfenster angezeigten Informationen und Meldungen ganz nach Ihren Wünschen sortieren und gruppieren. Zudem lassen sich die unterschiedlichen angezeigten Informationen erweitern oder einschränken, indem Sie Spalten hinzufügen oder entfernen. Hierzu stellt **Outpost Firewall** einige sehr einfach bedienbare Funktionen zur Verfügung, wenn Sie im Menü des Hauptfensters das Menü „**Anzeige**“ auswählen. Es zeigt sich dann folgendes Menü:



Wählen Sie die Option „**Layout...**“ aus, zeigt sich folgendes Bild mit Einstellungsmöglichkeiten über die anzuzeigenden Informationen:



Im oberen Bereich lässt sich die Anzeige von folgenden Funktionen einstellen:

- Ordnerleiste
- Symbolleiste
- Statusleiste

Im unteren Teil lassen sich die anzuzeigenden Komponenten einstellen:

- Alle Verbindungen
- Hergestellte Verbindungen
- Offene [Ports](#)
- Ankommende Verbindungen
- Abgehende Verbindungen
- Erlaubte Verbindungen
- Blockierte Verbindungen
- Protokollierte Verbindungen

Je nach Einstellung werden im linken Teil der Benutzerschnittstelle mehr oder weniger Komponenten angezeigt.

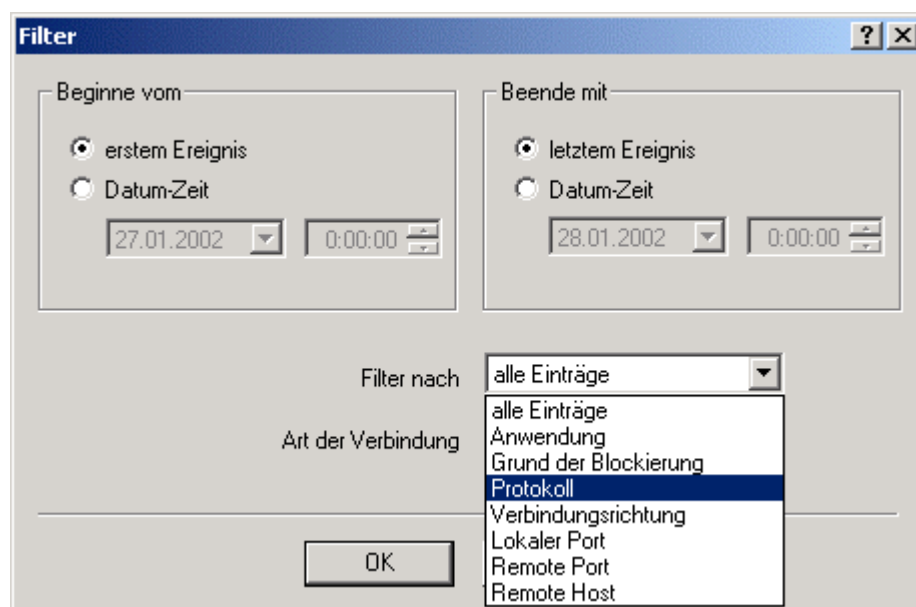
9.2 Filter

Mit der Filter-Funktion von **Outpost Firewall** können Sie Daten ausfiltern, die für Sie aktuell nicht interessant sind und legen damit den Fokus auf die wirklich interessanten Daten. Sie müssen gewünschte Daten dann nicht erst umständlich suchen sondern sehen sie auf einem Blick. So können Sie Daten filtern, die in einem bestimmten Zeitraum erfasst wurden oder Daten anhand von bestimmten Ereignissen.

Sie rufen den Filter für zeitliche Ereignisse auf, indem Sie folgendes Icon in der

Iconleiste anklicken: 

Es öffnet sich dann folgender Dialog zur Eingabe der Filterkriterien:



Dieser Dialog kann verwendet werden, um folgende Informationen nach bestimmten Kriterien zu filtern:

Beginnen von:

- **erstem Ereignis** – entspricht der Auflistung vom ersten Fall, der geloggt wurde.
- **Datum-Zeit** – entspricht der Auflistung vom ersten Fall ab einem bestimmten Datum.

Die Anzeige lässt sich noch weiter spezifizieren mit dem:

Ende von:

- **letztem Ereignis** – entspricht der Auflistung vom letzten Fall, der geloggt wurde.
- **Datum-Zeit** – entspricht der Auflistung vom letzten Fall bis zu einem bestimmten Datum.

Die Filterung der Anzeigen lässt sich noch feiner spezifizieren mit:

Zeige Vergangenheit wo das folgende Ereignis stattfand:

- **alle Einträge** – entspricht der Auflistung aller Ereignisse.
- **Anwendung** – entspricht der Auflistung der Anwendungen, die im unteren Textfeld angegeben wurde.
- **Grund der Blockierung** – entspricht der Auflistung der Ereignisse, die im unteren Pulldown-Menü gewählt wurden.
- **Protokoll** – entspricht der Auflistung der Ereignisse eines im unteren Pulldown-Menü gewählten [Protokoll](#).
- **Verbindungsrichtung** – entspricht der Auflistung der Ereignisse für ankommende oder eingehende Verbindungen.
- **Localer Port** – entspricht der Auflistung der Ereignisse eines im unteren Pulldown-Menü gewählten [Ports](#).
- **Remote Port** – entspricht der Auflistung der Ereignisse eines bestimmten gewählten Remote-Ports.
- **Remote-Host** – entspricht einer Auflistung der Ereignisse für einen bestimmten Remote-Host.

9.3 Spalten

Mit der Spalten-Funktionen können Sie **Outpost Firewall** so einrichten, dass Ihnen nur interessante Informationen angezeigt werden. Sie rufen die Funktion auf, wenn Sie im Menü den Punkt „**Anzeige**“ wählen und dort den Menüeintrag „**Spalten**“.

Es zeigt sich dann folgender Dialog:

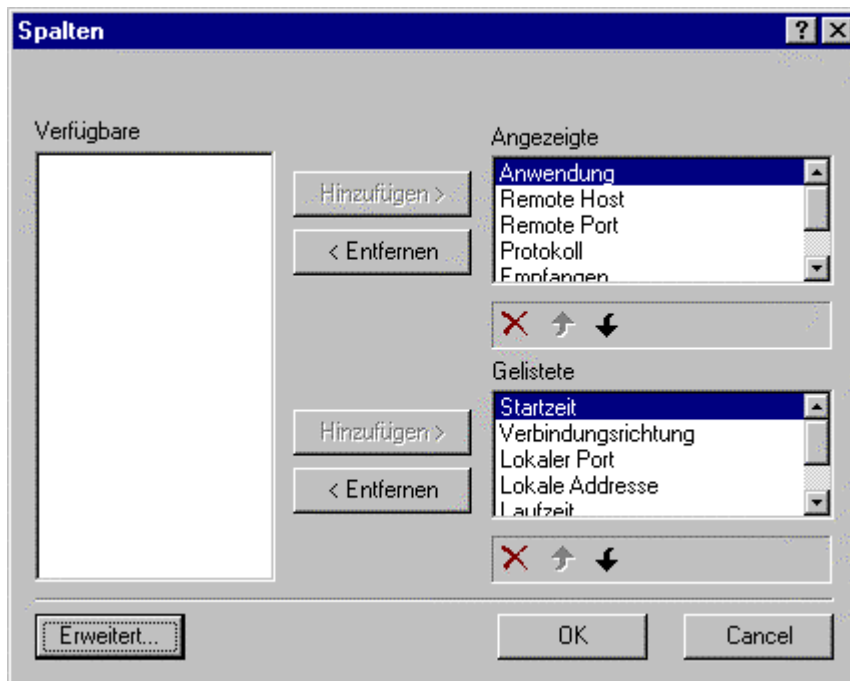


Sie haben hier die Möglichkeit, folgende Informationen im rechten Teil der Benutzerschnittstelle von **Outpost Firewall** anzeigen zu lassen:

- Den Grund der Verbindungsaufnahme
- Die Anwendung, die diese Verbindung ausgelöst hat
- Die Startzeit der Verbindung
- Der Remote-Host der Verbindung
- Der Remote-Port der Verbindung
- Die Richtung der Verbindung
- Das für die Verbindung verwendete Protokoll
- Der lokale Port
- Die lokale Adresse
- Die Laufzeit
- Gesendete Pakets
- Empfangene Pakets

- Die Geschwindigkeit, mit der Daten versendet wurden

Markieren Sie im rechten Teil der Benutzerschnittstelle eine bestehende Verbindung mit der rechten Maustaste und wählen im Kontext-Menü den Menü-Eintrag „**Spalten**“ aus, können Sie noch weitere Spalten zur gezielten Anzeige von Informationen definieren. Es zeigt sich dann folgendes Bild:



Klicken Sie hier auf den Button „**Erweitert...**“, stellen Sie noch feinere Anzeigeeoptionen ein. Es zeigt sich dann folgendes Bild:



So können Sie zum Beispiel definieren:

Ob IP-Adressen immer im [DNS](#) aufgelöst und angezeigt werden:

- Niemals
- Wenn Sie im Cache liegen
- Immer

Ports werden angezeigt als:

- Nummer
- Name

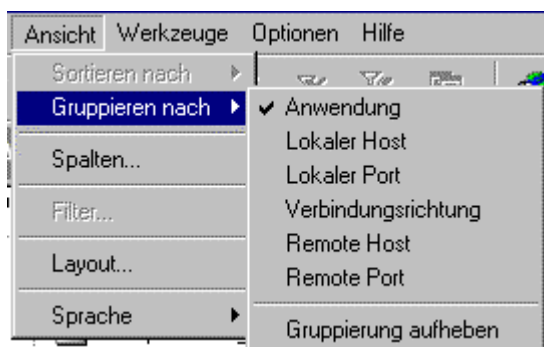
Zeige gesendeten Verkehr an als:

- Auto (es wird automatisch die richtige Größe angezeigt)
- Grundsätzlich die Größe in Bytes
- Grundsätzlich die Größe in Kilobytes
- Grundsätzlich die Größe in Megabytes

9.4 Gruppieren nach

Mit der Funktion „Gruppieren nach“ können Sie einfach und schnell alle Ihren Wünschen entsprechenden Informationen zu einer Gruppe zusammenstellen. Auf die Weise erhalten Sie schnell einen Überblick über zum Beispiel die Aktivitäten einer bestimmten Anwendung. Sie rufen Die Gruppierungs-Funktion auf, indem Sie das Menü „**Ansicht**“ auswählen und dort den Menüeintrag „**Gruppieren nach**“.

Es zeigt sich dann folgendes Bild:



Auf die Weise können Sie Gruppen von Informationen nach folgenden Kriterien anzeigen lassen:

Gruppierung nach:

- Anwendung
- Lokaler Host
- Lokaler Port
- Verbindungsrichtung
- Remote-Host
- Remote-Port
- Gruppierung aufheben

10 Appendix

10.1 ICMP-Nachrichten-Typen

Feldwert	Bezeichnung
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
10	IP Announcement
11	Time Exceeded For Datagram
12	Parameter Problem On Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ECHO Reply: Ist die Einfachste Methode zur Überprüfung von Betriebsbedingungen und Netzknoten. Sobald Ein Echosignal empfangen wird, erzeugt jeder mögliche Netzknoten ein ECHO Reply und gibt es zurück an die Quelle. Erhält die Quelle eine Antwort auf einen ECHO Reply, zeigt dies die gute Verfügbarkeit.

Destination Unreachable: Wird durch ein [Gateway](#) erzeugt, wenn es ein [IP-Datagramm](#) nicht liefern kann. Das IP-Datagramm ist die Masseinheit von Daten und Paketen, die über eine TCP-Verbindung verschickt werden. Jedes Datagramm enthält die Quell- und Zieladressen und die Daten.

Source Quench: Eine Quellenfrage wird gelöscht, wenn die Eingabewarteschlange des Ziels überfüllt wird und die Anfrage nicht mehr in ausreichender Zeit beantwortet werden kann. In diesem Fall wird das [Datagramm](#) aus der Warteschlange entfernt.

Redirect: Eine [ICMP](#) Nachricht wird umadressiert, wenn vom Gateway ein nicht optimaler Weg ermittelt wird. Es wird dann vom Gateway ein Antrag zum Kurswechsel in der Leitwegtabelle gestellt.

IP Announcement: Eine ICMP Nachricht verschickt eine Anzeige der [IP-Adresse](#) als [broadcast](#).

Time Exceeded for Datagram: Eine ICMP Nachricht mit der Information der Zeitüberschreitung wird versendet, wenn der Weg von einem Gateway zum anderen eine bestimmte Zeit überschreitet. Das Paket wird nach Erhalt dieser Nachricht nochmals abgeschickt, um Datenverluste zu vermeiden.

Parameter Problem on Datagram: Eine ICMP Nachricht mit einer „Parameter-Problem“ Information wird verschickt, wenn ein Gateway beim Empfang der Daten festgestellt hat, dass das Format der Daten einen bestimmten Bereich nicht mehr entspricht. In diesem Fall wird es als fehlerhaft markiert und muss neu gesendet werden.

Timestamp Request und Reply: Wird zum Zeitabgleich der Taktgeber zwischen zwei Netzknoten verschickt.

Information Request und Reply: Eine ICMP Nachricht mit einem „Information Request oder Reply“ wird verschickt, wenn der Antrag auf Informationen bereits abgelaufen und überholt ist. Es ist ein Hinweis, den Antrag nicht mehr zu verwenden.

Adress Mask Request und Reply: Eine ICMP Nachricht mit einem Adress-Schablonenantrag und die Anzeige einer Adress-Schablone werden verschickt, wenn ein lokaler Netzknoten die Adresse einer Subnetmaske ermitteln muss, um die Daten korrekt abzusenden.

10.2 Das Outpost Firewall Menüsystem

Das Menü Datei:

- **Neue Konfiguration:** Über diesen Menüpunkt kann eine neue **Outpost Firewall** Konfiguration angelegt werden.
- **Lade Konfiguration:** Hierüber kann eine bereits gespeicherte Konfiguration geladen werden.
- **Speichere Konfiguration:** Hier kann eine aktuelle Konfiguration mit einem bestimmten Namen gespeichert werden.
- **Immer im Vordergrund:** Hält das Fenster der Benutzerschnittstelle immer als oberstes Fenster.
- **Beenden:** Beendet **Outpost Firewall** komplett.

Das Menü Ansicht:

- **Anzeige:**
 - Gruppieren nach Anwendung
 - Gruppieren nach lokaler Adresse
 - Gruppieren nach lokalem Port
 - Gruppieren nach Verbindungsrichtung
 - Gruppieren nach Remote-Adresse
 - Gruppieren nach Remote-Port
 - Gruppieren aufheben

- **Sortieren nach:**
 - Anwendung
 - Remote-Host
 - Remote-Port
 - Protokoll
 - Empfangene Daten
 - Gesendete Daten
 - Aufwärts sortieren

- Abwärts sortieren

- **Spalten:** Öffnet die Funktion zur Anzeige der Informations-Spalten
- **Sprache:** Setzt die Programmsprache auf deutsch oder englisch

Das Menü Werkzeuge:

- **Lösche Log-Einträge:** Löscht die bisher protokollierten Einträge
- **Exportiere Log-Einträge:** Exportiert die bisher protokollierten Einträge in eine Datei

Das Menü Optionen:

- **Generell:** Öffnet den Options-Dialog für allgemeine Einstellungen von **Outpost Firewall**
- **Anwendungen:** Öffnet den Options-Dialog zur Einstellung von Anwendungen
- **System:** Öffnet den Options-Dialog zur Einstellung der globalen Systemaktivitäten
- **Police:** Öffnet den Options-Dialog zur Einstellung von Security-Level und vertrauten Zonen
- **PlugIns:** Öffnet den Options-Dialog zur Einstellung der installierten PlugIns

Das Menü Hilfe:

- **Kontext und Index:** Öffnet die kontextsensitive Hilfe beim Druck der Taste F1
- **Kontext Hilfe:** Verändert den Cursor zu einem Fragezeichen und zeigt spezifische Hilfe über das Thema, wenn ein Element mit dem Cursor angeklickt wird.
- **Readme:** Öffnet die Readme-Datei mit letzten und aktuellsten Informationen zu **Outpost Firewall**
- **Automatisch auf Update prüfen:** Nimmt Verbindung zum **Outpost Firewall** Update-Server auf und schaut nach neuen Programmteilen
- **Outpost Firewall im Web:** Leitet den Benutzer zu spezifischen Informationen auf den Agnitum-Webseiten
- **Über Outpost:** Öffnet den Dialog zur Anzeige der Programmversion und den Versionen der installierten Komponenten

10.3 Glossar

ActiveX: ActiveX ist eine Technologie zur Erstellung von aktiven Webseiten. Diese Technologie wurde eingeführt mit der ActiveX-Steuerung, ein Programm, das eine Schnittstelle zum Benutzer über den Web-Browser zur Verfügung stellt. Die ActiveX-Technologie automatisiert Installationen von ActiveX-Controls. Trifft der Web-Browser auf einen [HTML](#)-Link mit einer Verbindung zum Steuerelement, schaut er zunächst ob das Element schon auf dem Computer installiert ist. Wird das Element gefunden, werden sofort die Daten übertragen, die für den Betrieb notwendig sind. Wird das Element nicht auf dem lokalen Computer gefunden, wird es, je nach Sicherheitseinstellung des Browsers, automatisch installiert.

Banner: Ein Banner ist eine bestimmte Werbeform, die in einem Grafikformat wie zum Beispiel GIF oder JPG auf einer Webseite eingefügt wird. Ein Hyperlink stellt eine Verbindung zum Anbieter her, zu dem der Besucher geleitet wird, wenn er den Banner anklickt.

Broadcast: Broadcast ist eine spezielle Form der Kontaktaufnahme zu allen Computern in einem Netzwerk.

Es gibt zwei Formen von Broadcast-Verbindungen:

- **Begrenzter Broadcast oder begrenzte Broadcast Nachricht:** Das Paket wird zu den Computern im Netz geschickt, wenn das erste Bit in der [IP-Adresse](#) dieser Computer eine 1 ist. Heißt, wenn die IP-Adresse des Computers aus der C-Netz-Klasse kommt, die nur für den internen Gebrauch innerhalb eines LANs benutzt wird (z.B. 192.xxx.xxx.xxx).
- **Broadcast oder Broadcast Nachricht:** Das Paket wird zu allen Computern im Netzwerk geschickt, die irgendwo in der IP-Adresse eine 1 besitzen.

Client: Als Client wird ein Computer in einem Netzwerk bezeichnet, der Verbindung zu einem [Server](#) aufnimmt.

Cookie: Ein Cookie ist ein winziger Textschnipsel, der vom Server der besuchten Webseite über den Browser des Benutzers lokal auf die Festplatte seines Computers gespeichert wird. Einige Cookies werden nur während des Datenaustausches zwischen Server und [Client](#) gespeichert und beim Beenden der Verbindung wieder gelöscht. Einige Cookies bleiben aber dauerhaft auf dem Computer des Besuchers gespeichert,

um dort zum Beispiel Informationen für personalisierte Angebote auf dem besuchten Server zu speichern.

Cracker: Ist irgendjemand, der unbemerkt und unautorisiert Zugriff auf fremde Rechner nimmt (Anmerkung des Übersetzers: Cracker sind Leute, die Registrierungen von Programmen „knacken“ oder Tools zur Erstellung von illegalen Seriennummern erstellen. Hacker sind die Leute, die mitunter in fremde Rechner eindringen. Hier gibt es noch eine besondere Unterscheidung zwischen Hackern, die nach einem Ehrencodex arbeiten und niemals Daten zerstören würden. Sie „hacken“, um Sicherheitsprobleme bewusst zu machen. Eine wirkliche Gefahr stellen so genannte Script-Kiddies dar, die aus purer Lust an der Zerstörung fremde Rechner angreifen, Daten zerstören oder manipulieren und Benutzerdaten spionieren.).

Datagramm: Datagramm ist eine Maßeinheit von Daten oder von Paketen, die über ein TCP/IP Netz übertragen werden. Jedes Datagramm enthält Quelle und Zieladressen der Daten.

DHCP (Dynamic Host Configuration Protocol): DHCP ist ein Protokoll für die dynamische Vergabe von [IP-Adressen](#).

DNS (Domain Name System): DNS ist ein System, mit dem die IP-Adressen von Computern und Domains in einen Klarnamen übersetzt werden. Die Adresse einer Webseite einer Domain kann also sowohl 217.83.101.223 sein oder als Klarnamen die Adresse <http://www.network-secure.de/>. Dieses System wurde entwickelt, weil die IP-Adresse als Zahl schwerer zu merken ist. Aus dem Grund gibt es im Internet mehrere Server, die große Tabellen mit IP-Adressen verwalten und Server, die die gleiche Anzahl an Tabellen mit den Klarnamen pflegen. Bei jedem Aufruf einer Domain werden die beiden Daten miteinander verglichen und überprüft, ob sie noch aktuell sind und ob sie zusammenpassen.

DNS-Adresse: Die DNS-Adresse ist eine Netzwerk-Adresse, die aus einer 32bittigen Zahl besteht, die der einfachen Lesbarkeit wegen mit Punkten getrennt ist. Diese Adresse entspricht auch dem Klarnamen, wie unter DNS schon erklärt wurde.

DOS (Denial of Service) Angriff: Ein DOS Angriff ist ein spezifischer Angriff auf irgendjemand's Computer mit dem Ziel, den normalen Betrieb des Computers derart zu stören, dass er keine normalen Aufgaben mehr ausführen kann. Es gibt diverse Formen von DOS Angriffen, die jeweils eine bestimmte Art und Weise der Netz-

Kommunikation ausnutzen. Im einfachsten Fall wird ein Computer mit einer unglaublich großen Anzahl an Anfragen regelrecht bombardiert. Da jede Anfrage eine Antwort auslöst, ist der Ziel-Computer schon sehr bald nur noch mit der Beantwortung der Anfragen beschäftigt und wirkt wie eingefroren.

FTP (File transfer protocol): Das FTP ist ein spezifisches Netzwerk-Protokoll, mit dem Daten von einem Computer über das Netz zu einem anderen Computer transportiert werden können.

Gateway: Ist eine Vermittlungsstelle, die die Kommunikation zwischen zwei Netzwerken organisiert. Ein [Router](#) kann als solches Gateway bezeichnet werden.

GGP (Gateway to Gateway protocol): GGP ist ein spezifisches Protokoll, mit dem Gateways untereinander spezielle Control-Tasks ausführen, um den Datenverkehr über Netzwerkgrenzen hinweg zu organisieren.

GUI (Graphics user interface) : Ein GUI ist die grafische Oberfläche, das Frontend eines Programms, über das ein Benutzer das Programm bedienen kann.

HTML (Hypertext Markup Language): HTML ist eine Seitenbeschreibungssprache, die spezifische Befehle zur Erstellung und Anzeige von Webseiten besitzt.

ICMP (Internet control message protocol): ICMP ist ein Protokoll, mit dem Computer im Netzwerk Informationen über den Zustand der Verbindung und der vermittelten, gesendeten oder empfangenen Daten austauschen können.

IGMP (Internet group message protocol): Das IGMP ist ein Hilfsprotokoll, mit dem Netzwerkpunkte und Router Informationen darüber austauschen, wo in welchen Gruppen Nachrichten untereinander ausgetauscht werden.

IP (Internet protocol): Das IP-Protokoll ist ein Protokoll-Standard, über den der gesamte Internet-Verkehr abgewickelt wird. IP ist ein Oberbegriff für eine ganze Reihe von Protokollen, die sich wie die Schichten einer Zwiebel übereinander stülpen. Jede Schicht trägt spezifische Informationen über gesendete Daten.

IP-Adresse: Die IP-Adresse ist die eindeutige Kennzeichnung eines jeden Computers im Netzwerk. Die IP-Adresse ist eine 32bittige Zahl, die der leichten Lesbarkeit wegen durch einzelne Punkte getrennt ist. So ist zum Beispiel die IP-Adresse 217.83.101.223 aktuell die Adresse unserer Domain <http://www.network-secure.de/>.

IP-Datagramm: Das Datagramm ist eine Maßeinheit für Daten und Pakete, die über ein TCP/IP Netzwerk verschickt werden. Jedes Datagramm enthält Angaben über die Quelle und das Ziel.

JAVA Applet: JAVA ist eine Websprache und ein Applet ist ein Programm, das häufig in Webseiten eingebettet ist, um spezielle Funktionen wie zum Beispiel die Suchfunktion auf einer Webseite zu ermöglichen.

JAVA Script: JAVA Script ist eine Untereinheit von JAVA und ebenfalls eine Art Programmiersprache. Mittels JAVA Script lassen sich Webseiten dynamisch gestalten und mit umfangreicheren Funktionen ausstatten, die das normale HTML nicht beherrscht.

Loopback: Loopback ist eine spezielle IP-Adresse, die benutzt wird, um die Verfügbarkeit von Diensten auf einem Computer zu prüfen, ohne die Daten tatsächlich zu senden. Anhand der Rückantwort erhält die Quelle spezielle Informationen über die Verfügbarkeit.

Multicast: Multicast ist eine spezielle Gruppe von IP-Adressen, die mit der Reihenfolge 255 beginnen. Wenn eine Multicast-Adresse in einem Paket als Zuweisungsadresse spezifiziert wird, erhalten alle Computer, die diese Zahl in der IP-Adresse besitzen, dieses Paket. Diese Art nennt sich Gruppenanweisung und sie wird nicht in Netzwerk- und Computeradressen unterteilt. Der empfangende Router verarbeitet Multicast mit einer speziellen Art und Weise.

NetBIOS (Network Input/Output System): NetBIOS ist ein von IBM entwickeltes Hilfs-Protokoll, über das gemeinsam genutzte Ressourcen wie Verzeichnisse und Drucker verwaltet werden. Auf die Art und Weise können alle am Netz angeschlossenen Computer diese Ressourcen nutzen.

Port: Ein Port definiert eine Zahl, die einer bestimmten Datenart entspricht, damit unterschiedliche Arten von Daten leistungsfähig gesendet und dem zu ihnen passenden

Anwendungsprogramm zugeordnet werden kann. Ein Tor ist kein physikalischer Stecker sondern wird nur in der Software zugewiesen.

Protokoll: Protokoll definiert einen Satz geltender Richtlinien für eine bestimmte Art von Kommunikationsaustausch.

Proxy-Server: Ein Proxy-Server ist Software, die den Anschluß zwischen einem Absender und einem Empfänger verwaltet. Jede Zustellung wird zu einem anderen Port umadressiert, um zu verhindern, dass ein Angreifer Zugriff auf persönliche Daten erhält.

Referrer: Referrer ist ein Teil einer http-Anfrage, die die Adresse der zuletzt besuchten Seite enthält, die vorher besucht wurde.

Router: Ein Router ist Hardware oder Software, mit dem der Datenaustausch zwischen zwei Netzen organisiert wird.

Server: Ein Server ist ein Computer, der Daten oder Webseiten zu einem [Clienten](#) im Netzwerk sendet.

SSL (Secure sockets layer): SSL ist ein spezielles Protokoll, das entworfen wurde, um sicheren Zugang von einem Computer zu einem anderen Computer zu ermöglichen. SSL ist das vorherrschende Protokoll für verschlüsselten Austausch von Daten zwischen [Client](#) und [Server](#).

TCP (Transmission control protocol): TCP ist das zentrale Netzwerk-Protokoll zum Austausch von Informationen im Internet.

Telnet: Telnet, das Fernmeldenetzprotokoll ist ein Programm für die Verbindung der einzelnen Werkzeuge des Internets wie Web-Browser, Datenbanken, Inhaltsverzeichnissen einer Bibliothek und anderen weltweiten Informationen.

Trojaner: Trojaner sind Programme, die harmlose und sinnvolle Funktionen vorgeben und unbemerkt im Hintergrund Daten zerstören, spionieren oder manipulieren.

UDP (User datagramm protocol): UDP ist ein Protokoll mit einfachen niedrigen Werkzeugen, die zur direkten Übermittlung von Daten zur Anwendung benutzt werden. Das UDP steuert nicht die Datenübertragung und definiert auch nicht die Wechselbeziehung zwischen Sender und Empfänger (hierfür ist das TCP zuständig).

URL: URL (Universal resource locator) ist eine weltweite allgemein gültige Adresse zur Identifikation von Ressourcen im Netz.

VB Script: VB Script (Visual Basic Script) ist eine Untereinheit der Programmiersprache Visual Basic und sie wird häufig zur Programmierung von Webseiten benutzt. Eingebetteter VB-Code stellt besondere Funktionen zur Verfügung wie zum Beispiel die Suchfunktion einer Webseite.

Web: Das Web ist ein abstrakter Begriff für einen Raum, in dem Benutzer multiple Dateien und Dateiformate hinterlegen, um sie mittel Hyperlinks verfügbar zu machen.

11 Zur deutschen Übersetzung

11.1 Referenz Outpost Firewall

Das englische Original-Handbuch zu **Outpost Firewall** des Herstellers Agnitum Ltd. wurde im Rahmen des Beta-Programms von Network-Secure (<http://www.network-secure.de>) wörtlich deutsch übersetzt, um auch nicht englischen sprechenden Benutzern dieses außergewöhnlich guten Firewallsystems eine Grundlage zur Einarbeitung in das Programm zu ermöglichen.

Falls notwendig, wurden einzelne Abschnitte mit zusätzlichen Informationen versehen, die unserer Meinung nach einzelne Kapitel ergänzen oder schwierige Abschnitte erklären. Die zusätzlichen Informationen basieren auf unsere eigenen täglichen Erfahrungen, die wir bisher mit dem Firewallsystem **Outpost Firewall** gesammelt haben.

Unsere deutsche Übersetzung wurde dem Entwicklerteam von **Outpost Firewall** kostenlos zur Verfügung gestellt als kleines Danke Schön für den ausgezeichneten Support und die Unterstützung der Beta-Tester.

Wir legen Wert darauf, dieses Handbuch nicht zukünftig in irgendeinem Online-Shop als Kaufangebot zu sehen. In diesem Fall würden wir selbst entsprechende rechtliche Schritte einleiten bzw. unsere Rechte an das Entwicklerteam von **Outpost Firewall** für weitere Verwendung abtreten. Die Übersetzung war Knochenarbeit und ist als Geschenk an die Netzgemeinde zu betrachten. Wir möchten mit der deutschen Übersetzung einen kleinen Beitrag zu mehr Sicherheit im Internet beitragen.

Unser besonderer Dank gilt:

DauBert

Für seinen unermüdlichen Einsatz in unserem Forum, das zu einer Anlaufstelle für den deutschen Support zu **Outpost Firewall** geworden ist. Jederzeit hilfreich vorhanden, war und ist er eine wertvolle Unterstützung bei der Betreuung der deutschen Benutzer von **Outpost Firewall**.