Sicherheit für Anwender: Specials

Folgende Bücher zum Thema können Sie an der Auskunft des RRZN erwerben:

- Computersicherheit im Internet
  für Anwender — 2,50 EUR
- Internetworking: Sicherheit — 5,00 EUR

Infos unter http://www.rrzn.uni-hannover.de/Dokumentation/Handbuecher

Sicherheit für Anwender: Specials

Christine Peter

IT-Sicherheit RRZN

RRZN-Kurs: Sicherheit für Anwender – Specials

peter@rrzn.uni-hannover.de 762-8021

Sicherheit für Anwender: Specials

Themen:

Nicht auf die leichte Schulter nehmen!

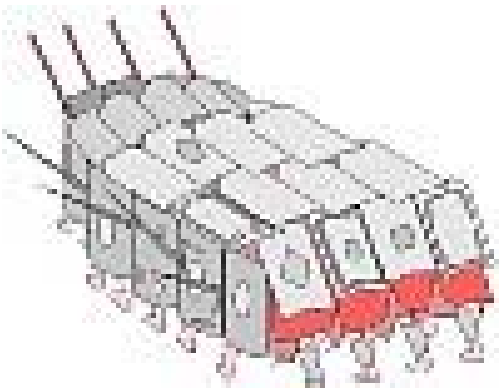
- Passwörter – Pflicht oder Paranoia?

Sicherheit für Anwender: Specials

Themen:

Tools zum Schutz

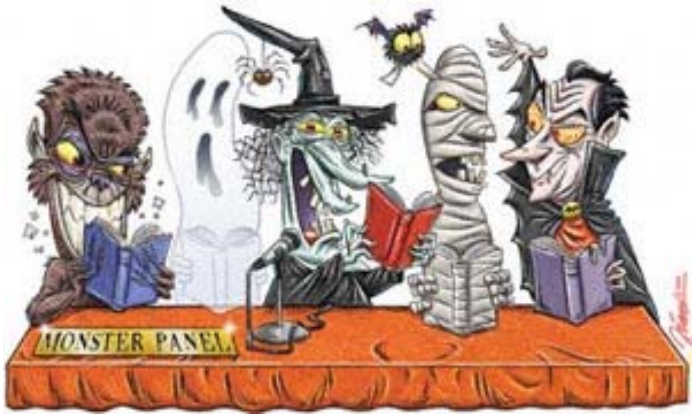
- Einsatz des IE-Controllers
- Installieren einer Personal Firewall



Sicherheit für Anwender: Specials

Themen:

Weitere Bosheiten, Belästigungen und Gefahren



- Hoaxes
- SPAM
- Spyware
- 0190-er Dialer

Sicherheit für Anwender: Specials

Themen:

Nicht auf die leichte Schulter nehmen!

- Passwörter – Pflicht oder Paranoia?

Passwörter - Pflicht oder Paranoia?

- Warum überhaupt Passwörter
- Wie werden Passwörter gecrackt
- Wie sehen schlechte Passwörter aus
- Wie bildet man sichere Passwörter
- Vom Umgang mit Passwörtern

Warum überhaupt Passwörter

- Zugang zu EDV-Systemen in der Regel nur über
  - Benutzername und
  - Passwort

- Vergleich aus dem Alltag:
  - Benutzername entspricht Ihrer Adresse
  - Passwort ist ihr Wohnungsschlüssel

Warum überhaupt Passwörter

- wenn Passwörter gecrackt werden,
  - dann selten
    - aus Interesse am Lesen Ihrer E-Mails
    - um Ihnen persönlich zu schaden
    - um genau Ihre Dateien zu stehlen
  - sondern eher
    - aus Interesse an Ihren Ressourcen
    - der Möglichkeit, der Identitätsverschleierung
    - Zugangsmöglichkeit in ein Netzwerk

Warum überhaupt Passwörter

Unsichere Passwörter unterminieren also sowohl

- **Ihre persönlichen Sicherheit**

als auch, wenn Sie mit einem Netzwerk verbunden sind

- **die Sicherheit des ganzen Netzwerkes**

Passwörter cracken: Die Idee

- prinzipiell hört sich alles ganz gut an:
  - Passwörter werden verschlüsselt abgelegt
  - Verschlüsselungsfunktion ist nicht umkehrbar
    - aus dem verschlüsselten Passwort sind keine Rückschlüsse auf das Passwort „im Klartext“ möglich.
- Aber: Die Verschlüsselungsfunktion ist allgemein bekannt
  - beliebige Wörter werden verschlüsselt
  - die Ergebnisse werden mit den verschlüsselten Benutzerpasswörtern verglichen
  - findet man Übereinstimmungen, ist das Passwort enttarnt

Passwörter cracken: Die Idee

Beispiel für eine Passwortdatenbank

```
root:u7pri3xpLGw:0:0:root:/root:/bin/bash
tgam:FeQoWwAzsDg:1:1:tgam:/tgam:/bin/bash
mban:FP0U2KY48DI:2:2:mban:/mban:/bin/bash
```

Username

verschlüsseltes Passwort

User-ID

Group-ID

Startverzeichnis

Default-Shell

Passwörter cracken: Die Idee

Passwortliste

Niagara —f(pw)→ ~~H5jkLi6wDma~~

Nashorn —f(pw)→ ~~mKo4SssP9aQ~~

Norbert —f(pw)→ ~~Gkm4sp6bwf3~~

⋮

Nordsee —f(pw)→ FeQoWwAzsDg

```
root: u7pri3xpLGw
tgam: FeQoWwAzsDg
mban: FP0U2KY48DI
```

⋮

gecrackter Account:
Benutzername: **tgam**
Passwort: **Nordsee**

Passwörter cracken: Die Dictionary-Methode

- Wörterbuch = ausführliche Listen
  - enthalten alle denkbaren wahrscheinlichen Passwörter
  - in schon verschlüsselter Form
  - sind sehr zahlreich
  - über das Internet leicht verfügbar

Passwörter cracken: Die Dictionary-Methode

- Die verfügbaren Wörterbücher werden immer ausgefeilter:
  - jedes enthaltene Wort wird auch in etlichen Variationen und Ableitungen getestet:
    - nur Großbuchstaben, abwechselnd Groß- und Kleinbuchstaben, der Begriff rückwärts geschrieben usw.
    - an irgendeiner Position wird eine Ziffer oder ein Sonderzeichen zusätzlich eingefügt
    - Buchstaben werden durch ähnliche Zahlen ersetzt oder umgekehrt (3 und E, 1 und I, 7 und T)
    - eine beliebige Kombination der obigen Varianten

Passwörter cracken: Die Dictionary-Methode

- es gibt Wörterbücher in allen möglichen Sprachen (auch finnisch, japanisch...),
  - inklusive der in dem jeweiligen Land gängigen
    - Ortsnamen
    - Vor- und Nachnamen
    - berühmten Persönlichkeiten

- es gibt Wörterbücher zu speziellen Themengebieten wie Medizin, EDV, Kunst, Literatur, Fantasy oder Science-Fiction.

Passwörter cracken: Die brute-force-Methode

- **brute force = „rohe Gewalt“**

- es werden einfach der Reihe nach sämtliche möglichen Zeichenkombinationen durchgetestet
- gegen diese Methode ist man letztlich machtlos **ABER**
  - sie nimmt sehr viel Rechenleistung in Anspruch
  - benötigt viel mehr Zeit als die Dictionary-Methode

Passwörter cracken: Die brute-force-Methode

Rechenbeispiel:

	Größe des Zeichenvorrates			
Länge PW	**26** klein	**52** groß+klein	**62** gr+kl+Ziff	**95** +Sonderz.
5	11.881.376	380.204.032	916.132.832	95^5
6	308.915.776	19.770.609.664	62^6	95^6
7	8.031.810.176	1.028.071.702.528	62^7	95^7
8	208.827.064.576	53.459.728.531.456	62^8	6.634.204.312.890.625

Passwörter cracken: Die brute-force-Methode

schnelles System:

300.000 Kombinationen pro Sekunde werden getestet:

Länge PW	**26** klein	**52** groß+klein	**62** gr.+kl.+Ziff.	**95** +Sonderz.
5	39 Sekunden	21 Minuten	51 Minuten	7,2 Stunden
6	17 Minuten	18 Stunden	2,2 Tage	28 Tage
7	7,4 Stunden	39 Tage	135 Tage	7,4 Jahre
8	8 Tage	5,6 Jahre	23 Jahre	700 Jahre

Passwörter cracken: Die brute-force-Methode

Fazit:

es gibt einen Schutz gegen die brute-force Methode:

ausreichende Passwortlänge wählen
mindestens 7, besser 8 Zeichen
gesamten Zeichenvorrat verwenden

Wie sehen schlechte Passwörter aus

- typische **persönliche Daten**
- Name des **Betriebssystems** oder des **Rechners**
- Name der **Institution** oder des **Arbeitsplatzes**
- **Firmenlogo** am Monitor, Tastatur, PC
- Wörter aus dem **Sprachschatz** (div.Wörterbücher)
- Wörter aus **anderen Sprachen** (ebenfalls wegen div.Wörterbücher)
- Wörter, die häufig für Gastkennungen als Passwörter vergeben werden (**guest, gast, public, common, …**)
- Ebenso problematisch: **einfache Modifikationen** dieser Worte

Wie sehen schlechte Passwörter aus

- **bekannte Eselsbrücken**
  - GDaEhFis = G-Dur-Tonleiter: Geh Du alter Esel hole Fische
  - EaDGhe = Gitarrensaiten: Eine alte Deutsche Gitarre hält ewig
  - BAlGaInTl= Periodensystem: Bei Al gabs indische Teller
- Anfangsbuchstaben von **bekannten Sprichwörtern**, Liedern, etc.
  - AmEsadS = Alle meine Entchen schwimmen auf dem See,
  - WrssdNuW = Wer reitet so spät durch Nacht und Wind

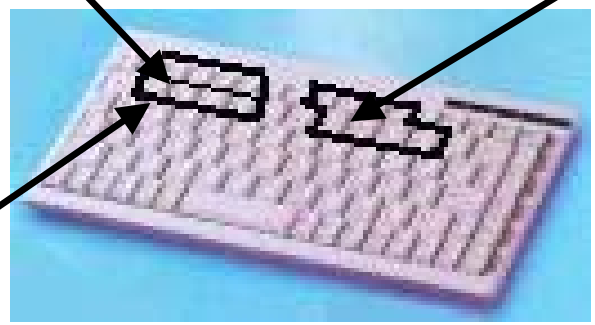
Wie sehen schlechte Passwörter aus

Vermeintlich unsinnige Kombinationen aus Buchstaben und Zahlen

1234qwer

0987poiu

asdf1234



jklö7890

qwertz/qwerty

Wie sehen schlechte Passwörter aus

Alle diese Passwörter haben einen gravierenden Nachteil:

Passwortcracker ermitteln diese Passwörter unter Umständen innerhalb von Minuten!

Wie bildet man sichere Passwörter

- **Nicht das Passwort wird gemerkt, sondern die Methode, mit der es gebildet wird!**
  - Akronym-Methode
    - v9b10:Rv **v**on **9** **b**is **10:** **R**auchen **v**erboten
    - W?nA-zA! **W**ohin**?** **n**ach **A**ldi **nein** **z**u **A**ldi**!**
  - Methode Doppelwort:
    - Ba+ac;Fo **Ba**lz**ac** **;** **Fo**ntane
    - S:LaO!Ha **S**tan **:** **La**urel **O**liver **!** **Ha**rdy
  - Collage-Methode (Leibniz Rechenzentrum München)
    - P:rs$val **P**ferd **:** Ho**rs**e **$** che**val**
    - hou:17Hau **hou**se **:** Hausnummer **Hau**s

Wie bildet man sichere Passwörter

- Umstritten: Die Methode Zufall
  - wirklich willkürliche Auswahl von 8 Zeichen
  - schlecht zu tippen ➔ gut beobachtbar
  - schlecht zu merken
  - prädestiniert das Passwort dafür, auf Zetteln am Monitor zu enden

Wie bildet man sichere Passwörter

- weitere Hinweise
  - nach einer Passwortänderung ruhig ein paar Mal hintereinander einloggen
  - Regeln zur Passwortbestimmung überdenken und für sich abändern
  - NICHT die Passwörter aus den Beispielen benutzen

Vom Umgang mit Passwörtern

- Für verschiedene Kennungen auch **verschiedene Passwörter** verwenden.
- das Passwort soll nur **einer einzigen Person** bekannt sein
- Passwort auch **nicht** in Ausnahmefällen **weitersagen**
- **Niemals** jemandem **am Telefon** ihr Passwort mitteilen.
- **Initialpasswörter** sind (zwingend) bei der ersten Benutzung zu ändern.

Vom Umgang mit Passwörtern

- Das Passwort **schnell und sicher** eintippen und sich dabei **nicht über die Schulter schauen** lassen!
- Wenn Sie Ihren Arbeitsplatz verlassen, **sperren** Sie Ihre Sitzung oder melden sich ab.
- Das Passwort soll **regelmäßig geändert** werden.
- **Keine alten Passwörter** wiederverwenden.

Vom Umgang mit Passwörtern

- **Die Passwörter nicht aufschreiben**
- Wenn dies unumgänglich ist, folgende Ratschläge beherzigen:
  - niemals als Passwort **erkennbar notieren**
  - ein Passwort **nie in elektronischer Form** aufbewahren (programmierbare Tasten, Merkzettel-Dateien)
  - den Zettel mit dem Passwort **nicht in der Nähe des Gerätes** unterbringen, nur bei Ihnen persönlichen (Portemonnaie)

80% der aufgeschriebenen Passwörter befinden sich am Arbeitsplatz im Umkreis von 2 Metern

Passwörter: Zusammenfassung

- Ein gutes Passwort
  - ist acht Zeichen lang
  - enthält mindestens
    - 2 Buchstaben (Groß- als auch Kleinbuchstaben)
    - 2 Ziffern
    - 2 Sonderzeichen
  - kann man sich leicht merken
  - kann man schnell eintippen
  - erscheint wie eine zufällige Zeichenfolge (keine erkennbare Systematik)
  - ist kein Wort einer bekannten Sprache
  - ist nur dem Inhaber der Kennung bekannt
  - wird in angemessenen Abständen geändert - ca. alle drei Monate

Passwörter: Demo Crackprogramm

12 Testbenutzer mit unterschiedlich komplizierten Passwörtern:

Benutzername	Passwort	Benutzername	Passwort
meier	meier2	**lehmann**	qwer
schulz	schulz?	**klein**	abcd
peter	Schiller	**heinz**	geheim
aust	Mozart	**schlau**	v9b10:Rv
werner	Stuhl	**clever**	S:LaO!Ha
moeller	test	**smart**	P:rs$val

Passwörter: Demo Crackprogramm

12 Testeinträge in der Passwortdatei

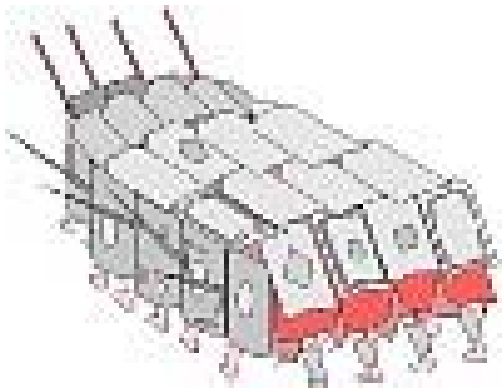
```
meier:JyB3TKxd0KRzg:1:2:Martin Meier:/home/meier:/bin/ksh
schulz:XTeM6s8lbpjdw:2:2:Siegfried Schulz:/home/schulz:/bin/ksh
peter:R1n69gkbVEOgc:3:2:Christine Peter:/home/peter:/bin/ksh
aust:Z1Ic6N1gkthn.:4:2:Angela Aust:/home/aust:/bin/ksh
werner:N2YkoFa8MC8ds:5:2:Willi Werner:/home/werner:/bin/ksh
moeller:pv12fMa1tSN6U:6:2:Manfred Moeller:/home/moeller:/bin/ksh
lehmann:IbopEBjVt41Rs:7:2:Lothar Lehmann:/home/lehmann:/bin/ksh
klein:ai1n/KoLuOoio:8:2:Karsten Klein:/home/klein:/bin/ksh
heinz:epkhOSde5apoY:9:2:Herbert Heinz:/home/heinz:/bin/ksh
schlau:xFwtsqb2Bsln s:10:2:Sabine Schlau:/home/schlau:/bin/ksh
clever:GZfv1u4jdlEf6:11:2:Carola Clever:/home/clever:/bin/ksh
smart:NwDdwY7fPcCII:12:2:Stefan Smart:/home/smart:/bin/ksh
```

Sicherheit für Anwender: Specials

Themen:

Tools zum Schutz

- Einsatz des IE-Controllers
- Installieren einer Personal Firewall



Tool: IE-Controller

Zur Motivation:
http://www.rrzn.uni-hannover.de/BIs Jan.2003 / 364

Bei Meldungen über Sicherheitslücken bei Browsern handelt es sich zum größten Teil um den Internet Explorer und um

- Probleme mit aktiven Elementen, hauptsächlich
  - ActiveX und
  - Active Scripting (VBScript und Jscript)

Tool: IE-Controller

- AxtiveX
  - Microsoft-Technik, betrifft nur Internet Explorer
  - eng mit Betriebssystem verflochten:
    - Zugriff auf alle Systemressourcen
    - Zugriff auf Daten auf der Festplatte
    - Zugriff auf Daten auf verbundenen Netzlaufwerken

Tool: IE-Controller

- **sehr großes Sicherheitsrisiko**
- hat viele Sicherheitslücken
- und sehr viele Rechte (unabhängig von den vergebenen Benutzerberechtigungen) und ermöglicht dadurch
  - das auslesen und löschen von Daten
  - unbemerktes Installieren von Programmen mit Schadensfunktion (siehe auch 0190er-Dialer).

Tool: IE-Controller

Der IE-Controller

- schaltet sich als Kontrollinstanz zwischen den Internet Explorer und Windows.

- kann den Start von einzelnen Modulen unterbinden, die der IE zur Ausführung aktiver Inhalte benötigt.

- bietet eine flexiblere und restriktivere Verwaltung der gewünschten Sicherheitseinstellungen.

Tool: IE-Controller

- Nimmt keinerlei Eingriffe in den IE oder das Betriebsystem vor:
  - Man kann den IE auch jederzeit direkt starten.
- Das Tool funktioniert mit den ganz normalen Benutzerberechtigungen.
- Download und Anleitungen
  - http://www.heise.de/ct/ftp/projekte/iecontroller/

Tool: IE-Controller

- Arbeitet mit 3 verschiedenen Filterlisten
  - Greylist
    - Fest vorgegebene Einträge
    - Erlaubt nur, was zum Start des IE nötig ist.
    - Möglichkeit zur De-/Aktivierung von Java, VBScript, ...
  - Blacklist
    - Enthält alle verbotenen Module, ist frei editierbar.
  - Whitelist
    - Enthält alle erlaubten Module, ist frei editierbar.

Tool: IE-Controller

- Filterlisten werden in festgelegter Reihenfolge abgearbeitet
  - Höchste Priorität: Blacklist
  - An zweiter Stelle: Greylist
  - Niedrigste Priorität: Whitelist

- Heise stellt verschiedene vorbereitete Filterlisten zum Download bereit:
  - http://www.heise.de/ct/ftp/projekte/iecontroller/downloads/iec_filter.zip
  - Können importiert und editiert werden

Tool: IE-Controller

- Es können mehrere Konfigurationen angelegt werden , die mit unterschiedlichen Optionen und Filterlisten arbeiten

Tool: IE-Controller

c't-IEController 1.0 Experten-Konfiguration (c) 2003 c't/Matthias Withopf, wit@heise.de

Blacklist (gesperrte Objekte): Importieren

Aktiv	Einstellung	CLSID	Beschreibung
+	Sperren	0D43FE01-F093-11CF-8940-00A0C9054228	Zugriffe aufs Dateisystem sperren: FileSyst...

Whitelist (erlaubte Objekte): Importieren

Aktiv	Einstellung	CLSID	Beschreibung
-	Erlauben	2318C2B1-4965-11D4-9B18-009027A5CD4F	Google-Toolbar: &Google aus googlenav.dll

Erzeugen unbekannter COM-Objekten

- ○ Immer sperren (sicherste Einstellung)
- ○ Immer erlauben (unsichere Einstellung)
- ◉ Nachfragen

Starten externer Programmen

- ○ Immer sperren (sicherste Einstellung)
- ○ Immer erlauben (unsichere Einstellung)
- ◉ Nachfragen

Anregungen zur Konfiguration richten Sie an: iec@ct.heise.de

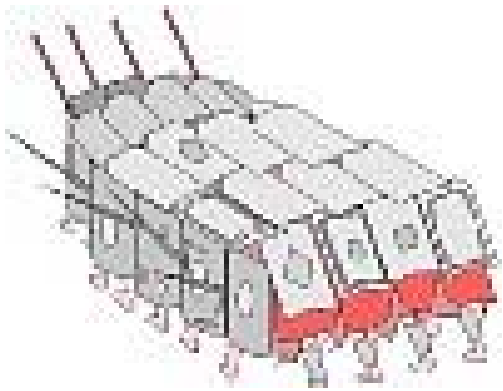
Ok

Sicherheit für Anwender: Specials

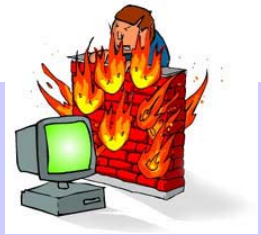
Themen:

Tools zum Schutz

- Einsatz des IE-Controllers
- Installieren einer Personal Firewall

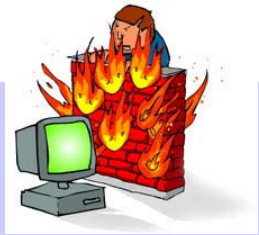


Personal Firewalls



- Grundsätzlich gilt:
  - nur eine Personal Firewall auf dem System installieren;
  - doppelt hält nicht besser.
- Zugrundeliegende Philosophie sollte sein:
  - Erst alles verbieten, dann nach und nach gezielt erlauben was unbedingt nötig ist.
- Passwort-Schutz für die Firewall aktivieren.
- Im Folgenden: Standard-Konfiguration einer Personal Firewall am Beispiel von Kerio Version 2.1.4 (http://www.kerio.com)

Personal Firewalls

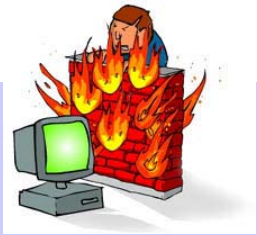


Arbeitsweise von Kerio PF

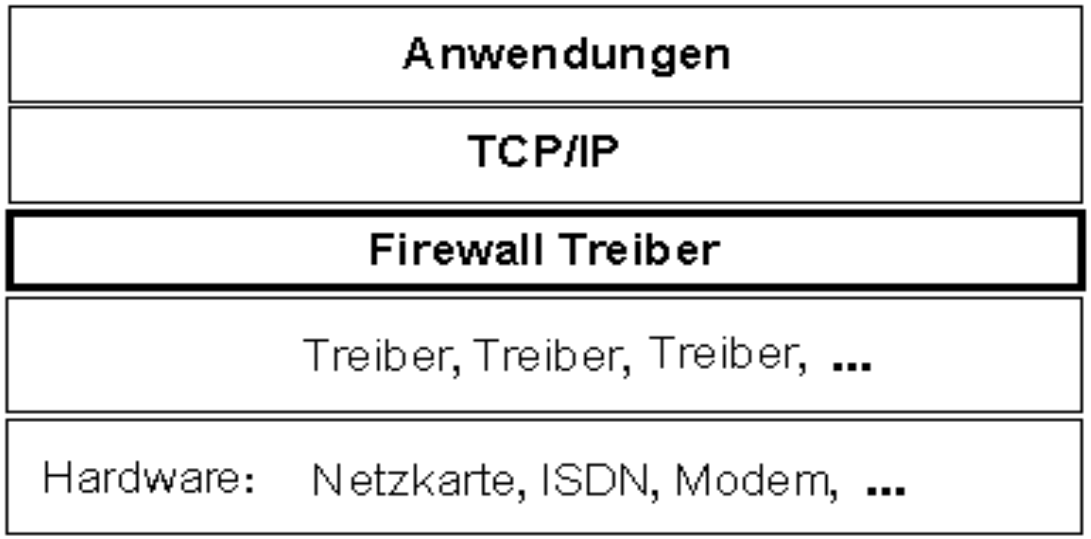
- Die Protokolle
  - TCP (Transmission Control Protocol) und
  - IP (Internet Protocol)

  versehen die einzelnen Datenpakete mit bestimmten Kennungen (Headern).
- Diese Kennungen enthalten standardisierte Informationen, u.a.:
  - von wo kommt das Paket,
  - wohin soll das Paket
  - über welche Kanäle (Portadressen) findet die Kommunikation statt.
- Kerio Firewall arbeitet mit einem Treiber, der diese Kennungen auslesen kann.
- Je nach gesetzter Filterregel wird das Datenpaket dann freigegeben oder blockiert.

Personal Firewalls

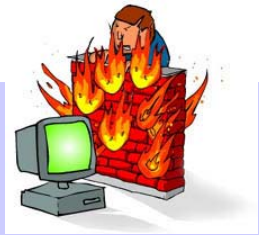


- Der Kerio Treiber setzt sich auf die niedrigste mögliche Stufe, direkt nach den Hardware-Treibern.



- Auf diese Weise ist die Firewall immer die erste Verteidigungslinie bzw. letzte Bastion.
- Durch die Ansiedelung auf dieser Ebene steht der Schutz auch während des Ladevorgangs von Kerio bereits vollständig zur Verfügung .

Personal Firewalls



Die Kerio-Firewall besteht aus drei Komponenten:

PERSFW.exe
Kerio Personal Firewall Engine
Kerio Technologies

1. **Die Firewall-Engine:** Sollte beim Systemstart automatisch geladen werden.

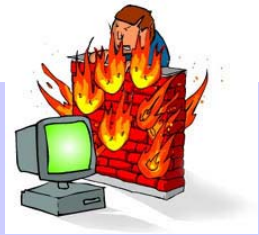
PFWADMIN.exe
Kerio Personal Firewall Console
Kerio Technologies

2. **Das Administrations-Tool:** Zur Konfiguration der Firewall; enthält Regel-Editor und Möglichkeit zur Einstellung allgemeiner Parameter.

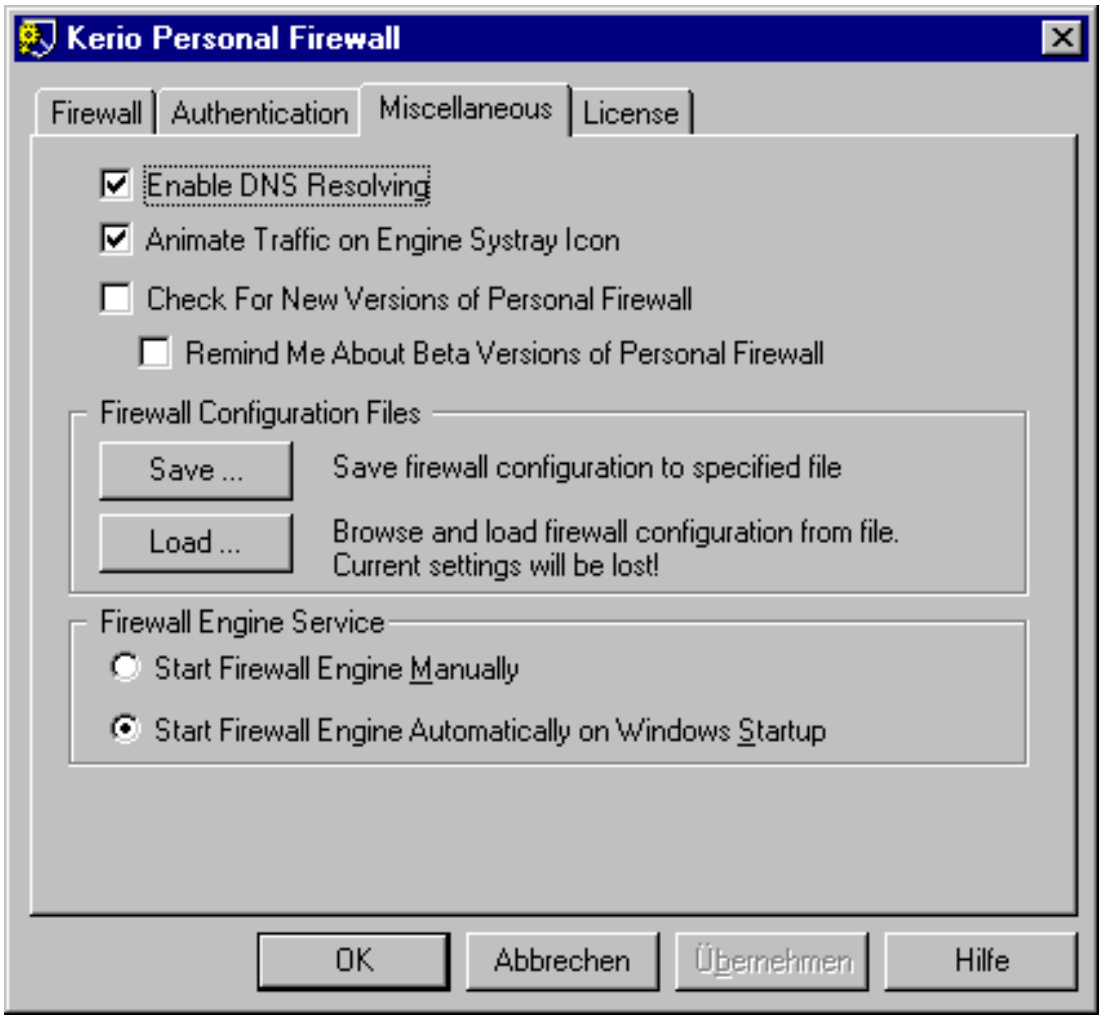
Firewall Status
Kerio Technologies

3. **Der Statusmonitor:** dient zur Anzeige von Logdaten und Status-Parametern wie z.B. die momentan offenen Verbindungen.

Personal Firewalls



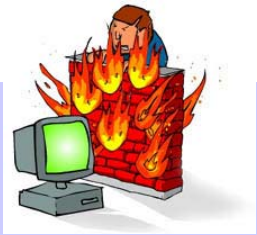
Admin-Tool – Miscellaneous:



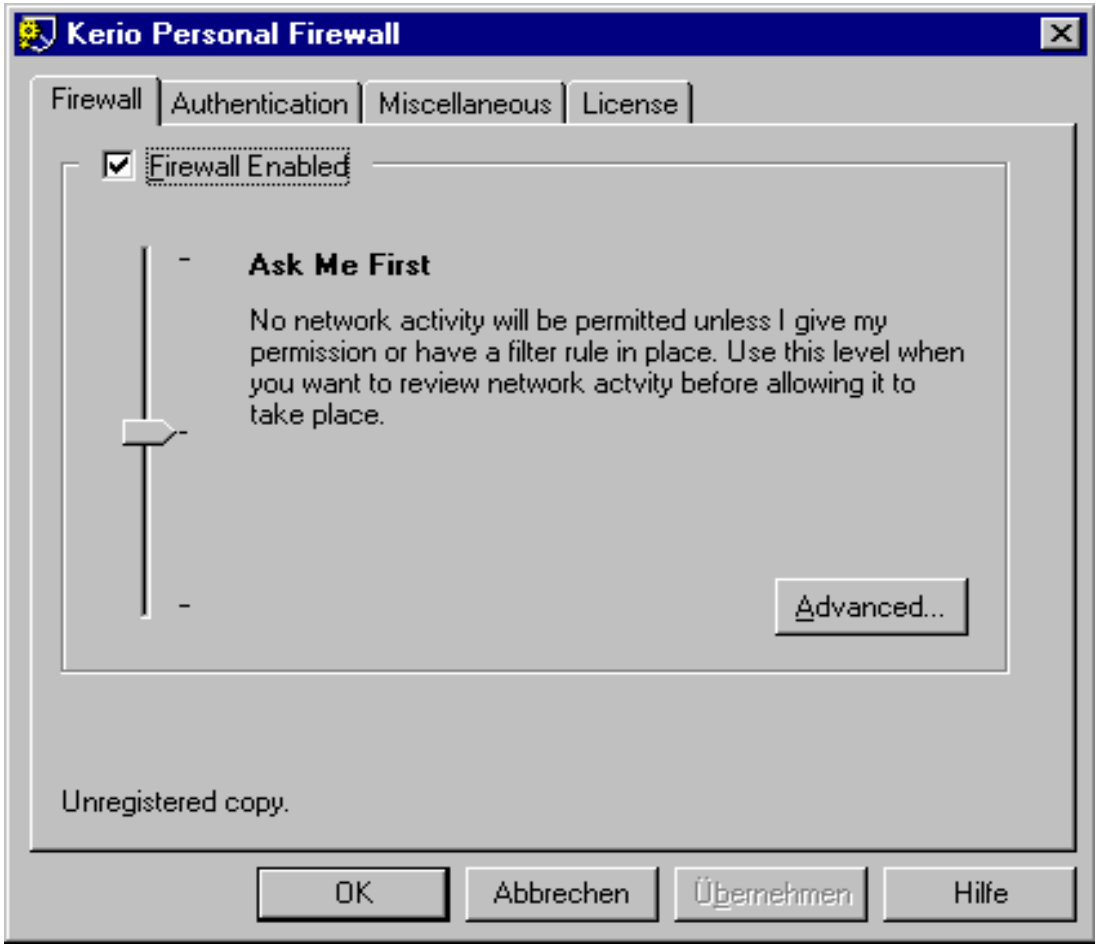
relevante Konfigurationseinstellungen:

- Möglichkeit, alle persönlich vorgenommenen Einstellungen in eine Datei zu speichern.
- Möglichkeit eine Konfigurationsdatei zu laden.
- Hier kann eingestellt werden, dass die Firewall-Engine bei jedem Systemstart automatisch geladen werden soll.

Personal Firewalls



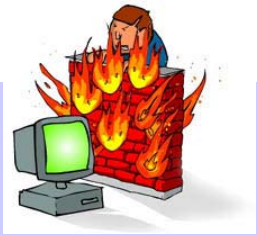
Einstellung des Security-Levels:



Legt Verfahrensweise für Verbindungsanforderungen fest, für die keine Regel existiert:

- Maximum (**Cut Me Off**):
  Alle Verbindungsanforderungen werden ohne Nachfrage verboten.
- Mittlere Einstellung (**Ask Me First**):
  Es wird nachgefragt, ob die Verbindung zugelassen werden soll.
- Minimum (**Permit Unknown**):
  Alle Verbindungen werden zugelassen.

Personal Firewalls



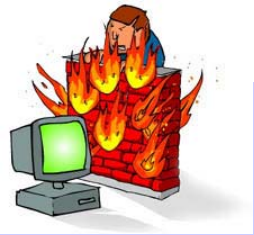
Konfigurationsstrategie 1 :

Security-Level auf „**Permit unknown**“ einstellen.

- Vorteil: Sie sind schnell fertig und die Firewall stört Sie kein bisschen mit unliebsamen Meldungen.

- Ist natürlich nicht zu empfehlen,
- außer Sie haben einen für Ihre Arbeiten perfekt angepassten Regelsatz konfiguriert
- und Sie sind sich 100%-ig sicher, alles bedacht und alles richtig gemacht zu haben.
- Es bleibt also dabei: NICHT ZU EMPFEHLEN!

Personal Firewalls



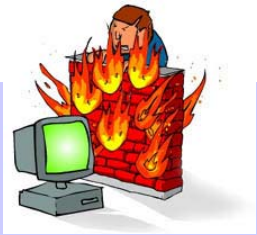
Konfigurationsstrategie 2 : „Lernmodus“

Security-Level auf „**Ask Me First**“ einstellen.

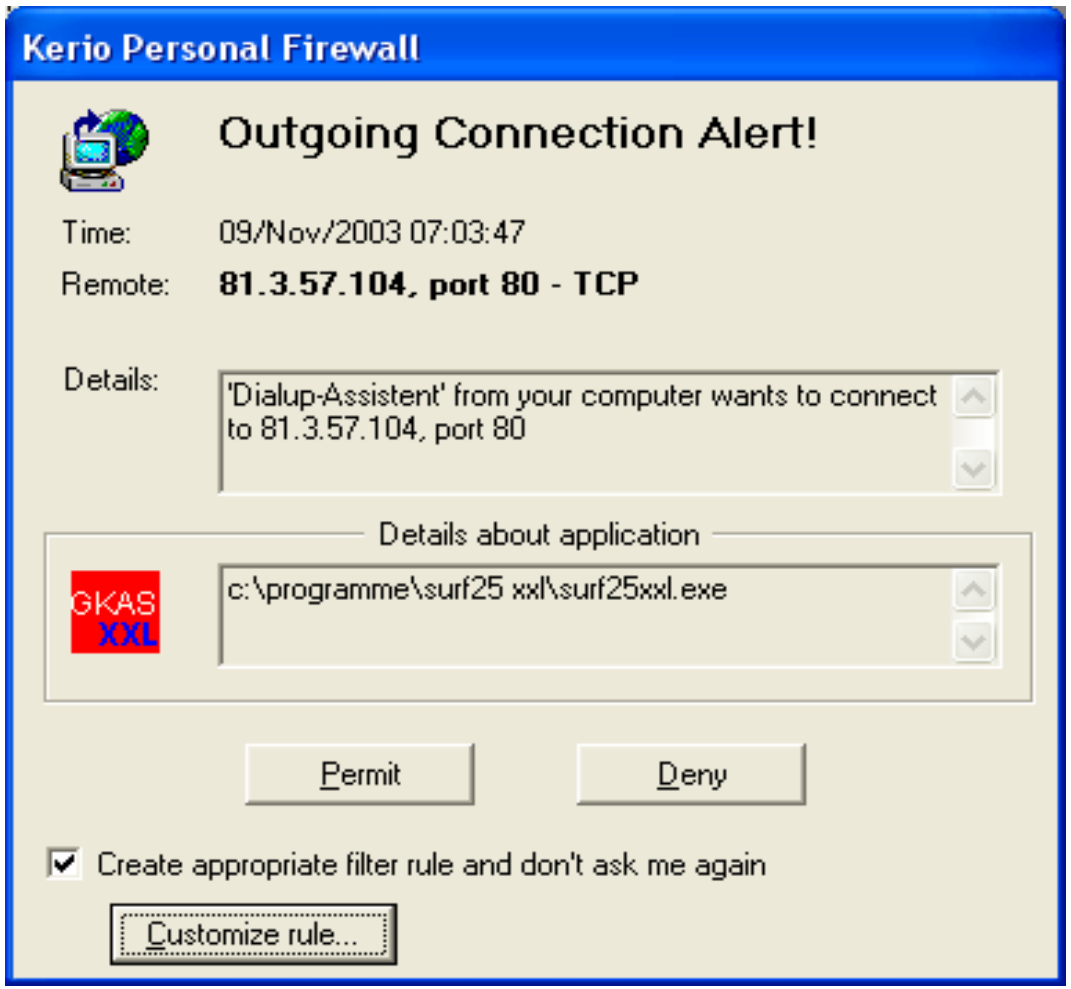
Vorteile:

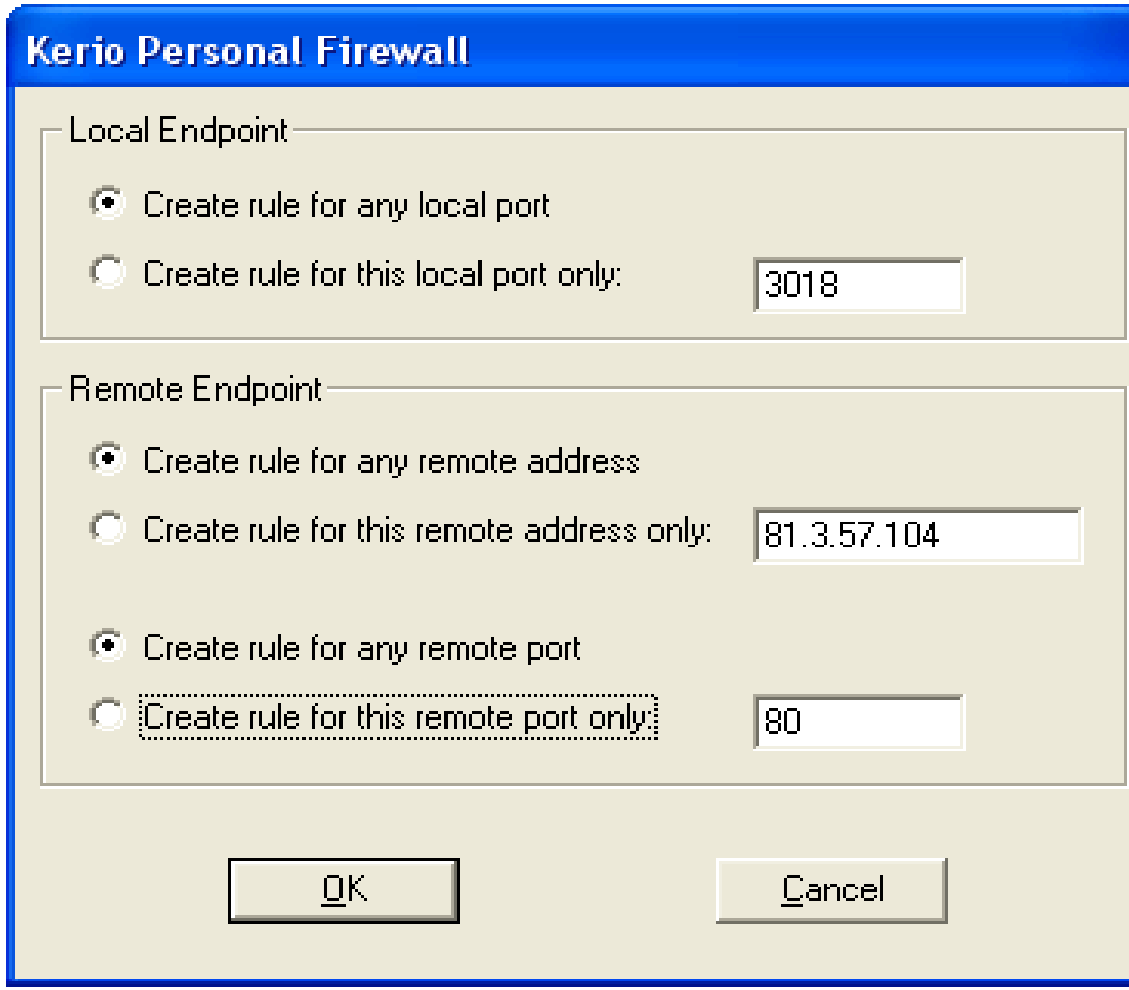
- Sie bekommen alle Verbindungs-Aktivitäten gemeldet und **können** für jeden Vorgang entscheiden, ob die Verbindung erlaubt oder verboten werden soll.
- Sie können die Firewall anweisen, eine passende Regel zu erzeugen und diese auch gleich „nacheditieren“ (dringend empfohlen!).
- Die Firewall lernt auf diese Weise nach und nach, was auf Ihrem Rechner erlaubt und was verboten ist.

Personal Firewalls

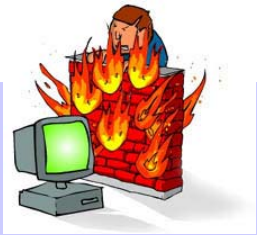


Konfigurationsstrategie 2 : Nacheditieren (Customize rule)





Personal Firewalls

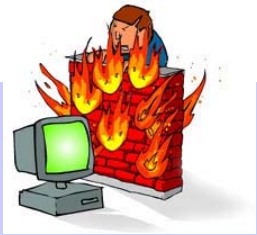


Konfigurationsstrategie 2 : „**Ask Me First**“

Nachteile:

- Sie bekommen alle Verbindungs-Aktivitäten gemeldet und **müssen** für jeden Vorgang entscheiden, ob die Verbindung erlaubt oder verboten werden soll.
- Sie werden wahnsinnig, weil alle 2 Sekunden ein Fenster aufpoppt und Sie entscheiden sollen, ob irgendein xyz.exe raus oder rein darf.
- Sie haben am Ende der Lernphase ein sehr ausuferndes, undurchsichtiges Regelwerk, da für viele eigentlich gleichartige Verbindungen eine eigene Regel erstellt wurde

Personal Firewalls



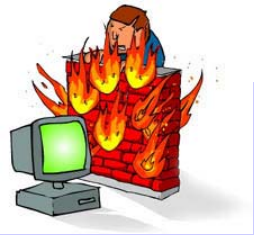
Prognose:

- Völlig entnervt, werden Sie irgendwann anfangen, irgendwelche Verbindungen zu erlauben:
  - Weil Sie nicht genau wissen was die gerade anfragende xyz.exe macht.
  - Weil Sie befürchten, dass sie für Ihr Vorhaben womöglich dringend benötigt wird.
  - Weil Sie endlich mit Ihrer Arbeit anfangen wollen.

Fazit:

- Methode 2 ist nur empfehlenswert für Menschen mit starken Nerven, die immer schon mal ganz genau wissen wollten, was im Hintergrund ihres Rechners so alles läuft.

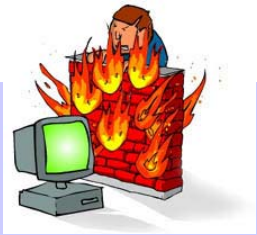
Personal Firewalls



Konfigurationsstrategie 3 : „Geplantes Vorgehen“

- Überlegen Sie, welche Anwendungen Sie benutzen, die Kontakte zu anderen Rechnern benötigen, z.Bsp.:
  - Mailer, Browser,Internet-Einwahlsoftware
  - Netzwerkdrucker usw.
- Erstellen sie das entsprechende Regelwerk.
- Letzte Regel der Liste: die „**Cleanup-Regel**“, die alles von überall nach überall verbietet.
  - Diese Regel soll alle Aktivitäten mitloggen.
  - Diese Regel **muss immer** die letzte Regel sein.

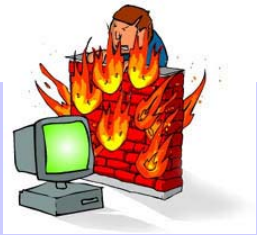
Personal Firewalls



Konfigurationsstrategie 3 : „Geplantes Vorgehen“

- Für jedes Paket, welches an der Firewall vorbei will, wird die Regelliste in der bestehenden Reihenfolge abgearbeitet.
- wird eine „passende Regel“ gefunden wird dementsprechend gehandelt: das Paket darf passieren oder eben nicht.
- Spätestens bei der „Cleanup-Regel“ bleibt das Paket hängen, wird verboten und – entscheidend – in den Logdaten erfasst.
- Der Security-Level auf sollte in diesem Fall „**Ask Me First**“ sein, es kann aber auch „**Deny Unknown**“ gewählt werden.

Personal Firewalls

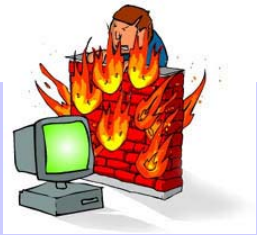


Konfigurationsstrategie 3 : „Geplantes Vorgehen“

Vorteile:

- Ihre wichtigsten Anwendungen sind von vornherein „geregelt“ und laufen gleich.
- Sie brauchen sich nicht mit all den anderen unzähligen Verbindungs-Anfragen beschäftigen (durch „Cleanup“)
- Permanent aufpoppende Verbindungsanfragen fallen weg.
- Durch das Mitloggen der Cleanup-Regel verlieren Sie keine Informationen.
- Nur wenn Sie etwas ausführen wollen und es funktioniert nicht, müssen Sie sich noch einmal mit der Frage der Konfiguration beschäftigen.

Personal Firewalls

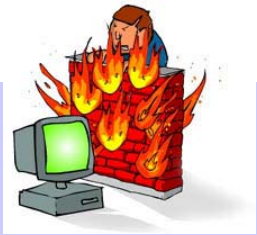


Vorgehen im Fall „etwas funktioniert nicht“:

- Führen Sie die geplante Aktivität durch und merken Sie sich die Uhrzeit.
- Aus den Logdaten können Sie ersehen, welche Art Verbindung für Ihre gewünschte Aktivität nötig ist.
- Erstellen Sie eine entsprechende Regel.
- Testen Sie erneut, ob ihre Anwendung nun funktioniert.
- Wenn nicht: Erneute Überprüfung der Logdaten.
- Anschließende Anpassung der Regel (ev. Erweiterung der Portliste oder des IP-Bereiches).

Wiederholen Sie diese Schritte , bis die Regel richtig angepasst ist.

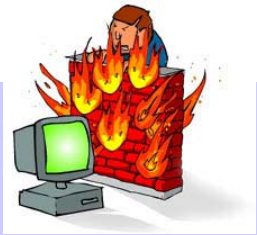
Personal Firewalls



Kerio Personal Firewall - Log Window

```
[08/Nov/2003 19:01:02] Rule 'Block All': Blocked: In ICMP [8] Echo Request, 212.188.99.28->localhost, Owner: Tcpip Kernel Driver
[08/Nov/2003 19:01:10] Rule 'Block All': Blocked: In ICMP [8] Echo Request, 212.188.96.97->localhost, Owner: Tcpip Kernel Driver
[08/Nov/2003 19:01:59] Rule 'Block All': Blocked: In TCP, 212.183.243.235:4307->localhost:135, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:02:31] Rule 'Block All': Blocked: In TCP, 212.183.200.120:2458->localhost:135, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:04:12] Rule 'Block All': Blocked: In TCP, 212.185.208.79:1619->localhost:135, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3035->194.25.134.97:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3036->194.25.134.24:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3037->194.25.134.25:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3038->194.25.134.26:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3039->194.25.134.27:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3040->194.25.134.32:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3041->194.25.134.33:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3042->fwd01.sul.t-online.com [194.25.134.88:25], Owner: C:\PROGRAMME\NETSCAF
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3043->194.25.134.89:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3044->194.25.134.90:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3045->194.25.134.91:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:05:00] Rule 'Block All': Blocked: Out TCP, localhost:3046->194.25.134.96:25, Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\NETSCP.I
[08/Nov/2003 19:06:38] Rule 'Block All': Blocked: In TCP, 213.93.37.152:3055->localhost:443, Owner: no owner
[08/Nov/2003 19:06:41] Rule 'Block All': Blocked: In TCP, e37152.upc-e.chello.nl [213.93.37.152:3055]->localhost:443, Owner: no owner
[08/Nov/2003 19:06:47] Rule 'Block All': Blocked: In TCP, e37152.upc-e.chello.nl [213.93.37.152:3055]->localhost:443, Owner: no owner
[08/Nov/2003 19:07:56] Rule 'SMTP': Permitted: Out TCP, localhost:3051->fwd11.sul.t-online.com [194.25.134.97:25], Owner: C:\PROGRAMME\NETSCAF
[08/Nov/2003 19:09:01] Rule 'Block All': Blocked: In TCP, 212.185.214.128:3710->localhost:135, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:09:54] Rule 'Block All': Blocked: Out TCP, localhost:3091->localhost [127.0.0.1:3090], Owner: C:\PROGRAMME\NETSCAPE\NETSCAPE 7\I
[08/Nov/2003 19:11:54] Rule 'Block All': Blocked: Out UDP, localhost:3093->239.255.255.250:1900, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:11:54] Rule 'Block All': Blocked: Out UDP, localhost:3093->239.255.255.250:1900, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
[08/Nov/2003 19:11:57] Rule 'Block All': Blocked: Out UDP, localhost:3093->239.255.255.250:1900, Owner: C:\WINDOWS\SYSTEM32\SVCHOST.EXE
```

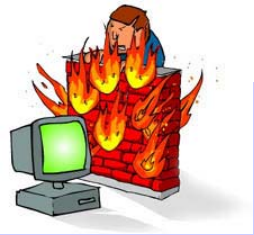
Personal Firewalls



Kerio Personal Firewall - Log Window

```
[04/Nov/2003 10:01:06] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:01:07] Rule 'Asterix bpinetd.exe': Permitted: In TCP, 130.75.6.20:569->localhost:13782, Owner: C:\PROGRAMME\VERITAS\NETBACKUP
[04/Nov/2003 10:01:10] Rule 'Asterix bpcd.exe': Permitted: Out TCP, localhost:521->asterix-a.rrzn.uni-hannover.de [130.75.6.20:517], Owner: C:\PROGR.
[04/Nov/2003 10:01:28] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:01:37] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:01:59] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:02:08] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:02:30] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:02:39] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:03:00] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:03:10] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:03:13] Rule 'Block All': Blocked: In TCP, ring.ifa.uni-hannover.de [130.75.60.38:3182]->localhost:445, Owner: no owner
[04/Nov/2003 10:03:16] Rule 'Block All': Blocked: In TCP, ring.ifa.uni-hannover.de [130.75.60.38:3182]->localhost:445, Owner: no owner
[04/Nov/2003 10:03:32] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:03:41] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:04:03] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:04:12] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:04:34] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:04:43] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:05:05] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:05:14] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:05:36] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:05:45] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:06:07] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:06:16] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:06:38] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:06:47] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:07:09] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
[04/Nov/2003 10:07:18] Rule 'Block All': Blocked: In UDP, pc213-1b.rrzn.uni-hannover.de [130.75.5.14:631]->localhost:631, Owner: no owner
```

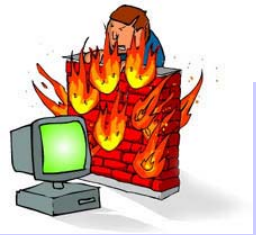
Personal Firewalls- Standardregeln

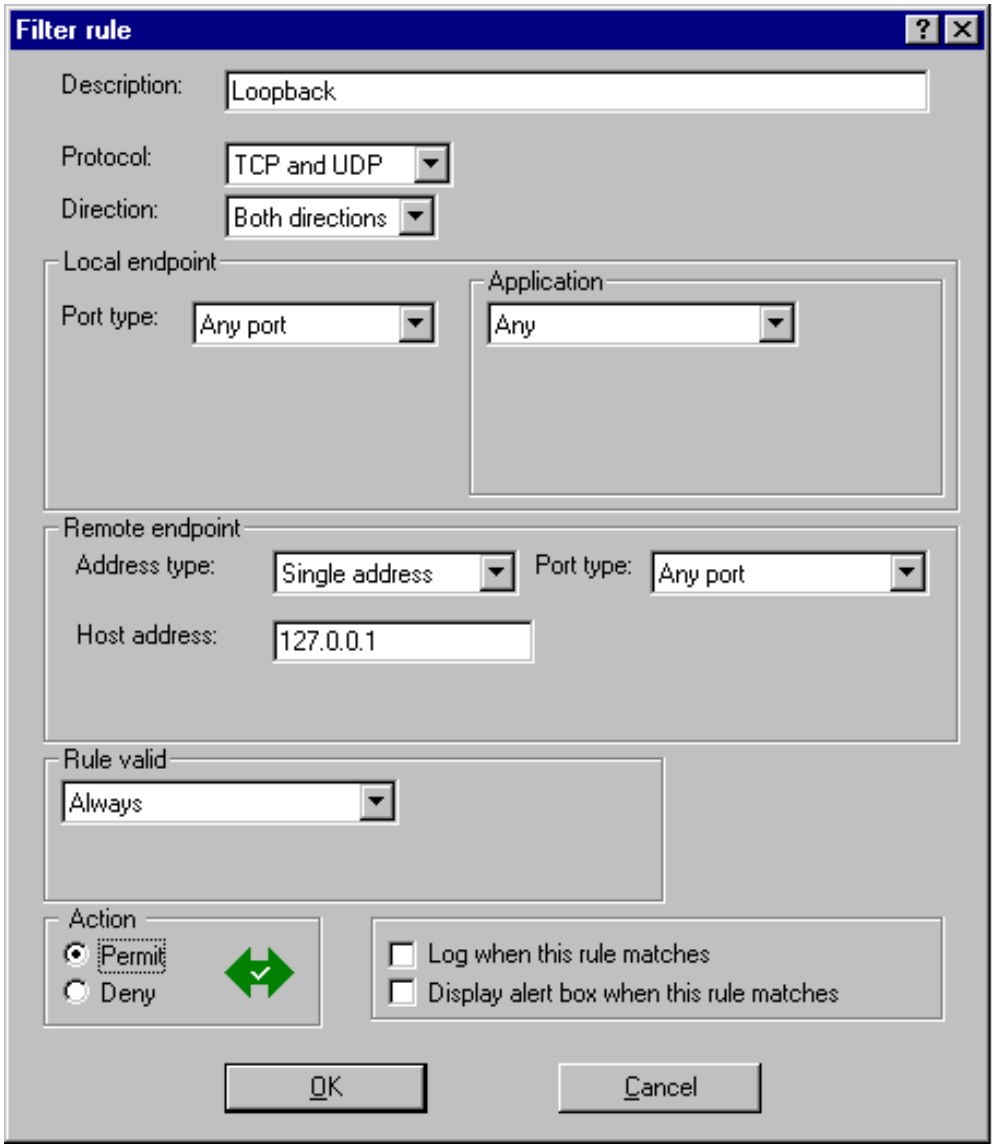


Abkürzungen für Beschreibung der Standardregeln:

D:	Description	Vergeben Sie einen Namen für die Regel
P:	Protokoll	[Any] [TCP] [UDP] [TCP and UDP] [ICMP] [Other]
DI:	Direction	[Incoming] [Outgoing] [Both directions]
LP:	Local Port	[Any port] [Single port] [Port/Range] [List of ports]
A:	Application	[Any] [Only selected below]
RP:	Remote Port	[Any port] [Single port] [Port/Range] [List of ports]
RA:	Remote Address	[Any addr.] [Single addr.] [Network/Mask] [Network/Range] [Custom address group]
Val:	Rule Valid	[Always] [In this interval only]

Personal Firewalls - Standardregeln





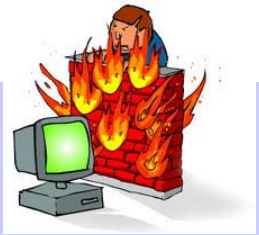
Loopback-Regel:

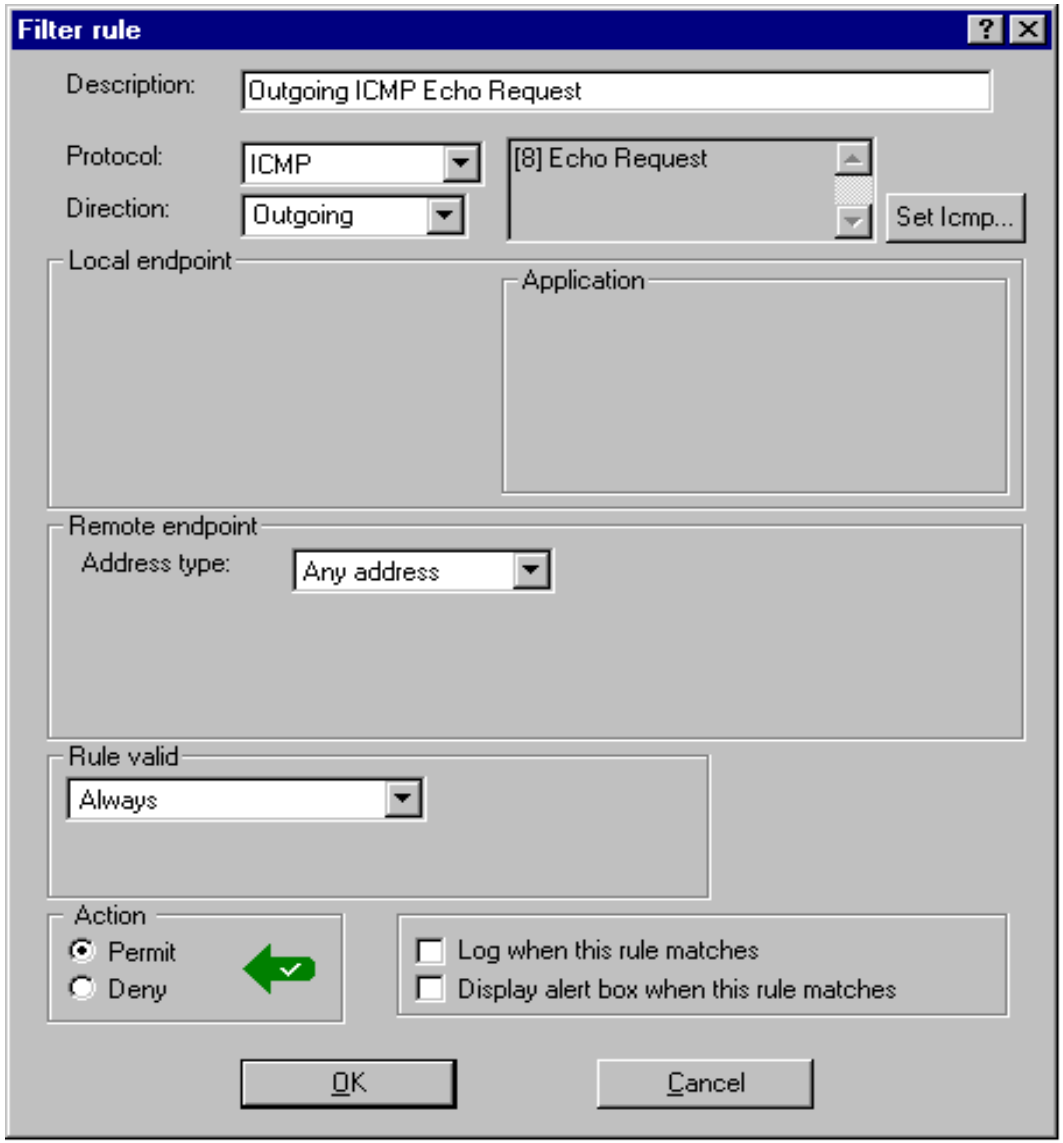
- Die besondere IP 127.0.0.1 repräsentiert den lokalen Rechner.
- Dient der Überprüfung, ob TCP/IP korrekt arbeitet.

D: Loopback
P: TCP and UDP
DI: Both
LP: Any port
A: Any
RA: Single: 127.0.0.1
RP: Any port
Val: Always

Permit

Personal Firewalls - Standardregeln





ICMP : Internet Control Message Protocol

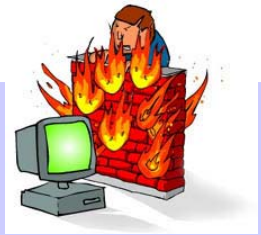
- Protokoll zur Übermittlung von Fehlermeldungen und Informationen.

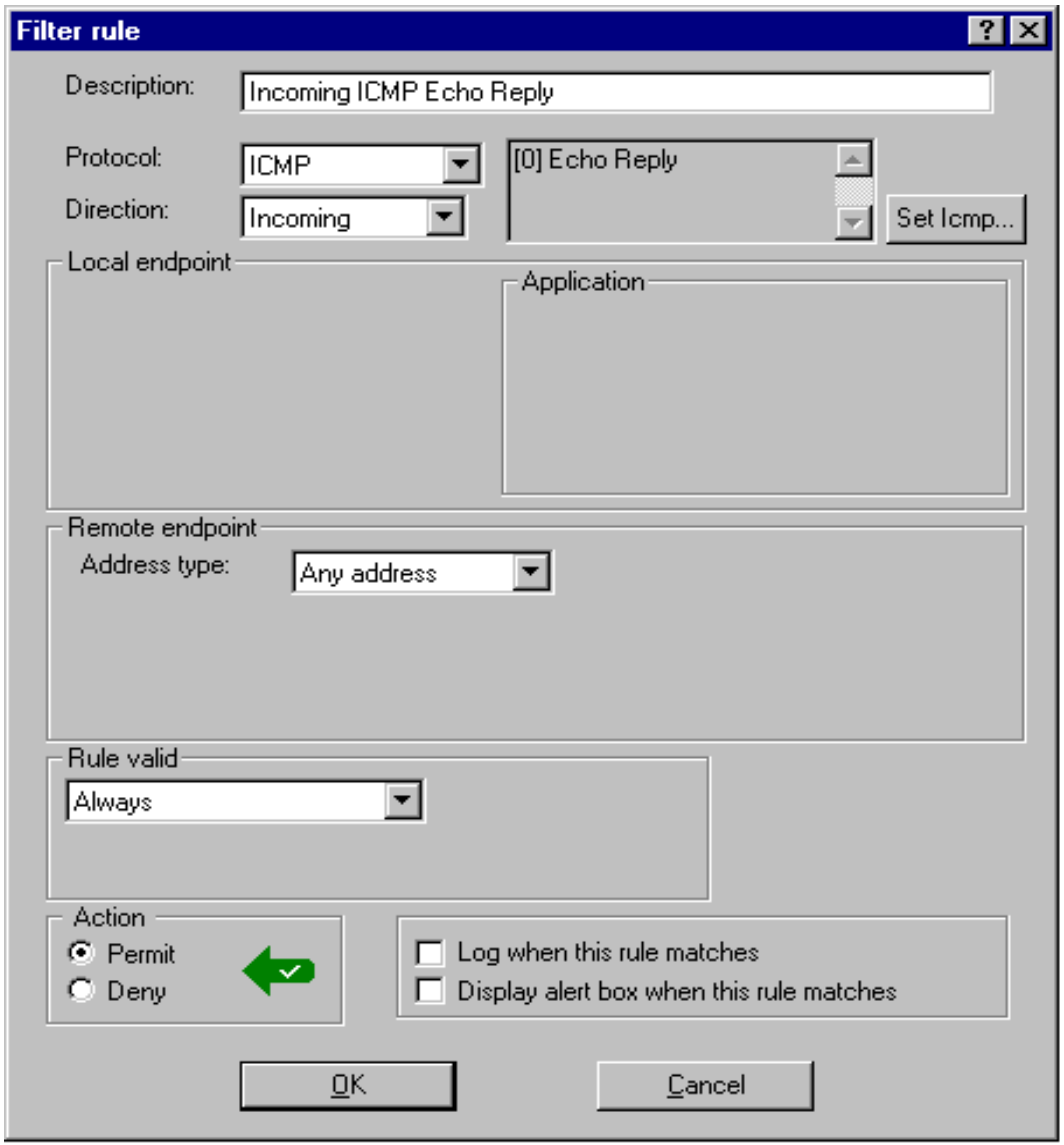
Echo Request = Ping

D: Outgoing ICMP Echo Request
P: ICMP / Echo Request
DI: Outgoing
LP: -
A: -
RA: Any address
RP: -
Val: Always

Permit

Personal Firewalls - Standardregeln



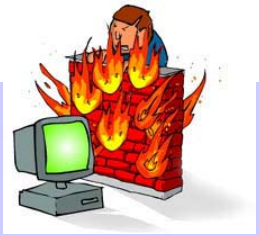


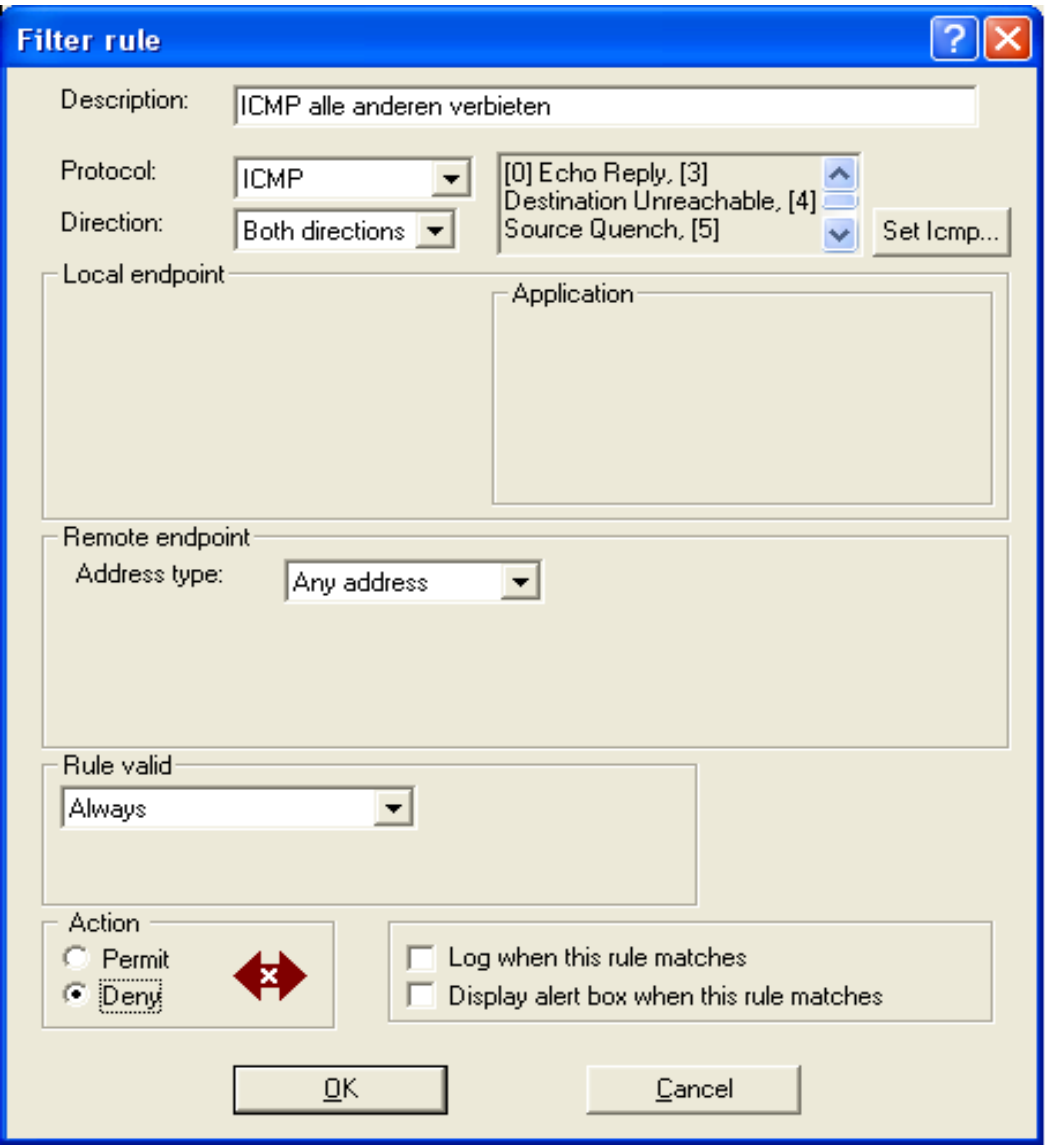
ICMP Echo Reply = Antwort auf Ping

D: Incoming ICMP Echo Reply
P: ICMP / Echo Reply
DI: Incoming
LP: -
A: -
RA: Any address
RP:-
Val: Always

Permit

Personal Firewalls - Standardregeln





Alle restlichen ICMP-Kommandos verbieten:

D: ICMP alle anderen

P: ICMP / Echo Reply

DI: Both directions

LP: -

A: -

RA: Any address

RP: -

Val: Always

Deny

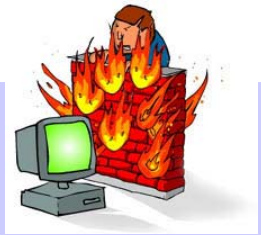
Eventuell noch folgende ICMP erlauben:

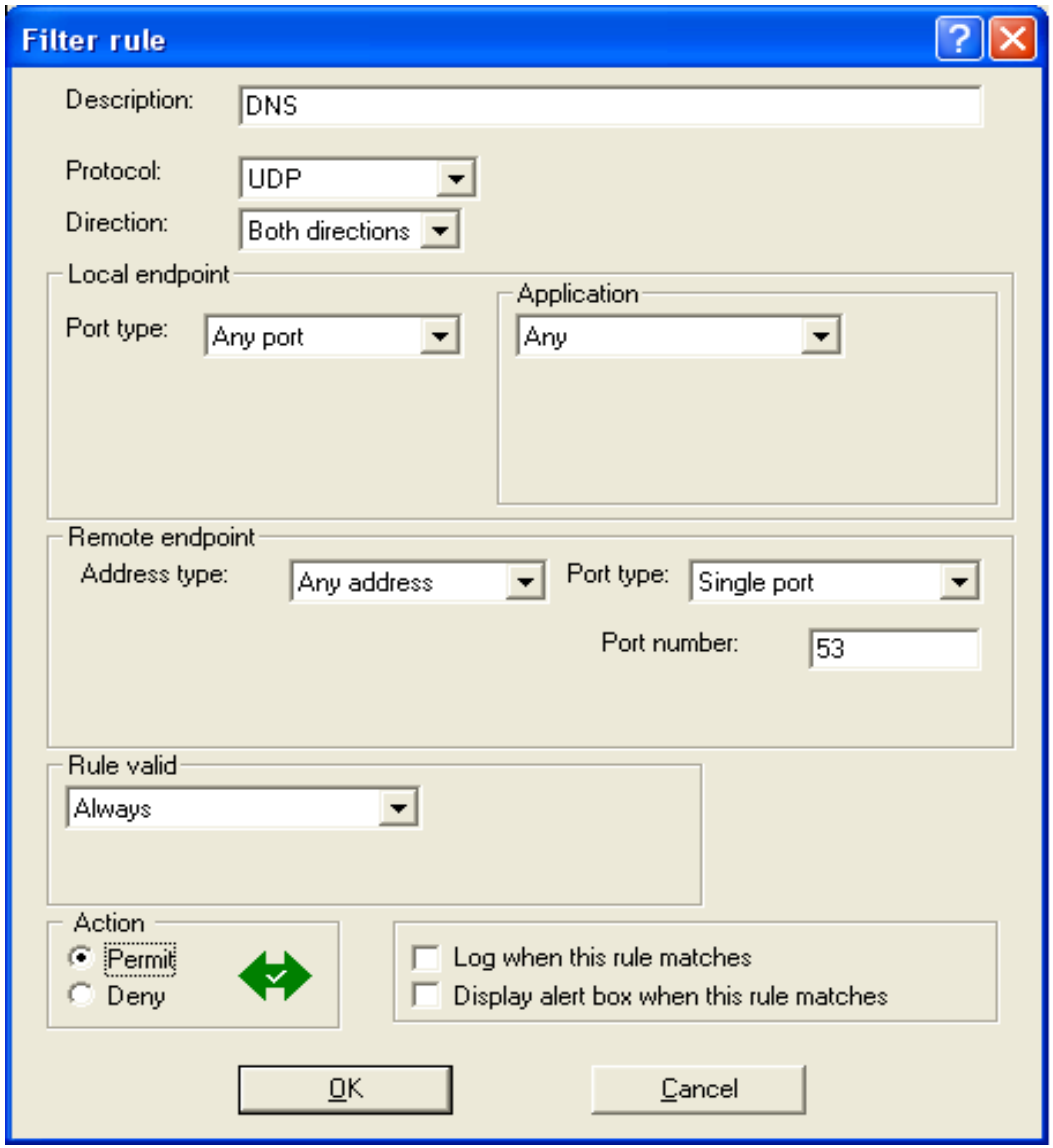
outgoing: Traceroute und

incoming: Time Exceeded,

Destination unreachable

Personal Firewalls - Standardregeln





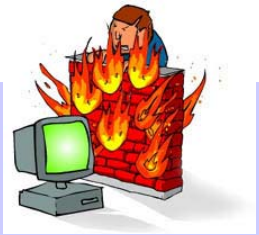
DNS (Domain Name Service):

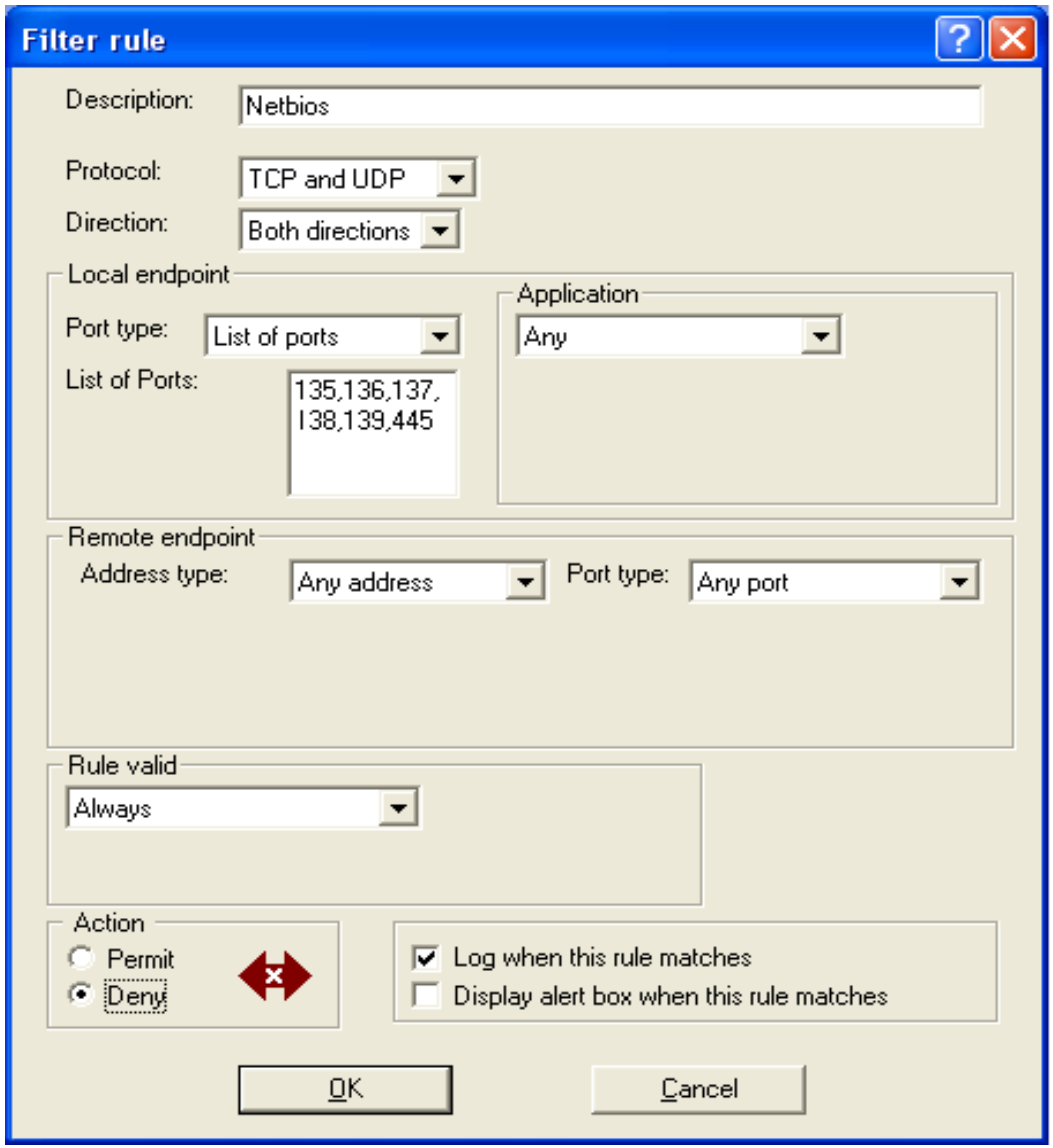
- Der Kontakt zwischen PC und Name-Server muss möglich sein, damit die IP-Adresse in einen Hostnamen aufgelöst werden kann.

D: DNS
P: Any
DI: Both
LP: Any port
A: Any
RA: Single address 130.75.x.x
RP: Single port 53
Val: Always

Permit

Personal Firewalls - Standardregeln





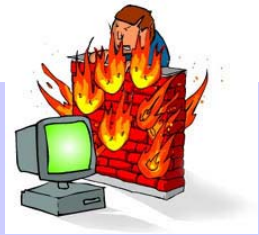
Netbios:
(Net-Basic-Input-Output-System; IBM)

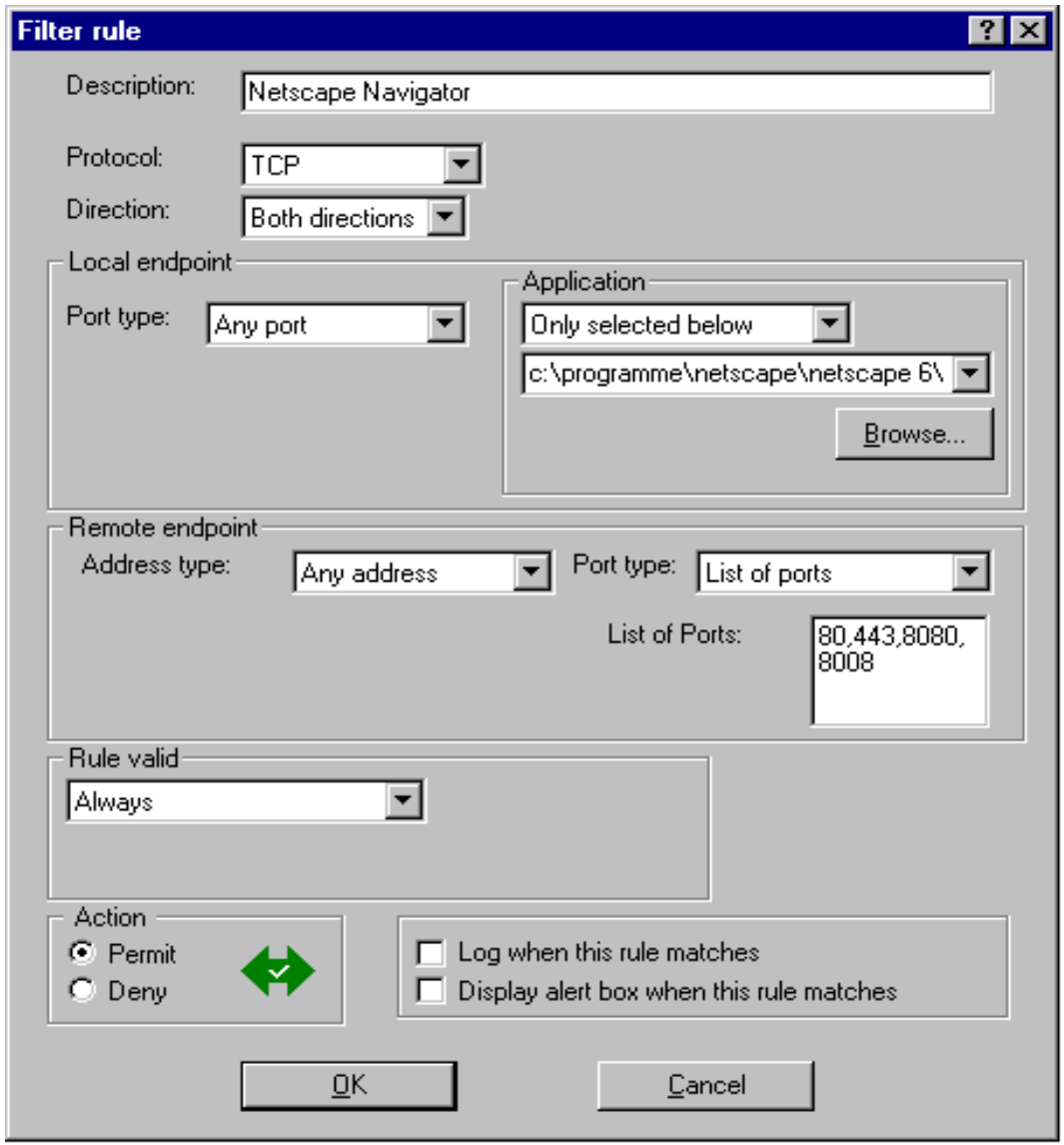
- Möglichkeit, Drucker und Ressourcen für das Netz freizugeben.
- Wird abgewickelt über die Ports 135-139 bzw. 445
- Großes Einfallsstor für Angriffe (Blaster!)

D: Netbios
P: TCP and UDP
DI: Both
LP: List of ports 135-137,445,
A: Any
RA: Any
RP: Any port
Val: Always

Deny

Personal Firewalls - Standardregeln





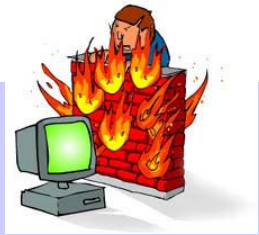
Internet-Anwendung: Browser

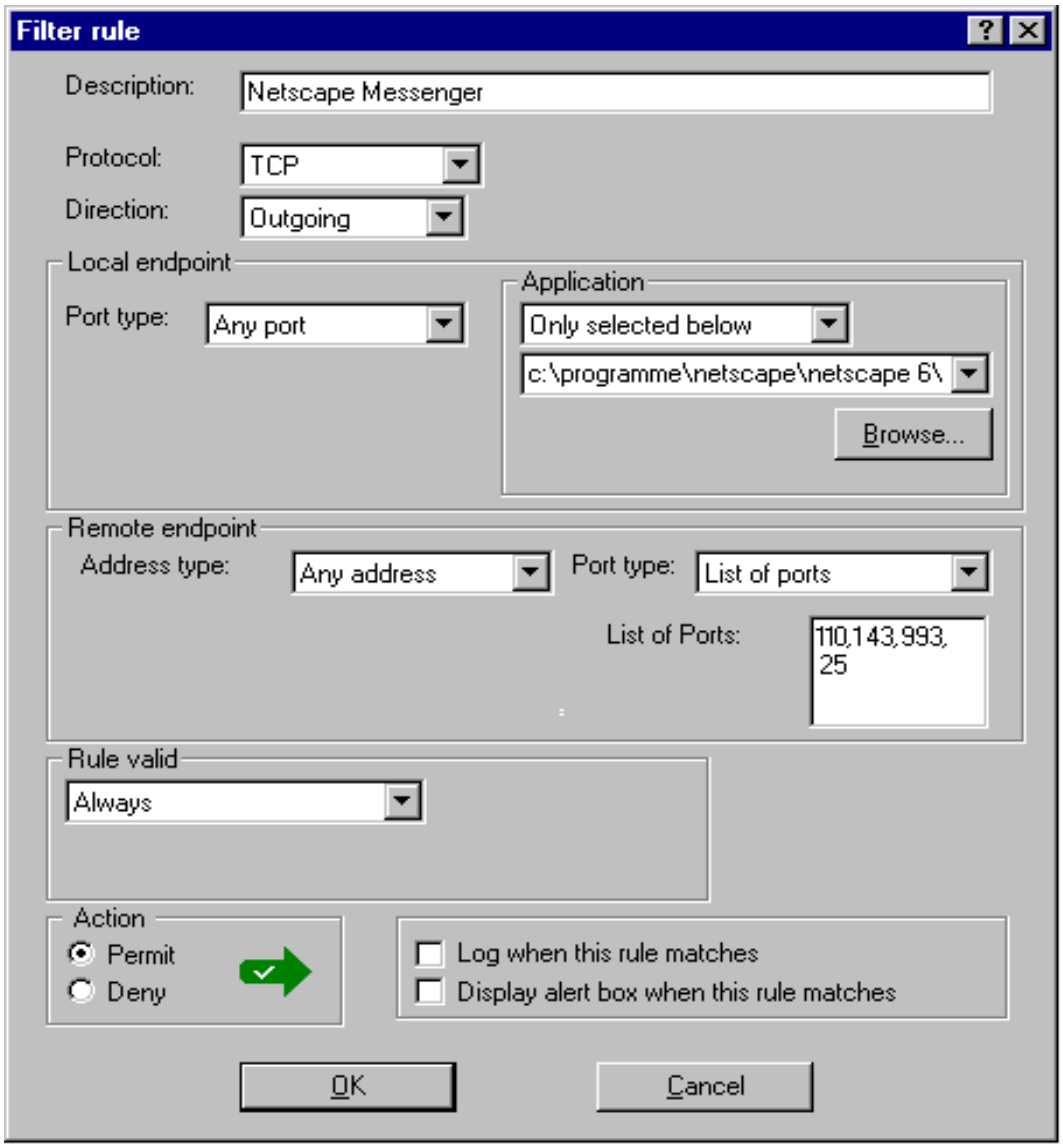
D: Hier: Netscape Navigator
P: TCP
DI: Both
LP: Any port
A: Only selected below: hier: Netscape
RA: Any address
RP: List of ports; 80,443,8080
Val: Always

Permit

Wenn Sie sich über eine Anwendung ins Internet einwählen, wie z.B. T-Online, müssen Sie die entsprechende Datei ebenfalls erlauben.

Personal Firewalls - Standardregeln





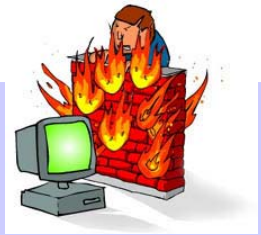
Internet-Anwendung: E-Mail

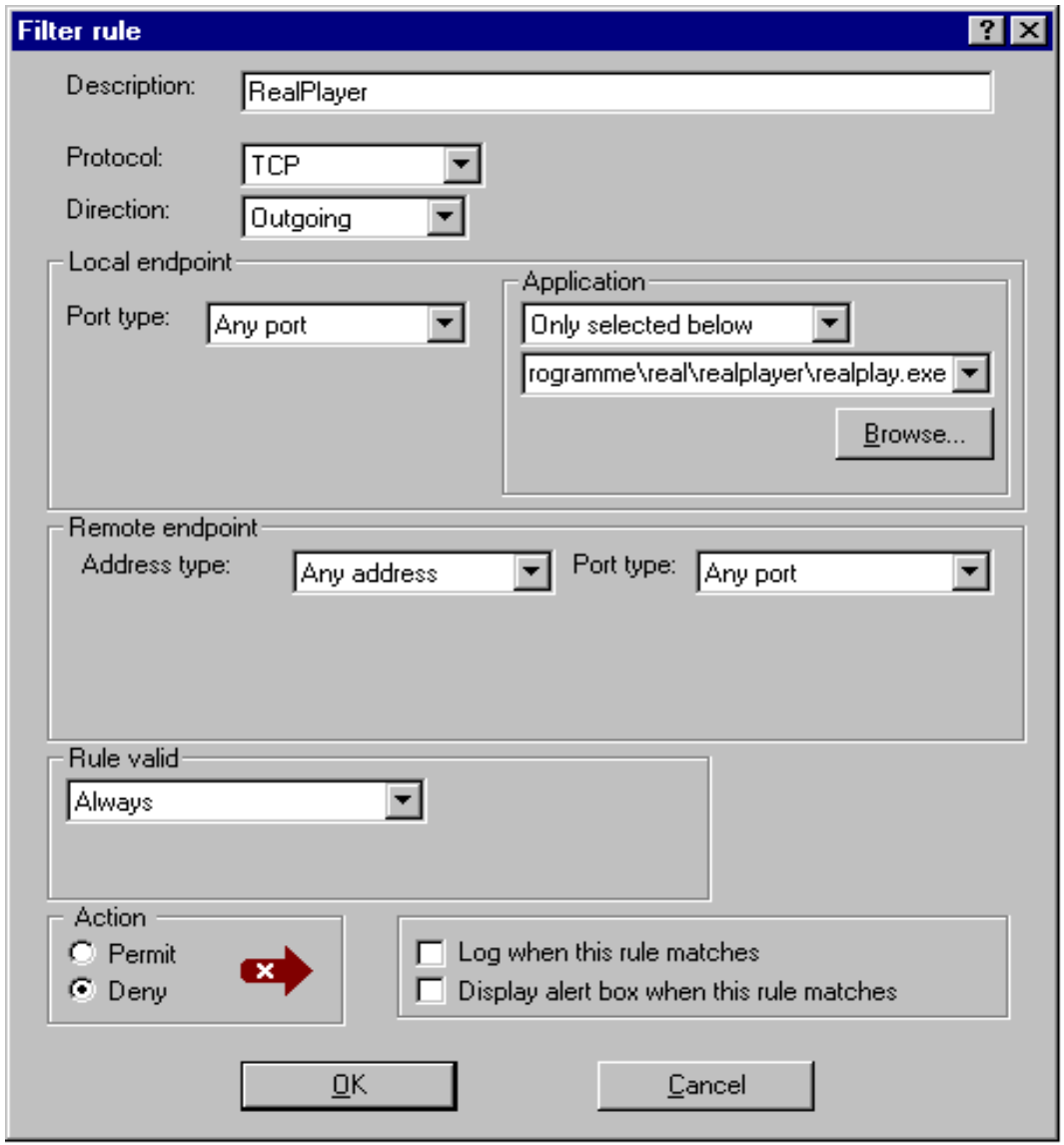
Mail versenden: Port 25 (SMTP)
Mail empfangen: Port 110 (POP)
Port 143 (IMAP)
Port 993 (secure imap)
Port 995 (secure pop)
Port 119 (News)

D: Hier: Netscape Messenger
P: TCP
DI: Outgoing
LP: Any port
A: Only selected below: hier:Netscape
RA: Any address oder Single address
RP: List of ports; 25, 110,143, 993, 995, (119)
Val: Always

Permit

Personal Firewalls - Standardregeln





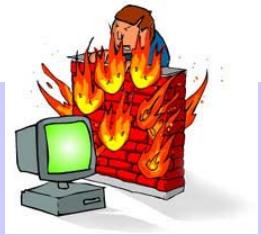
Real Player als Beispiel für kontaktfreudige Anwendung:

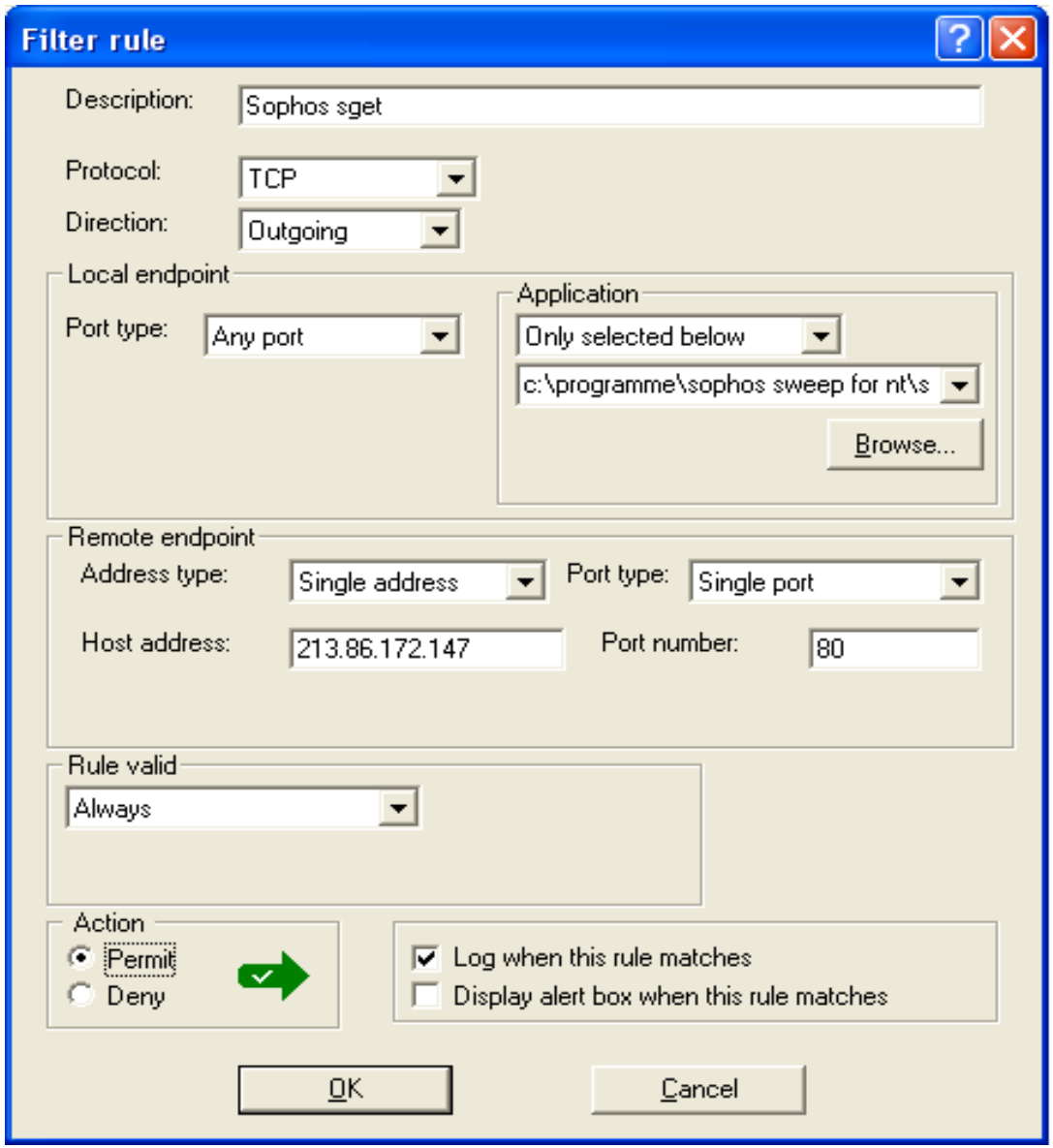
- Real Player versucht dauernd Kontakt nach außen aufzunehmen und Informationen zu versenden.
- Wenn man Ihn nicht deinstallieren möchte, wenigstens die Kontakte nach außen verbieten.

D: Real Player
P: Any
DI: Both
LP: Any port
A: realplay.exe
RA: Any address
RP: Any port
Val: Always

Deny

Personal Firewalls - Standardregeln





Regel für sget:

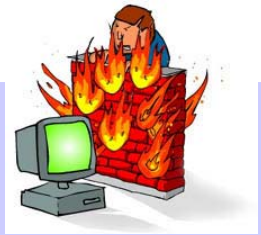
- sget.exe hold von Sophos-Server die aktuellsten DIE-Dateine auf den lokalen Rechner.
- Ab und zu überprüfen, ob Sophos ev. die IP gewechselt hat.

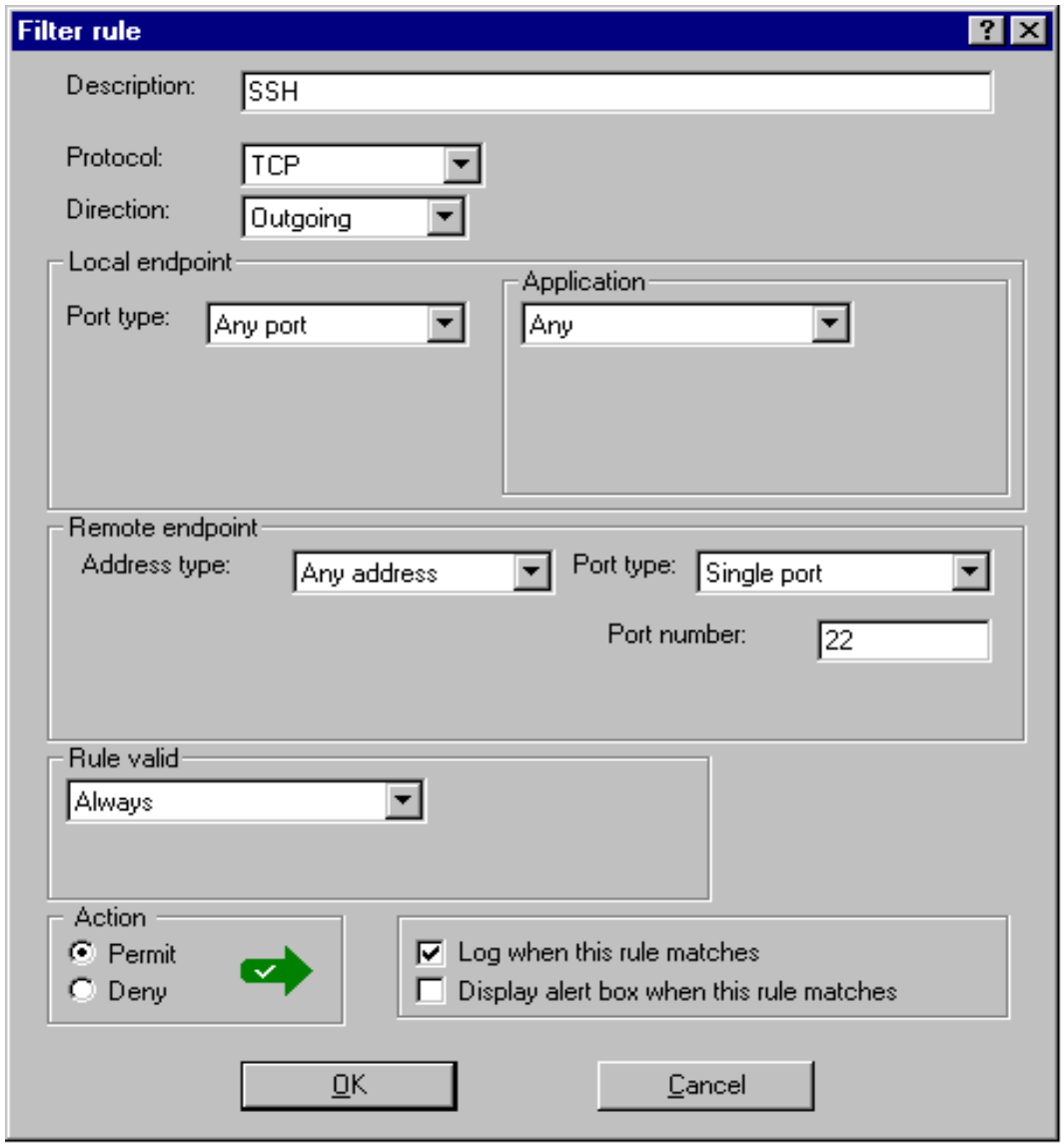
D: Sophos sget

P: TCP
DI: Outgoing
LP: Any port
A: sget.exe
RA: Single: 213.86.172.147
RP: 80
Val: Always

Permit

Personal Firewalls - Standardregeln



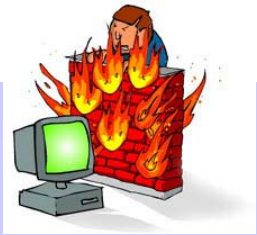


Optional: SSH

D: SSH
P: TCP
DI: Outgoing
LP: Any port
A: Any oder spezieller SSH-Client
RA: Any address
RP: Single port; 22
Val: Always

Permit

Personal Firewalls - Standardregeln



Optional: Netbackup über Asterix; es werden zwei Regeln benötigt

Regel 1

D: Asterix in bpinetd.exe
P: TCP
DI: Incoming
LP: Any port
A: Only selected below
C:\Programme\VERITAS\…
RA: Single address 130.72.6.20
RP: Any
Val: Always

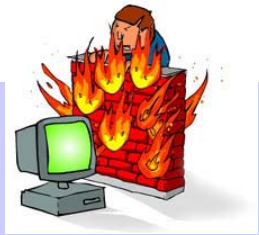
Permit

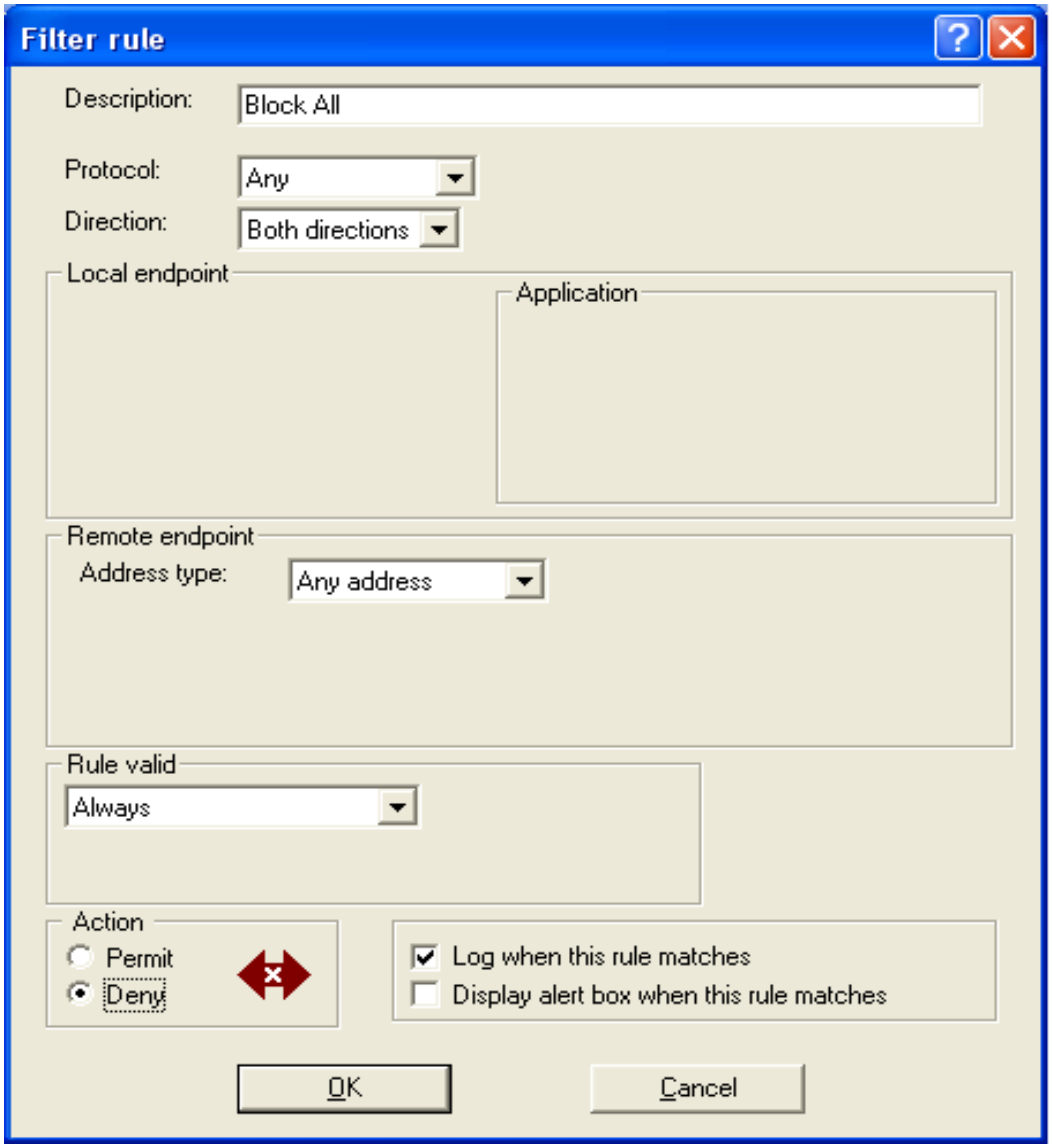
Regel 2

D: Asterix out bpcd.exe
P: TCP
DI: Outgoing
LP: Any port
A: Only selected below
C:\Programme\VERITAS\…
RA: Single address 130.72.6.20
RP: Any
Val: Always

Permit

Personal Firewalls - Standardregeln





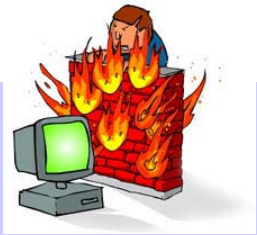
Cleanup-Regel:

- Alle Anforderungen, die zu dieser Regel „vorstoßen“ werden als unerwünscht behandelt und blockiert.
- **Bei dieser Regel immer mitloggen**, damit die Geschehnisse nachzuvollziehen sind

D: Block ALL
P: Any
DI: Both
LP: -
A: -
RA: Any address
RP: -
Val: Always

Deny

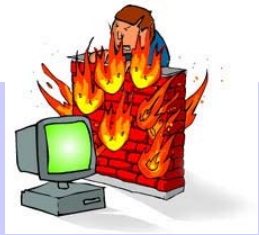
Personal Firewalls – svchost.exe



Hinweise zu **svchost.exe** unter Windows 2000 und XP:

- führt zwar keine „Spionage“ durch, ist aber in ihrer Tätigkeit etwas undurchsichtig
- svchost ist ein allgemeiner Prozessname, für eine vom Betriebssystem zusammengestellte Liste von Diensten.
- kann in mehreren Instanzen laufen, jede einzelne svchost.exe-Sitzung kann eine unterschiedliche Gruppe von Diensten enthalten
- Dabei können auch Dienste enthalten sein, die von Angreifern ausgenutzt werden können.
- Eventuell funktioniert die Internetanbindung nicht mehr , wenn der Datei svchost.exe alle Verbindungen gekappt werden.
- Vorgehen: zuerst probieren, ob eventuell alles läuft, obwohl svchost keine Verbindungen zugestanden werden.

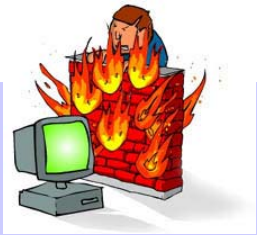
Personal Firewalls – svchost.exe



Im Fall von Problemen, benutzen Sie zusätzlich folgende Regeln für svchost.exe:

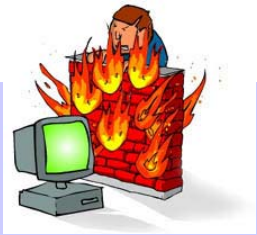
- **Erlaube DHCP**
  Protokoll: UDP
  Lokaler Port: 68
  Remote Host: Any
  Remote Port: 67
  Richtung: Incoming
  Aktion: Permit
- **Erlaube Zeitsynchronisierung**
  Protokoll: UDP
  Remote Port: 123
  Richtung: Both
  Aktion: Permit
- **Erlaube HTTP Verbindung**
  Protokoll: TCP
  Lokaler Port: Any
  Remote Host: Any
  Remote Port: 80
  Richtung: Outgoing
  Aktion: Permit
- **Erlaube HTTPS Verbindung**
  Protokoll: TCP
  Remote Port: 443
  Richtung: Outgoing
  Aktion: Permit

Personal Firewalls – svchost.exe



- **Blockiere „SSDP Discovery Service“ und „UPnP device Host“ Services**
  Protokoll: UDP and UDP
  Remote Host: 239.255.255.250
  Port List: 1900,5000
  Richtung: Incoming
  Aktion: Deny
- **Blockiere „Remote Procedure Call“ (Wenn nicht schon durch Netbios-Regel blockiert)**
  Protokoll: TCP
  Lokaler Port: 135
  Remote Host: Any
  Richtung: Both
  Aktion: Deny

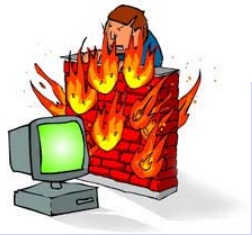
Personal Firewalls



Allgemeine Hinweise:

- Schauen Sie regelmäßig in die Logdaten.
- Sie werden erstaunt sein, was um Ihren Rechner herum alles los ist.
- Lassen Sie sich durch die Vielzahl der dokumentierten Kontakte nicht irritieren und verunsichern:
  - Dieser ganze Verkehr war auch schon existent, bevor Sie die Firewall installiert hatten.
  - Der Unterschied: jetzt können Sie sehen, was vorher unbemerkt blieb
  - Versuchen Sie nicht, jedem Portscan nachzugehen, „Ermittlungsarbeit“ bringt meistens nichts und vergeudet Ihre Zeit.

Personal Firewalls



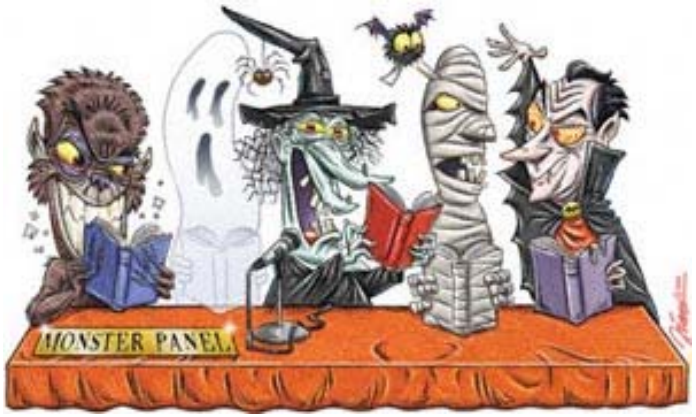
Outpost

- Version 1.0 ist unter http://www.agnitum.com/download/outpost1.html frei verfügbar.
- Möglichkeit. Plugins zu laden (reichen von Werbefiltern bis hin zu rudimentärer Abwehr von Angriffen)
- Sogenanntes „Preset“:
  - Vordefinierte „Regelszenarien“ für unerfahrene Anwender.
  - Können nach und nach ergänzt und verändert werden
- Sehr ausführliches Handbuch in deutscher Sprache verfügbar unter: http://www.agnitum.com/download/Outpost_User_Guide_(GER).pdf

Sicherheit für Anwender: Specials

Themen:

Weitere Bosheiten, Belästigungen und Gefahren



- Hoaxes
- SPAM
- Spyware
- 0190-er Dialer

Was ist ein Hoax

- Hoax = Scherz
- Hoaxes sind Warnungen vor Viren, die es gar nicht gibt
- Hoaxes werden per E-Mail verbreitet und
  - warnen vor angeblichen **Viren, die sich per E-Mail verbreiten** oder
  - vor angeblich **virenverseuchten Dateien**, die man auf seinem System suchen und löschen soll

Woran erkennt man Hoaxes

- Die Viren, vor denen gewarnt wird, werden ausnahmslos als „sehr gefährlich“ eingestuft.
- Meist wird noch darauf hingewiesen, dass noch kein Virenscanner den Virus identifizieren kann.
- Benennung namhafter Firmen, welche die Gefährlichkeit des Virus angeblich bestätigt haben - oft AOL, IBM oder Microsoft.
- **Ein untrügliches Anzeichen für einen Hoax ist die Aufforderung, die Warnung so schnell wie möglich an alle Bekannten weiterzuleiten**.
- Generell: es werden **NIE** echte Virenwarnungen per Kettenbrief durch die Welt geschickt, dabei handelt es sich **IMMER** um Hoaxes .

Wie geht man mit einem Hoax um

- Leiten Sie die Mail **auf gar keinen Fall** weiter.
- Löschen Sie aufgrund einer solchen E-Mail **niemals** eine Datei auf Ihrem PC.
- Informieren Sie gegebenenfalls den Absender, dass er einem Hoax aufgesessen ist.
- Löschen Sie die E-Mail und verschwenden Sie keine weitere Zeit damit.
- Bevor Sie sich hinreißen lassen, doch eine Mail weiterzuleiten, weil sie „wirklich echt“ klingt, informieren Sie sich auf der Hoax-Seite der Tu Berlin: http://www.tu-berlin.de/software/hoax.shtml

Wie geht man mit einem Hoax um

Beispiele:

- Warnungen vor den Dateien
  - Jdbmgr.exe
  - Sulfnbk .exe
- Warnungen vor sogenannten Handy-Viren:
  - Anzeige ACE-? im Display führt zu angeblichem Löschen aller Handy-Daten.
  - Bei Rückruf zu bestimmten Nummern entsteht eine nicht wieder zu beendende Verbindung.
  - Mitarbeiter von Netzbetreibern können bei Rückruf unter bestimmten Nummern persönliche Daten der Teilnehmer ausspionieren und auf deren Kosten telefonieren.
  - Die Inhalte solcher E-Mails sind alle unwahr. Und: **Handy-Viren gibt es nicht**

Andere Hoaxes

Nigeria Connection: E-Mails mit erwiesenermaßen kriminellen Absichten:

- Erfundene Geschichten um große Geldsummen (Erbschaften, Lottogewinne, Geschäftsgewinne, ...), die außer Landes geschafft werden sollen.
- Der angebliche Schauplatz ist meist Nigeria, oft aber auch andere afrikanische Länder und Asien.
- Der Empfänger der E-Mail sollen dabei helfen, das Geld zu transferieren. Es werden Beteiligungen schwindelnder Höhe in Aussicht gestellt.
- Oft soll der Empfänger der E-Mail finanziell in Vorleistung treten.
- Manche Geschädigte sind schon nach Afrika gereist, dort beraubt und sogar in Geiselhaft genommen worden.
- Die erfundenen Geschichten wechseln, werden immer ausgefeilter und werden inzwischen schon auf bestimmte Zielgruppen zugeschnitten.
- Extrablatt „Nigeria-Connection“ http://www.tu-berlin.de/www/software/hoax/419.shtml

Andere Hoaxes

- Auch Kettenbriefe im Allgemeinen zählen zu den Hoaxes.
- Es existiert kein realer Hintergrund, der eine Weiterleitung rechtfertigt.
- Mehrere Varianten:
  - Pyramidensysteme, Schneeballsysteme (illegal!)
  - Glücksbriefe
  - Sinnlose E-Mail-Petitionen: Regenwald, Taliban / Frauen in Afghanístan, Filmboykott
  - Briefe die auf die Tränendrüse drücken: Knochenmarkspender
  - Neu: Mails im Zusammenhang mit dem 11. September 2001
  - Kettenbriefe über vermisste Kinder.
- Aktuelle Informationen über Hoaxes finden Sie unter http://www.tu-berlin.de/software/hoax.shtml

Sicherheit für Anwender: Specials

Themen:

Weitere Bosheiten, Belästigungen und Gefahren

- Hoaxes
- SPAM
- Spyware
- 0190-er Dialer

SPAM-Mail

SPAM-Mail (auch Junk-Mail):

- **Unsolicited Bulk Email (UBE)** = unverlangte Massenmails
  - Oft Mails mit
    - betrügerischer Absicht (Pyramidensysteme, Nigeria-Connection)
    - bekannter Absenderadresse
  - Kettenbriefe, Werbung für Pornographieangebote
- **Unsolicited Commercial Email (UCE)**
  = unverlangte kommerzielle Werbung per E-Mail
- Angaben der Fa. Sophos zu Folge machte SPAM-Mail im Jahr 2002 mehr als 25% des E-Mail-Verkehrs im Internet aus.
- Im Jahr 2003 liegt der Anteil von SPAM-Mail schon über 50 %

SPAM-Mail

- SPAM steht für:
  - **S**piced **P**ork and h**AM** ,
  - Markenname einer Art Preßfleisch im Katzenfutter-Look aus den USA.

- Bekannt geworden durch den SPAM-Sketch von Monty Python.

SPAM-Mail

Der Sketch:
Dem Ehepaar Bun werden in einem Restaurant von der Bedienung ausschließlich Gerichte angeboten die SPAM enthalten, zum Teil sogar mehrfach. Ungeachtet der Tatsache, dass keiner der beiden SPAM möchte und dies auch Immer wieder zum Ausdruck bringt, taucht SPAM in den Empfehlungen immer und immer wieder auf. Zusätzlich bricht bei jeder Erwähnung des Wortes SPAM eine im Restaurant anwesende Gruppe Wikinger in einen jubilierenden Chor aus und singt: **SPAM, SPAM, lovely SPAM, wonderful SPAM!**. Jede Art von Konversation unter den anderen Gästen wird unmöglich und kommt zum Erliegen.

Insgesamt kommt das Wort SPAM in dem Sketch ca. 120mal vor.

SPAM-Mail

Gängige Rechtsprechung:

- Die Zusendung von Werbe-Mails ohne vorherigen geschäftlichen Kontakt zwischen den Parteien ist nicht zulässig. Es spielt keine Rolle, ob die Zusendungen an Privatpersonen oder Gewerbetreibende gingen oder für welchen kommerziellen Zweck in den Mails geworben wird.

Die EU-Richtlinie zu diesem Thema schreibt in Artikel 40 klar vor:

- „Bei solchen Formen unerbetener Nachrichten [u.a. elektronische Post] zum Zwecke der Direktwerbung ist es gerechtfertigt, zu verlangen, die Einwilligung der Empfänger einzuholen, bevor ihnen eine solche Nachricht gesandt wird“. (**Opt-In Regelung**)

  http://www.dud.de/dud/documents/eu-15396d-020121.pdf

- Diese Regelung musste das Parlament bis zum Sommer 2003 in deutsches Recht umsetzen, was im Rahmen der Reform des "Gesetzes gegen den unlauteren Wettbewerb" (UWG) stattgefunden hat.

SPAM-Mail

SPAM

- wird direkt vom Verursacher verschickt oder
- offene Mail-Relays werden ausgenützt:
  - Für den Versand von Massen-Mail missbrauchte Mail-Server „unbescholtener“ Institutionen durch
  - nicht geschlossene Sicherheitslöcher oder
  - unsachgemäß erfolgte Konfiguration.
- Viren hinterlassen Backdoors und Programme auf Systemen, die den Rechner unbemerkt vom Anwender zum automatischen SPAM-Versender machen (z.B. Backdoor-AVR über Port 19979)

SPAM-Mail

Grundsätzliche Verhaltensweisen:

1. Werbe Mails **niemals beantworten**, lassen Sie sich auch nicht durch verlockend platzierte Hinweise zur Abbestellung verleiten (Ihre E-Mail-Adresse wird dadurch als „echt“ bestätigt).
2. Werbe-Mails im HTML-Format nie im Vorschaufenster des Mail-Programmes betrachten (Mechanismen zur Nutzerüberwachung).
3. Für eventuelle Inanspruchnahme von Internet-Diensten vorzugsweise einen Freemail-Account verwenden (knappes Platzangebot unterbindet Werbeflut).

SPAM-Mail: Filterung

Filterung ankommender E-Mails:

- Nutzen Sie Filterungsmöglichkeiten der Mail-Programme:
  - Beobachten Sie, ob sich in den typischen Feldern einer E-Mail (Subject, From, etc.) bestimmte Textteile oder Absender-Namen wiederholen.
  - Definieren Sie sich Filter, die die entsprechenden Felder auf die beobachteten Werte und Textteile überprüfen.

SPAM-Mail

- Benutzen Sie Mail-Clients mit integriertem, lernfähigem SPAM-Filter
  - Mozilla ab Version 1.3
  - Netscape ab Version 7.1
- SPAM-Filter basiert auf einem statistischen Verfahren:
  - Einzelne Wörter werden gewichtet. und zwar nach der Häufigkeit in der sie in SPAM-Mails vorkommen.
  - Die Summe der SPAM-Wahrscheinlichkeit individueller Wörter einer E-Mail entscheidet, ob sie als SPAM bewertet wird.
- Bedienung des SPAM-Filters in der Lernphase
  - Der Benutzer entscheidet zunächst selbst, was SPAM ist
  - SPAM-Mails werden per Mausklick (Button **Junk** in der Symbolleiste) als SPAM gewertet und anschließend gelöscht.

SPAM-Mail


Junk-Mail-Filter
Konto:
Junk-Mail-Protokoll
Junk-Mail-Filter untersuchen Ihre eingehenden Nachrichten und kennzeichnen eMails, die aller Wahrscheinlichkeit Junk-Mails oder unangeforderte eMails darstellen. Ein Junk-Symbol wird angezeigt, wenn die Nachricht als Junk-Mail eingestuft wird.
Junk-Mail-Filter können über die Symbolleistenschaltfläche 'Junk-Mail' weiter angepasst werden, um Junk-Nachrichten entsprechend zu markieren.
Junk-Mail-Filter aktivieren
Nachrichten nicht als Junk-Mail markieren, wenn der Absender in meinem Adressbuch enthalten ist:
Eingehende Nachrichten, die als Junk-Mail eingestuft wurden, verschieben nach:
"Junk"-Ordner:
Klicken Sie hier, um ein Konto auszuwählen
Sonstige:
Junk-Nachrichten aus diesem Ordner automatisch löschen, wenn sie älter sind als
30
Tage
Manuell von mir als Junk markierte Nachrichten:
In den "Junk"-Ordner verschieben
Löschen
OK
Abbrechen
Hilfe

SPAM-Mail

- Nach und nach wird das Programm treffsicherer:
  - Erkannte SPAM-Mails werden in einen Ordner „Junk“ verschoben.
  - Diesen Ordner sollte man regelmäßig auf falsch-positive Bewertungen durchsuchen.
  - Bei falsch-positiven Mails die SPAM-Kennzeichnung per Mausklick wieder entfernen (erneut Button **Junk**) und die Mail weiterverarbeiten.
- Mit der Zeit steigt die Trefferquote der richtig klassifizierten Mails auf 98-99 %

Artikel über SPAM:

http://www.rrzn.uni-hannover.de/BIs März.2003 / 366

SPAM über Windows Nachrichtendienst

- Ist bei Windows XP und Windows 2000 per Default aktiviert.
- Wird missbraucht um SPAM zu versenden.
- Es gib Tools mit denen Nachrichten an ganze Adressbereiche zugestellt werden können.

SPAM über Windows Nachrichtendienst

- Nachricht geht an alle User des ausgewählten Adressbereiches, die gerade im Internet eingewählt sind:
  - So kann man aufs Einfachste z.B. alle User eines Internet-Providers erreichen.
- Für die Absender dieser Botschaften ist das Verfahren viel einfacher und effektiver als SPAM per E-Mail:
  - Es werden keine E-Mail-Adressen mehr benötigt.
  - Botschaft erreicht den Adressaten „in Echtzeit“.

SPAM über Windows Nachrichtendienst

- Beispiel für ein solches Nachrichtenfenster:

- Abhilfe:
  - blocken per Firewall (Port 139, tcp und udp)
  - Windows-Nachrichtendienst deaktivieren
    (nur praktikabel, wenn keine Freigaben für Dateien und Drucker benötigt werden, siehe auch:
    http://www.tu-berlin.de/www/software/winmsg.shtml)

SPAM über Windows Nachrichtendienst

Anleitung zum Deaktivieren unter Windows 98/ME

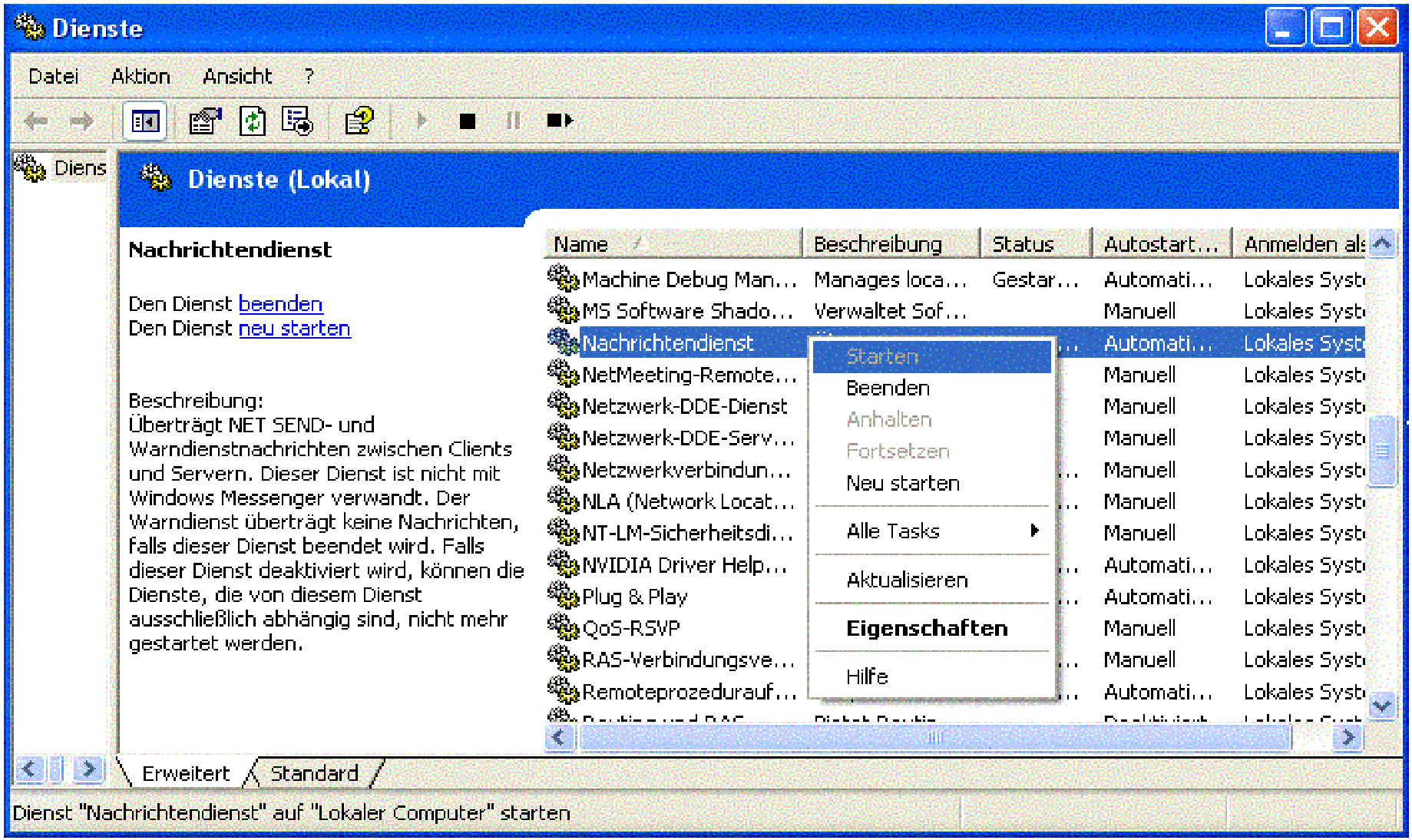
- Start ➔ Einstellungen ➔ Systemsteuerung
- Netzwerk auswählen
- Reiter Konfiguration auswählen
- Eintrag „Datei- und Druckerfreigabe für Microsoft-Netzwerke“ auswählen und entfernen

SPAM über Windows Nachrichtendienst

Anleitung zum Deaktivieren unter Windows XP

- Start ➔ Systemsteuerung ➔ Verwaltung ➔ Dienste
- Nachrichtendienst suchen und markieren
- nicht nur einfach beenden, sonst wird der Dienst beim nächsten Systemstart wieder gestartet
- mit der rechten Maustaste: Eigenschaften anwählen

SPAM über Windows Nachrichtendienst

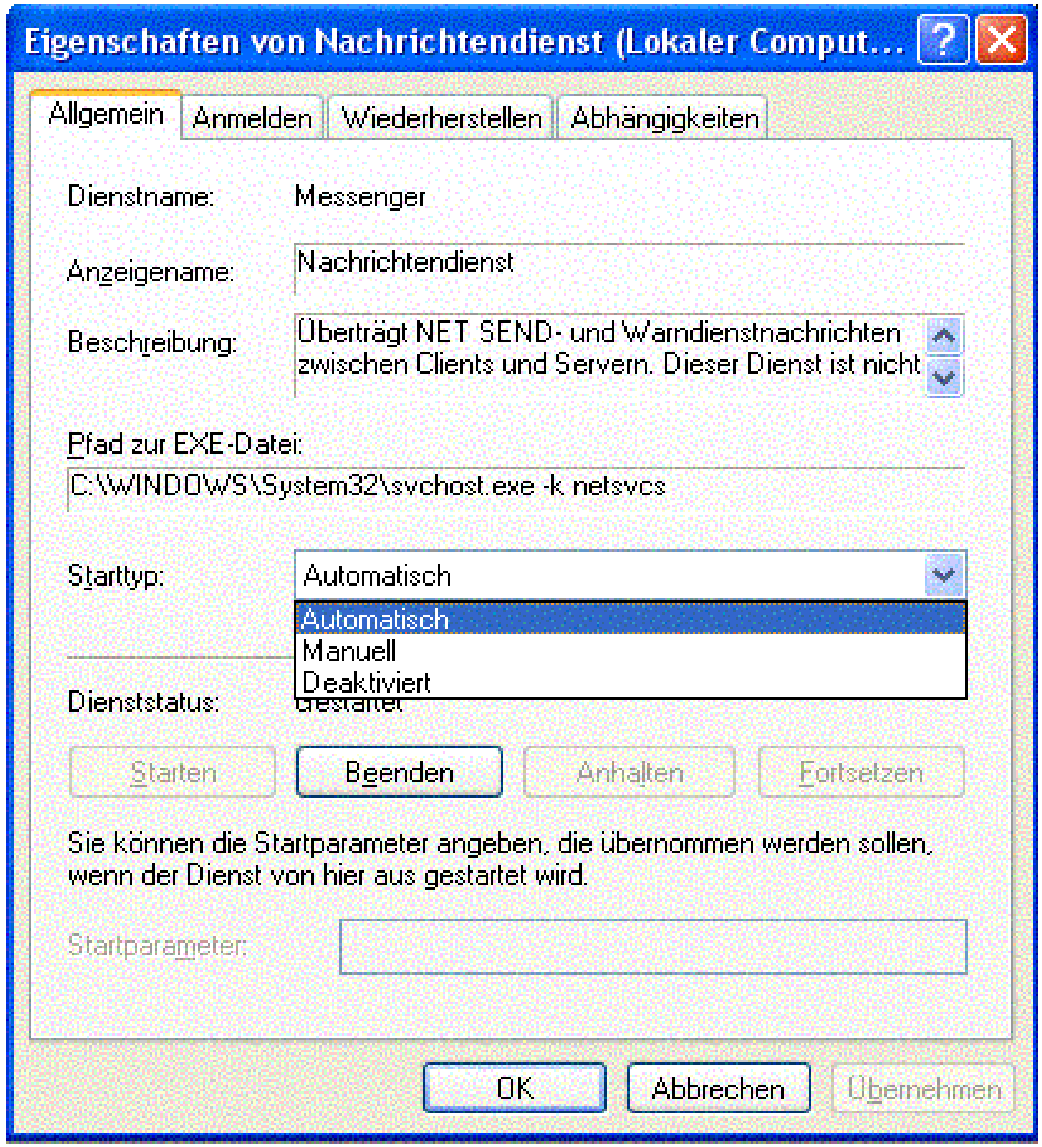


SPAM über Windows Nachrichtendienst

- Im Eigenschaftsfenster "Deaktiviert" auswählen und mit "OK" bestätigen

Für Windows 2000

- Start ➔ Einstellungen➔ Systemsteuerung ➔ Verwaltung ➔ Dienste
- ab dann analog zu XP



SPAM über Windows Nachrichtendienst

Heise-Meldung vom 29.10.2003 zu dieser Thematik:

- Microsoft plant seine Standardeinstellungen zu ändern:
  - Nachrichtendienst soll standardmäßig deaktiviert sein.
  - Die integrierte Internet Connection Firewall (ICF) soll standardmäßig aktiviert sein.
- Reaktion auf massive Vorwürfe von Unternehmern und Anwendern.
- geplanter Termin: erstes Halbjahr 2004
- Vorgehen: Service-Pack 2 für Windows XP soll die entsprechenden Einstellungen vornehmen.

Sicherheit für Anwender: Specials

Themen:

Weitere Bosheiten, Belästigungen und Gefahren

- Hoaxes
- SPAM
- Spyware
- 0190-er Dialer

Was ist Spyware

- Spyware, auch Adware genannt, ist Spionage-Software.
- Spyware läuft ohne Wissen des Benutzers und ist häufig versteckt in:
  - Freeware
  - werbefinanzierter Software
  - aber auch in Kaufsoftware.

Was macht Spyware

- Informationen über und Aktivitäten des Anwenders werden protokolliert
  - z.B. das persönliche Surfverhalten
  - Vorlieben beim Online-Shopping
  - persönliche Daten
- Diese Informationen werden unbemerkt an Internet-Firmen und -Datenbanken gesendet.
- Dadurch können „Werbeinformationen“ gezielt auf die Interessen das Anwenders zugeschnitten werden.
- Reklamefenster und –banner werden gehäuft auf dem Bildschirm dargestellt.

Was macht Spyware

Spyware sammelt und versendet nicht nur Daten, sie wird auch selbst aktiv:

- Reklamefenster und –banner werden inhaltlich zielgerichtet
  - auf dem Bildschirm dargestellt und
  - in andere Programme eingespielt.
- Internet-Suchen werden vom Anwender oft unbemerkt auf vorgegebene Seiten umgelenkt.
- Funktionen des Browsers werden geändert.

Was macht Spyware

- Spyware verbraucht Computerressourcen:
  - Einbußen in der Leistungsfähigkeit des Systems sind zu verzeichnen.
  - Es kommt vermehrt zu Systemabstürzen.
- Deinstallationsversuche führen oft zu Schädigung des Systems.
- Spyware nistet sich oft so im System ein, dass es nicht nur bei Start des „Wirtsprogrammes“ sondern bei jedem Rechnerstart aktiv wird.
- Spyware stellt oft eigenständig Internetverbindungen her.

Spyware: Blacklist

- Aureate/Radiate
  - Bleibt auch dann aktiv, wenn das eigentliche „Wirtsprogramm“ deinstalliert oder durch eine Vollversion ersetzt wurde.
  - Legt einen geschützten Cache auf der Festplatte an
    - dadurch kann der Anwender auch dann mit Werbefenstern versorgt werden , wenn er offline ist.
- Gator:
  - angebliche Funktion: automatisches ausfüllen von Web-Formularen
- Web Hancer
  - angebliche Funktion: Optimierung der Internet-Verbindungen und Erhöhung der Download-Geschwindigkeit

Spyware: Blacklist

- Bonzi-Software
- Cydoor
- SaveNow
- Netsonic Download Accelerator
- u.v.a.m.

Verbreitung: Der Code einer einzelnen Spyware läuft geschätzt auf ca. **20 Millionen PCs**.

Spyware: vorbeugendes Verhalten

- Keine ausführbaren Dateien auf Vorschlag einer Website auf Ihren Rechner laden.
- Seien Sie misstrauisch mit ausführbaren Dateien aus Tauschbörsen.
- Installieren Sie eine Personal Firewall .
- Deaktivieren Sie den Windows Messenger.
- Internet Explorer so konfigurieren, dass Browsererweiterungen von Drittanbietern deaktiviert werden.
  - Extras ➔ Internetoptionen ➔ Erweitert bzw.
  - Tools ➔ Internet Options ➔ Advanced

Anti-Spyware-Tools

AD-Aware

- Tool zur Entfernung aller gängigen Spyware-Programme
- Download unter **http://www.lavasoft.de**
- Standard-Edition ist für privaten Gebrauch frei nutzbar.
- Es werden Updates für neu auftauchende Spyware zur Verfügung gestellt.
- Für eine deutsche Benutzeroberfläche: Language-Pack unter **http://www-lavasoft.de/res/asw-lang-pack.exe**

Anti-Spyware-Tools

Spybot S&D (Search and Destroy)

- Tool zur Entfernung aller gängigen Spyware-Programme
- Download unter **http://www.spybot.info/**
- Freeware
- Kann zusätzlich auf Festplatten gespeicherte Surf-Spuren wie
  - Listen besuchter Webseiten,
  - Listen geöffneter Dateien und benutzter Programme,
  - Cookies,
  - Bestandteile von betrachteten Webseiten

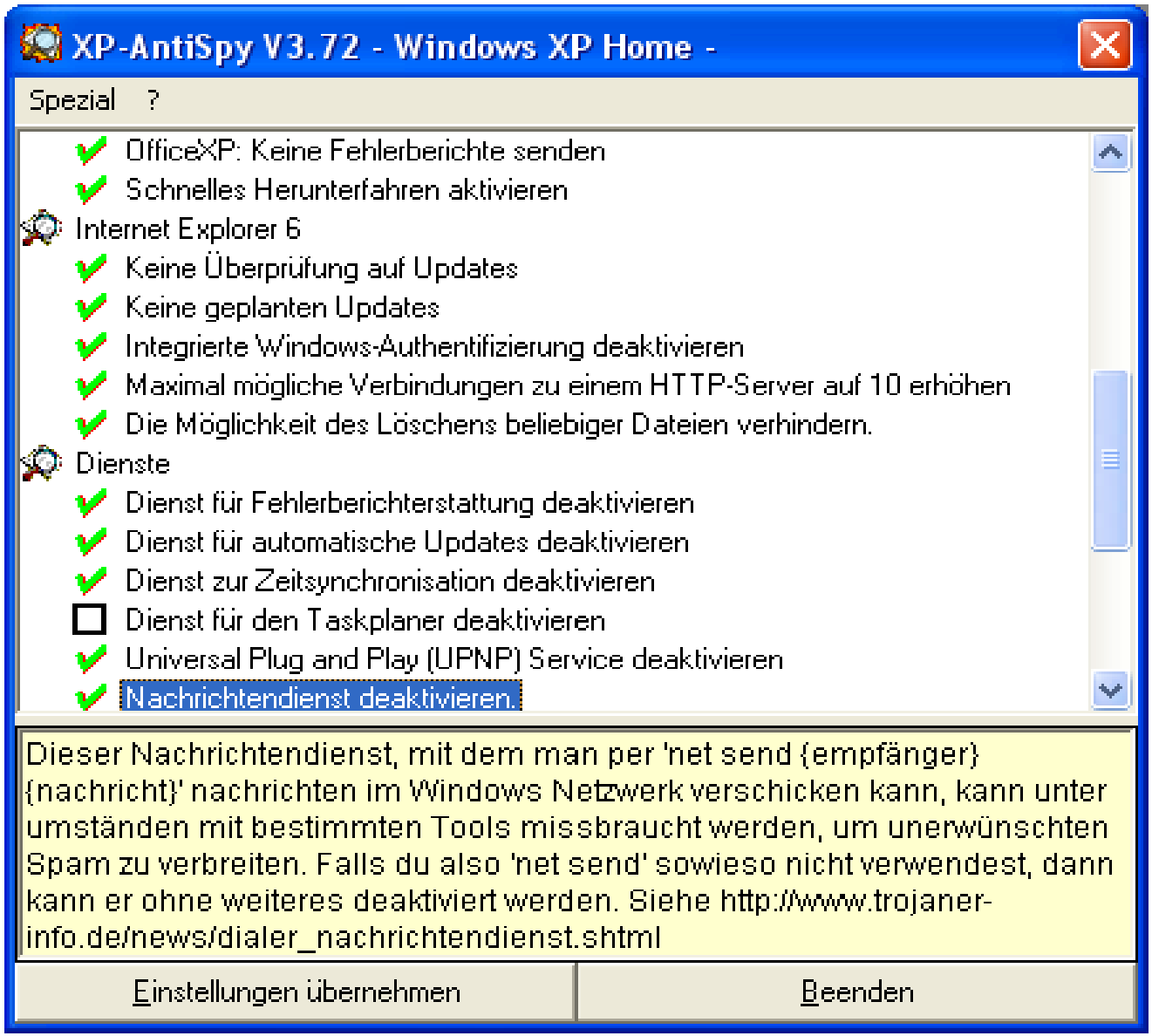
  entfernen.

Anti-Spyware-Tools

XP-Antispy (momentan aktuelle Version 3.72)

- Download unter **http://www.xp-antispy.org/**
- Für Windows XP, ab Version 3.6 auch für Windows 2000.
- Dieses Tool verhindert die dauernden Kontaktaufnahmen, welche die Windows-Systeme zu den Microsoftservern unternehmen.
- Das Programm ist ohne Installation sofort einsatzbereit.
- Stellt sehr übersichtlich die aktuell gültigen Einstellungen dar.

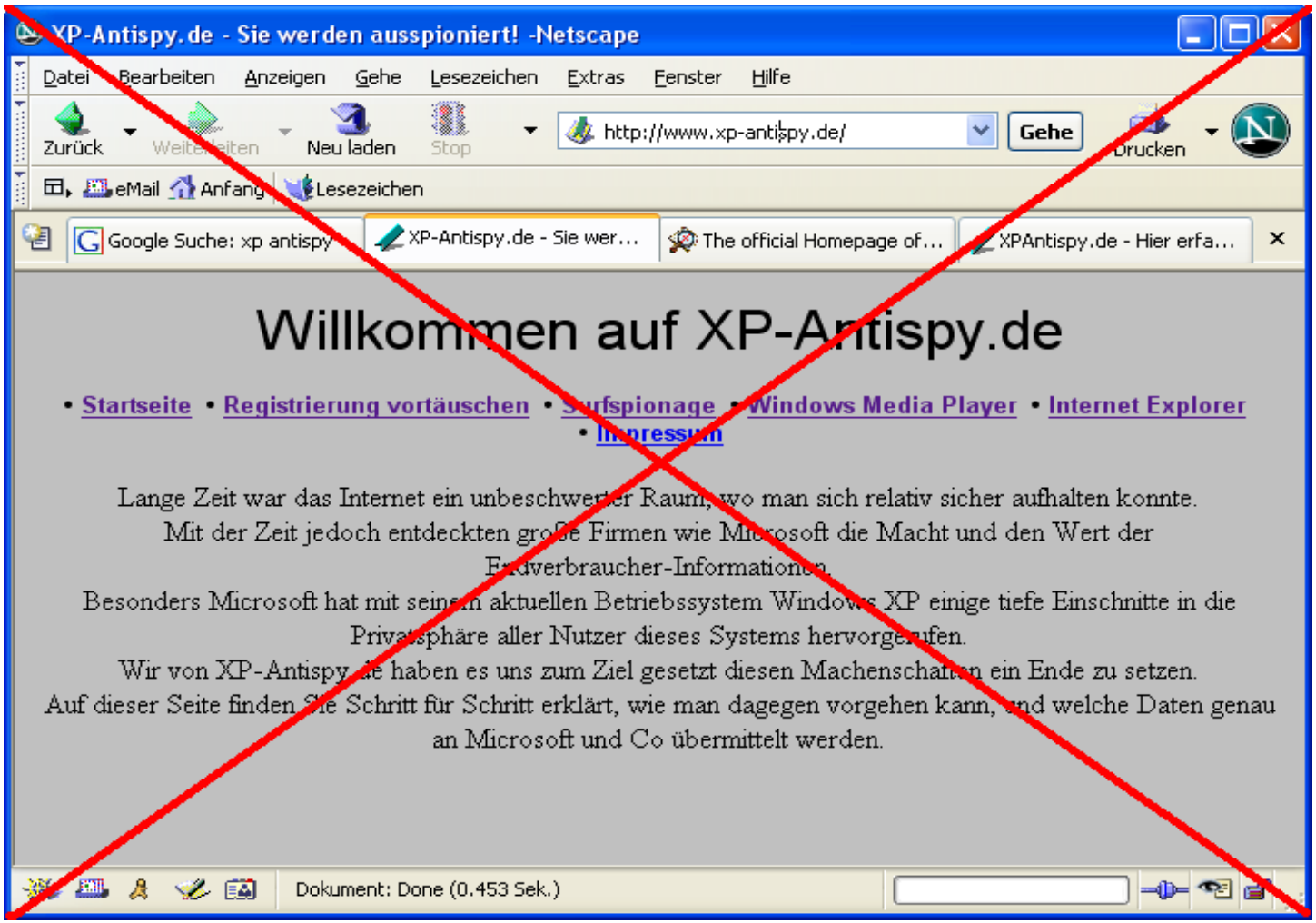
Anti-Spyware-Tools



- Die Anpassung kann schnell und einfach per Maus-klick erfolgen.
- Ebenso schnell kann per Klick zu den Standardeinstellungen zurückgekehrt werden.
- Um unteren Fensterbereich stehen Erläuterungen zur jeweils angewählten Einstellung.

Anti-Spyware-Tools

- **http://www.xp-antispy.de** und **http://www.xpantispy.de**



Vorsicht!
Diese beiden Seiten haben **nichts** mit dem empfohlenen Tool zu tun!
Dort lädt man sich stattdessen einen 0190er-Dialer auf sein System.

Anti-Spyware-Tools

Zwei weitere nützliche Links:

- Ausführliche Liste von Spyware-Einträgen unter
  - **http://www.spywareguide.com**

- Für IE-Benutzer: unter **http://www.spywareinfo.com** kann direkt das eigene System auf Spyware untersucht werden

Sicherheit für Anwender: Specials

Themen:

Weitere Bosheiten, Belästigungen und Gefahren

- Hoaxes
- SPAM
- Spyware
- 0190-er Dialer

0190er-Dialer

- Was ist ein Dialer / Was ist ein 0190er-Dailer?
- Wie unterscheidet man seriöse von unseriösen Dialern?
- Wie kommen Dialer auf Ihr System?
- Wie kann man sich vor Dialern schützen?
- Wie kann man Dialer finden und entfernen?
- Allgemeine Hinweise

Was ist ein Dailer?

- Dialer an sich sind kleine Programme zur Herstellung von Onlineverbindungen die oft von Internetprovidern angeboten werden.
- Dialer erleichtern die Einrichtung eines Internetzugangs und nehmen dem Anwender lästige Konfigurationsarbeit ab.
- In diesem Sinne sind Dialer nützliche Hilfsprogramme.

Was ist ein 0190er-Dailer?

- 0190er-Dialer wählen sich über sogenannte Premium-Rate-Nummern ins Internet ein.
- die Verbindungskosten unter diesen Telefonnummern sind **ungleich höher** als bei anderen Internet-Verbindungen**:**
  - Nummern beginnend mit 0190-8 kosten 1,86€ pro Minute.
  - Nummern beginnend mit 0190-0, 0193 und 0900 ist kein fester Tarif zugeordnet, der Anbieter kann die **Gebühren beliebig festsetzen,** auch schon für die reine Einwahl.
  - Der Kunde wählt sich über eine solche Telefonnummer ein, die vereinbarten Kosten werden über die Telefonrechnung eingezogen.
- Viele Abzocker treiben mit Dialern massiven Mißbrauch mit diesen Nummern.

Was ist ein 0190er-Dailer?

- Mit dem Begriff **0190er-Dialer** werden im Folgenden solche Programme bezeichnet,
  - die sich ohne Einverständnis und Wissen des Benutzers installieren,
  - die sich teilweise auch selbständig einwählen,
  - bei denen die anfallenden Kosten verschwiegen oder verschleiert werden.
- Im Universitätsnetz und bei DSL-Verbindungen sind sie nicht gefährdet, nur wenn Sie sich über Modem bzw. ISDN ins Internet einwählen.

0190er-Dialer: Vergleich seriöse/unseriöse Dialer

Kriterium	Seriöser Dialer	Dubioser Dialer
Download	Muss explizit angeklickt werden	Download-Popup öffnet sich automatisch Manchmal startet der Download automatisch Download lässt sich trotz Klick auf „Abbrechen“ nicht stoppen
Preishinweis vor dem Download	Deutlich auf der Web-Seite zu sehen	Kein Hinweis nur sehr unauffälliger Hinweis Verneinung von Kosten
Preishinweis vor der Einwahl	Deutlicher Hinweis auf den aktuell geltenden Tarif	Keine Angaben zum Tarif

0190er-Dialer: Vergleich seriöse/unseriöse Dialer

Seriöser Dialer:

Anzeige der Online-Zeit

ausführliche Tarif-Informationen

Anzeige des aktuellen Tarifes

verschiedene Tarife wählbar

bisher aufgelaufene Kosten

Surf25.de
Einfach ins Internet mit
www.surf25.de
www.1net4you.de
1net4you
Sie haben Fragen oder Anregungen? Hotline: 06033-73076
Setup
Online seit ... 20 Minute(n)
Citytarif
Tarifinfo <
Trennen
Statistik
0,2824 €
>Informationen zum Haftungsausschluss<
Tarifdetail: Citytarif
Eine Einwahl ist in 38 Städten möglich. Außerhalb der GKAS Cities ist die Einwahl gesperrt.
Genaue Informationen unter www.surf25.de.
Abrechnung: Sekundengenau.
Aktueller Tarif
1,18 Cent/Min.(4,64 Cent einmalig)
Beenden

0190er-Dialer:Wie kommen sie auf Ihr System?

- Die meisten Dialer werden vom Anwender **selbst installiert**.
- Manchmal wird der Dialer vollautomatisch, ohne Benutzereingriff und meistens auch im Hintergrund installiert.
  - Die Möglichkeit ist nicht nur unseriös, sondern sogar illegal.
  - Von dieser Art Dialer sind nur Benutzer des Internet Explorer bedroht, sie erfolgt auf der Basis von **ActiveX**.

0190er-Dialer:Wie kommen sie auf Ihr System?

Tricks der Anbieter:

- "Geheime" Webadressen mit versprochenen „tollen“ Inhalten:

  http://%33%3586%320%31%384%36/%73%32%62%6E%74%35%79%6A/
- Automatische Downloads
- Anbieten von Schutztools die vor Hackern bewahren sollen.
- Angebliche 'AntiVirus Teams' bieten per Werbe-Mail Virenschutzprogramme zum Download an.

Alle diese Verlockungen entpuppen sich oft als 0190-Dialer.

0190er-Dialer:Wie kommen sie auf Ihr System?

- WerbeMails bieten angeblich "gecrackte" Dialer an:
  - Es wird der Eindruck erweckt, unter Verwendung des "gecrackten" Dialers kostenlos Zugriff auf ansonsten kostenpflichtigen Inhalte erlangen zu können.
  - Dies ist Irreführung, es gibt keine "gecrackten" Dialer. Dem Anbieter ist es egal, mit welcher Software oder welchem Telefon die 0190-Nummer angewählt wird.

0190er-Dialer: Wie kann man sich vor ihnen schützen?

- Nicht den Internet Explorer verwenden:
  - Nur der Internet Explorer ist für die gefürchteten, sich über ActiveX selbst installierenden Dialer empfänglich.
- Wenn es nicht anders geht:
  - Unter Extras ➔ Internetoptionen ➔ Sicherheit ➔ Stufe anpassen wenigstens die ActiveX-Optionen auf "Eingabeaufforderung" einstellen.
  - Den IEController verwenden.

0190er-Dialer: Wie kann man sich vor ihnen schützen?

- Sperrung der 0190er- und 0900er-Nummern
- Einzelverbindungsnachweis bei Telefonnetzbetreiber bestellen:
  - Leichterer Nachweis des Sachverhalts im Schadensfall.
- Keine automatischen Downloads annehmen sondern grundsätzlich ablehnen!

0190er-Dialer: Wie kann man sich vor ihnen schützen?

- Seien Sie generell vorsichtig mit Downloads aus dem Internet:
  - Keine Programme aus zweifelhafter Quelle herunterladen ("testen")!
  - Nicht auf "heiße Tipps" oder "geheime Informationen" von unbekannten Menschen hören!
- Keine "gecrackten" Dialer testen - es gibt keine gecrackten Dialer!
- Virenscanner und Firewall-Software bieten keinen Schutz vor Dialern

0190er-Dialer: Wie kann man sie finden und entfernen?

- Dialer aufspüren:
  - neue Verknüpfungen auf dem Desktop (eventuell auch mit bekannten Symbolen)
  - DFÜ-Verbindungen kontrollieren (Systemsteuerung ➔ Netzwerk)
  - Im Taskmanager (Strg+Alt+Entf) laufende Tasks überprüfen
  - Autostart-Einträge überprüfen
- Werden Sie an einer dieser Stellen fündig und stoßen auf verdächtige Programm-Namen:
  - Namen für weiteres Vorgehen notieren

0190er-Dialer: Wie kann man sie finden und entfernen?

Überprüfen Sie die Registry :

- Die **Registry** ist das Herzstück Ihres Betriebsystems, eine immense Systemdatenbank mit allen wichtigen Konfigurationseinstellungen.
- Die Einstellungen sind in der Registry unter sogenannten Schlüsseln („Keys“) eingetragen.
- **Vorsicht walten lassen!** Wenn Sie in der Registry etwas löschen, ist es sofort und ohne Rückfrage weg!
- Aufrufen: **Start** ➔ **Ausführen** anklicken und „**regedit**“ eingeben
- Es öffnet sich ein Explorer-ähnliches Fenster.
- Unter **Bearbeiten** ➔ **Suchen** können Sie nach bestimmten Einträgen suchen.

0190er-Dialer: Wie kann man sie finden und entfernen?

Zu überprüfende Schlüssel und Pfade:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunService

Dieselben Pfade überprüfen unter:

- HKEY_CURRENT_USER
- HKEY_USERS

0190er-Dialer: Wie kann man sie finden und entfernen?

- Vollständige Liste der zu überprüfenden Dateien und Einträge:
  - http://www.trojaner-info.de/dialer/woranerkennen4.shtml
- Haben Sie in der Registry Einträge ungewünschter Software gefunden, gilt auch hier: verdächtigte Namen notieren.
- Nun die Schlüssel der ungewünschten Software entfernen (markieren und „ **Bearbeiten ➔ Löschen“)**.
- Anschließend nach der Software mit den notierten Namen suchen und diese deinstallieren/löschen.

0190er-Dialer: Allgemeine Hinweise

- Im Fall **erheblicher finanzieller Schädigung** sollten Sie auf keinen Fall etwas löschen, sondern versuchen **Beweismittel sichern**:
  - Das Dialer-Programm mit allen dazugehörigen Dateien sichern.
  - Wenn nachvollziehbar ist , woher der Dialer stammt (Webseite, E-Mail), diese Dateien auch sichern.
  - Aussagekräftige Screen-Shots erstellen und sichern.
  - Jemanden mit Fachkenntnissen zu Rate ziehen.

0190er-Dialer: Allgemeine Hinweise

- Informieren Sie sich so schnell wie möglich an entsprechenden geeigneten Stellen, wie Sie genau vorgehen sollen.

  Empfehlenswerte Anlaufstellen:

  – Telekommunikationsanbieter oder Rechnungssteller
  – Verbraucherschutzzentralen
  – Freiwilligen Selbstkontrolle Telefonmehrwertdienste (FST)
  – Kriminalpolizei

0190er-Dialer: Allgemeine Hinweise

Seit August 2003 ist ein Gesetz zum Schutz vor Mißbrauch von 0190-Nummern in Kraft

- Einige Regelungen aus dem neuen Gesetz:
  - Preisobergrenze pro Einwahl und Tarif werden festgesetzt.
  - Zwangsabbruch der Verbindung nach 1 Stunde vorgesehen.
  - Dialer-Programme müssen bei der RegTP registriert werden.
  - RegTP wird befugt, Nummern bei Missbrauch sperren zu lassen und Geldstrafen bis zu 1 Mio € gegen unseriöse Anbieter zu verhängen.
  - Der Lizenzentzug gilt rückwirkend zum Tag der Registrierung.

0190er-Dialer: Allgemeine Hinweise

- Als erste Folge des neuen Gesetzes wurden im Oktober bereits
  - 398.791 Dialer-Programmen die Registrierung entzogen (von insgesamt registrierten ca. 570.000).
  - Die RegTP hat beim Netzbetreiber angeordnet die entsprechenden Rufnummern, zu sperren: 0190 -88 04 61, 0190-88 04 60 und 0190-80 56 40.
  - Die unfreiwilligen Nutzer dieser Programme brauchen ihre Rechnungen nicht zu bezahlen.
  - Der Netzbetreiber muss ein Zwangsgeld bezahlen, wenn die Nummern weiterhin erreichbar bleiben.

0190er-Dialer: Allgemeine Hinweise

- Die RegTP betreibt auf ihrer Homepage eine Datenbank mit den Rufnummern und Hashwerten der registrierten Dialer.
  - http://www.regtp.de/
- Ist ein Dialer dort nicht registriert, muss der Nutzer dessen Kosten nicht bezahlen.
- Die RegTP stellt ein kostenloses Programm bereit, das den Hash-Wert eines Dialers berechnen kann.
  - http://www.regtp.de/imperia/md/content/mwdgesetz/hashanzeige.zip
- Anhand dieses Hashwertes kann man überprüfen, ob ein Dialer registriert wurde.

0190er-Dialer: Allgemeine Hinweise

- Aus Anwendersicht zu bemängeln:
  - Auskunftsanspruch der Benutzer ist nicht weitgehend genug berücksichtigt (Netzbetreiber, Diensteanbieter).
  - es ist nicht vorgesehen, dass der Diensteanbieter seinen finanziellen Anspruch belegen muss.
  - Die Neuregelungen sind auf die Nummern 0190 und 0900 beschränkt.
  - Es ist zu befürchten, dass unseriöse Anbieter auf andere Nummern ausweichen werden, die mit hohen Tarifen belegt werden können (0137; Auskunftsvorwahl 118)

0190er-Dialer: Allgemeine Hinweise

- Informationen zu den rechtlichen Aspekten der 0190-Dialer finden Sie unter:
  - http://www.dialerundrecht.de/
- Allgemeine Tipps und Informationen zum Thema:
  - http://www.computerbetrug.de/
- **Tipps der bayrischen Kriminalpolizei zum Thema:**
  - http://www.polizei.bayern.de/ppmuc/schutz/text10.htm
- Regulierungsstelle für Telekommunikation und Post:
  - http://www.regtp.de/
- Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V.
  - http://www.fst-ev.org/

Neue Ergebnisse beim Crack-Programm?

Passwörter: Demo Crackprogramm

12 Testbenutzer mit unterschiedlich komplizierten Passwörtern:

Benutzername	Passwort	Benutzername	Passwort
meier	abcd	**lehmann**	qwer
schulz	pass	**klein**	Baum
peter	geheim	**heinz**	Hase
aust	aust?	**schlau**	v9b10:Rv
werner	werner1	**clever**	S:LaO!Ha
moeller	rrzn	**smart**	P:rs$val