# Gefahrenabwehr beim Internetzugang mit Windows-Rechnern durch systeminterne Maßnahmen und Firewalls

**(am Beispiel des Firewall-Setups für die DrayTek-Router der Vigor 2200-Serie und der Kerio/Tiny Personal Firewall)**

**2. Auflage**
**Stand: 19. Februar 2003**

**von**
**Michael König, Köln**

# I. Einleitung, Entwicklungsgeschichte

Alle nachstehenden Angaben mache ich ohne Gewähr. Ich habe mich bemüht, Fehler zu vermeiden, bin aber natürlich auch auf Angaben in der Literatur und im Internet angewiesen. Dabei habe ich mich selbst gewundert, wie viele widersprüchliche und falsche Aussagen zu finden sind. Ich kann daher natürlich nicht ausschließen, dass ich gelegentlich einer Fehlinformation ausgesessen bzw. mich selbst geirrt habe.

## Entwicklungsgeschichte

### 1. Auflage, Stand: 01. Juni 2002

... war die erste Auflage dieser Anleitung

### 2. Auflage, Stand: 19. Februar 2003

... passt die Anleitung an die aktuelle Firmware 2.3 an

❖ Wenn Sie sich bereits durch die erste Auflage dieser Anleitung durchgearbeitet haben, gibt es nicht viel zu ändern, insbesondere sind die eigentlichen Firewall-Regeln gleich geblieben, wenn man davon absieht, dass ich bei der Vigor-Firewall die Block Source-Regel im Set 3 Nr. 1 gestrichen habe, weil DrayTek die Source Route-Option im WebInterface entfernt hat. Bei der Kerio-Firewall habe ich die Bezeichnung der einzelnen Anwendungen an die aktuellen Programmversionen angepasst.

Die folgenden Punkte könnten trotzdem interessant sein:

- Sollten Sie immer noch mit Administrator-Rechten im Internet surfen, sind vielleicht die ergänzenden Hinweise im Abschnitt *Hinweise → Keine Administrator-Rechte beim Internet-Surfen* wichtig.
- Wie Sie sich davor sichern können, dass die Kerio-Firewall durch ein Schadprogramm (z. B. den BugBear-Wurm) gewaltsam beendet wird, lesen Sie in Abschnitt VII. Dort finden Sie auch weiterführende Links, wenn Sie Hilfe brauchen oder den Eingangsbildschirm abstellen wollen.
- Falls Sie mit einer Firmware vor 2.3 Regeln eingegeben haben, bei denen Sie die Source Route-Option aktiviert hatten, lesen Sie bitte die wichtigen Hinweise unter *Source Route* bei den *Begriffserläuterungen*
- Im Abschnitt *IV. Hinweise→Kann die Firewall mehr ?* finden Sie bei den Überlegungen zu ‚ipf rule' einige interessante Feststellungen und eine Möglichkeit, sich weitere Infos über die Firewall in einem solchen Umfang zu beschaffen, dass diese Anleitung nur noch als ‚Randnotiz' Bestand haben kann. Einen persönlichen ‚Traum' konnte ich mir an dieser Stelle ebenfalls nicht verkneifen.
- Ebenfalls unter *IV. Hinweise→Kann die Firewall mehr ?* wird erstmals die Option ‚Branch to Other Filter Set' erklärt

- In den *Begriffserläuterungen* finden Sie jetzt auch Abschnitte zu *DDoS* und *DoS*

❖ Im übrigen ist folgendes neu:

- Alle Links sind geprüft und erforderlichenfalls angepasst. Die Liste der weiterführenden Hinweise und Links wurde erheblich erweitert.
- Keep State wird jetzt in den *Begriffserläuterungen* (hoffentlich) richtig erklärt
- Der Abschnitt NetBIOS in den *Begriffserläuterungen* wurde komplett überarbeitet. In diesem Zusammenhang wird das direct hosting und das SMB (Server Message Block)-Protokoll kurz angesprochen.
- Source Route wird in den *Begriffserläuterungen* vollständig erklärt (leider zu spät: Die Firmware 2.3 unterstützt diese Option nicht mehr).
- In den *Begriffserläuterungen* finden Sie zusätzliche Abschnitte zu *ActiveX, Cookies, Java,* dem *Referrer und Web Bugs (Clear GIFs).*
- Die Hinweise (Wie kann/sollte man den Rechner weiter absichern ?) enthalten einen Mini-Erfahrungsbericht über die Tiny Personal Firewall 3.0, eine Empfehlung für einen Autostart-Manager und Überlegungen zu einem Content-Filter für ausgehende Datenpakete.
- In den Hinweisen habe ich mir außerdem Gedanken darüber gemacht, ob Firewalls wegen der sogenannten Tunnel-Programme überhaupt einen Sinn machen.
- Das neue Kapitel VIII. enthält ein Quickstart-Regelwerk für den ersten Anfang

## II. Kommentierte Übersetzung des Handbuches

### Vorbemerkung

Die folgende Übersetzung gibt den Abschnitt 5.6 des Handbuches wieder, welches mit meinem Vigor 2200X (Firmware bei Auslieferung: 2.0a) ausgeliefert wurde. Der englische Text kann unter

ftp://ftp.draytek.com.tw/VIGOR2200/MANUAL/USER'S%20GUIDE.zip

nach wie vor heruntergeladen werden (im ZIP-Archiv ist es die Datei IPFILTER.PDF)

### Allgemeines

Die Einstellungen finden sich im Advanced Setup unter IP Filter/Firewall Setup.

Der Router enthält zwei Arten von Filtern, nämlich die Anruffilter (Call Filter) und die Datenfilter (Data Filter).

Die Anruffilter entscheiden, ob bei nicht bestehender Verbindung mit einem bestimmten Datenpaket eine Verbindung hergestellt werden darf, der Datenfilter entscheidet, ob der Pakettyp, der versandt werden soll, gesperrt ist oder nicht. Ist er gesperrt, so wird er verworfen, andernfalls zum Versand freigegeben.

Ein ankommendes Paket wird sofort durch den oder die Datenfilter geschickt und entweder verworfen oder an das LAN (Local Area Network) weitergeleitet.

Es gibt 12 Filter-Sets, die jeweils bis zu 7 Regeln enthalten können, so dass insgesamt 84 Filter-Regeln definiert werden können. In der Standardeinstellung sind die Anruffilter-Regeln im ‚Set 1' und die Datenfilter-Regeln im ‚Set 2'.

Um die Arbeitsweise der Filter besser zu verstehen, empfiehlt es sich, zunächst im Anhang unter *Socket* den Zusammenhang zwischen IP-Adresse und Port-Nr. nachzuschlagen.

**Das Eingangsmenu**

3 Menupunkte stehen zur Wahl:

| | |
|---|---|
| **General Setup** | generelle Einstellungen für die Firewall |
| **Filter Setup** | die 12 Filter-Sets können erstellt/bearbeitet werden |
| **Set to Factory Default** | die Filterregeln werden auf die Standardwerte zurückgestellt |

**General Setup**

**Call Filter** Anruffilter können ein- (Enable) und ausgeschaltet (Disable) werden. Außerdem kann eingestellt werden, mit welchem Set die Call-Filter beginnen (Start Filter Set). Standardmäßig beginnen die Call-Filter vor den Datenfiltern. Das macht deshalb Sinn, weil man von dem Filter-Set, mit dem die Call-Filter beginnen, auf weitere Filter-Sets verweisen kann, so dass die später definierten Datenfilter zugleich als Call-Filter fungieren. (vgl. zum Sinn der Call-Filter noch unter *Einige persönliche Anmerkungen*)

**Data Filter** Datenfilter können ein- (Enable) und ausgeschaltet (Disable) werden. Außerdem kann eingestellt werden, mit welchem Set die Datenfilter beginnen (Start Filter Set).

Um es klar zu machen: Durch die Unterscheidung zwischen Anruf- und Datenfilter habe ich die Möglichkeit, ein Filterset vor die eigentlichen Datenfilter zu setzen, welches nur durchlaufen wird, wenn keine Internet-Verbindung besteht. Hierdurch kann ich – wenn mir eine passende Regel einfällt –, die Verbindungsaufnahme zu einer bekannten IP-Adresse oder über bestimmte Ports verhindern, um z.B. unnötige Kosten zu verhindern. Gleichzeitig kann ich aber den Datenaustausch in den Datenfiltern zulassen, wenn bereits eine Verbindung besteht (z.B.: Ein Programm gleicht die Uhrzeit im Computer mit der Atomzeit ab, indem es sich mit einer bestimmten IP-Adresse verbindet. Dies soll das Programm auch tun, aber eben nur dann, wenn aus anderen Gründen bereits eine Verbindung besteht).

**Log Flag** für die Fehlersuche kann das Verhalten der Filter protokolliert werden

| | |
|---|---|
| **None** | nichts wird protokolliert |
| **Block** | alle blockierten (verworfenen) Pakete werden protokolliert |
| **Pass** | alle Pakete, die die Filter passieren durften, werden protokolliert |
| **No Match** | alle Pakete, auf die keine Regel zutraf, werden protokolliert |

Das Protokoll kann mit TELNET betrachtet werden. TELNET meint in diesem Zusammenhang das mit Windows mitgelieferte Terminal-Programm (Telnet heißt aber auch das zu TCP/IP gehörende Protokoll für virtuelle Terminals, s. Anhang). TELNET wird gestartet mit:

Start->Ausführen und der Eingabe

telnet 192.168.1.1

wobei die Zahl hinter Telnet die IP-Adresse des Routers angibt. Im obigen Beispiel wurde die Standard IP-Adresse des Routers verwandt. Falls diese geändert wurde, muss natürlich die geänderte Adresse angegeben werden. Nach Abfrage des (hoffentlich vergebenen) Passwortes kann mit

log –f

(Kleinschreibung beachten !)

die Protokoll-Datei betrachtet werden. Weitere Einzelheiten zu TELNET in Verbindung mit dem Vigor-Router befinden sich in Kapitel 8 des Original-Handbuches und nachfolgend unter ‚Hinweise'.

**MAC Address for Logged Packets Duplication**

MAC (Media Access Control) hat in diesem Zusammenhang nichts mit apple zu tun, sondern gibt eine in alle Netzwerkkomponenten fest eingebaute Adresse an, die weltweit einmalig sein soll (nicht mit IP-Adresse verwechseln). MAC-Adressen sehen z.B. so aus: 00-80-C7-6D-A4-6E. Die MAC-Adresse des Routers wird im Hauptbildschirm der Router-Konfiguration angezeigt.

Wenn also ein Duplikat der Protokoll-Datei an eine andere Netzwerkkomponente versandt werden soll, muss hier die entsprechende MAC-Adresse (im HEX-Format, Zahlensystem auf der Basis 16 [0....9 und A...F]) eingetragen werden. Soll diese Funktion abgeschaltet werden, so ist an Stelle der MAC-Adresse ‚0' einzugeben.

**Filter Setup**

| | |
|---|---|
| **Comments** | Beschreibung des Filter-Sets (max. 22 Buchstaben) |
| **Filter Regeln** | ein Klick auf den gewünschten Zahlenschalter ermöglicht das Erstellen/Bearbeiten der gewählten Regel |
| **Active** | Ein- und Ausschalten der Regel |
| **Next Filter Set** | Verweis auf ein weiteres Filter-Set, welches nach dem aktuellen Filter-Set bearbeitet werden soll. Das Original-Handbuch weist etwas missverständlich darauf hin, dass mit den Filtern keine Schleife gebildet werden darf (‚The |

Filters cannot be looped'). Gemeint ist damit, dass nur auf nachfolgende und nicht auf vorangehende Filter-Sets verwiesen werden darf.
***Wichtig:*** Der Verweis muss auch dann gesetzt werden, wenn das *nachfolgende* Filterset anschließend abgearbeitet werden soll. Wenn Sie hier ‚None' eintragen, macht die Firewall nach dem Filterset Schluss, was insbesondere dann fatal ist, wenn Sie Ihren Regelsatz so aufgebaut haben, dass am Ende im letzten Set eine ‚deny all'-Regel alles blockt, was nicht vorher erlaubt wurde (wird bei den Filterbeispielen noch erläutert).
Lediglich bei den Call-Filtern kann man überlegen, ob es Sinn macht, auf die nachfolgenden Datenfilter zu verweisen. Dies hängt davon ab, welche Regel-Arten man bei den Call-Filtern definiert hat.

**Bearbeiten der Filter-Regeln**

**Comments** Beschreibung der Filter-Regel (max. 14 Buchstaben)
**Active** Ein- und Ausschalten der Regel
**Pass or Block** gibt an, was zu tun ist, wenn die Regel zutrifft

**Block Immediately** Paket wird sofort verworfen, wenn die Regel zutrifft

**Pass Immediately** Paket wird sofort weitergeleitet, wenn die Regel zutrifft (Bei der Verwendung dieser Option ist natürlich Vorsicht geboten: Wenn diese Regel zu großzügig oder fehlerhaft formuliert ist, hilft es nichts mehr, dass später möglicherweise sehr detaillierte Sperrregeln formuliert sind, denn diese Regeln werden gar nicht mehr abgearbeitet !)

**Block If No Further Match** das Paket wird verworfen, es sei denn eine spätere Regel lässt es ausdrücklich zu. Ich habe diese Option ‚bedingte Verwerfung' genannt. Gemeint ist: Grundsätzlich sollen Pakete, die die Regel erfüllen, nicht weitergeleitet werden; in einer späteren Regel folgt aber eine Ausnahme für eine Untermenge aus der Menge der Pakete, für die die aktuelle Regel zutrifft, und diese Untermenge soll zugelassen werden.

**Pass If No Further Match** das Paket wird zugelassen, es sei denn eine spätere Regel verwirft es ausdrücklich. Ich habe diese Option ‚bedingte Zulassung' genannt. Gemeint ist: Grundsätzlich sollen Pakete, die die Regel erfüllen, weitergeleitet

werden; in einer späteren Regel folgt aber eine Ausnahme für eine Untermenge aus der Menge der Pakete, für die die aktuelle Regel zutrifft, und diese Untermenge soll verworfen werden.

**Branch to Other Filter Set** wenn die Regel zutrifft, verzweigt die nächste Filter-Regel zu dem hier angegebenen Filter-Set. Diesen Satz habe ich möglichst wortgetreu aus dem Originalhandbuch übersetzt. Die Beschreibung ist ebenso kurz wie falsch (genauer wird dies unter *IV. Hinweise→Kann die Firewall mehr ?* erläutert). Lassen Sie möglichst ‚None' stehen. Sie können aber auch irgendetwas anderes eintragen, wenn Sie es schaffen. Hierdurch wird nur Speicherplatz im Router verschwendet.

Der Router arbeitet in jedem Fall die nächste aktive Filter-Regel im aktuellen Set ab (beachte nochmals: bei den Filter-*Sets* muss ausdrücklich angegeben werden, dass das nächste Filter-*Set* aufgerufen werden soll).

**Log** Log-Funktion ein/ausschalten: Das erstellte Protokoll kann mit dem TELNET-Befehl log –f eingesehen werden (s.o.: General Setup) (eine genaue Beschreibung, wie Sie mit TELNET weiterkommen, finden Sie übrigens in den Erläuterungen zum Beispielfilterset unter ‚*Was fehlt ?*')

**Direction** bestimmt, ob ein- oder ausgehende Datenpakete von der Regel betroffen sind (der Menu-Punkt ist daher für Call-Filter irrelevant)

für Datenfilter**:**

**In** Regel gilt für ankommende Pakete

**Out** Regel gilt für abgehende Pakete

**Protocol** legt fest für welche Protokollart die Regel gilt (any [=jede], TCP, UDP, ICMP, IGMP, zur Erläuterung s. Anhang)

**IP Adress** bestimmt für welche Source- (=Quell-) Adresse bzw. für welche Destination- (=Ziel-) Adresse die Regel gilt. Dabei gilt es zu unterscheiden: Falls bei ‚Direction' ‚In' angegeben wurde, ist mit ‚Source' der externe Rechner und mit ‚Destination' der lokale Rechner gemeint, bei ‚Out' ist es genau umgekehrt. Ein ‚!'-Zeichen vor der Adresse bewirkt, dass die Regel für diese Adressen *nicht* gilt (entspricht

dem logischen Operator NOT (nicht)). Nicht mit dem unten beschriebenen Operator-Feld verwechseln. Achtung: die Angabe bestimmter Adressen für lokale Rechner macht natürlich nur dann Sinn, wenn diese fest und nicht dynamisch vergeben werden oder Sie mit einer passenden Subnetzmaske arbeiten.

**Subnet Mask** hier kann eine als Filter fungierende Subnet-Maske zur IP-Adresse eingetragen werden (dies führt an dieser Stelle zu weit, s. daher unter *Begriffserläuterungen* und bei der Beispielkonfiguration)

**Operator** logischer Operator mit folgenden Möglichkeiten:

= Wenn *End Port* leer bleibt, gilt die Regel für den bei *Start Port* angegebenen Port, andernfalls für alle Ports, die zwischen *Start Port* und *End Port* liegen (einschließlich *Start Port* und *End Port*). Wenn Sie gar nichts eintragen gilt die Regel für alle Ports.

!= Wenn *End Port* leer bleibt, gilt die Regel für alle Ports die nicht den bei *Start Port* angegebenen Wert haben, andernfalls für alle Ports, deren Werte nicht zwischen *Start Port* und *End Port* liegen (einschließlich *Start Port* und *End Port*)

**>** Die Regel gilt für alle Ports, die größer *oder gleich* dem bei *Start Port* angegebenen Wert sind.

**<** Die Regel gilt für alle Ports, die kleiner *oder gleich* dem bei *Start Port* angegebenen Wert sind.

**Keep State** Wenn dies angekreuzt wird, wird die Protokoll-Information über die TCP/UDP/ICMP-Kommunikations-Sitzung von der IP-Filter/Firewall aufbewahrt. Die Firewall-Protokoll-Möglichkeit setzt voraus, dass TCP oder UDP oder TCP/UDP oder ICMP ausgewählt wurde, damit diese Operation korrekt funktioniert.
Wer mit dieser (von mir möglichst wörtlich) übernommenen Übersetzung aus dem Original-Handbuch etwas anfangen kann, ist ein Künstler. Eine Erklärung finden Sie unter *Begriffserläuterungen.*

**Source Route** = Quell-Route (in den Handbüchern nicht erläutert, ab Firmware 2.3 aus dem WebInterface entfernt, wird aber unter *Begriffserläuterungen* trotzdem erklärt, beachten Sie bitte unbedingt die Hinweise dort, wenn Sie auf die Firm-

ware 2.3 umsteigen und vorher Regeln benutzt haben, bei denen die Source Route-Option aktiviert war !)

**Fragments** Behandlung fragmentierter Datenpakete

**Don't Care** Regel gilt unabhängig davon, ob das Datenpaket fragmentiert ist oder nicht

**Unfragmented** Regel gilt nur bei nicht fragmentierten Datenpaketen

**Fragmented** Regel gilt nur bei fragmentierten Datenpaketen

**Too Short** Regel gilt nur bei Datenpaketen, die zu klein sind, um einen kompletten TCP-Header zu haben. Anmerkung von mir: Bei der so genannten Tiny Fragment Attacke erzeugt der Hacker extrem kleine Datenpakete, von denen nur das erste den TCP-Header enthält. Dadurch soll der Router veranlasst werden, nur das erste Fragment zu prüfen und die restlichen ungeprüft durchzulassen. Nach meiner Auffassung sollte daher eine Regel verfasst werden, die nur für Pakete gilt, die ‚too short' (zu kurz) sind, und die diese Pakete auf allen Ports verwirft.

## III. Begriffserläuterungen

**ActiveX** ist eine von MicroSoft erfundene Technologie, die es ermöglichen soll, Funktionen des Windows-Betriebssystems für Web-Seiten nutzbar zu machen. Die Technologie umfasst ActiveX-Controls, Active Documents und Active Scripting. Mit Active Documents können Dokumente, die nicht im html-Format geschrieben wurden, im Browser angezeigt werden. Mit Active Scripting fasst Microsoft die Skript-Sprachen JScript (die stark erweiterte MicroSoft-Version von JavaScript) und das auf Visual Basic-basierende VBScript zusammen. ActiveX-Controls sind kleine Programme oder Programm-Module, die beim Aufruf einer Web-Seite über den Internet Explorer auf den Rechner des Surfers geladen und dort mit Hilfe des Internet Explorers ausgeführt werden. Die ActiveX-Controls können auf andere ‚Objekte', insbesondere Teile des Windows-Betriebssystems (z.B. DLL's), zugreifen und dadurch praktisch alle Aktionen ausführen, die auch dem aktuellen Benutzer erlaubt sind: Sie haben Zugriff auf den gesamten Arbeitsspeicher, können alle Betriebssystemfunktionen aufrufen und auf das Dateisystem des angemeldeten Benutzers und das Netzwerk zugreifen. Gerade deshalb ist es außerordentlich leichtsinnig, als Administrator im Internet zu surfen. MicroSoft hat versucht, mit der selbstentwickelten Authenticode-Technologie die Risiken einzugrenzen. Die Signatur erlaubt jedoch nur die sichere Identifizierung des Absenders und den Nachweis der Echtheit des übertragenen Codes. Die Signatur beinhaltet keine Beschränkung des Funktionsumfangs des Programms und gibt nur wieder, dass die Programmierer der Auffassung waren, ihr Programmcode stelle kein Sicherheitsrisiko dar. Unter Sicherheitsgesichtspunkten kann man daher nur empfehlen, das gesamte ActiveX im Internet Explorer abzuschalten. Nach meinen persönlichen Erfahrungen ist es dann aber praktisch unmöglich, im Internet zu surfen. Hier dürfte der Umstieg auf einen anderen Browser als den Internet Explorer eher zu befriedigenden Ergebnissen führen. Ergänzende Informationen und Hilfe bei dem Versuch, einen Kompromiss zu finden, liefert in hervorragender Weise der Browsercheck der c't [51].

**ARP** s. (R)ARP

**Clear GIFs** s. Web Bugs

**Cookies** (‚Kekse') sind kleine Textdateien, die eine angesteuerte Web-Seite auf dem eigenen Rechner ablegt, z.B. um den Besucher zu identifizieren, zu kontrollieren, welche Seiten der Besucher auf der Site ansteuert, und bestimmte Daten über den Besucher zu speichern, um diesem bei einem späteren Besuch, ‚das Leben zu erleichtern'. Welche Daten gespeichert werden, entscheidet der Programmierer der Web-Seite. Hier entsteht bereits die erste Verwirrung: Teilweise wird einfach behauptet, die Cookies könnten keine eMail-Adresse und keinen Namen speichern. Das ist so einfach unrichtig [50]. Die Hilfe zum Internet Explorer 6.0 erklärt es richtig: Wenn ich der angesteuerten Web-Seite diese Daten freiwillig – z.B. über ein Formular – zur Verfügung stelle, können sie auch im Cookie gespeichert werden. Eine andere Frage ist, ob die angesteuerte Web-Seite dies tut. Hierzu muss ich mir die Privacy Policy (Erklärung zum Datenschutz) der angesteuerten Seite ansehen (z.B. des Heise Zeitschriften Verlages [49]). Wenn ich dieser Seite vertraue und hier versichert wird, dass personenbezogene Daten, wie Name, Adresse, Postanschrift, Telefonnummer, eMail usw., nur auf besonders geschützten Servern in Deutschland abgelegt werden,

kann ich davon ausgehen, dass diese Daten nicht im Cookie enthalten sind, sondern nur von der Seite, die den Cookie gesetzt hat, über eine Kenn-Nr. im Cookie mit den Daten auf dem Server abgeglichen werden können. Gibt es auf der angesteuerten Web-Seite eine solche Erklärung nicht, kann ich eben nicht sicher sein, dass persönliche Daten nicht im Cookie landen.

Die Verwendung der Cookies ist in den meisten Fällen sicher ‚gut gemeint', Sie werden jedoch durch diese Cookies (auch wenn keine persönlichen Daten gespeichert werden) ausspioniert und es können ganze Benutzerprofile über Sie angelegt werden. Die Betreiber verschiedener Web-Seiten schließen sich zu Informations-Allianzen zusammen [48], durch die Informationen, die eigentlich nur dem Betreiber einer Web-Seite zur Verfügung stehen, auch anderen Betreibern zugänglich gemacht werden, so dass sich auf diese Weise umfassende Übersichten über Ihre Vorlieben erstellen lassen. Richtig gefährlich werden Cookies dann, wenn es einer anderen Web-Seite gelingt, die von anderen gesetzten Cookies auszulesen. Werden in Cookies Kreditkarten-Daten, Passwörter, PIN's und andere geheimhaltungsbedürftige Daten gespeichert, die eigentlich nur dem Betreiber der Web-Seite übermittelt werden sollten, der die Cookies gesetzt hat, dann hat man ein sehr ernstes Problem, wenn diese Cookies zu allem Überfluss auch noch von anderen Personen ausgelesen werden können. Die diesbezügliche Sicherheitslücke, die der Internet-Explorer in den Versionen 5.5 und 6 aufwies, soll nach Auskunft von MicroSoft [45] inzwischen geschlossen worden sein. Wichtig ist es daher zunächst einmal, den Sicherheits-Patch von MicroSoft einzuspielen. Davon unabhängig tauchen aber immer wieder neue Methoden auf, mit denen es nach wie vor möglich sein soll, die Cookies auszulesen [46]. Aus Sicherheitsgründen sollten Cookies daher nicht zugelassen werden (im IE 6.0 unter *Extras→Internetoptionen→Datenschutz* den Regler auf *Alle Cookies sperren* schieben). Mit dieser Einstellung werden Sie an allen möglichen Stellen Probleme bekommen: Insbesondere der Online-Einkauf und viele Seiten, auf denen Sie sich einloggen müssen (ebay, Foren etc.), werden Sie nicht mehr nutzen können. Hier müssen Sie selbst entscheiden (nachdem Sie sich die Privacy Policy der Seite angesehen haben), ob Sie auf diese Angebote verzichten oder das Risiko eingehen wollen, vorübergehend (!) die Datenschutz-Sicherheitsstufe so weit herunterzuschieben, bis Sie mit der angesteuerten Seite klarkommen. Im zuletzt genannten Fall würde ich aber sofort (!) – noch vor Verlassen der Seite – alle Cookies löschen (im IE 6.0 unter *Extras→Internetoptionen→Allgemein:* Cookies löschen) und die Datenschutz-Sicherheitsstufe wieder heraufschieben. Die Möglichkeiten, die der Internet Explorer selbst bietet, um die Cookies einzudämmen, erklärt die Hilfe zum Internet Explorer ausführlich und anschaulich. Als sehr nützlich habe ich auch den CookieCop 2 [47] empfunden, mit dem man nicht nur die Cookies und den Referrer (s. dort) blockieren (oder zulassen), sondern auch PopUp-Fenster verhindern kann. Ein weiteres nützliches Programm, welches Cookies, den Referrer und Web Bugs (s. dort) filtert, ist der WebWasher [59]. Wenn Sie Cookies auch nur eingeschränkt oder gelegentlich zulassen, würde ich diese aber regelmäßig, spätestens beim Schließen des Browsers, allerspätestens vor dem Herunterfahren des Rechners löschen.

**Dateien- und Druckerfreigabe** s. NetBIOS

**DDoS** ‚Distributed Denial of Service'-Angriffe unterscheiden sich von DoS-Angriffen (s. zunächst unter *DoS*) dadurch, dass sie von einer Vielzahl von Computern geführt werden. Der eigentliche Angreifer schmuggelt z.B. Trojaner auf die Computer ande-

rer Anwender, die hierdurch zugleich Opfer und Angreifer werden. Dies macht zum einen deshalb Sinn, weil hierdurch die IP des eigentlichen Angreifers geheim bleiben kann, und ist zum anderen bei den Angriffsmethoden erforderlich, die eine deutlich höhere Bandbreite auf Seiten des Angreifers erfordern.

**DHCP** (Dynamic Host Configuration Protocol) ist ein spezielles System, mit dem den angeschlossenen Rechnern z.B. vom Router automatisch IP-Adressen aus einem vorbestimmten Kontingent zugewiesen werden

**Direct Hosting** s. NetBIOS

**DNS** (Domain Name Service oder Domain Name System) dient dazu, den Internet-Adressen (Domain-Namen, z.B. www.xyz.de) konkrete IP-Adressen (z.B. 193.xxx.xx.xxx) zuzuordnen (Hinweis: An einigen Stellen im Internet wird verbreitet, die DNS-Server von t-online hätten die Adressen 194.25.2.129 bis 194.25.2.134, dies ist in dieser Allgemeinheit nicht richtig: Diese Adressen werden von meinem System nur in Ausnahmefällen verwandt, vermutlich dann, wenn der eigentlich ‚zuständige' Server ausgefallen oder überlastet ist (s. unter IP-Adresse wegen der Suche nach den ‚richtigen' Adressen). Der Vigor-Router besitzt einen Cache (Zwischenspeicher), der externe Anfragen speichert und bei der nächsten Anfrage zunächst versucht, diese aus dem Cache zu beantworten. Teilweise wird in den Vigor-Handbüchern empfohlen, im Menu *Basic Setup > Ethernet TCP/IP and DHCP Setup* im Unterpunkt *DNS Server IP Adressen* die vom ISP (Internet Service Provider = Internet Dienste Anbieter, z.B. t-online) verwandten oder empfohlenen Adressen einzutragen. Im Original-Handbuch steht dagegen, dass der Cache im Router nur dann eingreift, wenn *beide* Adressfelder leer bleiben. Ferner empfiehlt t-online, für die DNS-Server keine festen Adressen vorzugeben, weil t-online dann automatisch auf einen anderen Server umschalten kann, wenn einer gestört ist. Bei T-Online ist die Angabe bestimmter Adressen insbesondere auch deshalb problematisch, weil t-online über eine Vielzahl von Servern verfügt, die t-online austauscht und beim Router nur 2 Adressen eingegeben werden können (daher hier – jedenfalls bei t-online – nichts eintragen).

**DoS** steht natürlich einmal (mit großem ‚O') für das ‚Disk Operating System' (Laufwerk-Betriebssystem), aber auch für ‚Denial of Service' (frei übersetzt: Dienstverweigerung). Bei einer DoS-Attacke werden Dienste auf einem Server z.B. durch eine Vielzahl von Anfragen oder dadurch lahm gelegt, dass man versucht, den Server zum Absturz zu bringen.

Das WebInterface des Vigor-Routers hat unter der Firmware 2.3 unter diesem Menu-Punkt folgendes zusammengefasst (in der Fw 2.3.1 fehlt das Menu):

- **Fraggle**: funktioniert wie Smurf, verwendet aber UDP Echo Request-Pakete statt ICMP Echo Request-Pakete.

- **ICMP Flood**: Der Angreifer sendet ICMP-Pakete bis der Opferrechner zusammenbricht. Der Angreifer muss natürlich über eine größere Bandbreite als sein Opfer verfügen oder mehrere angreifende Rechner ‚bündeln' (‚Threshold' und ‚Timeout' werden unter *SYN Flood* erklärt*)*.

- **ICMP fragment**: Fragmentierte ICMP-Pakete können zum einen dafür verwandt werden, ein Netzwerk auszuforschen, denn wenn das Opfer nicht alle Pakete erhält, fordert es die restlichen an. Hierdurch erhält der Angreifer Informationen über sein Opfer. Zum anderen können solche Pakete, wenn sie in ausreichender Anzahl verschickt werden, natürlich auch den Opfer-Rechner stilllegen, weil dieser durch das Nachfordern der fehlenden Pakete ausgelastet wird.

- **IP Options** sind ein variables Feld im Header eines jeden IP-Paketes. Nur das Feld ist immer in den Paketen enthalten, die Optionen müssen allerdings nicht gesetzt sein. Ein Beispiel für solche Optionen sind ‚Strict Source and Record Route' und ‚Loose Source and Record Route' (s. unter *Source Route*). Die Optionen können z.B. aber auch Sicherheitsrestriktionen (von ‚unclassified' bis ‚Top Secret') enthalten. Da das Feld im Internet nur selten verwandt wird, werden Pakete, in denen die IP-Optionen ausgefüllt sind, oftmals nicht richtig verarbeitet. Dies kann zum Absturz des Systems oder dazu führen, dass Sicherheitsmechanismen umgangen werden.

- **Land**: dient wie SYN Flood ebenfalls dazu, mittels des IP-Handshake (s. unter Keep State) den Rechner zum Absturz zu bringen. Der Angreifer schickt ein Paket, dessen gefälschte Absenderadresse und Port der angegriffene Rechner selbst ist. Das SYN-Flag, welches die Verbindungsaufnahme einleitet, ist gesetzt. Falls das System keine Absicherung beinhaltet, versucht der Rechner, sich selbst zu antworten und stürzt irgendwann ab. Dürfte bei neueren Betriebssystemen keine Gefahr mehr darstellen.

- **Ping of Death**: Bei dieser Angriffsmethode werden ICMP Echo Request-Pakete (Pings) mit mehr als 65.535 byte (= maximal zulässige Größe für ein IP-Paket) verschickt. IP-Pakete, die größer als 65.535 byte sind, werden vor dem Versenden in Fragmente zerlegt und erst beim Empfänger anhand eines Offset-Wertes wieder zusammengefügt. Der Offset des letzten Paketes wird so manipuliert, dass beim Empfänger ein Paket mit mehr als 65.535 byte entsteht. In älteren Betriebssystemen lief hierdurch der Buffer für IP-Pakete über. Der Rechner stürzte ab oder bootete neu. Windows-Rechner ab w98 sind nicht gefährdet.

- **Port Scan detection**: Nach der sehr dürftigen Hilfe des WebInterfaces sollen durch diese Option Port-Scan-Angriffe abgewehrt werden, um dieses Sicherheitsloch zu schließen. Leider gibt es eine Vielzahl von Port-Scan-Methoden und es würde an dieser Stelle zum einen zu weit führen, diese alle zu erläutern, und zum anderen auch nichts bringen, weil unklar ist, was und wie der Router solche Angriffe genau abwehrt, wenn man diese Option aktiviert (ein Beispiel habe ich unter *TCP flag scan* erklärt). Ganz allgemein gesprochen, ist ein Port-Scan der Versuch, offene Ports auf einem Rechner zu finden. Zu diesem Zweck werden alle, in der Regel aber nur speziell ausgesuchte Ports auf dem Zielsystem der Reihe nach angesprochen, um festzustellen, ob dieser Port ‚offen' ist (wie das gehen kann, ist ebenfalls beispielhaft unter *TCP flag scan* aufgeführt). Sinn macht ein solcher Port-Scan z.B., um zu ermitteln, ob sich auf dem angegriffenen System ein Trojaner eingenistet und einen oder mehrere Ports geöffnet hat, um seine Dienste anzubieten. Eine Firewall kann

Port-Scans daran erkennen, dass von einer IP ungewöhnlich viele Verbindungsanfragen an verschiedene Ports gestartet werden. Die Firewall sollte solche IP's für eine bestimmte Zeit sperren. Hier sieht man auch gleich die erste Schwachstelle der ‚Port Scan detection' des Vigor: Man kann zwar den Schwellenwert (‚Threshold') in Paketen pro Sekunde einstellen. Wenn der Angreifer aber sein Angriffsprogramm noch langsamer einstellt, wirkt die Blockade nicht mehr. Da viele Port-Scanner die Möglichkeit bieten, die Absender-IP zu fälschen, kann ein Port-Scan auch von beliebig vielen IP's durchgeführt werden; die Firewall erkennt den Angriff nicht und der Angreifer hat durch die Fälschung der IP außerdem seine richtige IP getarnt. Die Fälschung kann außerdem dazu verwandt werden, dem angegriffenen System wichtige Zugänge zu sperren: Benutzt der Angreifer als Absende-IP z.B. die Adresse des DNS-Servers des angegriffenen Systems, so sperrt die Firewall dem eigenen System den Zugang zum DNS-Server mit der Folge, dass das angegriffene System nicht mehr ins Internet kommt. Natürlich kann man auf diese Weise auch ‚rechtmäßige' Benutzer des Systems ausschließen, indem man deren IP für den Angriff benutzt. Wie lange die verdächtigen IP's gesperrt werden, lässt sich der ‚Mini-Hilfe' des Vigors nicht entnehmen. Gut wäre es, wenn man bestimmte Adressen (z.B. den DNS-Server) von der Blockade durch die ‚Port Scan detection' ausnehmen könnte.

In letzter Zeit liest man häufiger von Fehlalarmen im Zusammenhang mit Port-Scans. Anwender glauben, das Ziel von Hackern geworden zu sein, weil sie eine Vielzahl von Verbindungsversuchen auf *einen* bestimmten Port feststellen. In Wirklichkeit hängt dies mit der dynamischen IP-Vergabe und der Tatsache zusammen, dass Tauschbörsen immer weitere Verbreitung finden. Wird nämlich eine IP vergeben, die vorher ein Teilnehmer an einer solchen Börse hatte, so versuchen die anderen Teilnehmer der Börse auch nach der Neuvergabe der IP mit dem früheren Inhaber dieser IP Kontakt aufzunehmen. Ob der Vigor die Blockade auch dann aktiviert, wenn er eine Vielzahl von Verbindungsversuchen auf *denselben* Port oberhalb des Schwellenwertes feststellt, lässt sich der Beschreibung nicht entnehmen.

- **Smurf Attack**: Es werden eine Vielzahl von Anfragen (ICMP Echo Request [Ping]) an die Broadcast-Adresse (255.255.255.255) eines Netzwerkes abgeschickt. Auf diese spezielle Adresse sollen alle in das Netzwerk eingebundenen Geräte antworten (auf diese Weise sucht z.B. auch der bei den Vigors mitgelieferte Virtual TA den Router). Als Source Adresse, also als Adresse des scheinbar Anfragenden, wird die IP des Opfers angegeben, welches vor lauter ‚Antworten' zusammenbricht.

- **SYN Flood**: Der Angreifer schickt eine Vielzahl von Datenpaketen mit gesetztem SYN-Flag und gefälschter Absenderadresse an den Opferrechner, und täuscht dadurch Verbindungsabsichten vor. Das Opfer schickt Antwortpakete mit gesetztem SYN- und ACK-Flag, bekommt aber keine Pakete mit gesetztem ACK-Flag zurück, wie es richtig wäre (s. auch unter Keep State), sondern weiter Pakete mit SYN-Flag, die eine weitere Verbindungsaufnahme ankündigen. Das Opfer schreibt die Verbindungsdaten in seine Connection Table. Sobald diese voll ist, werden bis zum Timeout keine neue Verbindungen angenommen. Der Server ‚steht'. Das WebInterface erlaubt es, diesen ‚Timeout'

einzustellen und den Schwellenwert (‚threshold'), mit dem angegeben werden soll, wie viele Datenpakete pro Sekunde ankommen müssen, bevor die Regel greift.

- **SYN fragment**: Fragmentierte Datenpakete mit gesetztem SYN-Flag dienen dazu, das Opfer zu veranlassen, eine Vielzahl von Paketen mit gesetzten SYN- und ACK-Flags abzuschicken. Ein Paket mit gesetztem SYN-Flag dient dazu, eine Verbindung einzuleiten (s. im einzelnen unter Keep State) und wird im ‚normalen' Verkehr mit einem Paket mit SYN/ACK-Flag beantwortet. Der Sender des Paketes mit gesetztem SYN-Flag müsste jetzt eigentlich mit einem Paket mit gesetztem ACK-Flag antworten. Wenn es ihm durch die Fragmentierung des Paketes mit gesetztem SYN-Flag gelingt, die SYN/ACK-Pakete ‚ins Leere' laufen zu lassen, wartet der Opfer-Rechner vergeblich auf die Antwort und kann abstürzen, wenn man nur eine ausreichende Anzahl an ‚kaputten' SYN-Paketen schickt.

- **TCP flag scan**: Nach der im WebInterface angezeigten Kurzbeschreibung werden TCP-Pakete mit irregulären Flags geblockt, wenn man diese Option aktiviert. Unter *Keep State* habe ich erklärt, wie eine Verbindung unter TCP zustande kommt (3-way-handshake: 1. Paket mit SYN-Flag – 2. Paket mit SYN+ACK-Flag – 3. Paket mit ACK-Flag). Leider können Angreifer Datenpakete so manipulieren, dass darin Flag-Kombinationen enthalten sind, die im Protokoll nicht vorgesehen sind. Wenn die Firewall auf diese Pakete nicht richtig reagiert, kann ein solcher Scan benutzt werden, um das angegriffene System auszuforschen. So kann man z.B. Pakete erzeugen, in deren TCP-Header überhaupt kein oder umgekehrt alle Flags gesetzt sind. Ein geschlossener Port sendet als Antwort ein Paket mit gesetzten RST+ACK-Flags (der Empfang des Paketes wird bestätigt, gleichzeitig wird die Verbindung sofort abgebrochen). Ein offener Port antwortet nicht und verwirft diese ‚verbogenen' Pakete. Der Angreifer hat auf einfache Weise einen offenen Port gefunden. Auch bei dieser Option der Router-Firewall scheint es mit etwas merkwürdig, sie im ‚DoS defense setup' unterzubringen, weil der Angriff eher der Ausforschung dient und nicht einfach nur den angegriffenen Server lahm legen will (letzteres wäre eher die Folge einer etwas zu intensiven ‚Suche').

- **Tear Drop**: Wie bei ‚Ping of Death' macht sich der Angreifer den Umstand zu Nutze, dass große IP-Pakete in kleine zerlegt (fragmentiert) werden. Die Stelle, an die die Stücke im Paket gehören, wird durch einen Offset-Wert angegeben. Manipuliert man diesen Offset-Wert dergestalt, dass ein späteres Paket in ein anderes Paket ‚hineingeschrieben' wird, entstehen negative Werte, die den Rechner zum Absturz bringen. Der Angriff funktioniert auf Windows-Rechnern nur mit w95 und NT4.

- **Trace Route**: Mit entsprechenden Programmen (z.B. unter Windows mit tracert.exe) können UDP-Daten-Pakete verschickt werden, um zu ermitteln, welche Route ein Datenpaket wahrscheinlich nehmen wird. Die Pakete werden dabei für einen nicht verwendeten Dienst (UDP-Pakete der Transportschicht mit ungültiger Portnummer) verschickt. Die sendenden Programme setzen dabei den TTL-Wert (time to live) im header des Paketes zunächst auf 1 und erhöhen diesen schrittweise. Jede Zwischenstation des Paketes reduziert den

TTL-Wert um 1. Ein Host, der ein Paket mit dem TTL-Wert 0 erhält, sendet eine ICMP-Nachricht vom Typ ICMP_TIME_EXCEEDED an den Sender zurück. Dadurch hat der Sender die IP-Adresse der Zwischenstation und zeigt sie an. Das gleiche Paket wird nunmehr mit einem TTL-Wert, der um 1 erhöht ist, verschickt. Der Sender hat jetzt die IP-Adresse der nächsten Zwischenstation. Dieses Spiel wiederholt sich bis das Paket sein Ziel erreicht hat. Jetzt sendet der Zielrechner eine ICMP-Nachricht vom Typ PORT_UNREACHABLE, weil das Paket für einen nicht verwendeten Dienst verschickt wurde. Auf diese Weise erkennt der Sender, dass das Ziel erreicht wurde. Der TTL-Wert kann höchstens 255 annehmen, was ausreichen dürfte.

Die sehr knappe Hilfe zu dem Menu-Punkt ‚Block Trace Route' im DoS defense Setup führt aus, durch diese Option werde ein Sicherheits-Loch geschlossen, welches ein Ausforschen von außen ermögliche. Dies deutet darauf hin, dass der Router auf Traceroute-Anfragen überhaupt nicht mehr antwortet, wenn die Option aktiviert wird. Dies würde allerdings nur noch mittelbar mit DoS-Attacken zusammenhängen, denn hierfür würde es ausreichen, wenn der Router solche Anfragen nur dann blockte, wenn Sie überhand nähmen. Leider ist es mir nicht möglich, genau herauszubekommen, was der Router macht, wenn man ‚Block Trace Route' aktiviert.

- **UDP Flood**: vom Prinzip her ähnlich wie SYN Flood und Smurf, allerdings wird das Opfer hier mit UDP-Paketen überflutet. Wie dies relativ einfach funktioniert, beschreibt PivX Solution [57]. Der Angreifer missbraucht einen Gameserver, indem er diesem per UDP eine Anfrage schickt. Die Gameserver beantworten solche Anfragen, indem sie Auskunft über ihren Zustand, die Anzahl der Spieler usw. liefern. Das anfragende UDP-Paket enthält eine falsche IP, nämlich die des Opfers. Der Gameserver kann dies nicht feststellen, weil UDP ‚verbindungslos' arbeitet, und schickt seine Antworten an den vermeintlich Anfragenden, in Wirklichkeit aber an das Opfer, welches vor lauter Antworten irgendwann zusammenbricht. (‚Threshold' und ‚Timeout' werden unter *SYN Flood erklärt)*

- **Unknown Protocol**: Das Internet Protokoll hat eine Reihe von IP-Protokoll-Typen, die undefiniert oder für eine spätere Verwendung reserviert sind [55]. Mit dieser Option im DoS defense Setup (!) soll es möglich sein, diese Typen zu sperren. Nach meiner persönlichen Auffassung gehört diese Sperre aber nicht ins DoS defense Setup und kann ebenso gut im ‚Filter Setup' mit geregelt werden.

**ftp** (File Transfer Protocol) Mit diesem Protokoll können Daten von einem entfernten Rechner geladen oder dort abgelegt werden

**http** (HyperText Transfer Protocol) Standarddatenübertragungsverfahren im Internet

**https** Absicherung des http-Übertragungsverfahrens durch SSL (Secure Socket Layer); ‚sichere Verbindung'

**ICMP** (Internet Control Message Protocol) dient hauptsächlich dem Austausch von Status- und Fehlermeldungen. Eigentlich sollte ICMP auf allen Ports verboten werden, weil hierdurch Firewalls ausgehebelt werden können (vgl. Jürgen Schmidt c't 11/97, S. 332). Allerdings funktioniert dann auch ‚Ping' nicht mehr. Eigentlich sollte es keine nennenswerten Schwierigkeiten geben, wenn ICMP bei einem privaten Internet-Rechner generell verboten wird (s. auch die Erläuterungen bei der *Beispielkonfiguration).*

**IGMP** (Internet Group Management Protocol) ist ein Hilfsprotokoll und unterstützt die Gruppenkommunikation. Es benutzt Class-D-IP-Adressen und wird für das Rundsenden an mehrere Interfaces eingesetzt. Eine Multicasting-Übertragung (z.B. für eine Videokonferenz) ist wirkungsvoller als eine Punkt zu Punkt Übertragung. Das Protokoll kann ebenfalls für Hackerangriffe missbraucht werden.

**IMAP** (Internet Message Access Protocol) ist ein Verwaltungs- und Übertragungsverfahren für e-mails (wird von den Providern seltener unterstützt, bietet im Gegensatz zu POP3 die Möglichkeit, die elektronische Post bereits auf dem Server zu bearbeiten/zu löschen)

**IP** (Internet Protocol) dient der Adressierung und Fragmentierung der Datenpakete und übermittelt diese vom Sender zum Empfänger

**IP-Adresse** (s. Socket, IP-Adressen) So kann man die IP-Adresse zu einem bestimmten Hostnamen finden:
Wenn Sie Windows NT/2000/XP benutzen geben Sie ein:
Start → Ausführen nslookup [Enter] *{Hostname}* [Enter] eingeben

Für Windows 95/98 können Sie unter www.pcpitstop.com/internet/nslook.asp das kleine Programm nslook kostenlos herunterladen, das ähnliche Funktionen hat.

Auf www.swhois.net unter ‚nslookup' kann ebenfalls der Hostname in eine IP-Adresse aufgelöst werden.

Schließlich habe ich unter http://www.atelier89.de/users/dirk/index.html die gültigen Adressen der DNS-Server von t-online gefunden.

Für t-online lauten die Host-Namen

www-proxy.t-online.de für den DNS-Server
pop.btx.dtag.de für den Posteingangsserver
mailto.btx.dtag.de für den Postausgangsserver
news.btx.dtag.de für den Newsserver
ftp-proxy.btx.dtag.de für den ftp-Proxy

Meine praktischen Erfahrungen mit den verschiedenen Ermittlungsmöglichkeiten sind folgende: Völlig korrekt arbeitet das w2k-Programm nslookup. www.swhois.net ermittelt alle Server richtig mit Ausnahme des DNS-Servers. Das w95/98-Programm nslook findet diesen und den Newsserver richtig, die Mailserver aber nur unvollständig. Unter www.atelier89.de/users/dirk/index.html kann nur der DNS-Server gesucht werden; dieser wird richtig gefunden.

**IP-Adressen** werden im Format x.x.x.x dargestellt, wobei die Punkte nur der besseren Lesbarkeit dienen; die Netzwerkkomponenten lesen die dargestellte Zahl als eine Zahl. Jedes ‚x' kann (theoretisch) Werte zwischen 0 und 255 ($2^8$ = 1 byte = 8 bit) annehmen. Die IP-Adresse ist also eine Zahl mit 32 bit.
Um dieses Zahlenformat zu verstehen, muss man sich klarmachen, dass ein bit nur die Werte 0 und 1 annehmen kann. Daher werden die IP-Adressen häufig in dualer Schreibweise dargestellt, Beispiele:

| Wertigkeit | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
|---|---|---|---|---|---|---|---|---|
| Bit-Nr. | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit-Wert | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Dezimalwert | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| Summe | 255 | | | | | | | |

| Wertigkeit | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |
|---|---|---|---|---|---|---|---|---|
| Bit-Nr. | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Bit-Wert | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Dezimalwert | 128 | 0 | 32 | 0 | 8 | 0 | 2 | 0 |
| Summe | 170 | | | | | | | |

Das duale Zahlensystem basiert also auf der Zahl 2, während wir es gewohnt sind, mit dem dezimalen Zahlensystem zu arbeiten, das auf der Zahl 10 basiert. Beim dezimalen Zahlensystem ist die rechte Ziffer einer jeden Zahl mit $10^0$ (also mit 1), die nächste, links danebenliegende Ziffer mit $10^1$ (also mit 10) usw. zu multiplizieren, beim dualen System ist mit $2^0$ (also mit 1), $2^1$ (also mit 2) usw. zu multiplizieren.

Von den Standardisierungsgremien sind die IP-Adressen in fünf Klassen aufgeteilt worden, von denen nur die drei Klassen A, B und C von praktischer Bedeutung sind.

Klasse A Adressen können theoretisch Werte von 1.0.0.0 bis 126.255.255.255, Klasse B Adressen von 128.0.0.0 bis 191.255.255.255 und Klasse C Adressen von 192.0.0.0 bis 223.255.255.255 annehmen.

Tabellarisch sieht das wie folgt aus:

| Adress-Klasse | als Standard vorgegebene bits | resultierender Wertebereich des ersten Byte (dezimal) | Netzwerk- (N)/ Rechner- (R) Teil* | Anzahl der möglichen Netze | Anzahl der verfügbaren Rechneradressen |
|---|---|---|---|---|---|
| Klasse A | 0xxx xxxx | 0 - 127 | N.R.R.R | 256 | 16.777.216 |
| Klasse B | 10xx xxxx | 128 - 191 | N.N.R.R | 65.536 | 65.536 |
| Klasse C | 110x xxxx | 192 - 223 | N.N.N.R | 16.777.216 | 256 |

* wird im Zusammenhang mit der Subnetzmaske erläutert

Wie Sie der Tabelle entnehmen können, ist für ein Klasse A-Netz das erste bit des ersten bytes vorgeschrieben (muss ‚0' sein), während für Klasse-B- bzw. Klasse-C-Netze die ersten beiden bzw. drei bits vom Standardisierungsgremium vorgegeben sind.

Für lokale Netze ohne Internetanbindung gibt es ausgesuchte Nummernkreise, die von keinem Router nach außen gegeben werden und mit denen man daher lokale Netze betreiben kann. Diese "privaten" Adressen sind:

- Class-A-Netz: 10.0.0.0 - 10.255.255.255
- Class-B-Netz: 172.16.0.0 - 172.31.255.255
- Class-C-Netz: 192.168.0.0 - 192.168.255.255

Die Werkseinstellung der Vigor-Routers hat sich aus diesem Nummernkreis die Nr. 192.168.1.1 für die eigene Adressierung herausgesucht und schlägt vor, den angeschlossenen Rechnern bei aktiviertem DHCP-Server 50 Nummern ab der Nr. 192.168.1.10 zuzuteilen. Diese Nr. vermittelt der Router nicht in das Internet, weil die Nrn. für den externen Verkehr gar nicht zugelassen sind. Vielmehr erhält der Router bei der Einwahl entweder vom Provider eine (in der Regel ständig wechselnde) IP-Adresse bzw. nimmt die Verbindung mit einer vom Provider fest zugeteilten IP-Adresse auf. Im Internet verkehrt der Rechner daher mit der vom Provider zugeteilten IP-Adresse, die der Router für den internen Verkehr auf die Adresse umsetzt (z.B. 192.168.1.10 bis 192.168.1.59), die er diesem Rechner selbst zugeteilt hat (bzw. bei fester Vergabe der IP-Adresse: mit der Adresse, unter der er mit dem Rechner in Verbindung steht).

Es leuchtet ohne weiteres ein, dass insbesondere ein Klasse-A-Netz mit bis zu 16.777.216 möglichen Rechnern unmöglich von einer Person verwaltet werden kann. Aus diesem Grunde gibt es die Möglichkeit, ein Netz durch eine so genannte Subnetzmaske (Subnet Mask) zu unterteilen. Dabei muss man sich diese Maske wie eine Art Filter vorstellen, der die IP-Adresse in einen Netzwerk-Teil und in einen Rechner-Teil aufspaltet. Jedes bit, welches in der Subnet-Maske auf ‚1' gesetzt ist, gibt an, dass es sich bei dem korrespondierenden Teil der IP-Adresse um einen Teil der Netzadresse handelt, während eine ‚0' angibt, dass das korrespondierende bit der IP-Adresse zur Rechneradresse gehört.

Einige Beispiele:

Die Default-Subnetzmasken, also die Masken, die anzuwenden sind, wenn man *keine* weitere Unterteilung haben will, sehen wie folgt aus:

| Adress-Klasse | Default-Subnetzmaske (binär) | Subnetzmaske (dezimal) |
|---|---|---|
| Klasse A | 11111111.00000000.00000000.00000000 | 255.0.0.0 |
| Klasse B | 11111111.11111111.00000000.00000000 | 255.255.0.0 |
| Klasse C | 11111111.11111111.11111111.00000000 | 255.255.255.0 |

Ändert z.B. der Verwalter eines Klasse-B-Netzes die vorbeschriebene Default-Subnetzmaske für dieses Netz nicht, liegen alle 65.536 Rechner, die ein solches Netz umfassen kann, in einem Netz, denn die beiden letzten byte jeder IP-Adresse geben bereits konkrete Rechner und nicht Netzwerke an (Beispiel: Der Betreiber des Klasse-B-Netzes hat die Nr. 128.159.xxxx.yyyy für sein Netz zugeteilt bekommen. Gleichgültig welche Zahlen für xxxx oder yyyy (zwischen 0 und 255) eingesetzt wer-

den, werden immer Rechner in demselben Netz angesprochen: 128.159.133.1 liegt in demselben Netz wie z.B. 128.159.1.189, 128.159.1.23, 128.159.77.89 usw.)

Ändert der Verwalter dagegen die Default-Subnetzmaske für ein Klasse-B-Netz in 255.255.***255***.0, so hat er damit 253 Subnets geschaffen (0, 127 und 255 sind für besondere Zwecke reserviert): Jetzt liegen im oben gebildeten Beispiel zwar die Adressen 128.159.2.1 und 128.159.2.15 in demselben Netz, jedoch nicht die Adressen 128.159.12.1, 128.159.12.15, 128.159.78.1, 128.159.78.187 usw..

Will der Verwalter nur zwei Netze schaffen, so kann er das mit der Subnetzmaske 255.255.128.0 (binär 11111111.11111111.***1***0000000.00000000) schaffen. Bei dieser Subnetzmaske ist nur das erste bit im dritten byte gesetzt, was bedeutet, dass die Rechner mit der Adresse 128.159.1.xxxx bis 128.159.126.xxxx in dem einen und die Rechner mit der Adresse 128.159.128.xxxx bis 128.159.254.xxxx im anderen Netz liegen.

Mit der Subnetzmaske 255.255.192.0 (binär 11111111.11111111.***11***000000.00000000) lassen sich in einem B-Klasse Netz vier Subnetze bilden.

Für ein C-Klasse-Netz sehen die Subnetzmasken wie folgt aus:

255.255.255.0 (binär 11111111.11111111. 11111111.00000000) >
255 Rechner in einem Netz

255.255.255.128 (binär 11111111.11111111. 11111111.***1***0000000) >
2 Netze mit ca. 128 Rechnern

255.255.255.192 (binär 11111111.11111111. 11111111.***11***000000) >
4 Netze mit ca. 64 Rechnern

Sie werden sich jetzt an dieser Stelle natürlich fragen, welchen Sinn eine Subnetzmaske bei den Filterregeln eines Routers machen soll, denn durch diese Filterregeln werden natürlich keine Subnetze gebildet. Die Antwort lautet, dass die Subnetzmaske als Filter fungiert, um ganze Bereiche von IP-Adressen zuzulassen oder zu sperren. Wenn Sie eine Regel definieren, nach der eine ausgehende Verbindung auf Port 25 (=SMTP=ausgehende Mail) nur an die Adresse 194.25.134.97 gerichtet werden darf und jetzt als Subnetzmaske 255.255.255.255 angeben, dann darf wirklich nur an die Adresse gesendet werden, die sie angegeben haben. Wenn Sie hingegen bei derselben Regel die IP-Adresse 194.25.134.0 und die Subnetzmaske 255.255.255.0 angeben, dann sind alle IP-Adressen von 194.25.134.0 bis 194.25.134.255 zugelassen. Jetzt wird vielleicht auch klar, warum in der Router-Konfiguration hinter den möglichen Einstellungen bei der Subnetzmaske immer ..../32, .../31 usw. eingeblendet wird: Die Zahlen hinter dem Schrägstrich geben an, welche Zahlen in dualer Schreibweise für den Router entscheidend sein sollen:

255.255.255.255/32 = 11111111.11111111.11111111.11111111 = alle Zahlen
255.255.255.000/24 = 11111111.11111111.11111111.00000000 = alle Zahlen außer denen hinter dem letzten Punkt

Mit dieser Information kommen Sie schon relativ weit, wenn Sie sich auf Subnetzmasken beschränken, die ganzzahlig durch 8 teilbar sind (.../32, .../24, .../16, .../8 = 255.255.255.255., 255.255.255.0, 255.255.0.0, 255.0.0.0): Bei 255.255.255.255 muss die IP-Adresse exakt stimmen. Bei 255.255.255.0 müssen nur die Zahlen vor dem letzten Punkt übereinstimmen, um die Regel in Kraft zu setzen usw.. Wollen Sie auch Zwischenwerte (.../31) definieren, so wird Ihnen nichts anderes übrig bleiben, als die zu sperrenden/zuzulassenden IP-Adressen zunächst in dualer Schreibweise zu notieren und mit einer entsprechenden Subnetzmaske in dualer Schreibweise zu ‚überlagern': Überall, wo in der Subnetzmaske eine ‚1' steht, prüft die Firewall auf exakte Übereinstimmung, überall, wo eine ‚0' steht, ist die Übereinstimmung gleichgültig.

Beispiel:

Zugelassen bzw. gesperrt werden sollen die Adressen 194.127.127.127 und 194.127.127.126

Sie geben als Subnetzmaske ein:

```
255.255.255.254/31 = 11111111.11111111.11111111.11111110

und als IP-Adresse:

194.127.127.127    = 11000010.01111111.01111111.01111111
```

Die ‚0' in der Subnetzmaske blendet die letzte duale Ziffer aus, so dass der Router nur auf Übereinstimmung der ersten 31 dualen Ziffern prüft; die letzte Ziffer ist gleichgültig (`11000010.01111111.01111111.0111111x` wird durchgelassen/gesperrt, egal welchen Wert ‚x' hat).

Durch die Subnetzmaske haben Sie mithin zugelassen/gesperrt:

```
194.127.127.127    = 11000010.01111111.01111111.0111111 1
194.127.127.126    = 11000010.01111111.01111111.0111111 0
```

Ein letztes Beispiel:

Sie geben als Subnetzmaske ein:

```
255.255.255.128/25 = 11111111.11111111.11111111.10000000
```

Dies bewirkt, dass nur die ersten 25 Stellen (in dualer Schreibweise !) der von Ihnen in der Konfiguration der Firewall angegebenen IP-Adresse maßgebend sind.

In der Konfiguration können Sie jetzt für die IP-Adresse z.B. Werte von 194.127.127.0 bis 194.127.127.127 angeben; das Ergebnis bleibt gleich: Wenn eine Verbindung zu einer Adresse angefordert wird, die zwischen 194.127.127.0 und 194.127.127.127 liegt, greift die Regel, wird eine Verbindung angefordert mit einer IP-Adresse zwischen 194.127.127.128 und 194.127.127.255, greift die Regel nicht.

Geben Sie hingegen für die IP-Adresse Werte von 194.127.127.128 und 194.127.127.255 an, so ist es genau umgekehrt: Wenn eine Verbindung zu einer Adresse angefordert wird, die zwischen 194.127.127.128 und 194.127.127.255 liegt, greift die Regel, wird eine Verbindung angefordert mit einer IP-Adresse zwischen 194.127.127.0 und 194.127.127.127, greift die Regel nicht.

Vergleichen sie hierzu die dualen Schreibweisen:

Subnetzmaske:

```
255.255.255.128/25 = 11111111.11111111.11111111.1 0000000
```

IP-Adresse

```
194.127.127.000    = 11000010.01111111.01111111.0 0000000
.
.
.
194.127.127.126    = 11000010.01111111.01111111.0 1111110
194.127.127.127    = 11000010.01111111.01111111.0 1111111

194.127.127.128    = 11000010.01111111.01111111.1 0000000
194.127.127.129    = 11000010.01111111.01111111.1 0000001
194.127.127.130    = 11000010.01111111.01111111.1 0000010
.
.
.
194.127.127.255    = 11000010.01111111.01111111.1 1111111
```

Die kursiv und unterstrichen dargestellten Teile der IP-Adresse sind unerheblich. Erst wenn an der 31. Stelle eine Abweichung auftritt, entscheidet sich, ob die Regel eingreift oder nicht.

**IPX/SPX-kompatibles Protokoll** (Internetwork Packet Exchange/Sequential Packet Exchange-kompatibles Protokoll): Das IPX/SPX-Protokoll wurde ursprünglich von Novell entwickelt. Die Microsoft Version entspricht diesem Protokoll. In Netzen mit älteren Novell-Servern ist dieses Protokoll zwingend erforderlich (neuere Novell-Versionen unterstützen TCP/IP). In (reinen) Windows-Netzen kann es als Alternative zu NetBEUI eingesetzt werden, insbesondere wenn große Netze vernetzt werden müssen. Das Protokoll ist – jedenfalls mit entsprechenden Vorkehrungen – routingfähig.

**ISN** (Initial Sequence Number) s. Keep State

**Java** ist eine im Jahre 1995 von der Firma Sun Microsystems eingeführte plattformunabhängige Programmiersprache. Alle gängigen Browser (insbesondere Internet Explorer, Netscape Navigator, Opera) sind in der Lage, sogenannte Java-Applets auszuführen. Im Gegensatz zu den Java-Applikationen, die ‚richtige' Programme sind, handelt es sich bei den Applets nicht um eigenständige Programme. Vielmehr lädt der Browser den sogenannten Byte- oder Pseudocode, der eine Vorstufe zu ‚richti-

gem‘ Maschinencode darstellt, in die Java Virtual Machine (JVM). Der Java-Quellcode und der vom Java-Compiler erzeugte Bytecode sind für alle Plattformen identisch. Die JVM muss für jede Plattform speziell angepasst werden, denn die JVM sorgt dafür, dass der Bytecode von der konkreten ‚Maschine‘ (dem Prozessor) verstanden wird. Damit von den Java-Applets nicht dieselben Gefahren ausgehen wie vom Active Scripting, hat Java das sogenannte ‚Sandkastenmodell‘ (Sandbox) entwickelt. Den Applets steht nur ein abgeschotteter Bereich zur Verfügung, so dürfen sie insbesondere keine Dateien schreiben, lesen, modifizieren oder löschen, keine beliebigen Betriebssystemkommandos oder externen Programme ausführen. Sie dürfen keine Internet-Verbindungen aufbauen außer zu dem Server, von dem sie geladen wurden. Leider ist nicht Java sondern die JVM und der Security Manager dafür verantwortlich, dass diese Beschränkungen auch eingehalten werden. Die JVM für den Internet Explorer stammt von MicroSoft [54] ... Damit ist die eigentlich von Java angestrebte Sicherheit auch wieder dahin. MicroSoft hat unlängst vor acht schweren Sicherheitslücken in der VM gewarnt und einen Patch zur Verfügung gestellt [53]. Dies dürfte nicht der letzte sein. Java ist weniger gefährlich als das Active Scripting, aber letztlich auch nicht ‚sicher‘.

Verwechseln Sie bitte Java und Java-Applets nicht mit Java-Script und Jscript. Java-Script ist eine von Netscape in den Navigator eingeführte Scriptsprache, die sich in der Syntax an Java anlehnt, im übrigen aber außer dem Namen wenig mit Java zu tun hat, insbesondere bei weitem nicht dieselben Sicherheitseinrichtungen hat. Jscript ist die von MicroSoft ‚aufgebohrte‘ Version von Java-Script. Java-Script und Jscript müssen als wesentlich gefährlicher eingestuft werden als Java (s. dazu unter ActiveX).

**Java-Script** s. unter ActiveX (nicht mit Java [s. dort] zu verwechseln)

**JScript** s. unter ActiveX (nicht mit Java [s. dort] zu verwechseln)

**Keep State** (Status halten) Um diese Checkbox bei den Filter-Regeln des WebInterfaces zu verstehen, muss man sich klarmachen, wie der Verbindungsbau unter dem TCP-Protokoll abläuft, wobei ich mich bemühe, dies hier stark vereinfacht wiederzugeben: Der Client, der eine Verbindung zu einem Server aufbauen will, schickt ein Datenpaket, bei dem das SYN-Flag gesetzt ist und welches eine zufällig gewählte Sequenznummer (ISN = Initial Sequence Number) enthält. Der angesprochene Server schickt ein Datenpaket, in dem das ACK- und das SYN-Flag gesetzt sind, das eine eigene Sequenznummer enthält und welches außerdem die Sequenznummer des Clienten als Quittung enthält (tatsächlich werden die Sequenznummern bei jeder Antwort um die Anzahl der übertragenen Datenpakete, mindestens aber um eins, erhöht).Der Client antwortet wiederum mit einem Datenpaket mit richtiger Sequenz- und Bestätigungsnummer, in dem das ACK-Flag gesetzt ist. Damit ist die Verbindung aufgebaut. Der Verbindungsabbau kann von beiden Seiten durch ein Paket mit gesetztem FIN-Flag eingeleitet werden, nachdem der Sendepuffer geleert wurde. Die Gegenstelle antwortet mit einem Paket mit gesetztem FIN-Flag, leert ebenfalls den Sendepuffer und versieht das letzte Paket nochmals mit einem FIN-Flag, was der Auslöser des Verbindungsabbaus mit einem Paket mit gesetztem ACK-Flag quittiert.

Wie man der vorstehenden Beschreibung entnehmen kann, ist jede etablierte Verbindung über die Sequenznummern, eindeutig identifizierbar (allerdings werden im-

mer wieder Warnungen veröffentlich, aus denen sich ergibt, dass das Verfahren missbraucht werden kann, indem Angreifer die ISN ermitteln oder erraten). Mit Keep State macht sich der Router diese Identifizierungsmöglichkeit zunutze, weil es einfach keinen Sinn macht, innerhalb derselben Verbindung nur den Anfang haben zu wollen. Wenn die Keep State-Option gesetzt ist, prüft der Router nur noch das erste ein- oder ausgehende Datenpaket mittels der Firewall-Regeln. Wenn dieses zugelassen ist, werden auch alle Folgepakete derselben Verbindung zugelassen. Ist das erste Paket nach dem Regelsatz zu blocken, gilt dies auch für alle Folgepakete.

**Loopback** (Rückschleife) bezeichnet in IP-Netzen eine spezielle Diagnoseart, bei der ein Datenpaket an eine der reservierten Adressen 127.xxx.xxx.xxx versandt wird. Datenpakete mit diesen Adressen sollen und dürfen nicht in das Internet, sondern sind an den absendenden lokalen Rechner selbst gerichtet. Dieses Verfahren dient eigentlich der Überprüfung der korrekten Installation von TCP/IP. Manche Internetprogramme nutzen Loopback für eigene Zwecke (z.B. der Internet-Explorer, Outlook [Express] und diverse andere MicroSoft-Programme, nach meinen Informationen aber auch Virenscanner, die aus- und eingehende Mails prüfen, bevor sie den Rechner verlassen bzw. bevor diese den Mail-Klienten erreichen). Bei der Router-Firewall ist eine spezielle Filterregel für solche Loopback-Pakete nicht erforderlich, weil diese eben nicht an den Router gelangen sollen, sondern auf dem einzelnen Rechner bleiben. Desktop-Firewalls brauchen eine spezielle Regel, die Loopback zumindest für die Programme freischaltet, die von dem Verfahren Gebrauch machen.

**MAC** (Media Access Control) gibt eine in alle Netzwerkkomponenten fest eingebaute Adresse an, die weltweit einmalig sein soll (nicht mit IP-Adresse verwechseln). MAC-Adressen sehen z.B. so aus: 00-80-C7-6D-A4-6E. Die MAC-Adresse des Routers wird im Hauptbildschirm der Router-Konfiguration angezeigt. Wer sich wundert, dass IP-Adressen notwendig sind, obwohl alle Netzwerkkomponenten weltweit bereits eine eindeutige MAC-Nr. haben, sollte sich klar machen, dass die gesamte Software bei einem Hardware-Austausch (z.B. dem Auswechseln der Netzwerkkarte) neu konfiguriert werden müsste, wenn die Adressierung über die MAC-Adresse erfolgte.

**NetBEUI** (NetBIOS Extended User Interface) ist ein Netzwerkprotokoll, das als Weiterentwicklung aus NetBIOS (s. dort) entstanden ist. Es wird zur Vernetzung (kleinerer) Windows-Netze verwandt und ist nicht routingfähig. Unter Windows XP wird das Protokoll nicht mehr automatisch installiert, ist aber auf der CD enthalten. Eine Anleitung zur Installation finden Sie unter [23].

**NetBIOS** (Network Basic Input / Output System) ist eine Programmierschnittstelle (API = Application Program Interface) zur Einrichtung von Kommunikationssitzungen, zum Senden und Empfangen von Daten und zur Benennung von Netzwerkobjekten. NetBIOS ist kein Netzwerkprotokoll, kann aber an eine Vielzahl von Protokollen (u.a. IPX/SPX und TCP/IP) gebunden und – obwohl selbst nicht routingfähig – über TCP/IP geroutet werden, wodurch erhebliche Sicherheitsrisiken entstehen können (s.u.). Die Schnittstelle wurde ursprünglich 1984 von IBM entwickelt und danach von Microsoft in die MS-Betriebssysteme integriert. Sie ist (noch) in allen Windows-Versionen enthalten und Teil des Betriebssystems, so dass sie weder gesondert installiert noch mit normalen Konfigurationsmenus aus dem Windows-Betriebssystem entfernt werden kann (im Internet finden sich allerdings Tools und Tipps, wie NetBIOS entfernt oder zumindest deaktiviert werden kann [28]).

Um NetBIOS zu verstehen muss man eine Stufe vorher ansetzen. Alle Windows-Betriebssysteme nutzen das SMB (Server Message Block)-Protokoll, um auf Netzwerkressourcen, insbesondere Dateien und Drucker, zuzugreifen. Über das genannte Protokoll sendet der Client eine Anfrage an den Server mit der Bitte, bestimmte Netzwerkressourcen nutzen zu dürfen. Um diese Anfrage starten zu können, benötigt der Client Transportmechanismen, um Kommandos (SMBs) an den Server schicken zu können. Die wichtigsten Transportmechanismen sind in der PC-Welt NetBEUI, TCP/IP und IPX/SPX. Auf NetBEUI kann der SMB sofort zugreifen, für den Zugriff auf TCP/IP und IPX/SPX benötigte er - vor w2k/XP - die NetBIOS-API (daher auch die Namen NetBIOS over TCP/IP oder kurz NBT und NetBIOS over IPX/SPX). Mit w2k hat MicroSoft das direct hosting eingeführt [27], mit dem der SMB direkt, also ohne zwischengeschaltetes NetBIOS, auf TCP/IP zugreifen kann. Während NBT die Ports 137 bis 139 benutzt, verwendet das direct hosting den Port 445.

Sie werden sich möglicherweise fragen, warum bei einer so nützlichen Schnittstelle wie dem NetBIOS immer wieder vor ‚NetBIOS-Angriffen' gewarnt wird, wenn es um den Internetzugang geht. Dies hängt weniger mit NetBIOS zusammen, sondern damit, ob und gegebenenfalls an welches oder welche Protokolle Sie NetBIOS binden. Benutzen Sie für das LAN ausschließlich NetBEUI, dann ist ein NetBIOS-Angriff nicht möglich, denn mit diesem Protokoll kommen Sie nicht ins Internet und andere Teilnehmer des Internets können nicht auf Ihre Dateien und Drucker zugreifen.

Wenn Sie unter w9x/ME den internen Datenverkehr aber über TCP/IP regeln, also NetBIOS auf dieses Protokoll aufsetzen, dann läuft sowohl der interne Netzverkehr als auch das Internet über dasselbe Protokoll, d.h. nicht nur die internen Netzteilnehmer, sondern das ganze Internet kann auf die freigegebenen Netzwerkressourcen zugreifen. Ein Angreifer, der sich die internen Daten zunutze machen will, muss nur das Internet nach einer Adresse scannen, bei der auf Port 139 Dienste angeboten werden. Hat er eine solche Adresse gefunden, genügen einfache Bordmittel, um auch die Freigaben zu ermitteln. Für die Ermittlung des Passwortes (wenn ein solches überhaupt vergeben ist) findet man im Internet passende Tools.

Unter NT/w2k/NT gestaltet sich der Angriff etwas schwieriger, weil diese Betriebssysteme die Autorisierung auf Benutzerebene vornehmen, d.h. es ist eine Übermittlung von Benutzername und Passwort notwendig. Auf weitere Einzelheiten möchte ich nicht eingehen. Wer sich dafür interessiert, wird hier [29] fündig.

Unabhängig davon, welches Windows Betriebssystem Sie verwenden, ist das Betreiben von NetBIOS über TCP/IP grundsätzlich keine sinnvolle Konfiguration, zumal MicroSoft für NetBIOS ab wXP keinen Support mehr leistet:

- In reinen w2k/XP-Netzen brauchen Sie NBT nicht mehr, weil das direct hosting den Transport übernimmt. Aus Performance-Gründen muss man sogar davon abraten, NBT und direct hosting parallel zu betreiben, denn wenn beide Transportmöglichkeiten bestehen, versucht Windows auch, beide zu verwenden und nutzt schließlich den Weg, der am schnellsten zu einer Verbindung führt.

- In reinen w9x/ME-Netzen oder gemischten Netzen (w9x/ME mit w2k/XP) brauchen Sie NetBIOS verbunden mit einem Transportmechanismus oder NetBEUI, sollten aber wegen der oben dargestellten Sicherheitsbedenken NetBEUI und eben nicht NBT verwenden. Auf einem wXP-Rechner setzt dies voraus, dass NetBEUI (s. dort) nachinstalliert wird.

Sollten Sie noch alte Soft- oder Hardware verwenden, die NBT zwingend erfordern, müssen Sie allmählich über ein Update oder eine Neuanschaffung nachdenken. Da MicroSoft den Support für NetBIOS eingestellt hat, können Sie nach meiner Auffassung davon ausgehen, dass es im nächsten Windows ohnehin nicht mehr enthalten sein wird. Die Vernetzung von w9x/ME Rechnern über das Internet mittels TCP/IP ist keinesfalls sinnvoll.

Sie sollten daher ganz unabhängig von der Einrichtung Ihrer Firewall folgendes kontrollieren/ändern:

Unter Windows 98: Start → Einstellungen → Systemsteuerung → Netzwerk anwählen.

Wenn Sie nur eine Netzwerkkarte in Ihrem Rechner haben, müssten Sie u.a. folgende Einträge sehen (wenn Sie auch noch den DFÜ-Adapter entfernt haben, was Sie ohne weiteres tun können, wenn Sie Ihre Verbindungen zu anderen Rechnern/Netzen ausschließlich über den Router herstellen, also weder eine zusätzliche ISDN-Karte oder ein Modem eingebaut haben noch die Direktverbindungsmöglichkeiten [parallel, seriell, Infrarot usw.] nutzen, fehlen die Angaben hinter den Pfeilen, denn es ist physikalisch nur noch ein ‚Gerät' vorhanden, welches die Protokolle ansprechen können):

Windows-Netze:
NetBEUI → *{Name Ihrer Netzwerkkarte}*
TCP/IP → *{Name Ihrer Netzwerkkarte}*

Novell-Netze (IPX/SPX kann auch zur Vernetzung von Windows Netzen verwandt werden):
IPX/SPX-kompatibles Protokoll→ *{Name Ihrer Netzwerkkarte}*
TCP/IP → *{Name Ihrer Netzwerkkarte}*

In gemischten Netzen kann es natürlich sein, dass sowohl NetBEUI als auch das IPX/SPX-kompatible Protokoll vorkommen.

Markieren Sie jetzt TCP/IP → *{Name Ihre Netzwerkkarte}* und klicken auf Eigenschaften. Wählen Sie den Reiter ‚Bindungen' aus und entfernen alle Häkchen, Klicken Sie auf ‚OK' und ignorieren Sie die Beschwerde von Windows, es sei kein Treiber installiert (‚Nein' anklicken).

Unter Windows 2000: Start → Einstellungen → Systemsteuerung → Netzwerk- und DFÜ-Verbindungen anwählen. Hier müssten Sie jetzt eigentlich einen Eintrag LAN-Verbindung mit dem Gerätenamen Ihrer Netzwerkkarte sehen. Trifft das nicht zu, muss zunächst der entsprechende Dienst gestartet werden: Start → Ausführen → ‚compmgmt.msc' eingeben und [ENTER] drücken. Dienste und Anwendungen →

Dienste wählen. ‚Netzwerkverbindungen' anwählen und als Starttyp entweder ‚automatisch' (wird in Zukunft immer gestartet) oder manuell wählen.

Bei den Netzwerk- und DFÜ-Verbindungen markieren Sie jetzt den Eintrag LAN-Verbindung und wählen im Menu ‚Erweitert' den Eintrag ‚Erweiterte Einstellungen'. Bei ‚Datei- und Druckerfreigabe für Microsoft-Netzwerke' und bei ‚Client für Microsoft-Netzwerke' sind die Häkchen vor Internet-Protokoll (TCP/IP) zu entfernen (die Häkchen bei den Protokollen, die Sie für die interne LAN-Verbindung verwenden wollen [z.B. NetBEUI], müssen natürlich stehen bleiben !).

Bei den Netzwerk- und DFÜ-Verbindungen markieren Sie bitte nochmals den Eintrag LAN-Verbindung und klicken diesen mit der rechten Maustaste an. ‚Eigenschaften' wählen, Internet-Protokoll (TCP/IP) markieren, ‚Eigenschaften' → ‚Erweitert' wählen und Reiter ‚WINS' anklicken: Dort NetBIOS über TCP/IP **de**aktivieren einschalten.

NetBIOS setzt jetzt nicht mehr auf TCP/IP auf. Beachten Sie aber bitte, dass Sie unbedingt die vorbeschriebenen Einstellungen kontrollieren müssen, wenn Sie eine neue Netzwerkkomponente (z.B. eine neue Netzwerkkarte) installieren, weil dadurch die Einstellungen verändert werden können !
Die NetBIOS-Verwundbarkeit Ihres Systems können Sie durch [6] überprüfen lassen.

Beachten Sie bitte: Wegen des direct hosting besteht unter w2k/XP nach wie vor eine Verbindungsmöglichkeit über TCP/IP und den Port 445. Sie müssen daher bei diesen Betriebssystemen die Freigaben und die Passwörter sehr sorgfältig konfigurieren und bei wXP zumindest die mitgelieferte Internet Connection Firewall (besser natürlich die in dieser Anleitung vorgestellten Firewalls) benutzen.

Theoretisch kann man auch ‚Direct Host' abstellen (unter w2K: Computerverwaltung (lokal) → Gerätemanager markieren unter ‚Ansicht': Ausgeblendete Geräte anzeigen' aktivieren und unter Nicht-PnP-Treiber den Eintrag NetBIOS over TCP/IP suchen, diesen rechts anklicken und ‚deaktivieren' auswählen), dann können Sie aber weder LAN- noch WAN-Verbindungen nutzen, Sie können nicht einmal mehr die Konfigurations-Oberfläche Ihres Routers aufrufen, so dass sich dieses Vorgehen ***nicht*** empfiehlt !

**POP** (Point of Presence) ist ein lokaler Einwahlpunkt des Providers

**POP3** (Post Office Protocol) ist ein Ablageverfahren für elektronische Post (ist das von den Providern meistens verwandte Verfahren für eingehende/abzuholende mails, s. aber auch IMAP)

**Port** s. Socket

**Proxy- (Caching-) Server** (Stellvertreter) nimmt die Anfragen der angeschlossenen Klienten hinsichtlich der Ziel- und Quelladressen entgegen und besorgt die gewünschten Daten aus dem Internet. Häufig wird ein Cache zwischengespeichert, wodurch die Anfragen schneller beantwortet werden können, wenn sich die gewünschten Daten bereits im Cache befinden. Es gibt externe (z.B. bei t-online) und lokale (z.B. Jana) Proxy-Server, die im Prinzip die gleichen Aufgaben erfüllen. Die lokalen Proxy-Server nehmen Anfragen der lokalen Rechner entgegen, leiten diese

an die externen Proxy-Server weiter, um die von diesen ankommenden Pakete wiederum an den Anfragenden im lokalen Netz weiterzuverteilen. In Beschreibungen entsteht oft der Eindruck, die Anfragen an einen Proxy-Server müssten über Port 8080 (und diverse andere Ports oberhalb von 1024) abgewickelt werden. Dies trifft nicht zu. Der Proxy-Server kann so eingestellt sein, dass er nur Anfragen auf dem Port 8080 (und anderen >1024) entgegennimmt, muss es aber nicht. So arbeiten die Proxy-Server von t-online auch auf dem Standard-Port 80 für http.

**(R)ARP** ([Reserve] Address Resolution Protocol) dient der Umsetzung von 48-bit-Ethernet-Adressen in 32-bit-IP-Adressen.

**Referrer** (‚Verweiser') gibt an, von welcher Stelle innerhalb oder außerhalb der eigenen Web-Präsenz auf die konkrete Seite gesprungen (verwiesen) wurde. Die Auswertung der externen Referrer beeinträchtigt Ihre Privatsphäre und sollte unterbunden werden. Eine Reihe von Sicherheitspaketen bietet diese Option, ebenso der CookieCop 2 und der WebWasher (s. unter Cookies).

**SMB** (Server Message Block) s. NetBIOS

**SMTP** (Simple Mail Transport Protocol) ist ein Dienst zur Übertragung von e-mails (wird für abgehende mails verwandt).

**Socket** bezeichnet die Kombination von IP-Adresse und Port. Die Art der Adressierung wird häufig mit der Arbeitsweise einer Telefonanlage verglichen. Während die IP-Adresse den Hauptanschluss kennzeichnet, gibt der Port die ‚Durchwahl' an. Im Gegensatz zur Telefonanlage wird durch den Port (Durchwahl) aber nicht ein bestimmtes Gerät (Computer), sondern eine Anwendung (browser, e-mail-Programm, Terminalprogramm etc.) angesprochen. Es kann keine zwei identischen Socket-Paare zur gleichen Zeit geben. Wohl aber kann eine Anwendung (z.B. ein Terminalprogramm) zur gleichen Zeit über unterschiedliche Port-Nrn. mehrere Verbindungen zu einem Zielrechner unterhalten.

**Source Route** Diese Checkbox, die in der Firmware 2.3 nicht mehr vorhanden ist, wird bei den Einstellungen für die Filter-Regeln im Handbuch nicht erläutert.

Gemeint ist folgendes: Source Routing ist im TCP/IP-Standard vorgesehen. Wenn die entsprechende Option im Datenpaket gesetzt ist, gibt der Absender des Paketes eine konkrete Route, die das Paket nehmen soll, vor. Dieses Source Routing kommt im normalen Datenverkehr kaum zum Einsatz, wird aber von Hackern verwandt, um Sicherheitsmaßnahmen zu umgehen (Source Routing Attacke). Gelingt es einem Hacker, bei den ausgehenden Datenpaketen eine bestimmte Route vorzugeben, so kann er den gesamten Datenverkehr über seinen Rechner leiten und entsprechend auswerten. Deshalb sollten Pakete, bei denen dieses Flag gesetzt ist, von einer Firewall verworfen wurde.

DrayTek hat diese Möglichkeit mit der Firmware 2.3 abgeschafft. Bereits vorher hatte ein Anwender im Gästebuch der www.vigor-users.de ein Entschuldigungsschreiben von DrayTek veröffentlicht, in dem DrayTek mitteilt, diese Option sei "invalid".

Ob es sich hierbei um ein grundsätzliches Problem gehandelt hat, weil die im Router eingebaute Firewall die Optionen in TCP-Header gar nicht auswerten konnte, weiß ich nicht; jedenfalls hat DrayTek die Regeln, bei denen die Source Route-Option gesetzt war, denkbar unglücklich in den ipf-Befehlssatz (näheres zu diesem Befehlssatz bei den *Allgemeinen Hinweisen* unter V.) umgesetzt, nämlich z.B. so:

block out quick from any to any *with opt lsrr,ssrr*

sssr steht dabei für ‚Strict Source and Record Route' und lssr für ‚Loose Source and Record Route'. In der Strict-Variante gibt der Angreifer die Router, die das Paket verwenden soll, genau vor, während bei der Loose-Variante die angegebenen Router angesteuert werden sollen, das Paket zwischenzeitlich aber auch andere Router benutzen darf. Dass beide Vorgaben von einem Angreifer gemacht werden (und nur dann hätte die vom WebInterface produzierte Regel eingegriffen), gibt es nicht.

Das WebInterface hätte daher zwei Regeln erzeugen müssen, nämlich im oben wiedergegebenen Beispiel:

block out quick from any to any *with opt lsrr*
block out quick from any to any *with opt ssrr*

Damit wären beide Angriffsformen abgewehrt worden.

DrayTek hat sich dafür entschieden, die Option ganz zu entfernen. Damit müssen wir vorerst (?) leben.

Deshalb der folgende ***wichtige Hinweis***:

Entfernen Sie bitte alle Regeln, bei denen die Source Route-Option gesetzt ist, bevor Sie auf die Firmware 2.3 updaten (Sie können die Regel selbstverständlich auch nach dem Update löschen, könnten aber Probleme haben, die Regel überhaupt zu finden, weil die Option im WebInterface der Fw 2.3 nicht mehr angezeigt wird), und zwar aus folgendem Grund:

Wenn Sie mit einer Vorgängerversion der Firmware 2.3 eine Regel definiert hatten, bei der die Source Route-Option aktiviert war, passiert beim Update auf die Firmware 2.3 zunächst nichts, außer dass man die Regel nicht mehr versteht, wenn man sie sich im WebInterface ansieht (unter Telnet wird sie mit ipf view -r unverändert angezeigt; im WebInterface sieht man nicht, dass die Regel nur für Pakete mit den vorumschriebenen Optionen gilt). Ändert man aber auch nur eine einzige Firewall-Regel, so übersetzt das WebInterface alle Regeln neu und aus "block out quick from any to any *with opt lsrr,ssrr*" wird "block out quick from any to any". Danach ist Schluss mit Internet.

**Spyware** (Spionage-Software) übermittelt ohne Ihr Wissen Informationen über Sie oder Ihren Rechner an andere Stellen im Internet, die hieran ein Interesse haben.
In der Computer-Literatur wird manchmal der Eindruck erweckt, Viren, Trojaner, Würmer etc. müssten abgewehrt, Werbebanner gnadenlos bekämpft und Spyware notgedrungen geduldet werden. Ich teile diese Auffassung nicht: Viren etc. stehlen die Daten und die Verwendbarkeit der Hard- und Software, Spyware die Persönlich-

keit. Durch die Möglichkeit abgefangene Daten auf Dauer zu speichern, mit anderen abgefangenen Daten zusammenzuführen oder weltweit zu vernetzen, besteht die Gefahr, dass in einer Datenbank ein sehr genaues Abbild des Anwenders gespeichert wird, welches diesen in seiner Lebensführung erheblich beeinträchtigt. Zwei plumpe Beispiele: 1. Sie kaufen im Internet ein Netzwerkkabel und ein halbes Jahr später *einen* Virenscanner. Dies ist verdächtig, weil man aus der Anschaffung eines Netzwerkkabels schließen kann, dass Sie mehrere Rechner betreiben und sich fragen muss, warum Sie keine Mehrfachlizenz des Scanners erwerben. 2. Sie suchen im Internet längere Zeit nach Informationen über eine gefährliche Krankheit und wundern sich, warum Ihnen einige Zeit später der Abschluss einer Lebens- oder Krankenversicherung verweigert wird.
Ich bin daher der Auffassung, dass sich der Anwender mindestens genauso intensiv um die Bekämpfung von Spyware kümmern muss wie um die Abwehr anderer Angriffe. Hierbei kann Ihnen die Router-Firewall natürlich kaum helfen. Deutlich mehr leistet eine Desktop-Firewall, weil sie anwendungsbezogen bestimmten Programmen den Zugang verwehren/erlauben kann. Auch hier gilt es jedoch zu bedenken, dass Spyware oft Bestandteil von Programmen ist, denen Sie arglos den Zugang gestatten, weil sie für den Internet-Zugang nützlich sind. Die Spyware-Komponente haben Sie dann gleich mit freigeschaltet. Mit Ad-Aware (zu laden unter [2]) können Sie versuchen, auch diese Spione zu entfernen. Ferner empfehle ich, in kurzen Abständen die Cookies, den Verlauf und alle Offline-Inhalte zu löschen (im Internet Explorer: Extras → Internetoptionen: ‚Cookies löschen', ‚Verlauf leeren', ‚Dateien löschen ... → Alle Offline Inhalte löschen → OK'). Ferner sollte die Index.dat (bei w2k zu finden unter {Systemlaufwerk}\Dokumente und Einstellungen\{User-Name}\Lokale Einstellungen\Temporary Internet Files\Content.IE5, Administrator-Rechte erforderlich !) gelöscht werden (wird danach automatisch neu angelegt), weil diese Datei andernfalls außerordentlich lang wird und ebenfalls interessante Aufschlüsse über Ihr Surf-Verhalten ermöglicht. Bei dieser Gelegenheit würde ich auch gleich das Verzeichnis {Systemlaufwerk}\Dokumente und Einstellungen\{User-Name}\Lokale Einstellungen\Temp aufräumen. Es ist erschreckend, welche Datenmassen (!) sich in diesem Verzeichnis im Laufe der Zeit verewigen.

**Subnet Mask** (Subnetzmaske) s. IP-Adressen

**TCP** (Transmission Control Protocol) = Internet-Protokoll, das die Übertragung jedes Paketes sicherstellt (eingesetzt für HTTP, FTP, E-Mail u.a.)

**Telnet** (Remote Terminal Login) ist das Protokoll für virtuelle Terminals. Es stellt eine interaktive Verbindung zwischen zwei IP-Rechnern her und erlaubt die Nutzung von Programmen, die auf einem entfernten Rechner liegen. Telnet heißt aber auch das mit Windows mitgelieferte Terminalprogramm, welches das Internet-Protokoll benutzt, um die Verbindung zwischen 2 Computern herzustellen (nicht zu verwechseln mit *Hyperterminal*, welches ein ebenfalls mit Windows mitgeliefertes Terminalprogramm bezeichnet. *Hyperterminal* verwendet andere Protokolle).

**UDP** (User Datagram Protocol) = Ungesichertes (Verbindungsloses) Internet-Protokoll, bei dem im Gegensatz zu TCP nicht geprüft wird, ob die Pakete (in der richtigen Reihenfolge) ankommen, die Übertragung erfolgt schneller, weil keine Überprüfung stattfindet und der Anteil der Nutzdaten im Paket höher ist (eingesetzt bei Online Spielen und Media-Streaming, z.B. Quicktime, Real-Player, Windows-

Streaming: hier ist die Geschwindigkeit entscheidend: wenn ein Paket verloren geht, ist es ohnehin zu spät, sie können die zweite Szene nicht nachholen, nachdem bereits die dritte angezeigt wurde)

**Web Bugs** (Web-Käfer, auch Clear GIFs) [52] sind Grafiken (meist nur 1 x 1 Pixel groß und daher unsichtbar), auf die z.B. in html-Dokumenten (Web-Seiten, eMails) aber auch in Office-Dokumenten verwiesen wird. Sie sind aber nicht in diesem Dokumenten enthalten, sondern in den Dokumenten steckt ein html-Tag, mit denen die ‚Bilder' nachgeladen werden. Durch das Herunterladen der Grafik werden dem Server, der die Grafik liefert, gleichzeitig auch eine Reihe von persönlichen Informationen über den Nutzer übermittelt, der die Grafik ‚angefordert' hat, u.a.: die für die aktuelle Internet-Sitzung gültige IP-Adresse, die URL (Uniform Resource Locator) der Seite, von der das ‚GIF' geladen wurde, die URL der Seite, in der der Web Bug enthalten ist, den Browser-Typ, die Uhrzeit und den Inhalt eines vorher gesetzten Cookies. U.U. verweist der Tag auch gar nicht auf eine Grafik, sondern auf ein CGI-Script, welches die Grafik liefert und im übrigen die Auswertung scriptgesteuert vornimmt. Die Web Bugs dienen also dazu, Sie auszuspionieren und Benutzerprofile zu erstellen. Sie können (derzeit) nicht wie Cookies im Browser abgeschaltet werden und gelten daher als Cookie-‚Nachfolger'.
Besonders ärgerlich ist es, wenn Web Bugs in Werbe-eMails im html-Format eingebunden werden: Der Absender meint, Ihre eMail-Adresse zu kennen, weiß es aber nicht genau. Also baut er in die URL des Web Bug die Mailadresse ein, an die er die Werbung verschickt. Wird die Mail geöffnet und der Web Bug tatsächlich heruntergeladen, weiß der Werbeversender nicht nur, dass seine Werbemail gelesen wurde, sondern hat auch eine Bestätigung, dass die vermeintlich richtige eMail-Adresse tatsächlich richtig ist und kann sich die Adresse für seine Zwecke speichern. Eine Desktop-Firewall kann Sie hiervor schützen, wenn Sie Ihrem eMail-Programm z.B. nur die Ports 25 (SMTP) und 110 (POP3), aber nicht den Port 80 (http) öffnen. Die Freeware bugnosis (http://www.bugnosis.org/) enttarnt die bösen Käfer, WebWasher [59] verspricht, die Käfer herauszufiltern.

# IV. Hinweise

## Call Filter

### Welchen Sinn haben eigentlich Call Filter ?

*Der* ‚klassische' Call-Filter, der in fast jeder Router-Konfiguration vorgegeben wird, ist der NetBIOS-Blocker, mit dem beim TCP/IP-Protokoll Anfragen von den NetBIOS Ports 137-139 an den DNS-Port 53 für alle Ziel- und Quell-Adressen unterbunden werden, um unerwünschte Verbindungen zu verhindern (s. dazu im einzelnen noch bei den Beispielregeln Sets 1 + 2).

Mit einem Call Filter kann man aber beispielsweise auch einstellen, dass nur zu bestimmten IP-Adressen (=Internet-Adressen) eine Verbindung hergestellt werden darf (z.B. www.heise.de). Dazu muss man allerdings die dem Domain-Namen entsprechende IP-Adresse kennen oder erfragen (z.B. 193.141.40.129). Achtung: Als alleinige Sicherheitseinstellung reicht das natürlich nicht, denn der Call-Filter wird ja nur dann abgearbeitet, wenn keine Internet-Verbindung besteht. Daher wirkt der vorbeschriebene Call-Filter nicht mehr, wenn die Verbindung besteht, so dass der Anwender von der zugelassenen Adresse weitersurfen kann, ohne dass der Filter dies verhindert. Will man daher wirklich nur Verbindungen mit einer bestimmten Adresse zulassen, so ist zusätzlich entweder ein gleichlautender Daten-Filter erforderlich oder man definiert im General Setup für die Datenfilter das gleiche Regelset als Anfangspunkt wie für die Call-Filter. In Zusammenarbeit mit einem solchen Daten-Filter macht der Call-Filter deshalb Sinn, weil bereits die Verbindungsaufnahme unterbunden wird.

Eine weitere Anwendungsmöglichkeit besteht darin zu verhindern, dass ein bestimmtes Programm von sich aus eine – u.U. kostenpflichtige – Verbindung eigenmächtig aufbaut (z.B. um die Uhrzeit mit einer Atom- oder Funkuhr abzugleichen). Bei den Datenfiltern kann man diesen Datenverkehr dann zulassen, weil hier nur eine bereits bestehende Verbindung genutzt wird. Die immer häufiger anzutreffende Unsitte, dass Programme bei ihrem Start oder sogar schon beim Start von Windows eine Internet-Verbindung herstellen, um auf der Homepage des Herstellers nach Updates zu suchen, kann man so ebenfalls bekämpfen, indem man einen passenden Call-Filter benutzt. Der Nachteil besteht darin, dass die Update-Funktion – auch wenn man sie bewusst benutzen will – jetzt nur noch funktioniert, wenn man vorher eine Verbindung aufbaut. Auch andere Programm-Funktionen können beeinträchtigt sein. Deshalb ist es in jedem Fall besser, im Programm selbst nach einer Möglichkeit zu suchen, das Auto-Update abzuschalten (unter w2k/XP muss man in jedem Fall unter Start->Einstellungen->Systemsteuerung->Automatische Updates-> „Computer auf dem neuesten Stand halten" deaktivieren). Nicht selten fehlt in den Programmen eine solche Funktion. Dies ist sehr schlecht für alle Anwender, die über einen Router ins Internet gehen. Das Programm will ‚nur' prüfen, ob eine Verbindung zu einer bestimmten Internet-Seite möglich ist und schickt eine Anfrage an diese Seite. Aufgabe des Routers ist aber gerade, die Beantwortung einer solchen Frage zu ermöglichen. Also schickt der Router nicht etwa eine Info an das anfragende Programm mit der er mitteilt, zur Zeit bestehe keine Verbindung, sondern stellt (pflichtgemäß) die Verbindung her, damit die Anfrage beantwortet werden kann. Vielleicht ist mit der Unsitte Schluss, wenn der erste Anwender, der über einen Rou-

Schluss, wenn der erste Anwender, der über einen Router ins Internet geht, keine Flatrate hat, die Verbindungen im Hintergrund nicht bemerkt hat, weil er keinen Kontroll-Monitor hat und vom Programmhersteller auf automatischen Verbindungsaufbauten nicht hingewiesen worden ist, die hierdurch entstandenen Kosten erfolgreich als Schadensersatz von seinem Vertragspartner eingefordert hat.

Ich persönlich mag die ‚unerklärlichen' Verbindungsaufbauten überhaupt nicht (und viele andere Anwender auch nicht, wenn man sich die diesbezüglichen Anfragen in den Foren ansieht), weil sie auch ein Anzeichen dafür sein können, dass sich ein Schädling (z.B. ein Trojaner) im System breit gemacht hat.

Leider kann der Router – im Gegensatz zu einer Software Desktop-Firewall - natürlich keine Anwendungen erkennen, weil er nur Datenpakete bekommt. Daher lässt sich ein solcher Call-Filter nur dann realisieren, wenn die ‚lästige' Anwendung z.B. einen atypischen Port benutzt, der sich sperren lässt, ohne dass der gewöhnliche Internetverkehr (z.B. über Port 80: http) unterbunden wird oder die lästige Anwendung eine bestimmte IP-Adresse ansteuert, die bekannt ist oder sich ermitteln lässt.

Schließlich kann der Call-Filter eingesetzt werden, wenn man bestimmten Rechner im Netzwerk zwar nicht die Internet-Nutzung, wohl aber die selbständige Verbindungsaufnahme untersagen will. Dies setzt allerdings voraus, dass den einzelnen Netzwerk-Rechnern die IP-Adressen nicht dynamisch, sondern fest zugewiesen werden. Die IP-Adressen der auszusperrenden Rechner müssen dann bei der Source-(Quell-) IP-Adresse eingetragen werden, wobei bei Destination (Ziel) ‚any' (jede) Adresse anzugeben und die Port-Nrn. freizulassen sind. Durch eine entsprechende Subnetzmaske (s. bei Begriffserläuterungen) können auch Gruppen mit einer einzigen Regel ausgesperrt werden.

**Welche Ports sollte man definitiv sperren und welche müssen in jedem Fall offen bleiben ?**

Sperren sollte man die TCP- und UDP-Ports 137 bis 139, weil dies die NetBIOS-Ports für die Netzwerk-Freigaben sind. Grundsätzlich sollte man bereits in der Netzwerk-Konfiguration die Datei- und Druckerfreigabe für TCP/IP abschalten (s. unter Begriffserläuterungen → NetBIOS), eine zusätzliche Sicherheit im Router schadet aber nicht.

Wenn man nicht darauf angewiesen ist, entfernte w2k/XP-Netze über TCP/IP zu verbinden, sollte man in der Router-Firewall auch den TCP-Port 445 abschalten, weil w2k/XP über diesen Port die Datei- und Druckerfreigabe managen (direct hosting, s. unter Begriffserläuterungen → NetBIOS). Bei der Desktop-Firewall, muss man natürlich aufpassen, dass die netzinternen IP-Adressen (z.B. 192.168.1.xxx) nicht blockiert werden, wenn auch der LAN-Verkehr mittels direct hosting über TCP/IP läuft.

Der DNS-Port (53) muss für den DNS-Server offen gehalten werden. Dazu muss man die IP-Adresse(n) des verwandten DNS-Servers (z.B. beim Provider) erfragen (Glauben Sie nicht den Behauptungen auf einer Vielzahl von Internet-Seiten, die DNS-Server von t-online hätten die Adressen 194.25.2.129 bis 194.25.2.134. Das ist in dieser Allgemeinheit nicht richtig. Wie Sie die richtigen Adressen finden, habe ich unter Begriffserläuterungen → IP-Adresse beschrieben.).

Offen bleiben müssen die Ports 80 (http) und 443 (https) bzw. die entsprechenden Proxy-Ports 8080 oder 3128, wenn der Provider einen Proxy-Server verwendet und (!) diese Ports vorgibt (was z.B. bei t-online nicht der Fall ist).

Für E-Mail müssen die Ports 110 (POP3) und 25 (SMTP) bzw. 143 (IMAP) offen bleiben (u.U. auch Port 995 [SPOP3], wenn eingehende Mails über eine sichere Verbindung laufen). Der Newsreader benutzt den Port 119 (NNTP).

Port 75 ist reserviert für jede Art privater Telefonieanwendungen (also insbesondere für Telefax). Dieser Port muss *nicht* explizit freigeschaltet werden, damit die Anwendungen [z.B. RVS COM Lite, WinPhone Phone Tools], die auf den virtuellen Terminal-Adapter aufsetzen, funktionieren.

Über die UDP-Ports 67 und 68 wird die Adressvergabe vom Router an die angeschlossenen Rechner bei eingeschaltetem DHCP abgewickelt. Auch diese Ports müssen *nicht* explizit freigeschaltet werden, damit DHCP funktioniert.

Wenn man ftp: (File Transfer Protocol) benutzt, sind in der Router-Firewall umfangreiche Freigaben erforderlich *(s. hierzu c't 21/01 S. 153 sowie die Beispielkonfiguration)*. Der Remote-Port 21 muss für alle IP-Adressen freigeschaltet werden. Bei aktivem ftp (bei dieser Form werden die Daten *aktiv* von der Gegenstelle auf den eigenen Rechner geladen, während man sich beim passiven ftp die Daten selbst herunterlädt) muss der Port 20 für eingehende Datenpakete mit beliebiger Absende-IP-Adresse auf alle Ports oberhalb 1024 des eigenen Rechners freigeschaltet werden. Passives ftp erfordert die Freigabe aller Ports oberhalb 1024 für ausgehende Verbindungen auf dem eigenen und allen Zielrechnern. Das Risiko kann man vielleicht dadurch reduzieren, dass man eine Regel erstellt, die normalerweise den ftp-Verkehr unterbindet und diese Regel im Einzelfall deaktiviert, weil man tatsächlich eine ftp-Übertragung starten will. Sonst kann nur eine Software-Desktop-Firewall helfen, die nur bestimmte Programme für diese Übertragungsart zulässt (s. dazu noch unten).

Eine komplette Port-Liste gibt es im Internet: www.iana.org/assignments/port-numbers (ca. 175 DIN A4-Seiten !)

**Sicherheits- und Port-Test**

Die Sicherheit des eigenen Rechners und die offenen Ports kann man unter [5] testen.

**Warnung vor der Konfigurations-Oberfläche des Filter/Firewall Setup**

Es wird sich kaum verhindern lassen, dass man im Setup unsinnige und gefährliche Eingaben macht. Für nicht vertretbar halte ich es aber, wenn das Setup Eingaben zunächst zulässt, die unmöglich sind, und diese dann ohne jede Warnung und Hinweis eigenmächtig in einer Art und Weise abändert, die dem Router passt. Ein Beispiel finden Sie im deutschen Handbuch eines der DrayTek-Vertriebe: Von den dort abgedruckten Beispielen können Sie zwei überhaupt nicht dauerhaft eingeben, weil der Verfasser der Regeln als Protokoll ‚any' angibt und die Regel dann auf bestimmte Ports beschränken will. Das geht nicht, weil nur die Protokolle TCP und UDP mit

Ports umgehen können. Der Router lässt diese Eingabe aber zunächst zu und entfernt die Port-Angaben ersatzlos und ohne jede Warnung, wenn Sie auf ‚OK' klicken, was Sie ohne weiteres selbst nachprüfen können, wenn Sie sich unmittelbar danach noch einmal die Regel ansehen: Die Port-Felder sind jetzt leer. Bei einer Erlaubnisregel kommt dies einer Katastrophe gleich, weil Sie jetzt den gesamten ein- oder ausgehenden Verkehr (je nach Angabe bei ‚Richtung') für *alle* Ports freigeschaltet haben, obwohl Sie nur einen Port freischalten wollten. Das Konfigurations-Programm für ELSA-Router arbeitet hier wesentlich besser, weil es die Eingabefelder für die Ports sofort abblendet, wenn man andere Protokolle als TCP und UPD anwählt. Bei den Draytek-Routern müsste das Verhalten unbedingt geändert werden. Wenn es schon keine Warnung gibt, sollte der Router sich zumindest weigern, das Fenster für die Eingabe der Filterregeln mit ‚OK' zu schließen, wenn die Regel logisch nicht möglich ist.

Bis zu dieser Änderung kann ich nur empfehlen, die Regeln zunächst auf Papier zu notieren und alle Regelsätze nach der Eingabe nochmals gesondert aufzurufen und mit Ihren Aufzeichnungen zu vergleichen (vgl. aber auch unter *Einige nützliche Telnet Kommandos)*.

In eine andere recht originelle Falle können Sie tappen, wenn Sie z.B. zu Versuchszwecken ein Set erstellen und dann das komplette Set mit ‚Clear' löschen. Es wird nicht nur das Set gelöscht, sondern auch ein etwaiger Verweis auf ein anderes Set. Hier steht danach ‚None'!

**Warnung vor Rad-Mäusen**

Passen Sie bitte auf, wenn Sie eine Rad-Maus benutzen ! Wenn ein Listenfeld den Fokus besitzt (in diesem Listenfeld also gerade eine Eingabe gemacht werden kann) genügt ein kleiner Ruck am Rädchen, um aus einem ‚block immediately' ein ‚pass immediately' zu machen !

**Warnung vor dem Barricade Monitor**

So nützlich und gut der Barrmon auch sein mag, aus Sicherheitsgründen muss man zur Zeit von seiner Verwendung abraten, weil er das Zugangspasswort zum Router nicht nur als Tooltipp im Klartext anzeigt, sondern auch noch an mehreren Stellen im Klartext auf der Festplatte abspeichert.

**Keine Dauerverbindung**

Ich wundere mich über die Vielzahl der Artikel in Computerzeitschriften, die sich mit der Frage befassen, wie eine Zwangstrennung verhindert werden kann, als müsse man die Flat-Rate auch wirklich bis zur letzten Sekunde ausnutzen, wenn man sie schon bezahlt. Kein Mensch kommt auf die Idee, Essen und Getränke bis zur Krankenhausreife in sich hineinzustopfen, wenn er eingeladen ist und nichts bezahlen muss. Dementsprechend habe ich auch noch nie einen Artikel zu der Frage gelesen, wie ich bei einem solchen Verhalten die Krankenhausreife verhindern kann.
Ich halte die Zwangstrennung und den Verbindungsabbau nach einer bestimmten Zeit bei Inaktivität für einen erheblichen Sicherheitsgewinn. Der ‚normale' Surfer bekommt von seinem Provider bei jeder Einwahl eine neue IP-Adresse. Wenn sich ein

Angreifer an Ihrem Router verbissen hat und z.B. mittels eines Port Scans versucht, auf Ihre Rechner zu kommen, schlagen Sie diesem Angreifer quasi die Tür zu, wenn sie die Verbindung auch nur kurz trennen und damit eine neue IP-Adresse bekommen. Ich habe mir sogar angewöhnt, die Leitung in regelmäßigen Abständen eigenhändig zu kappen und wieder neu herzustellen, wenn mir die Suche nach einer Problemlösung zu lange dauert. Dementsprechend würde ich den Vigor-Router auch nicht so konfigurieren, dass er eine Dauerverbindung herstellt (*Hinweis:* Bei der Firmware 2.2 funktioniert der Idle Timeout im Gegensatz zu allen anderen Firmware-Versionen, mit denen ich gearbeitet habe (2.0a, 2.1a, 2.3), nicht zuverlässig, was natürlich für alle Anwender, die keine Flatrate haben, sehr problematisch ist).

**Keine Administrator-Rechte beim Internet-Surfen**

Zunächst empfehle ich, von den Win 95/98/ME-Betriebssystemen umzusteigen auf Windows 2000/XP, weil es die besseren, vor allem aber sicheren Betriebssysteme sind. Als Dateisystem sollten Sie mit diesen Betriebssystemen natürlich NTFS und nicht eine der FAT-Varianten verwenden, weil Sie nur mit NTFS die Zugriffsrechte vernünftig reglementieren können. Als Administrator sollte man mit w2k/XP aber wirklich nur dann arbeiten, wenn es etwas zu verwalten gibt (Benutzer einrichten, Software installieren, Einstellungen des Betriebssystems ändern, Änderungen an der Registry usw.). Ich habe für mich einen Benutzer mit einfachen Benutzerrechten eingerichtet und nur unter diesem Namen gehe ich ins Internet. Ein einfacher Benutzer darf eine Vielzahl gefährlicher Aktionen (Schreibzugriff auf die Registry, Installation von Programmen usw.) nicht ausführen, so dass allein hierdurch bereits ein gewisser Grundschutz verwirklicht ist. Machen Sie sich bitte klar, dass ein dreizeiliges Script, das Sie sich auf jeder Web-Seite, die Sie ansteuern, einfangen können, ausreicht, um Ihre gesamte Festplatte zu formatieren, und zwar ohne dass Sie gefragt werden oder eine sonstige Möglichkeit hätten, dies zu verhindern. Sie können zwar das gesamte aktive Scripting (s. auch unter *Begriffserläuterungen→ActiveX*) in Ihrem Browser abschalten (und müssen dies nach meiner Auffassung auch in jedem Fall, wenn Sie Administrator-Rechte haben), werden dann aber nicht mehr viel Freude beim Internet-Surfen haben. Auf die Virenscanner, die inzwischen fast alle auch einen Script-Schutz beinhalten und heuristische Verfahren verwenden, können Sie sich ebenfalls nicht verlassen, denn mit einer vergleichbaren Erfolgsquote wie beim Virenscannen, bei dem es ja ‚nur' darum geht, vorhandene Muster zu erkennen, können Sie sich bei diesen Verfahren nicht verlassen. Die Hersteller der Virenscanner schweigen sich aus gutem Grund zu diesem Thema aus, denn mit jeder Information würden Sie gleichzeitig auch den potentiellen Angreifern wichtiges Material liefern. Die nachfolgend beschriebenen Firewalls nützen gegen diese Gefahren überhaupt nichts, denn die Scripte laden Sie sich zusammen mit der Web-Seite, die Sie freiwillig ansteuern. Es hängt ausschließlich von den Einstellungen Ihres Browsers ab, ob die mitgeladenen Scripte auch ausgeführt werden dürfen. Nach meiner ganz persönlichen Einschätzung ist die Gefahr für einen privaten Anwender, durch ein Script geschädigt zu werden, wesentlich größer, als eine Schädigung durch einen Virus. Ein weiterer Gesichtspunkt: Wenn ich z.B. mit [2] mein System auf Spyware untersuche, ist der Unterschied zwischen w98- und w2k-Rechnern gewaltig: Auf den w2k-Rechnern findet sich so gut wie nie Spyware; auf den w98-Rechnern sieht das ganz anders aus. Schließlich müssen Sie sich darüber im Klaren sein, dass bei vielen, wenn nicht sogar bei den meisten gezielten Angriffen das sogenannte ‚social engineering' [30] eine Rolle spielt: Der Angreifer versucht, Zugangsdaten nicht über einen

Computer-Angriff herauszubekommen, sondern über das Befragen Eingeweihter. Das sieht dann z.B. so aus: Ein potentieller Angreifer ruft die Schreibkraft des Unternehmens an und gibt sich als Mitarbeiter des Unternehmens aus, welches für die Software-Wartung zuständig ist. Er fragt die Schreibkraft, ob sie mit Ihrem Computer zufrieden ist (Welche Schreibkraft würde das schon bejahen ?). Der Anrufer zeigt sich sehr verständnisvoll und es entwickelt sich ein angenehmes Gespräch, in dessen Verlauf der Anrufer anbietet, die schlimmsten Unannehmlichkeiten zu beseitigen. Er benötigt natürlich den Benutzernamen und das Passwort. Alles weitere können Sie sich denken. Wenn in diesem Fall die Schreibkraft auch noch Administrator-Rechte hat, können Sie einpacken.

Übrigens funktionieren fast alle Programme mit den Rechten eines einfachen Benutzers, so dass es kaum erforderlich ist, sich als Hauptbenutzer anzumelden. Manche Programme ‚schimpfen', weil sie nicht auf die Registry zugreifen dürfen (ohnehin eine Unart, die abgestellt gehört), funktionieren dann aber trotzdem einwandfrei. Mir sind mittlerweile eher die Programme suspekt, die Hauptbenutzerrechte fordern, ohne dass ich hierfür einen Grund erkennen kann. Es besteht ein gewisser Verdacht, dass solche Programme zumindest Spyware, wenn nicht Schlimmeres enthalten (Mir ist z.B. unbegreiflich, warum die Musicmatch Jukebox mindestens Hauptbenutzer-Rechte fordert). Bei Programmen, die mehr als einfache Benutzerrechte fordern, ohne dass Sie hierfür einen Grund erkennen können, würde ich mich nach einer Alternative umsehen oder mich an den Hersteller wenden. Z.B. erforderte beim TDSL-Speedmanager von t-online [31] bis zur Version 2.0 nicht nur die System-Optimierung Administrator-Rechte (was natürlich richtig ist), sondern auch die bloße Anzeige der Übertragungsrate. Ich habe mit den Technikern von t-online, die sich übrigens sehr viel Mühe gegeben haben, mehrfach korrespondiert, ohne eine Lösung zu finden, aber: Ab der Version 3.0 funktioniert die Anzeige auch mit einfachen Benutzerrechten.

Eine sehr gute Beschreibung, wie man Benutzer unter Windows XP (Home und Professional) einrichten und verwalten kann, finden Sie in der ct [20]. Mir ist es im übrigen unbegreiflich, wie MicroSoft auf der einen Seite ständig versichern kann, man sei um mehr Sicherheit bemüht, auf der anderen Seite aber das Einrichten und Verwalten von Benutzern in der Home-Edition erschwert. Die Benutzerverwaltung ist im Heimbereich mindestens genauso wichtig wie beim professionellen Einsatz, denn gerade im privaten Bereich werden auch völlig computerunerfahrene Anwender und Anwender, denen das nötige Sicherheitsbewusstsein fehlt (Kinder), mit dem Rechner arbeiten und im Internet surfen wollen.

Gegenüber der 1. Auflage dieser Anleitung habe ich die Warnung vor den Administrator-Rechten nochmals verschärft, weil die – ansonsten von mir sehr geschätzte – c't in Heft 01/2003 auf Seite 82, empfohlen hat, alle aktiven Nutzer mit Administrator-Rechten zu versehen, ‚damit auch alle Programme reibungslos funktionieren'. Insbesondere Personal Firewalls und Antiviren-Software müssten nicht nur mit Administrator-Rechten installiert werden, sondern auch mit diesen laufen. Das stimmt nicht, widerspricht allen sonstigen Ratschlägen (auch in der c't, vgl. [20]) und ist einfach unverantwortlich (in den Folgeheften sind auch entsprechende Leserbriefe erschienen). Die nachfolgend vorgestellte Kerio Personal Firewall funktioniert nicht nur mit eingeschränkten Benutzerrechten und kann mit diesen eingestellt werden, sondern die

Sicherheit dieser Firewall können Sie mit eingeschränkten Benutzerrechten sogar um mindestens eine Klasse erhöhen (s. unter VII.).

Norton Antivirus 2002/2003 funktionierte bei mir unter w2k mit eingeschränkten Benutzerrechten mit folgenden Einschränkungen einwandfrei:

- eine vollständige Systemprüfung erfordert Administrator-Rechte,
- Auto-Protect lässt sich nicht deaktivieren,
- Liveupdate ist nicht möglich.

Der erste Punkt ist völlig klar: Wenn ich das System vollständig prüfen will, muss ich uneingeschränkten Zugriff, also Administrator-Rechte, haben.
Der zweite Punkt ist eigentlich folgerichtig: Es darf nicht sein, dass ein eingeschränkter Benutzer einfach per Mausklick den Virenschutz deaktiviert. Gleichwohl würde ich mir eine Option in NAV wünschen, mit der ein einfacher Benutzer jedenfalls dann den Virenschutz vorübergehend deaktivieren kann, wenn er das Administrator-Passwort kennt. Manche Programme empfehlen das Abschalten des Virenschutzes. Meist sind dies Installations-Programme, für die ohnehin Administrator-Rechte erforderlich sind. Im übrigen habe ich noch keine praktischen Schwierigkeiten feststellen können, weil der Virenschutz nicht abzustellen war.
Der dritte Punkt ist ein schwerer Mangel von NAV, der eigentlich zur Abwertung des Programms in allen Tests führen müsste. Es ist mir ein Rätsel, dass NAV ständig gute Testergebnisse einfährt oder sogar Vergleichstests gewinnt. Es darf eigentlich nicht sein, dass ein einfacher Benutzer mit veralteten Virensignaturen arbeiten oder den Administrator bemühen muss. Symantec selbst betont die Bedeutung, die die aktuellen Virensignaturen für einen wirksamen Schutz haben. Dann müssen diese Signaturen aber auch möglichst verzögerungsfrei auf den Rechner kommen. Welche Entscheidungs-Alternativen soll ein Administrator denn haben, wenn Symantec neue Signaturen zur Verfügung stellt ? Er wird es kaum besser wissen, als Symantec. Wenn Symantec meint, die neuen Signaturen seien besser, wird sie auch der Administrator annehmen müssen. Praktisch habe ich mir dadurch beholfen, dass ich das Lifeupdate abgeschaltet habe, um mich zweimal in der Woche als Administrator anzumelden und Lifeupdate von hand auszuführen.

In Heft 03/2003, S. 177, hat die c't auf eine Leseranfrage mitgeteilt, NAV vertrage sich mit wXP nur dann, wenn man die regelmäßigen Virenchecks abschalte oder ständig mit Administrator-Rechten arbeite. Sollte dies zutreffen, so wäre NAV nicht nur mit ‚ungenügend' zu bewerten, sondern schlichtweg unbrauchbar. Ich würde das Programm meiden und erforderlichenfalls zurückgeben und mir das Geld erstatten lassen. Für mich sind die eingeschränkten Benutzerrechte die zweitwichtigste Sicherheitseinrichtung (nach dem Virenscanner) und es kann nicht sein, dass die wichtigste Sicherheitseinrichtung mich zwingt, die zweitwichtigste abzuschalten. Ich darf aber nochmals betonen, dass ich die geschilderten Schwierigkeiten mit w2k und eingeschränkten Benutzerrechten nicht hatte. Das Liveupdate muss aber abgeschaltet werden, denn NAV reagiert sehr ‚zickig', wenn es versucht, ein Liveupdate durchzuführen und dies nicht gelingt.

Sollten Sie ein Programm unbedingt benötigen, welches Administrator-Rechte erfordert, und es wirklich gar keine Alternative in Form eines Updates oder eines andern Programms geben, dann könnten Ihnen vielleicht die folgenden Tipps helfen:

Zunächst kann man jedes Programm mit systeminternen Mitteln mit anderen Rechten ausführen: Lassen Sie sich die auszuführende Datei z.B. im Windows-Explorer anzeigen, drücken Sie dann die Shift-Taste und klicken Sie danach die Datei mit der rechten Maustaste an (Reihenfolge beachten !). Es erscheint der Menupunkt ‚Ausführen als ...'. Hier können Sie den Benutzernamen und das Passwort des Benutzers angeben, mit dessen Rechten das Programm ausgeführt werden soll. Wenn Sie die Eigenschaften eines vom aktuellen Benutzer angelegten Links aufrufen, können Sie dort ein Kästchen ankreuzen mit der Bezeichnung ‚Unter anderem Benutzernamen ausführen'. Schließlich kann man sich auch mit dem Programm ‚runas' einen entsprechenden Link anlegen. Alle Optionen des Programms ‚runas' werden angezeigt, wenn Sie mit Start→Ausführen→cmd ins DOS-Fenster wechseln und dort ‚runas' eingeben (zurück mit ‚exit'). Der Nachteil dieser Verfahren besteht darin, dass Sie das Passwort stets von Hand eingeben müssen. Dies ist besonders lästig bei Programmen, die bereits beim Windows-Start gestartet werden sollen.

Deshalb gibt es die Möglichkeit, ein Programm als Service zu starten. Hierzu benötigen Sie z.B. das Programm ‚Apptoservice' [32] oder die Programme srvany.exe und instsrv.exe aus dem NT Resource Kit und eine passende Anleitung [33].

Klappt auch das nicht, hilft in jedem Fall das Programm ‚runasPWD.exe' [34] von Richard MacDonald. Ich habe allerdings lange gezögert, den Hinweis in diese Anleitung aufzunehmen, denn der entscheidende Vorteil dieses Programms ist zugleich ein sicherheitstechnisch schwerer Nachteil: Das Programm arbeitet ähnlich wie ‚runas', kann aber außerdem das Passwort in der Befehlszeile mit verarbeiten, wodurch ein vollautomatischer Start möglich ist. Wenn Sie das Programm über einen entsprechenden Link z.B. in den Autostart-Ordner einbinden, haben Sie dieses Passwort (z.B. des Administrators) im Klartext auf der Festplatte, was eigentlich unverantwortlich ist. Dies dürfte in keinem Fall in einer ‚echten' Mehrbenutzerumgebung in Frage kommen, in der wirklich mehrere Menschen an demselben Rechner arbeiten und in der unbedingt verhindert werden muss, dass einzelne dieser Benutzer sich Administrator-Rechte aneignen. Wenn allerdings nur ein Mensch mit mehreren Benutzerkonten an dem Computer arbeitet oder alle Benutzer ohnehin das Administrator-Passwort kennen, kann man sicher auf die vertretbare Idee kommen, es sei jedenfalls sicherer, das Administrator-Passwort auf der Festplatte zu speichern als sich ständig mit Administrator-Rechten im Internet zu bewegen (gut ist beides nicht).

Bei XP erzeugt Windows bei der Installation selbst eine Sicherheitslücke, indem es für den abgesicherten Modus ein kennwortloses Administrator-Konto anlegt. Um diese Lücke zu schließen, müssen Sie den Rechner einmal im abgesicherten Modus starten (‚F8'-Taste während des Start-Vorgangs gedrückt halten und ‚abgesicherter Modus' in dem dann erscheinenden Menu auswählen). Melden Sie sich dann als ‚Administrator' an. Unter *Start→Systemsteuerung→Benutzerkonten* können Sie das Administrator-Konto anwählen und über *Kennwort erstellen* ein Kennwort vergeben.

**Wie kann/sollte man den Rechner weiter absichern ?**

1. In jedem Fall sind eine anwendungsbezogene Desktop-Firewall (z.B. ZoneAlarm, Tiny Personal Firewall, Outpost [60]) und ein Virenscanner (wei-

terführende Informationen unter [7] bis [19] und [35] bis [38]) erforderlich, weil man nur mit solchen Programmen (hoffentlich) verhindern kann, dass schädliche (oder auch unbekannte) Programme (z.B. Trojaner) die offenen Ports benutzen, um unerwünscht Daten zu übermitteln oder Schadprogramme zu laden und auszuführen. Die Hardware-Firewall kann ja nur Adressen und Ports sperren. Nützlich erscheint mir auch TrojanCheck [61]. Jeder Trojaner muss sich in irgendeiner Weise in den Startpunkten von Windows verankern. Diese Punkte überwacht TrojanCheck.

2. Sehr interessant fand ich die Sandbox-Idee, die Aladdin mit eSafe Desktop [3] umzusetzen versucht hat. Leider hat das Programm nur durchschnittliche Kritiken bekommen, vor allem weil es schwierig zu konfigurieren ist und nicht absolut zuverlässig funktioniert. Vereinfacht arbeitet eine Sandbox wie folgt: Programme, die eine Internet-Verbindung aufbauen dürfen, haben nur sehr eingeschränkten Zugriff auf die Rechner-Ressourcen (insbesondere Festplattenverzeichnisse, Dateien, Registry), während Programme, die uneingeschränkten Zugriff haben, eben nicht in das Internet dürfen. Wie schwierig es ist, die Idee umzusetzen, haben mich meine Erfahrungen gelehrt: Zum einen gibt es kaum noch neuere Programme, die ohne Internetzugang auskommen. Zum anderen (und das ist viel schwerwiegender) wollen die klassischen Zugangsprogramme (z.B. Outlook) einen derart weitreichenden Systemzugriff, dass die ganze Idee nicht mehr klappt. Insbesondere Outlook verknüpft sich in derart umfassender Weise mit den anderen Office-Programmen, dass man sehr schnell die ganze Office-Familie freigegeben hat. Wenn dann die wichtigsten und sensibelsten Daten mit Word, Excel und Access bearbeitet werden sollen, müssen diese Programme auch auf die Daten zugreifen können, so dass diese Daten eben nicht mehr geschützt sind, wenn die Hauptprogramme in irgendeiner Weise ins Internet kommen. Die neuesten Versionen der Norman Personal Firewall [4] sowie der Tiny Personal Firewall (Version 4.0) [22] enthalten ebenfalls Sandbox-Module, welche ich aber noch nicht ausprobieren konnte. Die Sphinx PC Firewall (zuletzt wohl ebenfalls mit Sandbox) wird wegen Insolvenz nicht weitergeführt.

   Ausprobieren konnte ich inzwischen die Tiny Personal Firewall 3.0: Diese Version hat nichts mehr mit einem einfachen Port-Blocker zu tun. Wenn man sich die Oberfläche dieser Firewall und die hier angebotenen Möglichkeiten ansieht, wähnt man sich am Ziel seiner Träume. Wenn die Firewall all das könnte, was die Oberfläche verspricht, könnte das Programm der ideale Schutz sein. Allerdings ist das ‚Manual' derart knapp, dass ich das Programm hiermit nicht bedienen könnte. Der Rechner wird nach der Installation deutlich stärker belastet als mit der Tiny Personal Firewall 2.0 und der Kerio Personal Firewall 2.1.4, was angesichts der angebotenen Überwachungsmöglichkeiten auch nicht verwundert. Ich habe zunächst das Sandbox-Modul getestet und versucht, allen Programmen, die Zugriff auf das Internet haben, den Zugriff auf die Laufwerke und Ordner auf meinem Novell-Server zu verbieten – ohne jeden Erfolg. Ob dies mit den Besonderheiten des Novell-Systems zusammenhängt und das Sandbox-Modul in reinen Windows-Umgebungen funktioniert, habe ich nicht mehr probiert, weil ich nach dieser Fehlfunktion keinerlei Vertrauen mehr in die

Software hatte. Eine eMail-Anfrage an Tiny-Software wurde nicht beantwortet. Das Manual enthält keinerlei Hinweise, dass die Software nur in bestimmten Netzen (oder sogar nur auf Einzelrechnern) funktioniert. Auch die Deinstallation der Software war nur mit Mühe möglich.

Nach meinen Erfahrungen mit der Version 3.0 fehlt mir im Moment der Mut, die zum Jahreswechsel 2002/2003 herausgekommene Version 4.0 auszuprobieren [56]. Das bei tinysoftware separat herunterladbare Manual ist nach wie vor unzulänglich: Es nützt nichts, dem Kunden 102 Seiten anzubieten, wenn der größte Teil dieser Seiten leer ist.

3. Wenn Sie einen alten Rechner haben, können Sie natürlich auch darüber nachdenken, diesen an den Vigor anzuschließen, nur auf diesem das TCP/IP-Protokoll zu installieren, nur mit diesem ins Internet zu gehen und diesem Rechner den Zugriff auf andere Rechner zu verbieten (wird bei Virenupdates und Updates anderer Software [Windows-Service-Packs] etwas umständlich). Deshalb Alternative: Installieren Sie das TCP/IP doch auf allen Rechnern. Blocken Sie im Filtersetup des Routers über die lokalen IP-Adressen (feste Zuweisung erforderlich) alle Rechner außer dem ‚alten'. Die Blockade der anderen Rechner heben Sie nur kurzfristig auf und auch nur, um Updates über vertrauenswürdige Sites Ihrer Softwareherstellers zu laden.

   Haben Sie keinen ‚alten' Rechner, können Sie ähnliches auch auf einem ‚neuen' Rechner mit einem Dual-Boot-System erreichen: Nehmen Sie statt des ‚alten' Rechners einen ‚neuen' und installieren Sie auf diesem zwei Betriebssysteme (kann natürlich auch zweimal w2k/XP sein). Es würde den Rahmen dieser Hilfe sprengen, wenn ich versuchen wollte, auch dies zu erklären (ich empfehle Partition Magic). Bei der Installation des TCP/IP-Protokolls auf beiden Betriebssystemen geben sie unterschiedliche IP-Adressen für die Netzwerkkarte ein (hier beweist sich einmal mehr, wie nützlich es ist, dass es außer der MAC-Adresse auch eine frei zuweisbare IP-Adresse gibt). Die IP-Adresse des Systems, welches ins Internet ‚darf' schalten Sie im Router-Filter-Setup frei, die andere blockieren Sie. Sie müssen natürlich durch entsprechende Freigaben/Verschlüsselungen des zu schützenden Betriebssystem dafür Sorge tragen, dass das internetzugelassene System nicht auf die zu schützenden Daten zugreifen kann. Wenn Ihnen auch das noch zu gefährlich erscheint, können Sie für das zu schützende System w2k/XP einsetzen und für das internetzugelassene System w98. w2k/XP formatieren Sie mit NTFS und w98 mit FAT xx. Ohne spezielle Erweiterung kann w98 nicht auf die NTFS-Partitionen zugreifen.

4. In einer Newsgroup habe ich einmal den Ratschlag bekommen, doch den Stecker zu ziehen. Was auf den ersten Blick aussieht wie eine Unverschämtheit oder jedenfalls wie die Kapitulation vor den anstehenden Problemen, ist auf den zweiten Blick durchaus nachdenkenswert: Es bringt sicherlich zusätzliche Sicherheit, z.B. dem T-DSL-Modem den Strom abzuschalten, wenn Sie keine Internetverbindung haben wollen (sehr bequem mit einer fernbedienbaren Funk-Zwischensteckdose aus dem Baumarkt). Auch diese ‚mechanische Firewall' hat ihre Daseinsberechtigung. Das

ISDN-Fallback muss natürlich abgeschaltet werden (Quick Setup → Internet Access Setup → PPPoE Client Mode → ISDN Dial Backup Setup: None) ! ***Achtung:*** Bei meinen Firmware-Versionen 2.1, 2.2 und 2.3 funktionierte diese Abschaltung nicht. Die Rechner benutzten trotz der oben wiedergegebenen Einstellung die ISDN-Leitung, wenn der DSL-Zugang ausfällt. Daher ist es besser, das ISDN-Kabel abzuziehen.

5. Bekanntlich legt Windows an mehreren Stellen Verknüpfungen zu Programmen an, die beim Systemstart automatisch gestartet werden. Diese automatisch startenden Programme sollte man sich regelmäßig ansehen, und zwar einmal, um Verknüpfungen zu entfernen, die das System ausbremsen, zum anderen aber auch, um festzustellen, ob sich an diesen Stellen nicht ein Schädling eingenistet hat. So hat z.B. ein Trojaner den schwierigsten Teil seiner Arbeit bereits erledigt, wenn es ihm gelungen ist, sich unter die Autostart-Dateien zu schmuggeln. Zur Kontrolle reicht eigentlich das Programm msconfig (über *Start→Ausführen* aufrufen), welches aber nicht in allen Windows-Versionen enthalten ist. Wesentlich komfortabler und mit allen Windows-Versionen arbeitet der Autostart-Manager [44]. TrojanCheck [61] verspricht eine automatische Überwachung.

6. Viele Sicherheitspakete enthalten einen sogenannten Content-Filter, der eingehende Pakete inhaltlich untersucht und bei bestimmten im Filter vorgegebenen Inhalten verwirft. Ein solcher Filter könnte auch umgekehrt, bei ausgehenden Paketen für zusätzliche Sicherheit sorgen. Man könnte z.B. in geheimhaltungsbedürftigen Dateien einen bunten Zahlen- und Buchstaben-‚Salat' unterbringen und dem Filter vorgeben, Dateien, die diese Buchstaben- und Zahlenkombination beinhalten, von einer Versendung ins Internet auszunehmen. In WORD-Dateien könnte man die Kombination notfalls in weißer Schrift im eigentlichen Text, besser aber in den Texteigenschaften oder in einem verborgenen Textteil unterbringen. Erstellt man sich eine entsprechende Dokumentenvorlage, klappt das Ganze in Zukunft vollautomatisch. Leider habe ich noch kein Programm gefunden, das einen Content-Filter für ausgehende Pakete beinhaltet.

7. Für den Umgang mit Cookies und dem Referrer finden Sie bei den Begriffserläuterungen unter den entsprechenden Stichworten Hinweise.

8. Wie Sie mit den erheblichen Risiken umgehen, die bei der Verwendung des Internet Explorers und aktiviertem ActiveX entstehen, müssen Sie selbst entscheiden. Erste Hinweise finden Sie in den Begriffserläuterungen unter ActiveX.

**Machen Firewalls überhaupt einen Sinn ?**

Gelegentlich findet man Berichte, in denen behauptet wird, Desktop Firewalls seien komplett sinnlos, weil man sie ohne weiteres ‚tunneln' kann, indem ein Schadprogramm die zugelassenen Programme quasi fernbedient, um seine schädliche Arbeit zu verrichten. Wer dies ausprobieren möchte, findet unter [42] 3 Testprogramme. Ich habe die Programme gestartet und folgendes festgestellt: Eines der Programme scheitert bei mir sowohl an der Router-Firewall als auch an der Desktop-Firewall, weil

es einen ganz ungewöhnlichen Port benutzen will, den beide Firewalls nicht zulassen. Origineller Weise behauptet das Programm, es habe einen erfolgreichen Angriff auf meinen Rechner gestartet, und zwar auch noch, nachdem ich sowohl den Stecker vom DSL-Modem als auch von der ISDN-Dose abgezogen hatte. Das zweite Programm scheiterte immerhin an der Desktop-Firewall und gab dies auch zu. Lediglich das 3. Programm konnte ungehindert Daten senden. Gleichwohl würde ich aber deshalb nicht auf die Idee kommen, die Desktop-Firewall zu deinstallieren, weil mir ohnehin klar ist, dass ich niemals eine absolute Sicherheit erreichen kann. Ich habe das erfolgreiche ‚Tunnel'-Programm freiwillig auf meinen Rechner geladen und gestartet. Ob das Programm auch gegen meinen Willen hätte gestartet werden können (und nicht z.B. vorher durch den Virenscanner geblockt worden wäre), ist eine ganz andere Frage. Durch die Kombination vieler für sich genommen vielleicht gar nicht einmal besonders sicherer Maßnahmen kann ich im Endergebnis gleichwohl eine sehr hohe Sicherheit erreichen. Selbst wenn das Tunnelprogramm mich aber erfolgreich angreift, kann ich mich immerhin noch damit trösten, dass eine Vielzahl anderer Angriffe erfolgreich abgewehrt worden ist.

Aus dem gleichen Grund macht es natürlich auch keinen Sinn, auf die meisten Sicherheitsprogramme zu verzichten, nur weil z.B. der Bugbear-Wurm die meisten davon ‚abschießt' [43].

**Einige nützliche Telnet Kommandos**

Starten Sie Telnet mit Start → Ausführen → *telnet 192.168.1.1* [Enter] und geben sie das Zugangspasswort ein.

Mit

| | |
|---|---|
| ipf view –r | können Sie sich alle (Call- und Daten-) Filter ansehen |
| ipf view –c | können Sie sich alle Call-Filter ansehen |
| ipf view –d | können Sie sich alle Daten-Filter ansehen |
| log –f | können Sie überprüfen, ob eine Regel eingegriffen hat, wenn Sie im General-Setup oder bei der einzelnen Regel die Log-Funktion entsprechend eingestellt haben (s. in der Handbuchübersetzung). |
| log –F a | löscht den Log-Puffer für alle Logs (es ist empfehlenswert, diese Funktion auszuführen, bevor Sie mit Ihren Untersuchungen beginnen, denn andernfalls sehen Sie logs, die aus früheren Sitzungen stammen und – die für Ihre konkreten Untersuchungen uninteressant sind). Wie bestimmte Logs gezielt gelöscht werden können, zeigt Ihnen der Router an, wenn Sie in einer geöffneten Telnet-Sitzung ‚log ?' eingeben. |

Die angezeigten Ergebnisse können Sie in die Zwischenablage kopieren und in einen Editor oder WORD einfügen, um Sie abzuspeichern oder auszudrucken.

**Kann die Firewall mehr ?**

Das unter V. nachfolgende Beispielfilterset lässt sich über das Webinterface des Routers eingeben. Eine Programmierung der Filterregeln mit Telnet scheint zur Zeit nicht möglich zu sein. Jedenfalls ist es mir nicht gelungen, auch nur eine einzige

simple Regel über das Telnet-User-Interface einzugeben. Im Internet kursieren an mehreren Stellen Beschreibungen zum Vigor *2000*, in denen beschrieben wird, wie man die Firewall-Regeln für *diesen* Router mit Telnet-Befehlen eingeben kann. Wenn man jedoch beim Vigor 2200 in einer Telnet-Sitzung ‚ipf ?' eingibt, fehlen die meisten Befehlsmöglichkeiten, die in den Beschreibungen zum Vigor 2000 erwähnt werden und die erforderlich wären, den Vigor 2200 hinsichtlich der Filterregeln zu programmieren. Nach der Eingabe ‚ipf view ?' erhält man einen Hinweis, der mit ‚Usage:' beginnt, gleiches fehlt, wenn man ‚ipf rule ?' eingibt (www.vigor-users.de vermitteln ebenfalls die Information, eine Konfiguration der Filter-Regeln mittels Telnet sei bei den aktuellen Firmware-Versionen nicht möglich). Das Original-Handbuch beschreibt ‚ipf rule' mit keinem Wort und in den technischen Spezifikationen im Anhang zum Handbuch wird als Eigenschaft des Routers u.a. angegeben: ‚IP-based packet filtering with *web-based* configuration', während bei anderen Konfigurationsbeschreibungen ausdrücklich das ‚Telnet-based user Interface (TUI)' beschrieben wird. Die fehlende Telnet-Konfiguration ist wirklich sehr bedauerlich, denn wenn man in einer Telnet-Sitzung mit dem Vigor 2200 ‚ipf rule ?' oder auch nur ‚ipf rule' eingibt, wird eine Vielzahl von Regelmöglichkeiten angezeigt, die – sollten sie tatsächlich zur Verfügung stehen – eine enorm leitungsfähige Firewall lieferten (z.B. kann das ACK-Flag abgefragt werden, bei ICMP-Paketen kann der genaue Typ herausgefiltert werden usw.), die mit dem Webinterface nicht erstellt werden kann. Durch meine Versuche mit dem ipf-Befehl ist mir allerdings aufgefallen, dass der mit ‚ipf rule' angezeigte Befehlssatz exakt mit dem Befehlssatz einer im Unix/Linux-Bereich weit verbreitete Freeware-Firewall übereinstimmt, die auf der Homepage [39] kostenlos heruntergeladen werden kann und zu der es sogar eine sehr gute deutsche Anleitung [40] gibt. Über die Links auf der zitierten Homepage können Sie auf einen riesigen Pool zusätzlicher Infos zur Firewall zugreifen.

Nun habe ich natürlich darüber nachgedacht, was ich aus dieser Übereinstimmung folgern kann. Da ich an Zufälle nicht glaube (es ist einfach nicht denkbar, dass zwei Programmierer völlig unabhängig voneinander eine Firewall entwickeln und am Ende zu genau demselben Befehlssatz kommen), gehe ich davon aus, dass die Vigor-Firewall tatsächlich auf dieser IPF-Firewall aus dem Unix/Linux-Lager beruht [41]. Eine andere Frage ist natürlich, ob die IPF-Firewall tatsächlich komplett übernommen wurde und durch das WebInterface des Routers ausgebremst wird oder ob DrayTek (z.B. weil der Speicher im Router nicht ausreicht) die Firewall zusammengestrichen hat, so dass die Firewall tatsächlich nur das kann, was das WebInterface anzeigt. Letzteres scheint mir eher unwahrscheinlich, auch wenn ich es leider nicht prüfen kann, weil ich in das Programm des Routers nicht ‚hineinsehen' und auch nicht testweise andere Regeln eingeben kann, als das WebInterface zulässt. Gleichwohl wird man doch folgendes überlegen müssen:

- Warum sollte DrayTek die Firewall kürzen, nicht aber die dazugehörige und mit ‚ipf rule' angezeigte Hilfeseite ?
- Das Kürzen der Firewall ist mit Arbeit und einem hohen Fehlerrisiko behaftet, inwieweit es urheberrechtlich zulässig ist, kann ich nicht beurteilen.
- Insbesondere das Verhalten des Routers beim Update auf die Fw 2.3 belegt, dass die Firewall mehr kann, als das WebInterface zulässt: Der Router arbeitete mit der Source-Route-Option weiter einwandfrei, obwohl sie nicht mehr eingegeben werden konnte und das WebInterface sie bei der ersten Änderung einer be-

liebigen Regel entfernt hat (s. dazu schon unter Begriffserläuterungen→Source Route).

Auch der Umstand, dass mit dem WebInterface nicht der gesamte IPF-Befehlssatz ausgenutzt werden kann, spricht nicht gegen meine Vermutung. Das WebInterface müsste ganz erheblich erweitert und mit weiteren Untermenus versehen werden, um den gesamten Befehlssatz nutzen zu können. Möglicherweise reicht hierzu der Speicherplatz im Router nicht oder DrayTek hat noch keine Gelegenheit gefunden, sich dieser Arbeit anzunehmen. Auf das WebInterface kann DrayTek nicht verzichten; der Router würde jeden Vergleichstest wegen mangelhafter Bedienbarkeit verlieren, wenn die Firewall nur über Telnet programmiert werden könnte. DrayTek kann es (sinnvollerweise) eigentlich auch nicht zulassen, dass die Firewall sowohl über Telnet als auch über das WebInterface eingestellt werden kann, solange diese beiden Zugangsmöglichkeiten nicht absolut die gleichen Optionen bieten. Es würde ein totales Chaos entstehen, wenn ich z.B. über Telnet Firewall-Regeln unter voller Ausnutzung des ipf-Befehlssatzes eingäbe und dann das WebInterface aufriefe: Alle Regeln würden unvollständig und unverständlich wiedergegeben und – noch schlimmer – bei der ersten Änderung im WebInterface völlig verkrüppelt, weil das WebInterface in diesem Fall alle Regeln in den ipf-Befehlssatz neu übersetzt und dabei aber nur die Möglichkeiten nutzt, die es selbst hat (wie beim Entfernen der Source Route-Option).

Nach meiner Auffassung gäbe es einen Ausweg (immer vorausgesetzt, der Router beherrscht tatsächlich alle ipf-Befehle, denn dann wäre es eigentlich schade, das verkümmern zu lassen): Wenn DrayTek eine Möglichkeit schüfe, die Firewall-Programmierung über das WebInterface durch eine zusätzliche Option in eben diesem Interface abzuschalten, könnte man eine andere Zugangsart öffnen:

Unter Linux lädt der Anwender sich die Firewall z.B. in den Kernel und kann die Regeln über ipf -F a -f {Datei} ändern (Der Parameter -F a löscht die vorhandenen Regeln, der Parameter - f {Datei} übergibt die neuen). In der {Datei} stehen die eigentlichen Regeln, die so aufgebaut werden müssen, wie es ipf rule vorgibt und wie sie auch vom Router mit , ipf view –r‘ wiedergegeben werden.

Denkbar wäre, dass DrayTek ein Hilfsprogramm verteilt, mit dem der Anwender die Firewall-Regeln, die in einer Text-Datei abgelegt sind, an den Router schicken kann (ähnlich wie das Programm für die Firmware-Updates). Dieses Programm müsste so ausgelegt sein, dass es nur funktioniert, wenn vorher die Programmierungsmöglichkeit für die Firewall-Regeln im WebInterface abgeschaltet ist. Umgekehrt müssten alle Firewall-Regeln im Router (natürlich nach einer entsprechenden Warnung) gelöscht werden, wenn der Anwender die Firewall-Programmierung über das WebInterface wieder aktivieren will.

Damit hätte DrayTek alle Anwender zufrieden gestellt: Für den Einstieg könnte man sich mit dem WebInterface zufrieden geben und danach auf die ‚richtige‘ IP-Firewall umsteigen. Die Vorteile wären immens:

- Der gesamte IPF-Befehlssatz stünde zur Verfügung.
- Die Anzahl der Regeln wären nur durch den Speicherplatz im Router begrenzt.
- Die Regeln könnten mit jedem Text-Editor bearbeitet werden. Man könnte sie nach oben und unten schieben, in die Zwischenablage kopieren usw. usw.

- Die eigentlichen Firewall-Regeln, die ja jetzt in einer einfachen Text-Datei stecken, könnten problemlos zwischen den Anwendern ausgetauscht werden.
- Man hätte das gesamte Linux-Lager mit unzähligen Beispiel-Konfigurationen als Hilfe zur Verfügung (soviel kann man gar nicht lesen, bevor der Router völlig veraltet ist).
- Man könnte sich verschiedene (und unbegrenzt viele) Regel-Sets in Textdateien ablegen und die gesamte Firewall per Mausklick in Sekundenbruchteilen austauschen und für jeden Benutzer verschiedene Firewalls anlegen.
- Es könnten Regel-Gruppen gebildet werden (dazu gleich mehr).

Es wäre doch wirklich schade, wenn das alles ein Traum bliebe (Vielleicht übersetzt ja jemand einmal diese Passagen ins Chinesische und schickt sie an DrayTek; die ersten Regel-Sets in Textform stelle ich.)

Eine Beispieltextdatei könnte z.B. wie folgt aussehen:

```
block in quick from any to any with short
pass in quick proto icmp from any to any
pass in quick proto tcp from any port = ftp-data to any port > 1024
block in quick from any to any
block out quick proto tcp/udp from any port = 445 to any
pass out quick proto icmp from any to any
pass out quick proto udp from any to 217.5.99.9/32 port = domain
pass out quick proto udp from any to 194.25.2.128/25 port = domain
pass out quick proto tcp from any to any port = www
pass out quick proto tcp from any to any port = 443
pass out quick proto tcp from any to 194.25.134.0/24
pass out quick proto udp from any port = ntp to 130.149.17.21/32 port = ntp
pass out quick proto tcp from any to 62.153.159.134/32 port = nntp
pass out quick proto tcp from any to 207.46.230.185/32 port = nntp
pass out quick proto tcp from any port > 1024 to any port = ftp
pass out quick proto tcp from any to any port = telnet
pass out quick proto tcp from any port > 1024 to any port > 1024
block out quick from any to any
```

Eine weitere recht originelle Methode, mit der das WebInterface den ipf-Befehlssatz nutzt, findet man, wenn versucht bei den einzelnen Filterregeln unter ***Branch to Other Filter Set*** etwas anderes als ‚None' einzutragen. Zunächst fällt auf, dass man diese Option in der Firewall nur bei einer einzigen Regel benutzen kann. Versucht man die Option bei einer zweiten Regel einzusetzen, verweigert sich der Router bzw. trägt eigenmächtig wieder ‚None' ein. Noch skeptischer wird man, nachdem man festgestellt hat, dass man nur nach ‚oben' auf das Set#1 verweisen kann und bekommt natürlich sofort Angst, hier eine nicht mehr endende Rekursion zu programmieren. Aber keine Sorge: Wenn man sich die Regel, bei der man den ‚Verweis' auf das Set#1 gesetzt hat, unter Telnet mit ‚ipf view –r' ansieht, stellt man fest, dass diese Regel den Zusatz ‚head 1' bekommen hat.

Um dies zu verstehen, musste ich wieder auf die Beschreibungen zur IP-Firewall zurückgreifen:

Wenn man einer Regel den Zusatz head # (z.B. 100) verpasst und die Regel zutrifft, arbeitet die Firewall zunächst alle Regeln ab, die zu dieser „Überschrift"-Regel gehören. Diese Zusammengehörigkeit wird dadurch gekennzeichnet, dass man diesen Regeln group # (z.B. 100) hinzufügt. Findet die Firewall eine Gruppenregel mit dem Zusatz „quick" wird diese Regel sofort ausgeführt und die Firewall ist mit ihrer Arbeit am Ende. Findet die Firewall keine zutreffende Gruppenregel, kehrt sie zur Überschrift-Regel zurück. Ist dies ein quick-Regel, wird diese Regel ausgeführt und die Firewall ist fertig; ist es keine quick-Regel, macht die Firewall mit den Regeln „hinter" den Gruppenregeln weiter, und zwar mit der Standard-Aktion, die die Überschrift-Regel setzt (pass if no further match oder block if no further match). Findet die Firewall eine zutreffende Gruppenregel, die keine quick-Regel ist, und wird auch in den folgenden Gruppenregeln keine quick-Aktion befohlen, dann ist die Überschrift-Regel „übersteuert" (gleichgültig, ob es sich um eine quick-Regel handelt oder nicht). Die Firewall macht mit den Regeln „hinter" den Gruppenregeln weiter, und zwar mit der Standard-Aktion, die die zutreffende Gruppen-Regel gesetzt hat (pass if no further match oder block if no further match).

Innerhalb einer Gruppe kann man sogar weitere Untergruppen bilden, indem man einer Regel z.B. den Zusatz „head 101 group 100" hinzufügt.

Der entscheidende Vorteil einer solchen Gruppierung besteht darin, dass sie die Arbeit der Firewall dramatisch beschleunigen kann: Ein Paket, auf das die Überschrift-Regel nicht zutrifft, überspringt alle Gruppenregeln, die zu dieser Überschrift-Regel gehören und durchläuft sofort die danach kommenden Regeln.

Beispiel:

```
block out quick from 192.168.1.10/32 to any head 1
        pass out quick proto icmp from 192.168.1.10/32 to any group 1
        pass out quick proto tcp from 192.168.1.10/32 port > 1024 to any port > 1024 group 1
        ... group 1
        ... group 1
        ... group 1
pass out quick from any to any
```

Alle ausgehenden Pakete vom Rechner mit der IP 192.168.1.10 werden einer genauen Prüfung unterzogen, indem sie das gesamte Regelwerk der group 1 durchlaufen. Finden sie dort keine Erlaubnisregel, werden sie durch die head 1-Regel sofort verworfen. Pakete von allen anderen Rechnern überspringen nach der head 1-Regel die dazugehörigen Gruppenregeln und werden durch die letzte Regel sofort durchgelassen.

Da der Router keine Regeln mit dem Zusatz ‚group 1' versieht, bringt es überhaupt nichts, unter *Branch to Other Filter Set* etwas anderes als ‚None' einzutragen. Es gibt keine zu ‚head 1' passende Gruppe. Alle Pakete durchlaufen die head 1-Regel und machen danach mit der nächsten Regel weiter. Es scheint mir auch etwas übertrieben, bei einer Router-Firewall, die überhaupt nur 84 Regeln zulässt, Gruppierungen vorzunehmen (zum Vergleich: In den Linux-Beschreibungen habe ich Berichte über ipf-Firewalls mit 45.000 (!) Regeln gefunden. Da muss der Vigor noch etwas üben.)

# V. Beispielfilterset für die Router Firewall

## Allgemeine Hinweise

***Sehr wichtig:*** Die Beispiele habe ich für einen Router erstellt, auf dem die ***Firmware 2.3*** (Build Date/Time Fri Jan 10 9:35:52.74 2003) und zwar in der Version eingespielt war, die ich von DrayTek/Taiwan unter ftp://ftp.draytek.com.tw heruntergeladen habe (die deutsche Oberfläche habe ich mir gespart). Vorher habe ich die Regeln auch mit den Firmware-Versionen 2.1a und 2.2 ohne Probleme im Einsatz gehabt. Mit der Firmware 2.0a - jedenfalls in der Fassung, mit der mein Router im Auslieferungszustand bestückt war - funktioniert das Regelset *nicht*. Bei dieser Firmware sind ziemlich genau doppelt so viele Regeln erforderlich, und zwar aus folgendem Grund: Ausgehende Verbindungen mit dem TCP-Protokoll werden immer eingehend bestätigt. Von anderen Firewalls war ich es gewohnt, dass diese eingehenden Quittungspakete automatisch zugelassen waren, wenn ich eine ausgehende Verbindung gestattet habe (so arbeiten jetzt offenbar auch die Versionen 2.1a bis 2.3). Die Firmware 2.0a blockte diese Pakete, wenn man sie nicht durch eine ausdrückliche Regel zuließ. Diese Voreinstellung macht natürlich beim TCP-Protokoll die Unterscheidung in den Filterregeln zwischen aus- und eingehenden Datenpaketen unsinnig, weil man dann ohnehin für jede erlaubte Ausgangsverbindung eine korrespondierende Eingangsverbindung erlauben muss. Außerdem schafft man hierdurch zusätzliche Risiken, denn die eingehende Verbindung ist jetzt generell gestattet, also unabhängig davon, ob es sich um Quittungspakete oder eine von außen eigenständig initiierte Verbindung handelt (Auch wenn ich bei den ausgehenden Erlaubnisregeln die 'Keep State'-Option aktiviert habe, habe ich ohne ausdrückliche Erlaubnisregel für eingehende Pakete keine Verbindung zustandegebracht, was mir inzwischen auch logisch erscheint: Wenn der Router bereits die Antwortpakete des angesprochenen Servers mit dem ACK-Flag blockt, wird eben gar keine Verbindung etabliert, deren Status gehalten werden könnte). Wenn Sie also unbedingt bei der Firmware 2.0a bleiben wollen, müssen Sie bei jeder ausgehenden Erlaubnisregel über das TCP-Protokoll eine eingehende Erlaubnisregel eingeben, bei der Sie im Vergleich zur ausgehenden Regel [Quell-Adresse + Port] gegen [Ziel-Adresse + Port] tauschen. Spiegelbildlich gilt Gleiches, wenn Sie eine eingehende Verbindung erlauben wollen.

Ich habe mich beim Abfassen des Regelsatzes bewusst darauf konzentriert, einen möglichst ungehinderten Internet-Verkehr zuzulassen, Sicherheitsgesichtspunkte mussten demgegenüber zurückstehen. Es handelt sich daher nicht um einen besonders sicheren Regelsatz, sondern um einen besonders zugangsfreundlichen. Jeder Anwender kann durch das Deaktivieren der einen oder anderen Regel zusätzliche Sicherheit schaffen. Die Anmerkungen im Anschluss an das Beispiel sollen dabei behilflich sein.

Ich habe mich ferner für einen Aufbau entsprechend der deny-all-Strategie entschieden, bei der durch die letzten Regeln alles verboten wird, was nicht vorher gestattet wurde. Diese Vorgehensweise scheint mir die sicherste zu sein, weil mir durch die Eingabe einer entsprechenden Erlaubnisregel unmittelbar vor Augen geführt wird, welche Tore ich öffne. Ich muss allerdings einräumen, dass die Eingabe einer einzigen ‚falschen' Erlaubnisregel 83 wohlüberlegte andere Regeln überflüssig machen kann. Man sollte daher jede Erlaubnisregel sehr genau überprüfen und Kontrollen

durchführen, indem man z.B. eine Erlaubnisregel, die für einen bestimmten Dienst eigentlich zwingend erforderlich ist (z.B. die Regeln für den DNS-Port 53), testweise deaktiviert: Kann man dann trotzdem problemlos im Internet surfen, ist ein Fehler im Regelset. Die deny-all-Strategie erleichtert außerdem die Fehlersuche: Wenn ich den Eindruck habe, bestimmte Dinge im Internet wegen der Router-Firewall nicht mehr nutzen zu können, so reicht es aus, die beiden letzten Regeln vorübergehend zu deaktivieren. Klappt es dann, ist eine weitere Erlaubnisregel erforderlich, während ich die Firewall als Ursache ausschalten kann, wenn trotz dieser Deaktivierung die gewünschte Verbindung nicht zustande kommt.

Schließlich habe ich es vermieden, Regeln nach den Vorgaben ‚Block If No Further Match' bzw. ‚Pass If No Further Match' einzusetzen oder in ein anderes Filterset als das nachfolgende zu verzweigen, weil ich Sorge habe, dass hierdurch das gesamte Regelgerüst unübersichtlich wird. Aus dem gleichen Grunde habe ich bei jedem Filterset (mit Ausnahme des Call-Fiter-Sets 1) einen Verweis auf das nachfolgende Filterset gesetzt, und zwar auch dann, wenn dieses z.Zt. gar nicht belegt ist (Vorsicht: Wenn Sie ein komplettes Set in der Übersicht mit ‚Clear' löschen, wird auch der Verweis auf ‚None' gesetzt, was bei dem von mir gewählten Aufbau zu einer ziemlichen Katastrophe führt, weil die gesamten Filterregeln unsinnig werden: Die zentralen Regeln sind in Set 12; dieses *muss* angesprungen werden !!).

Gegen meinen Regelaufbau ist einem Forum eingewandt worden, er sei zu riskant; es sei besser, zwei Regeln für ein- und ausgehende Pakete mit dem Befehl ‚Block If No Further Match' voranzustellen. Ich will wirklich niemanden davon abhalten, nach dieser Methode vorzugehen. Wer sich mit einem solchen Aufbau besser fühlt, kann ihn ohne weiteres wählen. Als Programmierer widerstrebt er mir, weil er langsamer und daher nicht sauber programmiert ist. Auch wenn diese Anleitung vielleicht gelegentlich einen anderen Eindruck erweckt: Hauptaufgabe eines Routers ist es, zu verbinden und nicht zu blocken. Deshalb gehören die wichtigsten Erlaubnisregeln (DNS, http und https) an den Anfang des Regel-Sets. Findet der Router diese Regeln kann er sofort verbinden und ist mit der Paketüberprüfung nicht weiter beschäftigt (es ist deshalb auch kein Zufall, dass alle meine Regeln mit dem Parameter ‚quick' in den ipf-Befehlssatz übersetzt werden). Bei Paketen, die geblockt werden sollen, muss er sich durch den ganzen Regelsatz durcharbeiten, was jedoch – zeitlich betrachtet – unschädlich ist, weil diese Pakete ohnehin verworfen werden sollen. Bei der ‚Block If No Further Match'-Variante muss der Router die ausgehende Regel und die eingehende Regel zunächst einmal zwischenspeichern, um sich den nächsten Regeln zu widmen. Erst wenn er eine passende ‚quick'-Regel findet, kann er aufatmen, die zwischengespeicherten Regeln löschen und endlich die gewünschte Verbindung herstellen. Diese Variante ist nach meiner Auffassung letztlich auch nicht wirklich sicherer: Wenn ich im folgenden versehentlich eine Regel mit dem Inhalt ‚pass out quick from any to any' einbaue, habe ich wieder eine völlig unbrauchbare Firewall. Wenn ich mehrere ‚...If No Further Match'-Regeln hintereinanderschalte, kann ich den Überblick unter Umständen sehr schnell verlieren. Auch deshalb würde ich diese Varianten nach Möglichkeit meiden. Ich persönlich halte daher meinen Aufbau für besser und ziehe es vor, die komplett fertiggestellten Regeln einmal unter Telnet mit ‚ipf view –r' zu kontrollieren (am Ende der eingehenden Regeln muss *block in quick from any to any* stehen, am Ende der ausgehenden *block out quick from any to any*), statt den Router tausendfach bei jedem Paket auszubremsen.

In- und Out-Filter habe ich in getrennten Sets untergebracht, um mir selbst klarzumachen, dass man hier auch bei Source- (Quell-) und Destination- (Ziel-) Adresse umdenken muss. Einfacher wäre es manchmal gewesen, die In- und Out-Regel unmittelbar hintereinanderzuschalten.

Die möglichen 84 Regeln mögen auf den ersten Blick viel erscheinen, sind es aber nicht, wenn man bedenkt, dass es um die Einstellung eines Routers geht, bei dem im Gegensatz zu einer Desktop-Firewall u.U. verschiedene Regelsätze für verschiedene Rechner erstellt werden müssen. Erheblich nachteilig wirkt sich in diesem Zusammenhang auch aus, dass für ein- und ausgehende Datenpakete separate Regeln erstellt werden müssen, weil es nicht möglich ist, eine Regel für beide Richtungen einzugeben. Schließlich erhöht sich die Anzahl der Regeln auch deshalb, weil man mit einer einzigen Regel nur dann mehrere Ports freischalten/sperren kann, wenn die Ports zusammenhängen (von ... bis ...). Die Möglichkeiten anderer Router, auch bei nicht zusammenhängenden Ports (z.B. http=Port 80 und https=Port 443) mit einer Regel auszukommen, bietet der Vigor im WebInterface nicht.

Sie werden sich vielleicht wundern, dass ich bei keiner einzigen Regel die Keep State-Option gesetzt habe. Dies hat mehrere Gründe: Nach meinen Erfahrungen mit anderen ‚Optionen' des Routers traue ich auch dieser Geschichte nicht mehr. Ferner haben mich Berichte irritiert, wonach es Angreifern möglich sein soll, auch in eine etablierte Verbindung Pakete einzuschmuggeln. Schließlich bin ich mir nicht sicher, ob diese Option beim Vigor mit maximal 84 Regeln tatsächlich die Firewall beschleunigt oder – zumindest im Einzelfall – nicht eher verlangsamt. Auch mit gesetzter Keep State-Option muss der Router schließlich die Daten der etablierten Verbindung zwischenspeichern und bei jedem Paket prüfen, ob dieses zur etablierten Verbindung gehört. Das kann u.U. langsamer sein als festzustellen, ob das Paket über den Port 80 nach draußen geht. Es schien mir daher wichtiger zu sein, die Regeln für die wichtigsten Ports (DNS, http, https) nach oben zu stellen. Bei einer Firewall mit 45.000 Regeln sieht das sicher anders aus.

Das Feld ‚Branch to Other Filter Set' sollten Sie aus den Gründen auf ‚None' stehen lassen, die ich unter *IV. Hinweise→Kann die Firewall mehr ?* erläutert habe.

Sollten Sie noch mit einer Firmware < 2.3 arbeiten, finden Sie bei den einzelnen Filterregeln eine Option ‚Source Route'. Kreuzen Sie dies nicht an. Nach einer Stellungsnahme von DrayTek ist diese Option ‚invalid', sie wird in jedem Fall in unbrauchbarer Weise in den ipf-Befehlssatz übersetzt.

**Einstellung im General-Setup:**

| | | | | |
|---|---|---|---|---|
| *Call-Filter* | ⊙ | Enable | *Start Filter Set* | Set#1 |
| *Data-Filter* | ⊙ | Enable | *Start Filter Set* | Set#2 |
| *Log Flag* | None | | | |
| *MAC Address for Logged Packets Duplication* | 0x000000000000 | | | |

❒ Accept Incoming Fragmented UDP Packets ( for some games, ex. CS )

***Anmerkung:*** Die Option für die fragmentierten UDP-Pakete (s. hierzu unter *Begriffserläuterungen→UDP*) ist neu in der Firmware 2.3. Offenbar weist der Router fragmentierte UDP-Paket standardmäßig ab (Ob das auch für TCP-Pakete gilt, konnte ich nicht ermitteln. Wäre es so, dann wäre die Regel in Set 3 Nr. 1 überflüssig.). Wenn Sie Probleme beim Media-Streaming oder bei Online-Spielen haben, also beim Ego-Shooter zu oft erschossen werden, können Sie versuchen, Ihre Chancen zu erhöhen, indem Sie bei dieser Option ein Häkchen setzen. Sie sollten dann allerdings auch die Regel in Set 3 Nr. 1 entsprechend anpassen (also bei ‚Protocol' statt ‚any' ‚TCP' eintragen) für den Fall, dass der Router diese Regel tatsächlich abarbeiten kann und nicht einfach nur ignoriert.

**Einstellung im DoS defense-Setup:**

❒ Enable DoS Defense

***Anmerkung:*** Diese Option ist in der Firmware-Version 2.3.1 (Build-Datum: Normal Mode 22.01.2003 11:55:46.73), die zum Zeitpunkt der Erstellung dieser Anleitung aktuell ist, nicht enthalten. Die Vorversion 2.3 vom 10.01.2003, die das DoS-defense enthielt, wurde von DrayTek wegen Stabilitätsproblemen zurückgezogen. Selbst wenn Sie also eine Firmware-Version verwenden, die das hier beschriebene Menu enthält, können Sie es nicht verwenden.

Alle nachfolgenden Anregungen gelten daher nur für den Fall, dass DrayTek den Menu-Punkt in eine künftige Firmware wieder einbaut und das ‚DoS defense' dann auch funktioniert.

Zunächst möchte ich darauf hinweisen, dass DrayTek bereits die Überschrift des Menus mit ‚DoS defense' nach meiner Auffassung unglücklich gewählt hat, denn bei den einstellbaren Optionen geht es nicht nur darum, Angriffe abzuwehren, die Server-Dienste stilllegen, sondern auch um Angriffe, die das angegriffene Systeme ausforschen und für ihre Zwecke nutzbar machen wollen. Solche Angreifer möchten das angegriffene System gerade nicht lahm legen; ihnen geht es im Gegenteil eher darum, möglichst nicht aufzufallen, um das Opfer missbrauchen zu können. Ich habe daher die Angriffsformen, die der Vigor abwehren soll, in ‚Forscher' und ‚Blockierer' unterteilt, ohne dabei verkennen zu wollen, dass ein allzu intensiver Forscher auch zum Blockierer werden kann. Die Angriffsformen werden in den *Begriffserläuterungen* erklärt.

Wichtig ist ferner, dass das ‚DoS defense' völlig unabhängig von der mit den Filter Sets einzustellenden IP-Firewall arbeitet. Die DoS-defense-Einstellungen werden daher auch nicht über ‚ipf view -r' angezeigt. Die von DrayTek festgestellten Stabilitätsprobleme wundern mich aus diesem Grunde nicht. Der Einsatz von zwei unabhängigen Firewalls im Router scheint mir genauso problematisch zu sein, wie die Installation von zwei Virenscannern oder zwei Desktop-Firewalls auf demselben Computer. Durch solche Maßnahmen erreicht man im Zweifel keine höhere, sondern eher eine geringere Sicherheit, weil sich die Schutzprogramme wechselseitig behindern. Eine ganze Reihe der Gefahren, die das DoS defense abwehren will, ließen sich durch die IP-Firewall deutlich besser abfangen, wenn man alle Möglichkeiten dieser Firewall nutzte (IP-Options, fragments, flags, icmp-type etc.). So kann diese

Firewall nicht nur Pakete abfangen, bei denen irgendeine IP-Option gesetzt ist, sondern detailliert nach den gesetzten Optionen (lsrr, ssrr, sec usw. usw.) filtern. Sie merken an dieser Stelle vielleicht, dass mich die Einführung des ‚DoS defense Setup' nicht gerade zu Begeisterungsstürmen hingerissen hat. Es wäre nach meiner Auffassung wesentlich besser, die Möglichkeiten der IP-Firewall weiter auszubauen und sich im DoS defense auf die eigentlichen Denial of Service-Attacken (Port Scan, flood) zu konzentrieren.

**Forscher**

**Block ICMP fragment:** aktivieren
**Block IP options:** IP-Options werden im Internet selten verwandt. Es dürfte zu keinen Problemen kommen, wenn diese Option aktiviert wird.
**Enable Port Scan detection:** würde ich aus den Gründen, die ich unter den *Begriffserläuterungen* dargelegt habe, nicht aktivieren. Außerdem sollten die nachfolgenden Filterregeln und die Desktop-Firewall verhindern, dass ein offener Port – selbst wenn er gefunden wird – missbraucht werden kann.
**Block TCP flag scan:** immer aktivieren. Pakete mit irregulären Flags deuten mit ziemlicher Sicherheit auf einen Angriff hin. Selbst wenn die Flags versehentlich falsch gesetzt sind, wird das Paket ohnehin verworfen.
**Block trace route:** würde ich nicht aktivieren, sondern mich auch insoweit auf die nachfolgenden Filterregeln und die Desktop-Firewall verlassen.
**Block Unknown Protocol:** wie *Block Trace Route*: Mit den Port-Filtern in der Vigor- und der Desktop-Firewall kann ich viel genauer arbeiten.

**Blockierer**

Bevor Sie irgendeinen der nicht unter ‚Forscher' aufgeführten Punkte aktivieren, müssen Sie darüber nachdenken, ob auf Ihrem System überhaupt Server-Dienste angeboten werden und welche Ports Sie für eingehende Verbindungen geöffnet haben. Einen hilfreichen Test finden Sie bei PC Flank [58]. Selbst wenn Sie aber zu dem Ergebnis kommen, dass Sie theoretisch angreifbar sind, sollten Sie nicht ohne weitere Überlegung alle vom Vigor angebotenen Optionen aktivieren. Nur wenn Sie der Auffassung sind, dass schon der erste DoS-Angriff und der damit verbundene Ausfall von Server-Diensten für Sie eine Katastrophe bedeutet, müssen Sie sich den DoS-defense-Optionen zuwenden, wobei nach meinen Informationen Land, Ping of Death und Tear Drop für Windows-Rechner ab w98 keine Gefahr mehr darstellen. Sind hingegen die Server-Dienste für Sie nicht von existentieller Bedeutung, dann können Sie es auch darauf ankommen lassen, ob Sie überhaupt jemals Opfer eines solchen Angriffs werden, was nach meiner Auffassung eher unwahrscheinlich ist, da sich DoS- oder DDoS-Angreifer in der Regel große Institutionen aussuchen werden. Werden Sie nachhaltig durch solche Angriffe gestört, können Sie immer noch die Angriffsform, deren Opfer Sie geworden sind, abwehren. Dies ist nach meiner Auffassung die bessere Lösung, als durch das ‚blinde' Einschalten aller Abwehrmöglichkeiten im Vigor ständig Performance-Einbußen in Kauf nehmen zu müssen.

Allgemeine Tipps für die bei ‚Threshold' und ‚Timeout' einzustellenden Werte kann es nicht geben, weil einerseits der Angreifer bestimmt, mit wie vielen Paketen er Sie pro Sekunde bombardieren will, und weil es andererseits vom angegriffenen System abhängt, wie viele Pakete es pro Sekunde verkraftet, bevor es ernsthaft gestört ist.

Einstellung der einzelnen Filter-Regeln
(BI=Block Immediately – PI = Pass Immediately):
Bitte beachten Sie, dass die Sets 2 bis 11 jeweils auf das nachfolgende Filterset verweisen. Lediglich bei den Call-Filtern (Set 1) erfolgt kein Verweis auf ein anderes Set (None). Natürlich können Sie stattdessen auch auf das nächste belegte Filterset verweisen und die nicht belegten überspringen. Weil ich aber Sorge habe, dass dies später einmal übersehen werden könnte und Regeln in ein Set eingetragen werden, die nie zum Zuge kommen, weil das ganze Set übersprungen wird, habe ich aus Sicherheitsgründen hiervon abgesehen.

| Filter Set 1 | | | | | | | | Comments | | | | | Default Call Filter | | | | Next Filter Set | | | | None | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN Log | | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | Block NetBIOS | X | BI | None | | | in | TCP/ UDP | any | 255.255.255.255/32 | = | 137 | 139 | any | 255.255.255.255/32 | = | | | | Don't Care |

| Filter Set 2 | | | | | | | | Comments | | | | | Default Data Filter | | | | Next Filter Set | | | | Set#3 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN Log | | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | NetBIOS - > DNS | X | BI | None | | | out | TCP/ UDP | any | 255.255.255.255/32 | = | 137 | 139 | any | 255.255.255.255/32 | = | 53 | | | Don't Care |

| Filter Set 3 | | | | | | | | Comments | | Block | | | Next Filter Set | | Set#4 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | Block Too Short | X | BI | None | | | in | any | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Too Short |

| Filter Set 4 | | | | | | | | Comments | | zugelassene Ports Out 1 | | | Next Filter Set | | Set#5 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | ICMP | X | PI | None | | | out | ICMP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |
| 2 | DNS (t-online) | X | PI | None | | | out | UDP | any | 255.255.255.255/32 | = | | | *217.5.99.9* ***s. Anm.*** | 255.255.255.255/32 | = | 53 | | | Don't Care |
| 3 | DNS (t-online) | X | PI | None | | | out | UDP | any | 255.255.255.255/32 | = | | | *194.25.2.128* ***s. Anm.*** | 255.255.255.128/25 | = | 53 | | | Don't Care |
| 4 | http (80) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 80 | | | Don't Care |
| 5 | https (443) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 443 | | | Don't Care |

| Filter Set 5 | | | | | | | | Comments | zugelassene Ports Out 2 | | | | Next Filter Set | Set#6 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | POP3(110) t-onl | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | *194.25.134.0* ***s. Anm*** | *255.255.255.128/25* ***s. Anm*** | = | 110 | | | Don't Care |
| 2 | SMTP(25) t-onl | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | *194.25.134.0* ***s. Anm*** | *255.255.255.128/25* ***s. Anm*** | = | 25 | | | Don't Care |
| 3 | NNTP T-Online | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | *62.153.159.134* ***s. Anm.*** | 255.255.255.255/32 | = | 119 | | | Don't Care |
| 4 | NNTP MicroSoft | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | *207.46.248.16* ***s. Anm.*** | 255.255.255.255/32 | = | 119 | | | Don't Care |
| 5 | ftp (21) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | > | 1024 | | any | 255.255.255.255/32 | = | 21 | | | Don't Care |
| 6 | pass.ftp>1024 | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | > | 1024 | | any | 255.255.255.255/32 | > | 1024 | | | Don't Care |
| 7 | Telnet (23) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 23 | | | Don't Care |

| Filter Set 6 | | | | | | | | Comments | | | | | Next Filter Set | Set#7 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| **<nicht belegt>** | | | | | | | | | | | | | | | | | | | | |

| Filter Set 7 | | | | | | | | Comments | | | | | | Next Filter Set | | | | | | Set#8 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| **<nicht belegt>** | | | | | | | | | | | | | | | | | | | | | |

| Filter Set 8 | | | | | | | | Comments | | | | | | Next Filter Set | | | | | | Set#9 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | ICMP | X | PI | None | | | in | ICMP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |
| 2 | akt.ftp-data/20 | X | PI | None | | | in | TCP | any | 255.255.255.255/32 | = | 20 | | any | 255.255.255.255/32 | > | 1024 | | | Don't Care |

| Filter Set 9 | | | | | | | | Comments | | | | | | | Next Filter Set | | | | | | Set#10 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | | Keep State | Fragments |
| **<nicht belegt>** | | | | | | | | | | | | | | | | | | | | | | |

| Filter Set 10 | | | | | | | | Comments | | | | | | Real Player | Next Filter Set | | | | | | Set#11 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Source | | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | | Keep State | Fragments |
| 1 | 554 OUT | | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | | any | 255.255.255.255/32 | = | 554 | | | | Don't Care |
| 2 | 7070 Out | | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | | any | 255.255.255.255/32 | = | 7070 | | | | Don't Care |
| 3 | UDP | | PI | None | | | in | UDP | any | 255.255.255.255/32 | = | | | | any | 255.255.255.255/32 | | 6970 | 7170 | | | Don't Care |

| Filter Set 11 | | | | | | | | Comments | Notfall53-25-110-119auf | | | | Next Filter Set | Set#12 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | DNS OUT any | | PI | None | | | out | UDP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 53 | | | Don't Care |
| 2 | SMTP OUT any | | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 25 | | | Don't Care |
| 3 | POP3 OUT any | | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 110 | | | Don't Care |
| 4 | NNTP any | | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 119 | | | Don't Care |

| Filter Set 12 | | | | | | | | Comments | Block all | | | | Next Filter Set | None | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Source | | | | | Destination | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | Block out | X | BI | None | | | out | any | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |
| 2 | Block in | X | BI | None | | | in | any | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |

Leerformular zum Eintragen eigener Filterregeln für die Router-Firewall:

| Filter Set ____ | | | | | | | | | Comments | | | | | | Next Filter Set | | | | | Set# | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Source | | | | | | Destination | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | | | | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | | | | | | | |

# VI. Anmerkungen zu den Beispielen für die Router-Firewall

### Set 1 Nr. 1 (Call-Filter) und Set 2 Nr. 1 (Daten-Filter)

Diese ***Regeln stammen nicht von mir***, sondern waren im Auslieferungszustand meines Routers mit der Firmware 2.00 a als Default-Regeln eingetragen. Ich verstehe die Regeln nicht und gehe davon aus, dass sie vertauscht sind.

Zur Erläuterung: Über die Ports 137 bis 139 regelt NetBIOS die Datei- und Druckerfreigabe. Die Regeln dürfen keinen Anwendungsfall haben, wenn Sie meiner Empfehlung gefolgt sind (s. bei Begriffserläuterungen unter NetBIOS), NetBIOS über TCP/IP abzuschalten. Haben Sie aber bewusst oder versehentlich die Datei- und Druckerfreigabe für TCP/IP aktiviert, dann stellt NetBIOS über den DNS-Port 53 eine Vielzahl von Verbindungen her, weil NetBIOS ständig auf der Suche nach anderen Rechnern ist und diese Suche zu den DNS-Servern weiterleitet, wenn die Rechner nicht gefunden werden. Die Regel Set 2 Nr. 1 verhindert das, wenn sie als *Call-Filter*, also in das Set 1, eingetragen wird. Die Regel Set 1 Nr. 1 soll den Datenverkehr über die Ports 137 bis 139 verhindern, also Zugriffe auf Festplatten blocken. Als Call-Filter macht das keinen Sinn, weil die Call-Filter nach den Beschreibungen im Original-Handbuch nur bei nicht bestehender Verbindung angesprungen werden. Wenn ich aber den Datenverkehr über die NetBIOS-Ports unterbinden will, dann will ich dies unabhängig davon, ob eine Verbindung besteht oder nicht. Die Regel Set 1 Nr. 1 gehört daher als Daten-Filter in das Set 2. Nach meiner Auffassung und nach den Empfehlungen in anderen Firewalls muss sie außerdem durch eine Filterregel ergänzt werden, durch die alle ausgehenden Verbindungen (Direction:Out) von allen Adressen über die Ports 137-139 auf alle Adressen mit allen Ports unterbunden wird (Block Immediately). Wenn Sie sich jedoch an die Empfehlungen in meinem Beispielset halten, brauchen Sie diese Regeln nicht, weil die Block-Regeln im letzten Set ohnehin auch den NetBIOS-Verkehr stoppen.

Meine Empfehlung: Regel Set 1 Nr. 1 ersatzlos löschen und Regel Set 2 Nr. 1 unverändert als Regel Set 1 Nr. 1 eintragen, wobei man sogar noch hierüber diskutieren könnte: Lässt man nämlich diesen Call-Filter weg, bemerkt man durch die unerklärlichen Verbindungsaufnahmen möglicherweise schneller, dass NetBIOS über TCP/IP läuft und kann etwas dagegen tun.

**Set 3**
**Nr. 1**
Dies ist die einzige Regel in meinen Sets, bei dem unter ‚Fragments' etwas anderes als ‚Don't Care' angewählt wurde, nämlich ‚Too Short'. Die Regel blockt alle ankommenden Pakete, die so kurz sind, dass sie keinen kompletten TCP-Header haben (s.a. die entsprechenden Erläuterungen in der Handbuchübersetzung).

**Set 4**
**Nr. 1**
Die Regel schaltet das ICMP-Protokoll ausgehend komplett frei, was aus Sicherheitsgründen nicht unproblematisch ist (s.a. bei Begriffserläuterungen zu ICMP sowie bei [1]). Es dürfte eigentlich nicht zu nennenswerten Problemen kommen, wenn man diese Regel für den ‚normalen' Internetverkehr abschaltet. Als Alternative kann man

darüber nachdenken, über eine Desktop-Firewall, die das ICMP-Protokoll detaillierter kontrollieren kann als die Vigor-Firewall, nur bestimmte Typen aus dem Protokoll zuzulassen.

**Nrn. 2 + 3**
Die Regeln geben zum Port 53 den Zugang zum DNS-Server frei, der die Web-Adresse (www.mueller.de) in die IP-Adresse im Zahlenformat (0000.0000.0000.0000) umwandelt. Ohne diese Regeln können Sie daher nur dann im Internet surfen, wenn der Router die Adresse aus seinem eigenen Cache holen kann oder Sie die Zahlenadresse im Kopf haben. Die Angabe der Destination-IP-Adresse ist nur als Beispiel zu verstehen. Hier müssen Sie die Adresse des DNS-Servers Ihres Providers eintragen (das Beispiel gilt für den DNS-Server von t-online bei einem Zugang aus Köln, beim Zugang aus anderen Städten oder beim Zugang über andere Provider gelten andere Nrn. s. unter Begriffserläuterungen → IP-Adresse).
In der Regel reichte bei mir die Regel Nr. 2. Zu bestimmten Zeiten schaltet t-online aber offenbar tatsächlich - wie auf deren Home-Page angekündigt - auf andere Server (in meinem konkreten Fall auf Server im Bereich 194.25.2.129 bis 194.25.2.134) um, so dass die Regel 3 erforderlich wurde. Bitte beachten Sie die Subnetzmaske: Freigeschaltet werden tatsächlich alle Adressen von 194.25.2.128 - 194.25.2.255 (der Adressbereich 194.25.2.0 bis 194.25.3.255 ist gemäß Auskunft von www.swhois.net der Deutschen Telekom zugeteilt).

**Nrn. 4 + 5**
erlauben den Zugriff auf das Internet für normale (http, 80) und gesicherte (https, 443) Verbindungen. Als weitere Absicherung kann man darüber nachdenken:

- über eine Desktop-Firewall nur bestimmten Programmen den Zugang über die Ports zu gestatten.

**Set 5**
**Nrn. 1 + 2**
sind erforderlich, um ein- (POP3, 110) und ausgehende (SMTP, 25) Mails zu ermöglichen. Falls die Mails über das IMAP-Protokoll (s. Begriffserläuterungen) abgeholt werden, muss statt Port 110 der Port 143 freigeschaltet werden. Falls die eingehenden Mails über eine sichere Verbindung (SPOP3) laufen, muss der Port 995 freigeschaltet werden.

Bitte beachten: Die Destination-IP-Adresse und –Subnetzmaske sind nur als Beispiel zu verstehen. Sie beziehen sich auf die Mail-Server von t-online und müssen durch die Mail-Server-Adressen Ihres Providers ersetzt werden. Mit der von den sonstigen Einstellungen abweichenden Subnetzmaske hat es folgende Bewandtnis: Ich habe insgesamt 12 Adressen für die Mailserver von t-online ermittelt, die leider nicht einmal fortlaufend sind. Wenn ich diese ausgehend für Port 110 und 25 eingebe, verbrauche ich 24 (!) Filterregeln, was nicht diskutabel ist. Durch die Filterregeln sind nur die ersten 25 Stellen (in dualer Schreibweise) der IP-Adresse maßgebend. Im konkreten Beispiel lässt der Filter daher Pakete an die Adressen 194.25.134.0 bis 194.25.134.127 durch. In diesem Bereich liegen die Mailserver–Adressen von t-

online. Ich habe jetzt zwar statt 12 Adressen 128 freigeschaltet, da jedoch nach Auskunft von www.swhois.net der gesamte Adressbereich von 194.25.134.0 bis 194.25.134.255 in der Hand der Deutschen Telekom liegt, gehe ich davon aus, dass hierdurch keine zusätzliche Bedrohung entsteht (durch den Aufbau der Vigor Firewall habe ich keine andere Möglichkeit).

Als weitere Absicherung sollte man:

- eine Desktop-Firewall einsetzen und nur dem verwandten Mail-Clienten den Zugriff über die Ports gestatten.

**Nrn. 3 + 4**
Zugriff auf die Newsserver: Die eingetragenen Adressen stehen für news.btx.dtag.de und msnews.microsoft.com und müssen im Bedarfsfall angepasst werden (die Adresse des Microsoft-Servers wechselt gelegentlich, keine Probleme dürfen Sie mehr haben, wenn Sie als Destination-IP-Adresse 207.46.0.0 mit der Subnetzmaske 255.255.0.0 eingeben, weil dadurch der gesamte Bereich von 207.46.0.0 bis 207.46.255.255 freigeschaltet wird, der nach Auskunft von swhois MicroSoft gehört).

Als weitere Absicherung sollte man:

- eine Desktop-Firewall einsetzen und nur dem verwandten News-Programm den Zugriff über die Ports gestatten.

**Nr. 5**
erforderlich für aktives und passives ftp. Die Regel ist bedenklich (s. unter Hinweise). Als Destination-IP-Adresse kann man auch die Adresse des ftp-Servers angeben, mit dem man die Daten austauschen will (für die t-online-Homepages [home-up.t-online.de] zum Beispiel 194.25.3.142). Für andere Server wird die Verbindungsaufnahme dann unterbunden.

Als weitere Absicherung sollte man:

- eine Desktop-Firewall einsetzen und nur den Programmen den Zugriff über den Port gestatten, mit denen man die Dateien verschiebt (einschließlich eines etwa eingesetzten Download-Managers).

Ferner würde ich mir überlegen, ob ich die Regel nicht im Normalbetrieb deaktiviere und damit den Port sperre, um diesen nur im Bedarfsfall freizuschalten.

**Nr. 6**
bei passivem ftp erforderlich, um die Daten abzuholen. Ebenfalls bedenklich (s. die Hinweise zur Regel Nr. 5).

**Nr. 7**
erforderlich, wenn mit Telnet auf andere Systeme zugegriffen werden soll. Es gelten die gleichen Hinweise wie zur Regel Nr. 5.

**Set 8**
**Nr. 1**
Die Regel schaltet das ICMP-Protokoll eingehend komplett frei, was aus Sicherheitsgründen problematisch ist (s. dazu Set 4 Nr. 1).

**Nr. 2**
Bei aktivem ftp baut der externe Rechner über den Port 20 zu einem beliebigen Port >1023 eine Verbindung auf, um die Dateien zu übertragen. Aus Sicherheitsgründen bedenklich. Da aktives ftp seltener verwendet wird und insbesondere die Browser nur passives ftp benutzen, sollte die Regel im Normalfall deaktiviert werden.

**Set 10**
Alle Regeln in diesem Set sind **de**aktiviert. Der Realplayer funktioniert allerdings in der Grundeinstellung nur dann, wenn Sie diese Regeln einschalten, was ich nicht empfehle. Das Set enthält derart weitreichende Freigaben, dass die Aktivierung aus Sicherheitsgründen nicht zu empfehlen ist. Wer den Player unbedingt braucht, mag das Set einschalten. Gleichwohl kann man mit dem Realplayer auch arbeiten, ohne den Regelsatz zu aktivieren. Zwingen Sie den Realplayer, für alle Verbindungen den http-Port (80) zu benutzen (Achtung: Unter Windows 2000 benötigen Sie für die Eingabe der Einstellungen Administrator-Rechte !!): Starten Sie den Realplayer: Unter Ansicht → Einstellungen → Transportprotokoll → RTSP-Einstellungen *und* PNA-Einstellungen kreuzen sie jeweils das Kästchen *nur http verwenden* an. Nach den Infos von RealNetworks soll dies mit Performance-Verlusten verbunden sein, was ich aber jedenfalls mit DSL subjektiv nicht bestätigen kann.

**Set 11**
Beachten Sie bitte, dass alle Regeln in diesem Set **de**aktiviert sind. Entsprechend der Bezeichnung dient das Set nur für Notfälle. Es werden die wichtigsten Ports für alle IP-Adressen freigeschaltet. Die Warnungen von t-online vor der Angabe fester IP-Adressen haben mich derart verunsichert, dass ich mir für ‚Notfälle' ein Set zurecht gelegt habe, welches ich benutzen möchte, falls ich den Verdacht habe, dass mein Internet-Verkehr deshalb nicht mehr funktioniert, weil t-online die IP-Adressen geändert hat.

**Set 12**
Dies sind mit Abstand ***die wichtigsten Regeln*** in der ganzen Konfiguration. Hier wird ein- und ausgehend alles gesperrt, was nicht vorher explizit zugelassen wurde.

**Was fehlt ?**

1. Wenn Sie den Instant Messenger von AOL benutzen, müssen Sie eine Erlaubnisregel für ausgehende Datenpakete über das TCP-Protokoll von allen lokalen IP-Adressen und allen Quell-Ports auf alle IP-Adressen (oder die IP-Adressen des Terminals) auf den Port 5190 erstellen.

2. Die Proxy-Ports 8080 oder 3128 (ggfs. weitere) müssen anstelle der Ports 80 (http) und 443 (https) freigeschaltet werden, wenn der Provider einen

Proxy-Server verwendet und diese Ports vorgibt (bei diesem erfragen). Bei t-online reichen die Standard-Ports 80 und 443.

3. Bei mir funktionierte mit dem Regelset t-online-Banking nicht mehr. In einem solchen Fall bleibt nichts anderes übrig, als Telnet zu bemühen. Starten Sie Telnet wie folgt: Start → Ausführen → Telnet 192.168.1.1 [Enter] – Eingabe des Passwortes [Enter] – log -F a [Enter], um alle alten Log-Flags zu löschen (die spätere Abfrage wird dann übersichtlicher). Minimieren Sie Telnet. Aktivieren Sie im General Setup des Filter/Firewall Setups im Router unter Log Flag den Listeneintrag ‚Block' oder kreuzen Sie bei den beiden Regeln im Set 12 die Checkbox ‚Log' an. Starten Sie dann das t-online-Banking-Programm und versuchen Sie, z.B. die Umsätze zu aktualisieren, was natürlich nach wie vor nicht funktioniert. Aktivieren Sie wieder Telnet und geben Sie folgendes ein: log -f [Enter]. Jetzt müssten Sie exakt sehen, was geblockt wurde. In meinem konkreten Fall hat mir Telnet angezeigt, dass es eine ausgehende Verbindung von der lokalen IP-Adresse meines Rechners (192.168.1.xxx) auf Port 1073 (!) auf die IP-Adresse 194.25.134.212 auf Port 866 (!) abgefangen hat. Also geben Sie jetzt eine Regel ein, die eine ausgehende Verbindung auf die gerade beschriebenen Adressen und Ports zulässt, wobei Sie als Source-IP-Adresse natürlich ‚any' oder (192.168.1.0 mit der Subnetzmaske 255.255.255.0/24) angeben, denn sonst kann nur der Rechner, der zufällig die von Telnet lokal angezeigte Adresse dynamisch oder fest bekommen hat, auf das Online-Banking zugreifen.

   Das Spiel geht weiter: Nach meiner Auffassung gibt es keinerlei Gewähr dafür, dass die Adressen und Ports, die Telnet bei einer Verbindungsaufnahme gezeigt hat, auch am nächsten Tag noch gelten. Wenn Sie t-online-Kunde sind, schlage ich Ihnen daher – ohne Gewähr für hiermit etwa verbundene Sicherheits-Risiken – folgendes vor: Ändern Sie die Regel Set 5 Nr. 1: wie folgt ab: Destination-IP-Subnetzmaske 255.255.255.***0/24,*** Destination-Start-Port löschen, also nichts eintragen. Die Regel Set 5 Nr. 2 können Sie dann gleich löschen. Damit haben Sie alle ausgehenden Verbindungen zu den Adressen 194.25.134.0 bis 194.25.134.255 auf allen Ports freigeschaltet und müssen darauf vertrauen, dass von dort keine Bedrohung ausgeht (gemäß Auskunft von www.swhois.net sind alle soeben freigeschalteten Adressen der Deutsche Telekom AG zugeteilt).

4. Apples Quicktime wird ebenfalls nicht funktionieren. Hier dürften Regeln erforderlich sein, die dem Set 10 gleichen. Wer dieses Programm unbedingt braucht, mag sich die Daten für die erforderlichen Freigaben selbst besorgen. Auch Quicktime können Sie aber zwingen, den Port 80 (http) zu benutzen. So geht's unter QuickTime 5 (unter w2k Administrator-Rechte erforderlich !!): Quicktime starten, Bearbeiten → Voreinstellungen → QuickTime Einstellungen → Streaming Transport → http, Port-ID verwenden ‚80' ankreuzen. Auch apple warnt vor Performance-Einbußen, die mir nicht aufgefallen sind.

5. Wenn Sie online spielen wollen, müssen Sie sich beim Betreiber des Spiels erkundigen, welche Ports in welche Richtung über welches Protokoll freigeschaltet werden müssen. Ich gehe davon aus, dass hierdurch erhebliche Risiken geschaffen werden können, und empfehle, die hierdurch bedingten Regeln in einem speziellen Set unterzubringen, welches nur zum Spielen freigeschaltet und im übrigen übersprungen wird. Bedenken Sie bitte, dass die Filterregeln im Router für alle angeschlossenen Rechner gelten, also auch für die Personen, die gar nicht spielen. Es erscheint mir daher auch sinnvoll, die ‚Spiel-Regeln' auf die konkreten IP-Adressen der Rechner der Spieler zu beschränken, was voraussetzt, dass die IP-Adressen der lokalen Rechner nicht dynamisch, sondern fest vergeben werden.

6. Wenn Sie an Tauschbörsen teilnehmen möchten, müsste Ihnen eigentlich die für den ftp-Datenkanal vorgesehene Regel im Set 5 Nr. 6 den Download ermöglichen, denn die Dateien werden idR über die Ports oberhalb von 1023 übertragen. Für den Upload (also wenn Sie Ihre Dateien anderen Nutzern zur Verfügung stellen wollen) sind weitere Regeln für einkommende Datenpakete erforderlich, was natürlich wiederum mit Risiken verbunden ist (vgl. im übrigen die Ausführungen zu 5.).

7. Durch die Regeln in Set 12 wird auch der gesamte Verkehr über den Port 445 geblockt, über den w2k/XP die Datei- und Druckerfreigabe managen, wenn TCP/IP mittels ‚direct hosting' benutzt wird. Wenn Sie entfernte Windows-Netze mit diesem Verfahren vernetzen wollen, müssen Sie entsprechende Erlaubnisregeln einfügen.

# VII. Konfiguration einer ergänzenden Desktop Firewall am Beispiel der Kerio Firewall (vormals Tiny Personal Firewall)

Vorstehend habe ich bereits mehrfach darauf hingewiesen, dass die Router-Firewall tunlichst durch eine Desktop-Firewall ergänzt werden sollte, weil diese insbesondere die generell freigegebenen Verbindungen dadurch weiter präzisieren kann, dass sie diese Verbindungen nur für bestimmte Programme freischaltet. Ein angenehmer Nebeneffekt ist, dass eine solche Desktop-Firewall bei den problematischen ICMP-Verbindungen bestimmte Unter-Typen dieses Protokolls ausschließen kann.

Hierzu stehen eine Vielzahl von Programmen zur Verfügung (s. [7], [14], [16], [18], [19], [60]). Für die Kerio Firewall (Version 2.1.4 vom 15.04.2002, im folgenden KF, Weiterentwicklung der Tiny Personal Firewall [22], im folgenden TPF) habe ich mich entschieden, weil

- sie für die private Nutzung kostenlos ist [21],
- sie auf allen MicroSoft-Betriebssystemen ab Windows 9x funktioniert,
- sie und die TPF – absehen von der Konfiguration, der nur spärlichen Hilfe in englisch und des Risikos, durch ein Schadprogramm gewaltsam beendet zu werden (dazu noch unten) – grundsätzlich in allen Tests gut abgeschnitten haben,
- sie mit ihrer deny-all-Strategie meiner vorgeschlagenen Konfiguration für die Router-Firewall sehr ähnelt, so dass man nicht grundlegend umdenken muss,
- sie sehr kompakt ist und keine Unmengen an Speicherplatz frisst und es auch bei den einzelnen Regeln sehr detailliert ermöglicht, eine Vielzahl von Fällen mit einer einzigen Regel abzudecken,
- ich subjektiv auch im laufenden Betrieb praktisch keine Performance-Einbußen feststellen konnte, was bei anderen Firewalls, mit denen ich gearbeitet habe, ganz anders aussieht,
- die Konfiguration nach meiner Auffassung sehr übersichtlich ist (wenn Sie sich durch die Anleitung für die Router-Firewall gekämpft haben, müssten Ihnen alle Menupunkte der KF auf Anhieb einleuchtend sein),
- die Firewall auch konfiguriert werden kann, wenn man nur mit einfachen Benutzerrechten angemeldet ist (Es mag zunächst merkwürdig erscheinen, dass ich dies positiv werte, entspricht aber meinen Sicherheitsvorstellungen: Ich versuche immer, Internetverbindungen zu vermeiden, wenn ich Administrator-Rechte habe. Wenn mich KF zwänge, die Konfiguration mit diesen Rechten vorzunehmen, müsste ich zur Konfiguration und zum Test eine Vielzahl von Verbindungen mit diesen Rechten herstellen. KF kann durch ein eigenes Passwort gesichert werden. Dies ist die richtige Lösung.),
- ich grundsätzlich Programme vorziehe, bei denen ich genau sehe, was ich einstelle, und demgegenüber Programme meide, die meinen, Sie wüssten, was ich will, und mir helfen wollen, indem sie Dinge für mich entscheiden, ohne mir genau zu sagen, was sie eigentlich eigenmächtig machen (deshalb teile ich die in den diversen Tests an der TPF (s. insbesondere [18]) geäußerte Kritik, die Firewall lasse gefährliche Regeln zu und sei für Einsteiger schwer zu konfigurieren, gerade nicht: Eine Firewall kann nur der sinnvoll einrichten,

der sich mit der Materie befasst hat. Wenn ein solcher Anwender eine gefährliche Regel möchte, soll er sie bekommen.)
- sie nach meiner Auffassung die Einrichtung eben doch sehr erleichtert, weil sie sich so einstellen lässt, dass sie bei allen Paketen, bei denen die Firewall keine Regel findet, nachfragt und die Erstellung einer generellen Regel ermöglicht,
- sie anhand von MD5-Checksummen prüft, ob eine Anwendung, die für bestimmte Verbindungen zugelassen wurde, modifiziert oder ausgetauscht wurde (Wenn der Sinn der ergänzenden Desktop-Firewall gerade darin bestehen soll, die Router-Firewall durch anwendungsbezogene Regeln zu verfeinern, wäre es natürlich eine Katastrophe, wenn sich die Desktop-Firewall schon dadurch aushebeln ließe, dass sich ein Schadprogramm in ‚Internet Explorer' umbenennt).

In der Bedienbarkeit erhält die KF in Vergleichstests regelmäßig nur durchschnittliche oder gar unterdurchschnittliche Noten. Das ist aber ein grundsätzliches Problem von Softwaretests, weil am Ende *eine* Gesamtnote herauskommen soll, durch die ganz unterschiedliche Gesichtspunkte vermengt werden. Die KF ist sicher nichts für Anwender, die davon ausgehen, nur den Knopf ‚Install' drücken zu müssen, um danach ein ‚sicheres' System zu haben. Man muss sich mit der Firewall auseinandersetzen und sich die Regeln erarbeiten. Wenn man dies aber getan hat, wird man nach meiner Auffassung feststellen, dass die Bedienbarkeit nicht nur sehr gut ist, sondern dass es auch nichts zu verbessern gibt (und dies behaupte ich nur von sehr wenig Software).

Viel ernster ist die – auf fast alle Desktop-Firewalls und auf viele andere Sicherheitsprogramme zutreffende – Feststellung, dass diese Firewalls durch Schadprogramme ‚abgeschossen' werden können (der derzeit am meisten verbreitete Schädling, nämlich der Bugbear-Wurm, ist eben auch deshalb so erfolgreich, weil er eine Vielzahl von Schutzprogrammen beenden kann, vgl. die Liste bei: [43]).

Bei der KF kann man dies durch einen Eintrag in die Registry verhindern [24] (unter NT/w2k/XP sind natürlich Administrator-Rechte erforderlich; auch hier der übliche Hinweis: bitte die Registry vor jeder Veränderung sichern):

Unter Start → Ausführen *Regedit* eingeben:

Unter win 9x/ME den Eintrag

HKEY_LOCAL_MACHINE→System→CurrentControlSet→Services→VxD→fwdrv

und unter NT/w2k/XP den Eintrag

HKEY_LOCAL_MACHINE→System→CurrentControlSet→Services→fwdrv

suchen und dort einen neuen DWORD-Wert mit der Bezeichnung ‚AlwaysSecure' anlegen und diesem Eintrag den Wert ‚1' zuweisen.

Danach muss der Rechner neu gestartet werden. Solange die KF läuft, funktioniert alles wie gewohnt. Wird die KF aber beendet, ist der gesamte TCP/IP-Verkehr gesperrt (NetBEUI funktioniert weiter). Sie kommen also weder ins Internet noch ans WebInterface des Routers, der Virtual TA Client und die Monitor-Programme für den Router funktionieren nicht mehr. Sie können nicht einmal mehr das Administrations-Menu der KF aufrufen, um diese wieder einzuschalten. Um dies zu können, müssen Sie zunächst mit regedit die oben wiedergegebenen Registry-Einträge aufrufen, den Wert von ‚AlwaysSecure' auf ‚0' setzen, den Rechner neu starten, das Administrations-Menu der KF aufrufen, diese wieder einschalten, den Wert von ‚AlwaysSecure' wieder auf ‚1' setzen und den Rechner neu starten. Sicherheit hat eben ihren Preis. Allerdings dürfte die KF mit diesem Registry-Patch jeden Vergleichstest zwischen Portblockern gewinnen. Gleichwohl bleibt natürlich das Risiko, dass ein Schadprogramm den vorerwähnten DWORD-Wert zunächst auf ‚0' setzt und erst dann die Firewall abschießt, und dieses Risiko wird durch die Verbreitung des oben wiedergegebenen Tipps noch größer. Deshalb auch an dieser Stelle nochmals mein Rat: Nicht mit Administrator-Rechten im Internet surfen !

Ich habe den Registry-Patch sowohl unter w98 als auch unter w2k getestet und keine weiteren Probleme feststellen können.

Abschließend möchte ich darauf hinweisen, dass die TPF in [18] abgewertet wurde, weil sich in diesem Test bei einer Installation auf Windows XP ein Schadprogramm den Namen ‚Explorer.exe' und dessen in der Firewall vergebenen Rechte aneignen konnte. Sollte dies zutreffen, so wäre das natürlich eine schwere Sicherheitslücke ! Die PC Welt hat die Firewalls allerdings unter erschwerten Bedingungen getestet, weil die Datei- und Druckerfreigabe auch für den Internet-Anschluss freigeschaltet war, was ich für den Normalanwender nicht empfehle (s.o. Begriffserläuterungen→ NetBIOS). Die Fehlfunktion hängt möglicherweise auch mit den nachstehend umschriebenen Freigaben zusammen, die KF automatisch bei einer Installation unter w2k erstellt und die ich abschalten würde (s.u.). Bei meinen Installationen ist ein solcher Fehler nie aufgetreten. Die KF hat mich jedes Mal gewarnt, wenn ein zugelassenes Programm durch ein Update geändert oder ausgetauscht wurde (und das ist bei den ganzen bugfixes und Sicherheits-Patches für den Internet Explorer gerade bei diesem Programm sehr häufig vorgekommen). Alle nachstehenden Ausführungen können Sie praktisch unverändert auch für die TPF übernehmen, denn die Oberflächen der KF und der TPF unterscheiden sich nur geringfügig.

Nach der Installation würde ich zunächst die Firewall durch einen Rechtsklick auf das in der Taskleiste rechts neu erscheinende Icon aufrufen und dann unter Administration → Miscellaneos die Checkbox ‚Check For New Versions ...' deaktivieren. Andernfalls stellt KF bereits eine Internetverbindung für die Suche nach einer neuen Version her, bevor Sie sich angemeldet haben. Bei Win9X würde ich im gleichen Menu auch ‚Enable DNS Resolving' deaktivieren, weil auch dies beim Start bereits zu einer Verbindung mit dem externen DNS-Server führt. Unter Windows 2000 passiert das nicht. Gleichzeitig würde ich zur Kenntnis nehmen, dass unter Administration → Authentication ‚Authentication Is Required' angekreuzt und ein Passwort vergeben werden kann, würde dies aber zunächst noch nicht aktivieren, sondern erst die wesentlichen Erlaubnisregeln eingeben bzw. erstellen lassen. Sonst müssen Sie bereits in der An-

fangsphase ständig das Passwort angeben, um die Firewall Administration aufzurufen und die Regeln zu verfeinern. Nach den Grundeinstellungen ist es aber unbedingt erforderlich, die Firewall durch ein Passwort zu sichern. Auch unter w2k hat sonst jeder einfache Benutzer Zugriff auf die Firewall und kann sie abschalten oder unsinnige Regeln eingeben.

KF erstellt unter w2k (nicht unter w98) nach der Installation eine Reihe von Erlaubnisregeln, die ich für bedenklich halte und die Sie nach meiner Auffassung auch nicht benötigen und deaktivieren sollten, wenn Sie den LAN-Verkehr nicht über TCP/IP (sondern über NetBEUI) betreiben (so wird zum Beispiel der Port 445 freigegeben, mit dem w2k die Datei- und Druckerfreigabe managt, und die Local Security Authority [LSASS.EXE], die u.a. dafür zuständig ist, ein sicheres Einloggen auf anderen Rechnern zu ermöglichen, usw.). In w2k/XP-Netzen, bei denen mittels direct hosting TCP/IP benutzt wird, werden Sie an diesen Regeln nicht vorbeikommen. Sie erkennen diese Freigaben daran, dass sie für Programme gelten, die im Verzeichnis ...\WINNT\System32 abgelegt sind, oder bei ihnen statt eines Programmes ‚system' angegeben ist.

DHCP funktionierte auf meinen Rechner ohne ausdrückliche Freigabe durch die KF.

Im übrigen können Sie sich die Konfiguration der KF ziemlich einfach machen: Lassen Sie den Regler der Firewall-Administration in der mittleren Stellung ‚Ask me First' und starten Sie alle Internetanwendungen. Bei fehlender Zulassung werden Sie gefragt, wie verfahren werden soll: Sie können mit ‚permit' die Verbindung einmal zulassen oder mit ‚Create Rule' gleich eine Regel erstellen. Im Anschluss an diese ‚Rundreise' würde ich mir allerdings unter Administration → Firewall → Advanced → Edit die einzelnen Regeln genau ansehen und verfeinern bzw. allgemeiner formulieren, denn je weniger Regeln Sie brauchen, um so weniger wird die Leistung Ihres Rechners durch die Firewall beeinträchtigt. Um Ihnen diese Arbeit zu erleichtern folgt ein Beispielset:

# Beispielfilterset für die Kerio Firewall

| Nr. | Rule Description | enabled | Direction | Action (Permit=P/Deny=B) | Protocol | Local Port | Remote Address | Remote Port | Rule Valid (always=a) | Application |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | DNS->Router | X | both | P | UDP | any | 192.168.1.1 | 53 | a | any |
| 2 | DNS (t-online) | X | both | P | UDP | any | *217.5.99.9* ***(s. Anm.)*** | 53 | a | any |
| 3 | DNS (t-online) Reserve | X | both | P | UDP | any | *194.25.2.129-194.25.2.134* ***(s. Anm.)*** | 53 | a | any |
| 4 | Outgoing PING command | X | Out | P | ICMP | any | any | entfällt | a | any |
| 5 | Outgoing PING command (Incoming Reply) | X | In | P | ICMP | any | any | entfällt | a | any |
| 6 | Incoming Icmp Time Exceeded (used by TRACEROUTE command) | X | In | P | ICMP | any | any | entfällt | a | any |
| 7 | Outgoing reply on PING command | X | Out | P | ICMP | any | any | entfällt | a | any |
| 8 | Other ICMP | X | both | **B** | ICMP | any | any | entfällt | a | any |
| 9 | IGMP | X | both | **B** | other-2 | any | any | entfällt | a | any |
| 10 | Virtual TA Broadcast | X | Out | P | UDP | any | 255.255.255.255 | 56415 | a | {Lw}:\programme\virtual ta client\rccicon.exe |
| 11 | Virtual TA<->Router | X | both | P | TCP and UDP | any | 192.168.1.1 | 56415 | a | {Lw}:\programme\virtual ta client\rccicon.exe |
| 12 | Telnet->Router | X | Out | P | TCP | any | 192.168.1.1 | 23 | a | {Lw:}:\winnt\system32\telnet.exe |
| 13 | Download Manger http, https | X | Out | P | TCP | any | any | 80,443 | a | {Lw}:\programme\{Pfad}\{Programmname} |
| 14 | Download Manager ftp Kommandokanal | X | Out | P | TCP | any | any | 21 | a | {Lw}:\programme\{Pfad}\{Programmname} |
| 15 | Download Manager ftp Datenkanal | X | Out | P | TCP | 1024-65535 | any | 1024-65535 | a | {Lw}:\programme\{Pfad}\{Programmname} |
| 16 | WS_FTP Pro (21) | X | Out | P | TCP | 1024-65535 | any | 21 | a | {Lw}:\programme\ws_ftp pro\ftp95pro.exe |
| 17 | WS_FTP Pro data | X | Out | P | TCP | 1024-65535 | any | 1024-65535 | a | {Lw}:\programme\ws_ftp pro\ftp95pro.exe |
| 18 | WS_FTP Pro aktiv | X | In | P | TCP | 1024-65535 | any | 20 | a | {Lw}:\programme\ws_ftp pro\ftp95pro.exe |
| 19 | Virenscanner-Update | X | Out | P | TCP | any | any | 80 | a | {Lw}:\programme\{Pfad}\{Programmname} |
| 20 | Internet Explorer Loopback | X | Out | P | TCP and UDP | any | 127.0.0.1 | any | a | {Lw }:\programme\internet explorer\iexplore.exe |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 21 | Internet Explorer | X | Out | P | TCP | any | any | 80,443 | a | {Lw }:\programme\internet explorer\iexplore.exe |
| 22 | Outlook Express Loopback | X | Out | P | TCP and UDP | any | 127.0.0.1 | any | a | {Lw}:\programme\outlook express\msimn.exe |
| 23 | Outlook Express POP3 | X | Out | P | TCP | any | *194.25.134.0-194.25.134 .128* ***(s. Anm.)*** | 110 | a | {Lw}:\programme\outlook express\msimn.exe |
| 24 | Outlook Express SMTP | X | Out | P | TCP | any | *194.25.134.0-194.25.134 .128* ***(s. Anm.)*** | 25 | a | {Lw}:\programme\outlook express\msimn.exe |
| 25 | NAV POP3 | X | Out | P | TCP | any | *194.25.134.0-194.25.134 .128* ***(s. Anm.)*** | 110 | a | {Lw}:\programme\gemeinsame datei-en\symantec shared\ccapp.exe |
| 26 | NAV SMTP | X | Out | P | TCP | any | *194.25.134.0-194.25.134 .128* ***(s. Anm.)*** | 25 | a | {Lw}:\programme\gemeinsame datei-en\symantec shared\ccapp.exe |
| 27 | NTVDM (t-online-Banking) | X | Out | P | TCP | any | *194.25.134.0-194.25.134 .255* ***(s. Anm.)*** | any | a | {Lw}:\winnt\system32\ntvdm.exe |
| 28 | OnlineBanking (Werbeblo-cker) | X | Out | **B** | TCP | any | any | any | a | {Lw}:\programme\t-online_40\ob4hbci\banking.exe |
| 29 | Realplayer | X | Out | P | TCP | any | any | 80 | a | {Lw}:\programme\real\realplayer\realplay.exe |
| 30 | QuickTime | X | Out | P | TCP | any | any | 80 | a | {Lw}:\programme\quicktime\quicktimeplayer.exe |
| 31 | WMPlayer Loopback | X | Out | P | TCP and UDP | any | 127.0.0.1 | any | a | {Lw}:\programme\windows media player\wmplayer.exe |
| 32 | WMPlayer | X | Out | P | TCP | any | 207.46.0.0/255.255.0.0 | 80 | a | {Lw}:\programme\windows media player\wmplayer.exe |
| 33 | MMJukebox Loopback | X | Out | P | TCP and UDP | any | 127.0.0.1 | any | a | {Lw}:\programme\musicmatch\musicmatch jukebox\mmjb.exe |
| 34 | MMJukebox | X | Out | P | TCP | any | any | 80 | a | {Lw}:\programme\musicmatch\musicmatch jukebox\mmjb.exe |
| 35 | Outlook Express NNTP t-online | X | Out | P | TCP | any | 62.153.159.134 | 119 | a | {Lw}:\Programme\outlook express\msimn.exe |
| 36 | Outlook Express NNTP Mi-croSoft | X | Out | P | TCP | any | 207.46.248.16 | 119 | a | {Lw}:\Programme\outlook express\msimn.exe |
| 37 | Block all | X | both | **B** | any | any | any | entfällt | a | any |

**Leerformular zum Erstellen eigener Regeln für die Kerio Firewall:**

| Nr. | Rule Description | enabled | Direction | Action (Permit=P/Deny=B) | Protocol | Local Port | Remote Address | Remote Port | Rule Valid (always=a) | Application |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

## Anmerkungen zu den Kerio-Regeln

**zu Nrn. 1 - 3**
Diese schalten die DNS-Server des Routers (Nr. 1) bzw. von t-online (Nrn. 2 + 3) frei. Die Remote-Adressen bei den beiden letzten Regeln dürfen Sie nur als Beispiel verstehen (s. die Anmerkungen bei den Router-Regeln).
Wenn Sie die Router-Firewall in der Weise eingerichtet haben, wie ich es vorstehend empfohlen habe, können Sie die Regeln auch zusammenfassen: Löschen Sie die Regeln 2 und 3 und tragen Sie bei der Regel Nr. 1 als Remote-Adress ‘any’ ein, alles andere filtern die DNS-Regeln im Router.

**zu Nrn. 4 - 9**
Die Regeln habe ich unverändert aus der Default-Einstellung bei der Installation übernommen. IGMP wird komplett abgeschaltet und ICMP nur mit bestimmten Typen zugelassen. Beim Editieren dieser Filterregeln sehen Sie rechts oben einen Button mit der Aufschrift 'Set Icmp...'. Hier können Sie das ICMP-Protokoll Ihren Wünschen entsprechend einstellen (nähere Informationen bei [1]).

**zu Nrn. 10 + 11**
Diese Regeln benötigt der Virtual TA Client, der für Telefonieanwendungen benötigt wird. Beachten Sie die merkwürdige Adresse bei der Regel Nr. 10: Dies ist die so genannte Broadcast-Adresse, mit der alle Geräte des Netzwerks angesprochen werden. Der Virtual TA Client sucht so den Router.

**Nr. 12**
ist erforderlich, damit Sie mittels Telnet auf den Router zugreifen können. Wenn Sie mit diesem Programm auch auf andere lokale oder externe Geräte zugreifen wollen, müssen Sie hierfür natürlich entsprechende Regeln erstellen. Gleiches gilt, wenn Sie ein anderes Terminalprogramm benutzen wollen.

**Nrn. 13 - 18**
Diese Regeln ermöglichen ftp-Übertragungen zum einen mit Ihrem Download-Manager und zum anderen mit einem speziellen FTP-Übertragungsprogramm. Die Angaben zu 'Application' dürfen Sie natürlich nur als Beispiel verstehen.

**Nr. 19**
ist wichtig, damit Ihr - hoffentlich installierter - Virenscanner seine Updates abholen kann

**Nr. 20**
ist interessant: Die Bedeutung von Loopback habe ich unter Begriffserläuterungen → Loopback dargestellt. Der IE benutzt dieses Verfahren für Zwecke, die mir nicht bekannt sind, und arbeitet ohne diese Zulassung nicht richtig. Die KF arbeitet in diesem Punkt übrigens präziser als die TPF, die Loopback per Standardeinstellung für alle Anwendungen freigab, was aus Sicherheitsgründen bedenklich ist (s. bei [1]).

**Nr. 21**
ist eine der wichtigsten Regeln und gibt dem IE die Ports 80 (http) und 443 (https) für alle Ziele frei. Die entsprechenden Proxy-Ports 8080 oder 3128 müssen freigegeben werden, wenn der Provider einen Proxy-Server verwendet und (!) diese Ports vorgibt.

**Nr. 22**
wie Nr. 20

**Nrn. 23 – 26**
ermöglichen den eMail-Verkehr über die POP3- und SMTP-Ports Falls die Mails über das IMAP-Protokoll (s. Begriffserläuterungen) abgeholt werden, muss statt Port 110 der Port 143 freigeschaltet werden. Falls die eingehenden Mails über eine sichere Verbindung (SPOP3) laufen, muss der Port 995 freigeschaltet werden. Eine Besonderheit stellen die Regeln 25 und 26 dar: Da mein Virenscanner die ein- und ausgehenden Mails prüft, stellt dieser (und nicht Outlook [Express]) die Verbindungen her. Die Regeln 23 und 24 wären daher eigentlich überflüssig und sind nur der Vollständigkeit halber und für den Fall eingefügt, dass der Virenscanner einmal abgeschaltet sein sollte (die Remote-Adressen sind nur als Beispiel für die Server von t-online/Deutsche Telekom zu verstehen).

**Nr. 27**
ist eine Besonderheit für WINNT- und w2k-Anwender: NTVDM (NT Virtual Dos Machine) stellt auf DOS basierenden Programmen eine DOS Umgebung zur Verfügung, damit diese überhaupt arbeiten können. Da das t-online-Banking (Version 4.0 !) immer noch auf solchen Programmen beruht, wird die Verbindung zur Bank über NTVDM.EXE hergestellt. W9x-Benutzer müssen die Regel entsprechend anpassen (die Remote-Adressen sind nur als Beispiel für die Server von t-online/Deutsche Telekom zu verstehen).
Die Regel passt mir natürlich überhaupt nicht, denn sie schaltet den Internet-Zugang eben nicht nur für das Banking-Programm frei, sondern allen Programmen, die auf DOS beruhen und den NTVDM für den Internet-Zugang bemühen. Das Risiko wird lediglich dadurch begrenzt, dass eine Verbindung nur zu Servern der Deutsche Telekom zugelassen ist. Sicherer ist es aber in jedem Fall, ein anderes Banking-Programm zu benutzen, welches ohne NTVDM auskommt.

**Nr. 28**
ist eigentlich nicht wichtig und blockiert nur die vom Banking-Programm eingeblendeten Werbebanner. Die Regel ist allerdings ein interessantes Beispiel dafür, wie mit einer Desktop-Firewall auch solche Banner verhindert werden können.

**Nrn. 29 + 30**
ermöglichen die Benutzung von RealPlayer und Quicktime, wenn Sie diese Programme entsprechend meiner Empfehlung so eingestellt haben, dass diese den http-Port 80 benutzen.

**Nr. 31**
wie Nr. 20

**Nr. 32**
Erlaubt dem Windows MediaPlayer, die Track-List herunterzuladen, beachten Sie bei der Remote-Adresse die Subnetzmaske 255.255.0.0: durch sie wird der gesamte Bereich von 207.46.0.0 bis 207.46.255.255 freigeschaltet (nach Auskunft von swhois gehören diese Adressen MicroSoft)

**Nr. 33**
wie Nr. 20

**Nr. 34**
erlaubt der musicmatch JUKEBOX den Zugriff, damit die Daten der eingelegten Musik-CD abgerufen werden können. Da alle Remote-Adressen freigeschaltet werden, ist die Regel natürlich bedenklich. Eine nähere Eingrenzung war mir aber nicht möglich, weil die Jukebox ständig eine Verbindung zu stets wechselnden Adressen aufbauen wollte und dadurch immer wieder neue Freigaben erforderlich wurden.

**Nrn. 35 + 36**
Zugriff auf die Newsserver: Die eingetragenen Adressen stehen für news.btx.dtag.de und msnews.microsoft.com und müssen im Bedarfsfall angepasst werden (die Adresse des Microsoft-Servers wechselt gelegentlich, keine Probleme dürfen Sie mehr haben, wenn Sie als Remote-Adresse 207.46.0.0 mit der Subnetzmaske 255.255.0.0 eingeben, weil dadurch der gesamte Bereich von 207.46.0.0 bis 207.46.255.255 freigeschaltet wird, der nach Auskunft von swhois MicroSoft gehört).

**Nr. 37**
sollten Sie – jedenfalls in der Anfangszeit – *nicht* eingeben, sondern den Regler auf der Eingangsseite der Firewall Administration auf ‚Ask Me First' stehen lassen. Wenn die Firewall bei dieser Einstellung keine Regel findet, fragt sie nach, was zu tun ist (Würden Sie die Regel 37 aktivieren, käme es zu dieser Frage nicht mehr, denn die Regel 37 passt immer.). Wenn Sie allerdings irgendwann den Regler auf ‚Permit Unknown' stellen, funktioniert diese deny-all-Regel als zusätzlicher ‚Sicherheitsriegel': Sie besagt, dass alles, was vorher nicht ausdrücklich zugelassen wurde, verboten ist. Die gefährliche Einstellung ‚Permit Unknown' reicht allein nicht, um den Rechner zu öffnen, sondern es muss auch die Regel 37 deaktiviert werden. Meine Empfehlung: Regler auf ‚Ask Me First' stehen lassen und Regel 37 *nicht* aktivieren.

**Sonstiges**
Sie werden wahrscheinlich eine ganze Reihe weiterer Regeln benötigen, die der Regel Nr. 19 ähnelt, weil viele Programme inzwischen eine Online-Hilfe anbieten bzw. per Menu-Aufruf aktualisiert werden können. Ich empfehle, diese Freigaben – wenn eben möglich – auf konkrete Remote-Adressen zu beschränken. Die nötigen Remote-Adressen müssen Sie entweder beim Hersteller des Programms erfragen oder versuchen, sie durch die Firewall ermitteln zu lassen.

Weitere Hilfe zur KF finden Sie auf diesen Seiten [25]. Der Eingangsbildschirm lässt sich mit diesem Programm [26] abstellen. Bitte sichern Sie vor dem Ausführen des

Programms die Datei *PERSFW.exe*, die durch dieses Programm verändert wird. Bei einem w2k-Rechner hatte ich nach dem Entfernen des Eingangsbildschirms Probleme mit dem Systemstart, die wahrscheinlich nicht auf den Patch zurückzuführen sind, sondern von einem Timing-Problem herrühren. Gleichwohl sollte man nicht auf die Möglichkeit verzichten, den Original-Zustand wiederherzustellen.

# VIII. Quickstart

Weil in den Foren immer wieder darum gebeten wird, doch einmal eine ‚einfache' Anleitung für das Firewall-Setup zu schreiben, habe ich mich in dieser Auflage der Anleitung dazu entschlossen, ein Quickstart-Regelwerk aufzunehmen (und wenn es nur dem Zweck dient zu belegen, dass es nicht geht).

**Einstellung im General-Setup:**

| | | |
|---|---|---|
| *Call-Filter* | ⊙ | Enable *Start Filter Set* Set#1 |
| *Data-Filter* | ⊙ | Enable *Start Filter Set* Set#1 |
| *Log Flag* | None | |
| *MAC Address for Logged Packets Duplication* | 0x000000000000 | |

❒ Accept Incoming Fragmented UDP Packets ( for some games, ex. CS )

| **Filter Set 1** | | **Comments** | | **Quickstart** | | **Next Filter Set** | | **None** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | **Source** | | | | | **Destination** | | | | | | | |
| Rule | Comments | Check to enable | Pass or Block | Branch to other Filter Set | Duplicate to LAN | Log | Direction | Protocol | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | IP-Adresse | Subnet Mask | Operator | Start Port | End Port | Keep State | Fragments |
| 1 | DNS | X | PI | None | | | out | UDP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 53 | | | Don't Care |
| 2 | http (80) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 80 | | | Don't Care |
| 3 | https(443) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 443 | | | Don't Care |
| 4 | POP3(110) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 110 | | | Don't Care |
| 5 | SMTP(25) | X | PI | None | | | out | TCP | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | 25 | | | Don't Care |
| 6 | Block out | X | ***BI*** | None | | | out | any | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |
| 7 | Block in | X | ***BI*** | None | | | in | any | any | 255.255.255.255/32 | = | | | any | 255.255.255.255/32 | = | | | | Don't Care |

**Anmerkung:** Mit diesem Filter-Set müssten die meisten Anwender mit einer Firmware ab 2.1a im Internet surfen und eMails verschicken und abholen können (Wenn das nicht klappt, bleibt nichts anderes übrig, als den Rest der Anleitung durchzulesen). Vieles (Newsgroups, ftp, Mediastreaming usw.) funktioniert natürlich nicht. In den übrigen Teilen der Anleitung finden Sie aber ausreichend Hilfe, um das Set Stück für Stück auszubauen, um alle Möglichkeiten des Internets trotz Firewall nutzen zu können (Die Anleitung ist übrigens weniger wegen der Vigor-Firewall so ‚dick', sondern weil sie sich mit einer Reihe von Sicherheitslücken befasst, die nur in sehr bescheidenem Umfang von der Firewall geschlossen werden können). Das Regelwerk ist auch nicht besonders sicher, aber selbstverständlich viel besser, als die Firewall abzuschalten. Als nächste Sicherheitsmaßnahme würde ich mir zu den Regeln 1, 4 und 5 vom Provider die Adressen der DNS- und Mail-Server besorgen und in das Regel-Set unter Destination-IP-Adresse eintragen. Danach würde ich mich entsprechend meiner ganz persönlichen ‚Hitliste' der wichtigsten Sicherheitsmaßnahmen in der folgenden Reihenfolge um die weitere Absicherung kümmern: 1. Virenscanner mit aktuellen (!) Virensignaturen – 2. Keine Administrator-Rechte beim Surfen (s. *Hinweise*) – 3. ActiveX abstellen, zumindest einschränken (s. *Begriffserläuterungen*) – 4. Desktop-Firewall installieren.

# IX. Fundstellen und weiterführende Hinweise

[1] www.saferhex.de/Security_Firewall/ruleset.html: Firewall & Ruleset Security Page von Lukas Wenz: Eine wirklich hervorragend gemachte Seite mit einer Vielzahl weiterführender Hinweise und Links.
[2] www.lavasoftUSA.com stellt kostenlos das Programm Ad-aware zur Verfügung, mit dem man den Rechner auf Spyware untersuchen und diese entfernen kann; in die Version 6.0 wurde inzwischen auch eine Funktion eingebaut, mit der man die referencefiles mit der Auflistung der SpyWare-Komponenten per Mausklick auf den neuesten Stand bringen kann
[3] www.eAladdin.com, Aladdin verkauft und unterstützt eSafe Desktop inzwischen nicht mehr und verlinkt auf www.esafedesktop.com
[4] http://www.norman.com/de/index.shtml
[5] www.grc.com: Gibson Research Corporation. (Shields Up) zum Test der Ports; einen wirklich guten und kompletten PC-Selbsttest (Browser-Informations- und Sicherheitseinstellungen, Datei- und Druckerfreigaben, Porttest) können sie mit http://check.lfd.niedersachsen.de/start.php starten (Achtung: ein kompletter Port-Test dauert über 5 Stunden !)
[6] www.it-sec.de/vulchk.html: it.sec ermöglicht die Überprüfung der NetBIOS-Verwundbarkeit des Systems
[7] ct 04/2000, S. 126 11 Personal Firewalls im Test, die zitierten Artikel aus der ct können unter www.heise.de/kiosk gegen geringes Entgelt heruntergeladen werden
[8] ct 04/2000, S. 214 Windows und Internet-Software sicher konfigurieren
[9] ct 04/2000, S. 224 Personal Firewall und Anti-Viren-Software richtig einsetzen
[10] ct 20/2001, S. 210 ADSL-Einrichtung
[11] ct 21/2001, S. 140 Sicherheitsrisiko MicroSoft
[12] ct 21/2001, S. 144 Mit Windows möglichst sicher durchs Netz
[13] ct 21/2001, S. 152 Personal Firewalls optimal einrichten
[14] ct 23/2001, S. 174 10 Personal Firewalls im Test
[15] PC Magazin 11/2000, S. 58 Sicherer PC
[16] PC Magazin 11/2000, S. 70 Firewalls im Test
[17] PC Magazin 05/2001, S. 178 Firewalls richtig konfigurieren
[18] PC Welt 05/2002, S. 80 9 Personal Firewalls im Test
[19] www.tecchannel.de liefert viele weiterführende Artikel zu Firewall-Grundlagen und Tests, die Artikel können in der Regel kostenlos betrachtet werden, das Ausdrucken oder Herunterladen kostet eine geringe Gebühr
[20] ct 11/2002, S. 138 Windows XP sicher nutzen
[21] www.kerio.com
[22] TinySoftware bietet die Version 2.0 der Desktop-Firewall unter www.tinysoftware.com weiterhin für die private Nutzung kostenlos an (die Version 3.0 ist leider auch bei einer privaten Nutzung kostenpflichtig)
[23] http://www.microsoft.com/IntlKB/Germany/Support/kb/D301/D301041.htm
[24] den tipp habe ich gefunden unter:
http://board.protecus.de/showtopic.php?threadid=211
[25] http://www.blarp.com/faq/faqmanager.cgi?toc=kerio und
http://www.dslreports.com/forum/kerio
[26] http://www.brightnova.com/downloads/KPFSplashKiller.exe
[27] http://support.microsoft.com/default.aspx?scid=kb;de;204279

[28] z.B. http://www.itp-journals.com/nasample/t1720.pdf
[29] http://www.hoelzner.de/security/freigabedienste.php
[30] vgl. z.B. http://www.bsi.de/gshb/deutsch/g/g5042.htm
[31] zu laden über: http://computer.t-online.de/comp/inte/tdsl/ar/CP/ar-tdsl-speedmanager.html
[32] welches z.B. in der Freeware-Version 2.2 (NT/w2k) unter http://www.chip.de/downloads_updates/downloads_updates_158263.html und in der aktuellen Version 2.6 (NT/w2k/XP) beim Hersteller für $ 20 unter http://www.basta.com geladen werden kann
[33] z.B. diese: http://www.rz.uni-freiburg.de/pc/systeme/srvany/
[34] www.richmac.org
[35] ct 22/2002, S. 198 Kostenlose Personal Firewalls für Windows
[36] ct 25/2002, S. 100 Sicherheitsrisiko Internet Explorer
[37] ct 25/2002, S. 192 Aktuelle Virenscanner für Windows
[38] ct 01/2003, S. 80 Windows absichern
[39] http://coombs.anu.edu.au/~avalon/ip-filter.html
[40] http://coombs.anu.edu.au/~avalon/IP%20Filter%20Based%20Firewalls%20HOWTO-German.pdf
[41] und zwar Version v3.3.1 (148), wie man unter Telnet mit ‚ipf –V' feststellen kann, übrigens stimmt auch die Anzeige von ‚ipf –V' exakt mit dem überein, was die Linux-Firewall mit demselben Befehl ausgibt, vgl. http://false.net/ipfilter/1999_09/0101.html
[42] http://www.computerbetrug.de/firewall/tunnel.php?p=0|17|74|
[43] http://www.bsi.de/av/vb/bugbear.htm
[44] zu beziehen von http://www.lab1.de, für den Privatgebrauch kostenlos
[45] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-055.asp
[46] z.B.: http://freenet.meome.de/app/fn/artcont_portal_news_article.jsp/85675.html
[47] kann z.B. hier kostenlos heruntergeladen werden: http://www.pcmag.com/article2/0,4149,6244,00.asp
[48] vgl. http://www.heise.de/tp/deutsch/inhalt/te/5482/1.html
[49] http://www.heise.de/privacy/
[50] vgl. z.B. http://www.techfak.uni-bielefeld.de/rechner/cookies.html
[51] http://www.heise.de/ct/browsercheck/
[52] ergänzende Informationen z.B. bei http://www.privacyfoundation.org/resources/webbug.asp
[53] http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-069.asp, vgl. auch http://www.astalavista.ch/news.php?cmd=detail&ID=702
[54] Sie können sich aber auch die Java Virtual Machine für den Internet Explorer von Sun herunterladen: http://java.sun.com/getjava/index.html
[55] die definierten Port-Nummern finden Sie unter: http://www.iana.org/assignments/protocol-numbers
[56] einen sehr positiven Test finden Sie unter: http://www.bluemerlin-security.de/Securetest_Tiny_Firewall40_151202.php3
[57] http://www.pivx.com/kristovich/adv/mk001/
[58] http://www.pcflank.com/exploits.htm
[59] http://www.webwasher.com, in der Classic-Version für private Nutzer kostenlos
[60] outpost kann als kostenlose Free-Version von www.agnitum.com geladen werden
[61] unter www.trojancheck.de kostenlos herunterzuladen

# X. Index