

# Personal Desktop Firewalls

Stand: 23.05.2006

<b>VORWORT:</b>	<b>2</b>
<b>1. <u>WAS SIND PERSONAL DESKTOP FIREWALLS?</u></b>	<b>2</b>
<b>2. <u>BIN ICH GEFÄHRDET?</u></b>	<b>2</b>
<b>3. <u>WIE FUNKTIONIEREN PERSONAL DESKTOP FIREWALLS?</u></b>	<b>4</b>
3.1 SCHICHTENMODELL:	4
3.2 ADRESSIERUNG:	5
3.3 PORTS:	6
3.4 PROTOKOLLE:	7
3.5 WO DIE DESKTOP FIREWALL ANSETZT:	8
3.6 WARUM AUCH IHR RECHNER MÖGLICHERWEISE IN GEFAHR IST:	9
<b>4. <u>NUTZEN VON PERSONAL DESKTOP FIREWALLS?</u></b>	<b>10</b>
<b>5. <u>WIE KANN ICH MEINEN COMPUTER OHNE DESKTOP FIREWALL SCHÜTZEN?</u></b>	<b>12</b>
<b>6. <u>SIND DANN ABER NICHT AUCH HARDWARE FIREWALLS NUTZLOS?</u></b>	<b>13</b>
<b>7. <u>WAS MUß ICH BEACHTEN, WENN ICH TROTZ ALLEM EINE PERSONAL DESKTOP FIREWALL EINSETZEN MÖCHTE?</u></b>	<b>15</b>
<b>8. <u>FIREWALL IST EIN KONZEPT UND KEIN PROGRAMM!</u></b>	<b>16</b>
<b>9. <u>GUTER SCHUTZ FÜR WENIG GELD – (DSL) HARDWARE ROUTER:</u></b>	<b>17</b>
<b>10. <u>DIE ROLLE DER FACHZEITSCHRIFTEN UND TESTMAGAZINE:</u></b>	<b>19</b>
<b>11. <u>WAS IST SONST NOCH WICHTIG?</u></b>	<b>20</b>
<b>12. <u>LINKS ZU INTERESSANTEN INTERNETSEITEN ZUM THEMA:</u></b>	<b>21</b>
<b>13. <u>WEITERFÜHRENDE INFORMATIONEN/LITERATURNACHWEIS:</u></b>	<b>22</b>
<b>14. <u>HAFTUNGSAUSSCHLUß/DISCLAIMER:</u></b>	<b>23</b>

## **Vorwort:**

Personal Desktop Firewalls gibt es wie Sand am Meer. Die Spanne reicht von kostenlosen Systemen wie der in Windows XP mit Service Pack 2 integrierten bis zu komplexen, kostenpflichtigen Systemen. Aber sind Personal Desktop Firewalls wirklich so zuverlässig, wie die Werbung behauptet?

## **1. Was sind Personal Desktop Firewalls?**

Personal Desktop Firewalls (auch als PFW, DFW, PDFW etc. bezeichnet) sind aus technischer Sicht sogenannte „Paketfilter“ [1], [2]. Sie sollen den Zugriff von außen (aus dem Internet) auf Ihren Computer verhindern bzw. sollen sie sicherstellen, daß keine Software Ihres PCs ungefragt Daten nach außen (in das Internet) sendet. PFWs sind darüber hinaus somit meistens auch „Applikationsfilter“ [2].

Firewalls sind also dafür zuständig, den Datenverkehr von und zu Ihrem Computer zu überwachen und bei Bedarf zu unterbinden.

Den Namen „Personal“ oder „Desktop“ tragen sie deshalb, weil die Firewall sich auf dem PC befindet, den sie schützen soll. Das ist aber das prinzipielle Problem von PFWs. Damit eine Firewall sicher funktioniert, muß sie sich **vor** dem zu schützenden PC befinden und nicht darauf! Siehe hierzu auch Abschnitt 8.

### Zusammenfassung:

Desktop Firewalls sind Software Produkte, die Ihren PC vor unberechtigten Zugriffen schützen sollen.

## **2. Bin ich gefährdet?**

Bevor Sie beginnen, sich tiefer in die Materie der Firewalls [3], [4] einzuarbeiten, wäre es vielleicht interessant für Sie zu wissen, ob Sie überhaupt gefährdet sind. Wenn Sie sich diese Frage stellen, erhalten Sie beispielsweise unter: <https://grc.com/x/ne.dll?bh0bkyd2> eine Antwort. Lesen Sie die Informationen dieser Seite, und wenn Sie einverstanden sind, wählen Sie „Proceed“. Sollte Sie die folgende Webseite mit dem Namen Ihres Nutzeraccounts oder des Rechnernamens begrüßen, haben Sie bereits die Antwort: ja! (Lesen Sie bitte vor den weiteren Tests Abschnitt 11.)

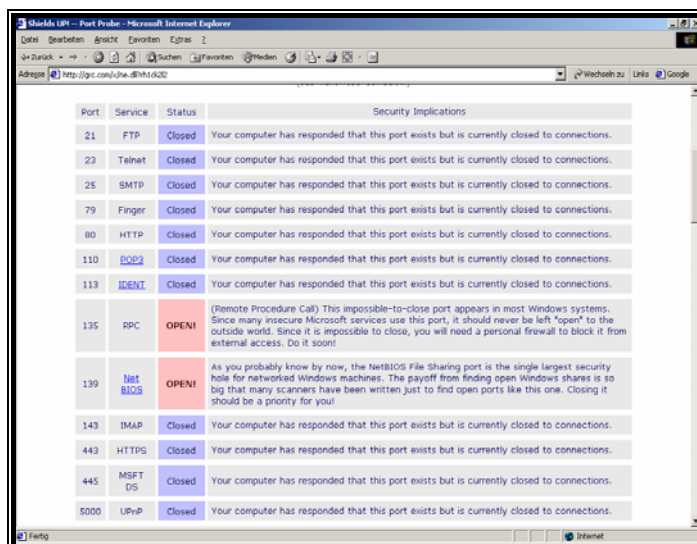
---

Zum Linnegraben 46      Telefon: +49 (069) 395955      e-mail: [oliver.klarmann@ingbuero-klarmann.de](mailto:oliver.klarmann@ingbuero-klarmann.de)  
65933 Frankfurt am Main      Fax: +49 (069) 38013651  
Mobil: +49 (0179) 2001336

---

Aber selbst wenn Sie noch nicht höflich mit Namen begrüßt werden, sollten Sie noch zwei weitere Tests durchführen, um sicherzugehen:

Sie haben auf der jetzt geöffneten Seite die Möglichkeit, den Punkt „File Sharing“ auszuprobieren - hier müssen Sie sehr aufmerksam lesen, was der Test Ihnen anzeigt, um eine mögliche Gefährdung beurteilen zu können; und bei dem nächsten Test „Common Ports“ können Sie sehr schnell erkennen, ob Ihr Computer den Inhalt Ihrer gesamten Festplatte dem weltweiten Internet anbietet (Ports 137-139). Sollte dieser Test einen offenen Port (siehe Abschnitt 3.3) anzeigen (bei Status „Open“ mit rotem Hintergrund), können Sie davon ausgehen, daß Sie in irgendeiner Weise gefährdet sind. Benutzer von Windows XP mit installiertem Service Pack 2 sollten zumindest für diese Tests nicht anfällig sein, sofern die SP 2 Firewall nicht abgeschaltet wurde.



Port	Service	Status	Security Implications
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
135	RPC	OPEN!	(Remote Procedure Call) This impossible-to-close port appears in most Windows systems. Since many insecure Microsoft services use this port, it should never be left "open" to the outside world. Since it is impossible to close, you will need a personal firewall to block it from external access. Do it soon!
139	NetBIOS	OPEN!	As you probably know by now, the NetBIOS File Sharing port is the single largest security hole for networked Windows machines. The payoff from finding open Windows shares is so big that many scanners have been written just to find open ports like this one. Closing it should be a priority for you!
143	IMAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
443	HTTPS	Closed	Your computer has responded that this port exists but is currently closed to connections.
445	MSFT DS	Closed	Your computer has responded that this port exists but is currently closed to connections.
8000	UPnP	Closed	Your computer has responded that this port exists but is currently closed to connections.

Abbildung 1: Screenshot der Ergebnisseite von Test 3. Port 139 ist offen. Wenn Sie Windows 95/98/ME benutzen, sollten Sie jetzt in höchstem Maße alarmiert sein. Jeder kann auf die Daten Ihrer Festplatte zugreifen! Verwenden Sie dagegen Windows NT/2000/XP oder Linux, kommt es auf die Konfiguration Ihres Systems an. Auch diese Systeme sind nicht per se sicher.

Allerdings sagt dies noch nichts darüber aus, ob Sie in hohem Maße gefährdet sind oder ob das Problem zu vernachlässigen ist. Sie brauchen etwas Hintergrundwissen, um dies verstehen und die Testergebnisse beurteilen zu können. Um eben dieses Hintergrundwissen geht es in den folgenden Abschnitten.

Ach so, auf den Ergebnisseiten der Tests steht, daß Personal Desktop Firewalls nützlich sind – Herr Gibson gilt zwar als ausgewiesener Sicherheitsexperte, er ist aber nicht ganz unumstritten. Wenn Sie das folgende lesen, können Sie die Lage selbst beurteilen und seiner Empfehlung folgen oder nicht. Oder aber einmal den Leaktest [5] ausprobieren. Den finden Sie nämlich auch auf <http://grc.com/>, und er demonstriert, wie man Desktop Firewalls umgeht! Ein wenig ironisch, dieser Steve, Gibson finden Sie nicht?

Einen alternativen Test, der alle Ports (siehe Abschnitt 3.3) prüfen kann, finden Sie unter <http://check.lfd.niedersachsen.de/start.php>.

---

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
---	---	--

---

### Zusammenfassung:

Testen Sie Ihren eigenen PC auf Sicherheitslücken. Wenn Sie einen standardmäßig installierten Windows-PC verwenden, auf dem bislang keine Firewall läuft und der direkt per ISDN oder DSL mit dem Internet verbunden ist, werden Sie Lücken feststellen. Verwenden Sie Windows XP mit installiertem Service Pack 2, sollten die Tests dagegen negativ ausfallen, vollständig sicher sind Sie deshalb trotzdem nicht.

## **3. Wie funktionieren Personal Desktop Firewalls?**

In Abschnitt 1 ist ein Stichwort bereits gefallen, welches auf die Funktion hindeutet: „Paketfilter“. Um zu wissen, wie eine Firewall arbeitet, ist ein sehr detailliertes Fachwissen über Netzwerke erforderlich! An dieser Stelle soll nur ein kurzer Abriss der Theorie dargestellt werden. Vertieftes Wissen ist aber im Internet leicht zu finden.

### 3.1 Schichtenmodell:

Ein Netzwerk ist grundsätzlich in Schichten aufgebaut. Im Normalfall sind dies 7 Stück [6], [7], [8]:

1. Physische Schicht: Übergang auf das Trägermedium (z.B. die ISDN- oder Netzwerkkarte, aber nicht das Kabel selbst)<sup>1)</sup>.
2. Datenverbindungsschicht: steuert, wie Daten (Frames/Pakete) über das Trägermedium übertragen werden.
3. Netzwerkschicht: steuert u.a., wie die Daten ihren Weg zu anderen Computern finden (Routing).
4. Transportschicht: steuert u.a., wie Daten zu versenden sind, und bereitet diese für die unteren Schichten auf.
5. Sitzungsschicht: ist u. a. für die Herstellung der Verbindung zweier Computer zuständig.
6. Präsentationsschicht: übersetzt die Daten der Anwendungsschicht in ein allgemeines Übertragungsformat und zurück.
7. Anwendungsschicht: Dienste, welche von den Anwendungsprogrammen benutzt werden, um deren Aufgaben zu erfüllen. Die Anwendungsprogramme selbst (z.B. Internet Explorer) gehören nicht zur Schicht.

<sup>1)</sup> Manche Literatur bezeichnet das Kabel als Schicht 0.

Wie habe ich mir das vorzustellen? Wenn Sie mit jemandem sprechen, kommen im Prinzip ähnliche Verfahrensweisen zustande. Bedenken Sie, daß „sprechen“ für Sie vermutlich ganz selbstverständlich ist. Ihre Gedanken sind die Anwendungsschicht,

Ihr Gehirn verkörpert die Präsentationsschicht, die Sitzungsschicht und die Transportschicht. Dann kommen die Nervenbahnen und Muskeln, welche die Stimmbänder und den Mund steuern – also die Netzwerkschicht und Datenschicht. Die Stimmbänder und der Mund stellen in dieser Analogie die physische Schicht dar. Datenübertragung ist für Computer das, was für den Menschen das Sprechen ist.

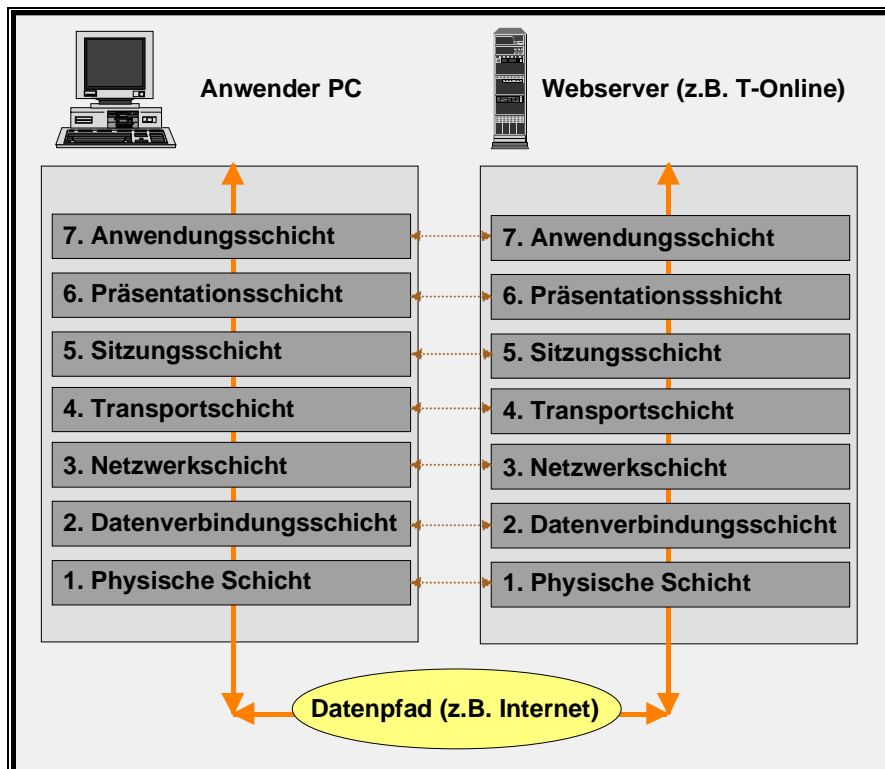


Abbildung 2: Das OSI-Schichtenmodell.

### 3.2 Adressierung:

Das hier kennen Sie vermutlich: [www.t-online.de](http://www.t-online.de) ?

Aber kennen Sie auch das hier: 194.25.134.153 oder 212.185.47.88 oder 194.25.134.146?

Bislang nicht?

Nun, ganz einfach: Wenn Sie in Ihrem Browser [www.t-online.de](http://www.t-online.de) eingeben, meinen Sie in Wirklichkeit 194.25.134.153 oder 212.185.47.88 oder 194.25.134.146.

Wenn Sie eine Webseite per URL (wie [www.t-online.de](http://www.t-online.de)) in Ihrem Browser aufrufen, wird diese nämlich (in der Regel von Ihnen unbemerkt) in ihren wahren Namen übersetzt. Nur daß das Ganze kein Name, sondern eine Nummer ist. Genauer eine sogenannte „IP-Nummer“. Probieren Sie es aus, geben Sie anstelle der URL ([www.t-online.de](http://www.t-online.de)) mal eine IP-Nummer ein (z.B. 194.25.134.153). Sofern die Telekom nicht

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

kurzerhand diese Nummer geändert hat, gelangen Sie somit auch auf [www.t-online.de](http://www.t-online.de).

Unter Adressierung [9], [10] bezeichne ich der Einfachheit halber ganz weitläufig die Umsetzung von URLs in IP-Nummern. Zuständig dafür ist der sogenannte DNS Dienst (Domain-Name-Service).

Warum das Ganze? – Weil es einfacher ist [www.t-online.de](http://www.t-online.de) zu behalten als eine dieser 3 Nummern. Zumal diese Nummern häufig geändert werden.

Wenn Sie unter Windows selbst einmal die IP Nummer zu einer URL erfahren möchten, probieren Sie mal den Befehl - nslookup „beliebige URL“ aus (also z.B.: nslookup [www.t-online.de](http://www.t-online.de)). Andererseits könnten Sie sofort, nachdem Sie die URL im Browser eingegeben haben, einen Blick auf die Statuszeile Ihres Browsers werfen. Dort erscheint nämlich für den Zeitraum eines Wimpernschlages die entsprechende Meldung der Umsetzung von URL in die zugehörige IP-Adresse.

Welche Analogie gibt es? Sie wissen, daß Ihr Freund Fritz Müller in Hamburg wohnt, haben aber seine Telefonnummer nicht. In so einem Fall rufen Sie die Telefonauskunft an. Adressierung ist nichts anderes: Ich suche [www.t-online.de](http://www.t-online.de), wie ist die IP-Nummer dazu?

### 3.3 Ports:

Daß Webseiten eigentlich unter ihrer IP Nummer zu finden sind, wissen Sie jetzt. Aber da fehlt noch etwas. Wenn Sie [www.t-online.de](http://www.t-online.de) eingeben, meinen Sie nämlich nicht bloß 194.25.134.153, sondern genauer: <http://194.25.134.153:80>.

Hierin sind noch zwei weitere Ergänzungen zu finden, wovon die letzte (also die :80) den sogenannten Port [11], [12] und das <http://> das gewünschte Protokoll (siehe Abschnitt 3.4) darstellt.

Ports gibt es 65535 Stück, wovon die ersten 1024 die sogenannten „well known“ Ports sind [11], [12]. Port Nummer 80 steht in der Regel für HTTP. Oder genauer spricht Port 80 einen Webserver an, um per „http“ Webseiten abzurufen.

Weitere häufig benutzte Ports sind zum Beispiel:

Port	Dienstname	Zweck
20	aktives FTP	dient dem Datenaustausch per FTP
21	passives FTP, aktives FTP	dient dem Datenaustausch per FTP
22	SSH	dient dem verschlüsselten Fernzugriff auf Computer
23	Telnet	dient dem Fernzugriff auf Computer
25	SMTP	dient dem Versenden von E-Mails
53	DNS	dient dem Umwandeln von URLs in IP-Nummern
80	http	dient dem Bereitstellen von Webseiten
110	POP3	dient dem Empfangen von E-Mails
135	RPC	dient der Kommunikation zwischen Computern

Zum Linnegraben 46      Telefon: +49 (069) 395955      e-mail: oliver.klarmann@ingbuero-klarmann.de  
65933 Frankfurt am Main      Fax: +49 (069) 38013651  
Mobil: +49 (0179) 2001336

137-139	NetBIOS	dient der Kommunikation zwischen Windows-Computern
443	HTTPS	verschlüsseltes HTTP (Port 80)
445	MS-DS (SMB Direct Hosting)	dient der Kommunikation zwischen Windows-Computern
5000	UPnP	dient der Kommunikation zwischen Netzwerkgeräten
8080	Proxy	dient meist der Kommunikation über einen Proxy-Server

Wie können Sie sich das vorstellen? Nehmen Sie ein Einkaufszentrum mit vielen Türen. Hinter jeder Tür verbirgt sich ein anderes Geschäft mit seinen Dienstleistungen. Hinter Tür 1 könnte ein Bäckermeister seine Waren anbieten, hinter Tür 5 der Metzger, und bei Tür Nummer 79 können Sie vielleicht Schuhe kaufen. Der Unterschied ist, daß im Internet hinter Tür 79 in der Regel immer der Schuhverkäufer sitzt, egal in welches Einkaufszentrum sie hineingehen. Übrigens muß man sich nicht daran halten. Niemand hält den Schuhverkäufer davon ab, seine Waren hinter Tür 37 anzubieten. Das muß er dann den Kunden allerdings mitteilen, weil diese aus Gewohnheit immer hinter Tür 79 suchen.

### 3.4 Protokolle:

Damit die Punkte 3.1 bis 3.3 auch irgendwie Sinn ergeben, sind noch die Protokolle [13] notwendig. Ein Protokoll können Sie sich wie eine Sprache vorstellen (genau genommen ist eine Sprache ein Protokoll!). Im Internet kommt die sogenannte TCP/IP-Protokoll-Familie zum Einsatz. TCP/IP legt fest, wie die Abwicklung der Kommunikation funktioniert. Jedoch ist es für diese Aufgabe nicht allein zuständig, sondern erledigt davon nur einen Teil. Deshalb sind weitere Protokolle daran beteiligt z.B. UDP, PPPoE, PPP, PPTP, HTTP, FTP, etc.

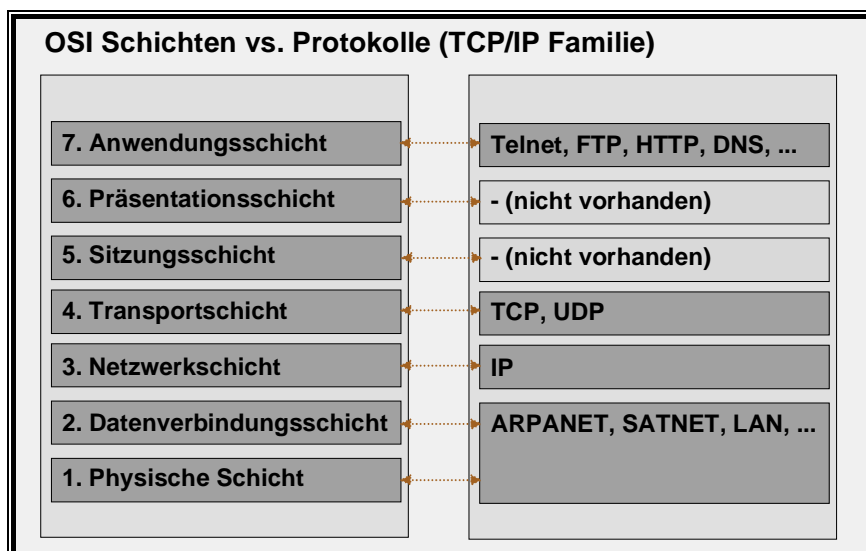


Abbildung 3: Das OSI-Schichtenmodell, verglichen mit den Protokollen der TCP/IP-Protokoll Familie. Quelle: [14]

### 3.5 Wo die Desktop Firewall ansetzt:

Damit eine Desktop Firewall funktionieren kann, drängelt sie sich nun zu den Protokollen und Netzwerkschichten und belauscht, welche Daten (Pakete – daher „Paketfilter“) an welche IP-Nummern und Ports gesendet werden bzw. welche empfangen werden. PFWs achten zudem darauf, welche Anwendung den Datenverkehr veranlaßt hat.

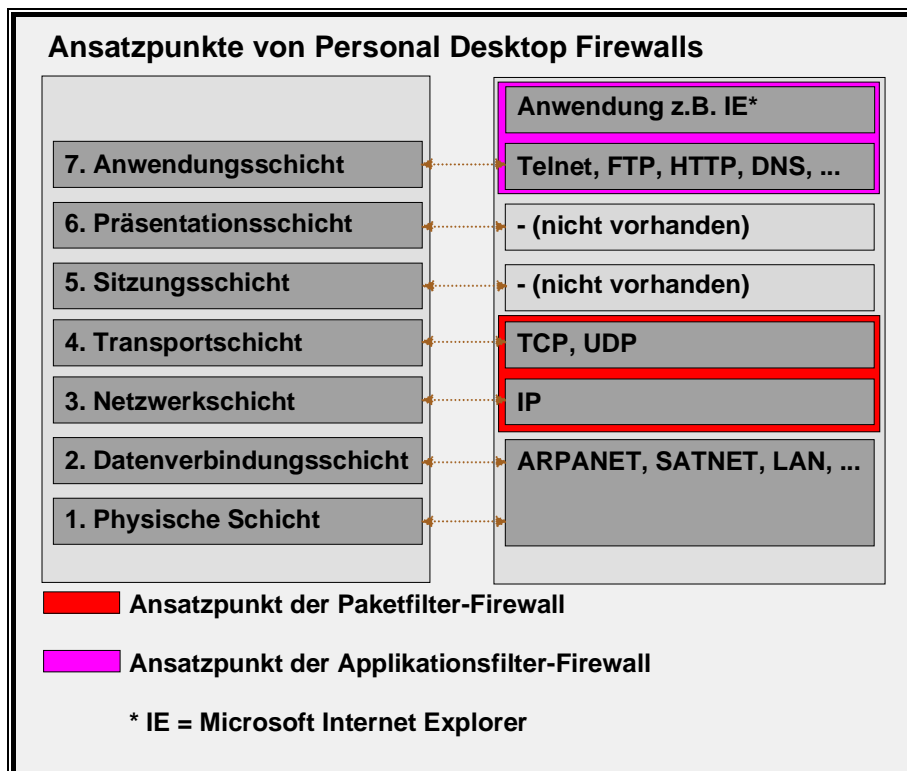


Abbildung 4: Ansatzpunkte von Paketfilter- und Applikationsfilter-Firewalls.

Wenn Sie zum Beispiel im Internet-Explorer die Webseite von T-Online aufrufen, registriert die Firewall etwa folgendes:

Ein Prozeß namens iexplore.exe in z. B. Version 6.00.2800.1106 möchte den vorgegebenen DNS-Server (z.B. 62.225.252.16) auf Port 53 nach der IP-Adresse von [www.t-online.de](http://www.t-online.de) befragen. Er erwartet die Antwort auf der eigenen IP-Adresse (z.B. 62.225.137.65) und Port 1025.

Daraufhin bemerkt die Firewall nachstehendes: Ein Computer mit der IP 62.225.252.16 sendet an IP 62.225.137.65 auf den Port 1025 die IP-Nummer 194.25.134.153, welche zu [www.t-online.de](http://www.t-online.de) gehört.

Als Reaktion wiederum wird nun der Prozeß iexplore.exe versuchen eine Anfrage an die 194.25.134.153 auf Port 80 zu stellen und erwartet die Antwort auf 62.225.137.65 und Port 1026.

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

Als letztes stellt die Firewall fest, daß ein Computer mit der IP 194.25.134.153 Daten an 62.225.137.65 auf Port 1026 senden will.

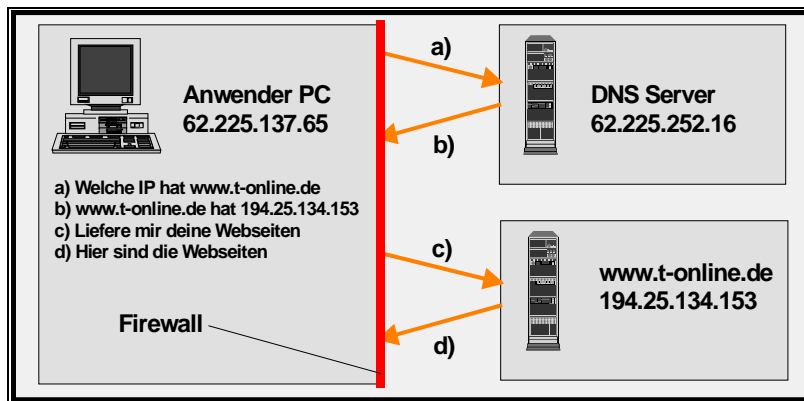


Abbildung 5: Ablauf zum Aufrufen der Webseiten von [www.t-online.de](http://www.t-online.de)

Solange die Firewall dabei nicht eingreift, wird im Browser jetzt die Webseite von T-Online erscheinen.

Je nachdem welche Desktop Firewall Sie benutzen (oder benutzen möchten), haben Sie jetzt verschiedene Möglichkeiten, diese Kommunikation zu beeinflussen. Sie könnten der Firewall z.B. sagen, daß sie Zugriffsversuche eines Prozesses mit dem Namen iexplore.exe und der Version 6.00.2800.1106 auf IP-Adressen außerhalb des eigenen Netzwerks (oder Computers) unterbinden soll. Als Ergebnis wird der Browser Ihnen die Fehlermeldung anzeigen, daß er die Webseite nicht finden konnte.

Es gibt Desktop Firewalls, die im Prinzip nur nach Prozessen filtern. Dazu gehört z.B. ZoneAlarm von ZoneLabs [15] (Ab Version 3.x sind auch begrenzte Filterungen nach Ports möglich).

Bessere Desktop Firewalls filtern nach Protokollen und IP-Adressen sowie Ports.

Damit könnten Sie dann ganz klar vorgeben, daß ein Zugriff von Ihrem PC an die IP-Adresse 194.25.134.153 auf Port 21 verboten ist, während ein Zugriff an diese IP auf Port 80 durchaus zustande kommen darf.

### 3.6 Warum auch Ihr Rechner möglicherweise in Gefahr ist:

Der Grund, aus dem auch Sie eine Desktop Firewall benutzen möchten ist, daß auch Ihr PC dem Internet Dienste [16], [17] (also offene Ports) zur Verfügung stellt. Fast immer stellt Windows z.B. seine Kommunikationsdienste auf den Ports 137-139 nach außen offen dar. Aber genau über diese Ports (verantwortlich ist die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“) kann jeder auf Ihre Festplatte zugreifen oder Ihren Drucker benutzen. Und das ist ja nur ein Dienst. Auf einem Standard-Windows-PC laufen oftmals mehrere Dutzend „offene“ Dienste, je nachdem welche Software installiert ist. Probieren Sie es aus, geben Sie in der Eingabeaufforderung

Zum Linnegraben 46      Telefon: +49 (069) 395955      e-mail: oliver.klarmann@ingbuero-klarmann.de  
65933 Frankfurt am Main      Fax: +49 (069) 38013651  
Mobil: +49 (0179) 2001336

den Befehl „netstat -a“ ein (Bei Windows 2000/XP). Alles, was dieser jetzt anzeigt, sind laufende Dienste in unterschiedlichen Zuständen. Wenn Sie Windows XP benutzen und das Service Pack 2 installieren, wird die bereits in älteren XP-Versionen vorhandene XP Firewall standardmäßig aktiviert. Zudem wird die Funktionalität der XP Firewall durch das SP 2 drastisch erhöht. Bei einer regulär laufenden Windows-XP-SP2-Installation sollten fürs erste keine Dienste nach außen zur Verfügung gestellt werden. Allerdings läßt sich auch die Microsoft-eigene-Firewall relativ einfach umgehen [18].

```

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Dokumente und Einstellungen\Administrator>netstat -a

Aktive Verbindungen

Proto Lokale Adresse Remoteadresse Status
TCP klw2k-ce11200:epmap klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:microsoft-ds klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:1025 klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:1027 klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:1029 klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:1031 klw2k-ce11200:0 ABHÖREN
TCP klw2k-ce11200:1031 klw2k-ce11200:2638 HERGESTELLT
TCP klw2k-ce11200:1031 klw2k-ce11200:2638 ABHÖREN
TCP klw2k-ce11200:2638 klw2k-ce11200:1031 HERGESTELLT
UDP klw2k-ce11200:microsoft-ds *:*
UDP klw2k-ce11200:1032 *:*
UDP klw2k-ce11200:1345 *:*
UDP klw2k-ce11200:1347 *:*
UDP klw2k-ce11200:2638 *:*

C:\Dokumente und Einstellungen\Administrator>

```

Abbildung 6: Ergebnisse eines Aufrufes von „netstat -a“ in einer Windows-2000-Konsole. Deutlich zu sehen: 7 Dienste warten auf Anfragen (Status Abhören), und 2 Dienste haben eine Verbindung „hergestellt“.

### Zusammenfassung:

Desktop Firewalls schützen Ihren PC, indem sie Zugriffe von oder auf Ihren Computer, auf Applikations- oder Protokoll-Ebene, im Rahmen des Schichtenmodells verhindern.

## 4. Nutzen von Personal Desktop Firewalls?

O.K., wir hatten jetzt viel Theorie über Netzwerke und Internetverbindungen. Wenden wir uns jetzt der spannenden Frage zu, warum Desktop Firewalls nutzlos sind.

Eingangs wurde ja bereits gesagt, daß PFWs auf demselben PC laufen, den sie schützen sollen.

Die Ursache liegt im Schichtenmodell. 7 Schichten, welche die Daten durchlaufen müssen, um ans Ziel zu gelangen. Das Problem ist, daß eine PFW nicht die unterste Schicht kontrollieren kann. In der Regel klinkt sich eine PFW in die Transportschicht oder die Netzwerkschicht ein. Das heißt, sie ändert die Kommunikation so ab, daß

Zum Linnegraben 46      Telefon: +49 (069) 395955      e-mail: oliver.klarmann@ingbuero-klarmann.de  
65933 Frankfurt am Main      Fax: +49 (069) 38013651  
Mobil: +49 (0179) 2001336

die PFW diese Schichten auf derselben Ebene überwacht, durch die alle Daten hindurchmüssen. Dies erreicht sie z.B. dadurch, daß sie die entsprechenden Dateien des Betriebssystems ersetzt oder ergänzt.

Ja - ist doch gut oder? Alle Daten müssen durch diese 7 Schichten, und wenn sich die Firewall dazugesellt, bekommt sie alles mit, was so läuft.

Das funktioniert, solange alle Programme die entsprechenden Betriebssystemdateien zur Kommunikation benutzen. Das Dumme an der Sache ist, daß niemand ein Programm zwingt, sich ans Betriebssystem zu halten. Jeder Software steht es frei, ihr eigenes Schichtenmodell mitzubringen und mit einem eigenen Treiber direkt mit der ISDN- oder Netzwerkkarte zu reden.

Das heißt: Die Firewall sitzt bei Schicht 3 oder 4. Wenn ein unfreundliches Programm die Schichten 3-7 selbst mitbringt und direkt auf Schicht 2 aufsetzt, bekommt die PFW davon nichts mit. Sie kann und wird davon niemals etwas erfahren.

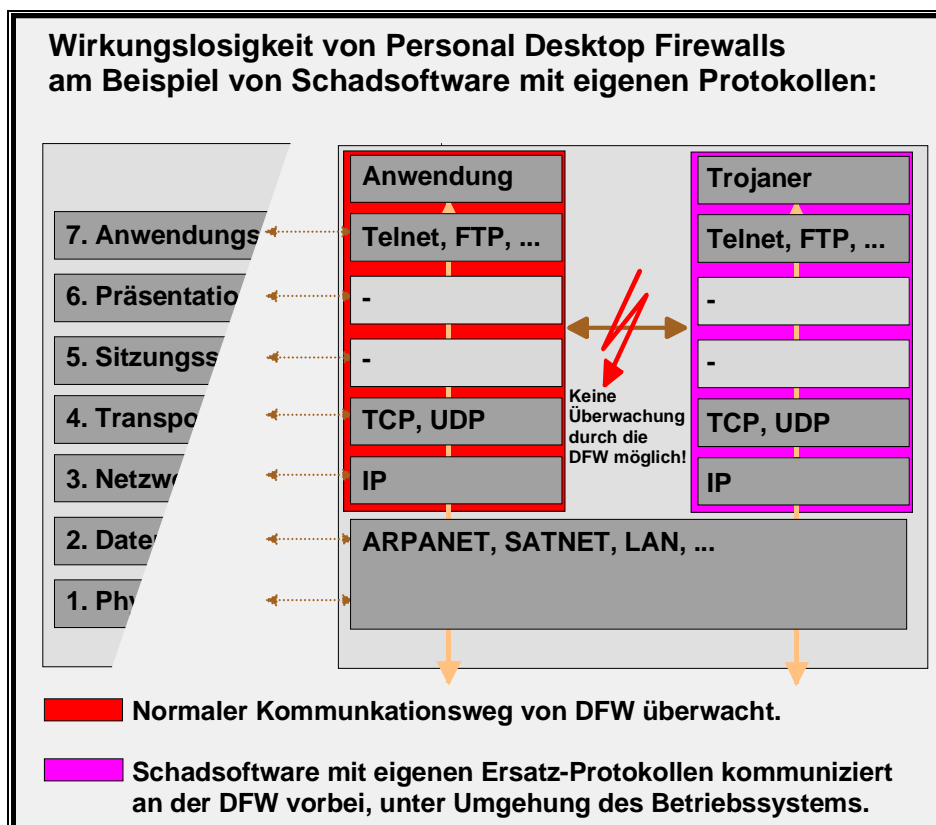


Abbildung 7: Umgehung der Desktop Firewall durch einen Trojaner, der eigene Protokolle zur Kommunikation mitbringt.

Analogie: Wenn der Schuhhändler hinter Tür 79 böse ist und einen Tunnel zu seinem Geschäft gräbt, kann die Tür ruhig bewacht werden – die benutzt ja niemand!

Ein weiteres großes Problem, warum PFWs nicht sicher sind, liegt in Windows begründet. Eine PFW kann von böswilliger Software (z.B. von einem per E-Mail erhal-

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

tenen Trojaner) einfach ausgeschaltet werden. Davon bekommen Sie als Anwender vermutlich nicht einmal etwas mit, weil das typische Programmsymbol, rechts neben der Uhr in der Taskleiste, meistens erhalten bleibt. Einziger Schutz dagegen wäre, daß Sie nicht als Administrator arbeiten, was bei Windows leider nicht der Standard ist. Welche Konsequenzen dies nach sich zieht, erfahren Sie in der c't 15/2004 auf den Seiten 110ff und 118ff.

Eine Firewall, welche also verhindern soll, daß ein Trojaner [19], [20] Dienste auf einem PC anbietet und Daten verschickt, kann von eben diesem Trojaner einfach beendet werden. Dieses Problem ist von prinzipieller Natur und liegt im Design von Windows und den üblichen Personal Desktop Firewalls selbst begründet.

Letztendlich könnte eine „böse“ Software auch einfach eine „brave“ Software (die zugelassen ist) mißbrauchen. Anders ausgedrückt: Ihrer Firewall haben Sie gesagt, daß der Internet-Explorer ins Internet senden darf. Niemand hält einen Trojaner davon ab, seine Kommunikation so zu gestalten, daß er dafür den Internet Explorer verwendet. Für die Firewall sieht das so aus, als wolle der Internet Explorer eine Webseite abrufen – in Wahrheit wird dieser aber ferngesteuert! Einigen Firewalls fällt diese Fernsteuerung auf, sicher ist dies aber nicht.

#### Zusammenfassung:

PFWs sind deshalb nutzlos, weil sie einfach umgangen bzw. abgeschaltet werden können. Diese Ursachen sind prinzipiell vorhanden und können nicht ohne weiteres verhindert werden.

## **5. Wie kann ich meinen Computer ohne Desktop Firewall schützen?**

Nun, die Sache ist ganz einfach und kostet Sie nicht mal Geld! In Abschnitt 3.3 haben Sie die Ports kennengelernt. Jegliche Kommunikation eines Computers mit dem Internet läuft über diese Ports (65535 Stück). Hinter jedem Port, der offen ist (siehe Test in Abschnitt 2), steckt ein Dienst – also ein Programm (eine Software).

Sie müssen nur verhindern, daß diese Programme ihre Dienste im Internet anbieten. Wie das funktioniert, lesen Sie hier: [21], [22].

Bei Windows betrifft dies den „Client für Microsoft-Netzwerke“ und die „Datei- und Druckerfreigabe für Microsoft-Netzwerke“. Um diese abzuschalten, müssen Sie einfach nur die sogenannten Bindungen lösen. Je nach Windows-Version und Trägermedium ist dies unterschiedlich zu bewerkstelligen. Wenn Sie z.B. Windows 2000 besitzen und über eine ISDN-Karte ins Internet gehen, haben Sie keine Sorgen. Bei

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

dieser Konstellation sind die Bindungen standardmäßig nicht gesetzt. Bei allen Systemen vor Windows 2000 müssen Sie das aber ändern. Bei Netzwerkkarten, die direkt mit einem DSL-Modem verbunden sind, müssen Sie diese Bindungen auch entfernen.

Mit dem Test in Abschnitt 2 können Sie den Erfolg der Maßnahme sogleich testen (ggf. müssen Sie Ihren PC noch einmal neu starten, bevor die Änderungen wirksam werden). War beim ersten Test der NetBIOS Port „Open“, sollte er jetzt „Closed“ sein, sofern auch „NetBIOS über TCP/IP“ abgeschaltet wurde!

Diese Prozedur müssen Sie für alle offenen Ports (Dienste) wiederholen. Sie müssen herausfinden, welches Programm für diesen Port verantwortlich ist, und in den Konfigurationseinstellungen dieser Software entsprechende Änderungen vornehmen.

Auf einem Einzel-PC, der direkt mit dem Internet verbunden ist, ist dies im Prinzip problemlos möglich. Sollte danach irgendeine Software nicht mehr laufen, muß der zuständige Dienst einfach wieder eingeschaltet werden. In diesem Fall sollten Sie weitere Informationen einholen: Um was für eine Art Dienst handelt es sich, und stellt dieser eine potentiell gefährliche Sicherheitslücke dar oder nicht. Fragen Sie einfach den Hersteller dieser Software, inwieweit es möglich ist, den Dienst auf den lokalen PC zu beschränken.

Ist dies nicht möglich, kann dies einer der ganz seltenen Fälle sein, in dem die Verwendung einer PFW sinnvoll ist.

Ist ein offener Port allerdings zu einem Trojaner gehörig, von dem Sie bislang gar nicht wußten, daß er überhaupt auf Ihrem PC ist, sollten Sie mit einem aktuellen Viren- oder Trojanerscanner [23], [24] Ihr Glück versuchen.

### Zusammenfassung:

Probleme entstehen durch Dienste und deren „offene“ Ports, die Ihre Anwendungen bzw. Ihr Betriebssystem bereitstellt. Wenn Sie diese Dienste beenden (Ports schließen), brauchen Sie auch keine PFW. Merke: Wo keine Tür ist, kann auch niemand durch sie hindurchgehen!

## **6. Sind dann aber nicht auch Hardware Firewalls nutzlos?**

Nein, „richtige“ Firewalls sind nämlich eigene Geräte, welche „vor“ dem zu schützenden PC sitzen. Auf unser Schichtenmodell bezogen bedeutet dies, daß sie in der Lage sind, alle Schichten zu kontrollieren. Die Verbindung von Ihrem PC zum Internet wird nämlich durch die Firewall unterbrochen. Somit muß definitiv die gesamte Kommunikation durch die Firewall hindurch.

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

Wieder ein Vergleich: Der böse Schuhverkäufer hatte ja einen Tunnel gegraben, damit man die Tür nicht benötigt. Dieser Tunnel kommt allerdings gleich neben der Tür heraus. Das ist die Situation mit einer PFW. Eine „richtige“ Firewall (auch Hardware Firewall genannt) müssen Sie sich als großen Parkplatz vorstellen, der das gesamte Einkaufszentrum umringt und von einer sehr hohen und dicken Mauer umgeben ist, welche nur ein Tor besitzt. Da alles, was zu dem Schuhverkäufer gelangt oder von ihm weg will, durch dieses Tor hindurchmuß, kann man es kontrollieren. Natürlich kann der Schuhverkäufer einen längeren Tunnel graben (oder einen zweiten neuen Tunnel). Auf Ihren PC umgesetzt bedeutet das allerdings, daß jemand von der Straße her ein neues Kabel in Ihr Haus legt. Das wird Ihnen doch hoffentlich auffallen? Gegeben hat es so etwas natürlich schon, aber da war der Wert der Daten den Dieben Aufwandsentschädigung genug.

Sie sollten nur verhindern, daß das Tor offensteht. Es sollte immer geschlossen sein und nur bei tatsächlichem Bedarf für kurze Zeit einen kleinen Spalt weit geöffnet werden. Auf die Hardware Firewall übertragen bedeutet das, daß das Gerät richtig konfiguriert (programmiert) werden muß – und das ist in der Regel recht kompliziert und erfordert viel Fachwissen.

Es ist zwar auch möglich, Hardware Firewalls zu umgehen (fachlich: zu tunneln) [25], [26], [27], Dafür ist aber sehr viel Know-how und oft auch der physische Zugang erforderlich. Wenn Sie nicht gerade Dieter Zetsche heißen und Ihre Firma DaimlerChrysler, wird kaum jemand diesen Aufwand betreiben, um Ihren PC zu hacken. Für den Fall einer getunnelten Firewall gibt es Intrusion Detection Systeme (kurz: IDS) – also Eindringlings-Erkennungssysteme [28], [29], [30] –, die dies feststellen können. Für unser Einkaufszentrum wäre das der Wachschatz.

Hardware Firewalls sind in der Regel sehr teuer, einige günstige Geräte werden in Abschnitt 9 erwähnt.

### Zusammenfassung:

Hardware Firewalls sind in der Lage, wirklich den gesamten Datenverkehr Ihres PCs zu kontrollieren. Die richtige und vollständige Konfiguration vorausgesetzt, können sie nicht ohne weiteres umgangen werden.

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

## **7. Was muß ich beachten, wenn ich trotz allem eine Personal Desktop Firewall einsetzen möchte?**

Vor allem dürfen Sie sich nicht in falscher Sicherheit wiegen!

Sie sollten bei allem, was Sie an Ihrem PC tun, bedenken, daß Sie nicht wirklich geschützt sind. Wenn Ihnen jemand per E-Mail einen Trojaner schickt, der in der Lage ist, Ihre PFW zu umgehen oder anzuschalten, und Sie diesen ausführen, nutzt Ihnen die beste PFW wenig.

Einen guten Schutz bietet ein täglich aktualisierter Virenschanner. E-Mail-Software und Browser müssen sicher konfiguriert sein. Programme/Dateien, die aus dem Internet heruntergeladen werden und E-Mails mit Anhang, sollten sehr kritisch betrachtet werden.

Wenn Sie eine PFW einsetzen, werden Sie feststellen, daß Ihnen das Programm alle 1 bis 2 Minuten etwas von einem Angriff auf Ihren Computer erzählt.

Wenn es sich um unterschiedliche IP Nummern und Ports handelt, von denen diese vermeintlichen Angriffe ausgehen, sind es keine Angriffe, sondern sogenannte „Port Scans“ – irgend jemand fragt alle Ports Ihres Rechners ab, ob sie offen sind. Aber warum gerade Ihren PC? Das macht der doch mit Absicht?

Nein, tut er nicht! Er verwendet einen Port-Scanner und fragt damit einfach tausende von IP Nummern und Ports in rascher Folge ab. Sein Port Scanner meldet ihm, was er gefunden hat, und wenn er das interessant findet, dann kommt er wieder. Dumm nur, daß Sie vermutlich eine „Dial UP“-Internetverbindung benutzen und schon gar nicht mehr online (Drinnen) sind. Außerdem erhalten Sie von Ihrem Provider bei jeder neuen Internetverbindung eine andere IP Nummer zugewiesen. Also kann er Sie nicht wiederfinden. Er kann Sie neu entdecken, aber das kennen Sie ja jetzt ...

Diese Port Scans werden meist von „Script Kiddis“ durchgeführt. Junge Leute, die sich einen Port Scanner besorgt haben und gar nicht wissen, was sie da eigentlich tun.

Vergleichen Sie es am ehesten damit, daß jemand eine Straße entlanggeht und an allen Autos prüft, ob sie verschlossen sind. Dies ist zwar unschön, aber nicht verboten! [31].

### Zusammenfassung:

Wenn Sie eine PFW einsetzen, bedenken Sie bitte, daß PFWs nicht wirklich sicher sind. Verwenden Sie einen aktuellen Virenschanner, öffnen Sie verdächtige E-Mail-Attachments nicht. Schön, daß Ihre Kollegen Ihnen gerne irgendwelche witzigen

---

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
---	---	--

---

Dinge per E-Mail schicken, aber dies ist höchst bedenklich. Löschen Sie solche E-Mails, ohne sie anzuschauen, und sagen Sie dem Absender, daß Sie so etwas nicht haben möchten. Wenn der Ihnen dann noch entgegnet, daß er Ihnen gar nichts geschickt hat, sollten sie ihn darauf aufmerksam machen, daß er sich vermutlich einen Virus oder Trojaner eingefangen hat.

## **8. Firewall ist ein Konzept und kein Programm!**

Das meiste, was in dieses Kapitel gehört, wurde bereits erwähnt. Sicherheit ist dynamisch, es reicht nicht aus, einmal eine Hardware Firewall zu installieren und diese dann zu vergessen. So wie für Ihre normalen Programme, gibt es auch für Ihre Hardware Firewall Updates. Diese Updates beseitigen Fehler in Ihrer Firewall, beziehungsweise bringen ihr neue Möglichkeiten bei. Auch wird sie damit auf neue Sicherheitsprobleme vorbereitet, die noch unbekannt waren, als Sie von Ihnen gekauft wurde.

Eine Firewall alleine reicht nicht. Sie benötigen auf jeden Fall einen guten und zuverlässigen Virens scanner. Der Virens scanner sollte mindestens täglich aktualisiert werden.

Der Internet Explorer und Outlook bzw. Outlook Express bieten sehr vielfältige Möglichkeiten, Browser und E-Mail-Programm zu sichern. Möglicherweise können Sie einige Internetseiten nicht mehr betrachten. Dies ist dann so! – Sie müssen sich entscheiden, was für Sie wichtiger ist. Ihre Sicherheit oder sich eine bunte Webseite betrachten zu können. Würden Sie bei Aldi einkaufen gehen, wenn man Sie zwingt eine grüne Mütze, einen gelben Schal und rote Pantoffeln zu tragen: – Nein? Warum lassen Sie sich dann vorschreiben, was Sie tun sollen, um eine Webseite anzusehen!

Ein Webseitenbetreiber, der viele Voraussetzungen von Ihnen verlangt, will nicht, daß Sie seine Webseite betrachten. Dies gilt vor allem für „Cookies“ [32], [33]. Technisch sind diese Schnüffler nicht mehr erforderlich. Sie zeigen nur die Bequemlichkeit des Betreibers, der auf Ihre Kosten sparen will.

Sind Sie geschäftlich auf eine Webseite angewiesen (Online Banking, Ausschreibungssysteme, Projektnetzwerke etc.), dann nehmen Sie diese in die „vertrauenswürdigen Seiten“ des Internet Explorer auf. Für diese Seiten können Sie andere Sicherheitseinstellungen wählen.

Wenn möglich, verzichten Sie gänzlich auf den Internet Explorer oder Outlook (Express). Es gibt genug Alternativen für Windows, die nicht schlechter sind.

Deinstallieren Sie den Windows Scripting Host (WSH). Wenn Sie nicht wissen, was das ist, ist die Wahrscheinlichkeit, daß Sie diesen benutzen, eher gering [34].

---

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
---	---	--

---

Überlegen Sie immer gut, was Sie gerade im Internet tun. Öffnen Sie keine E-Mail-Anhänge, die Sie nicht angefordert haben, und laden Sie Dateien nur von vertrauenswürdigen Quellen herunter.

### Zusammenfassung:

Firewalls und Virens Scanner sind wichtig und notwendig, viel wichtiger ist aber Ihr Verhalten. Wenn Sie sich falsch verhalten, werden Ihnen die beste Firewall und der beste Virens Scanner nichts nützen. Lassen Sie sich nicht den Willen von irgendwelchen Webseiten aufzwingen. Webseiten, die Sie nur mit niedrigen Sicherheitseinstellungen betrachten können, wollen nicht betrachtet werden! Sie sind schlecht gemacht, und der Auftraggeber hat viel Geld verschwendet. Technisch läßt sich so etwas auch anders ermöglichen. Ihre Sicherheit sollte wichtiger sein als die Bequemlichkeit des Webseitenbetreibers. Apropos, wie verhält es sich eigentlich mit Ihrer eigenen Webseite?

## **9. Guter Schutz für wenig Geld – (DSL) Hardware Router:**

Eine richtige Hardware Firewall ist für Sie vermutlich der Overkill. Es ist schwierig, sie richtig einzustellen, und man benötigt weitere Geräte, um die Kiste überhaupt anschließen zu können. Unter anderem benötigt man dafür in vielen Fällen einen Router [35]. Ein Router<sup>2)</sup> ist allerdings ein sehr interessantes Gerät – unter anderem dann, wenn man Zugriffe von außen verhindern will.

2) Ich gehe hier von den handelsüblichen DSL/ISDN-Routern aus, deren Funktion den Einsatz von NAT voraussetzt. NAT ist für diese Art von Routern die Funktionsgrundlage. Normale Netzwerkrouter verwenden in der Regel kein NAT, dazu später mehr.

Sie haben ja mittlerweile IP Nummern kennengelernt und auch etwas über Adressierung gelesen.

Nun verhält es sich so, daß „vollwertige“ IP Nummern theoretisch von 1.0.0.0 bis 126.255.255.255 bzw. von 128.0.0.0 bis 191.255.255.255 und von 192.0.0.0 bis 223.255.255.255 denkbar sind. Die Realität sieht anders aus! Die Normierung für IP Nummern sieht dabei viele Ausnahmen und Besonderheiten vor [36].

Eine dieser Besonderheiten sind die „privaten“ IP Nummern [36], [37]. Diese IP Nummern entsprechen den Nummernkreisen:

- 10.0.0.0 bis 10.255.255.255
- 172.16.0.0 bis 172.31.255.255
- 192.168.0.0 bis 192.168.255.255

---

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
---	---	--

---

Alle diese IP Nummern werden im Internet nicht „geroutet“, das bedeutet, daß sie im Internet nicht „adressierbar“ sind. Und da sie nicht adressierbar sind, kann man einen PC, der eine solche Nummer besitzt, nicht über das Internet erreichen.

Ihr PC sollte also eine private IP Nummer besitzen.

Ja was? Wie soll ich denn dann im Internet surfen? Ein Webserver kann ja nichts an mich weiterleiten.

Stimmt! - Genau das wollen wir ja, niemand soll an Ihren PC etwas weiterleiten können. Der entscheidende Punkt ist der Router.

Ein Router beherrscht nämlich normalerweise NAT (Network Address Translation) [38], [39]. Ein Router ist in der Lage, seine „öffentliche“ (offizielle und adressierbare) IP-Nummer auf Ihre interne (und private) IP-Nummer umschreibt.

Aber was bringt das dann, wenn er die einfach umschreibt?

Keine Angst, er wird nicht einfach seine IP-Nummer umlegen, das ist schon etwas komplizierter. Der Router merkt sich, daß Sie in ihrem Browser eine Webseite aufrufen wollen. Genau genommen speichert er die Information, daß der interne Rechner mit z.B. der IP Nummer 192.168.1.7 eine Anfrage an z.B. <http://194.25.134.153:80> gestellt hat. Und die Antwort von 194.25.134.153 auf Port 1025 erwartet. Wenn jetzt der Webserver von T-Online mit der IP-Adresse 194.25.134.153 darauf reagiert, erkennt der Router, daß es sich um eine „Antwort“ handelt, und leitet diese entsprechend weiter.

Wenn der Webserver von T-Online diese Daten von sich aus schicken würde, bekäme er vom Router die Antwort: Die hat niemand angefordert, also hör' gefälligst auf!

Wenn Sie jetzt einen guten Router gekauft haben, wird dieser keine Dienste, d.h. keine offenen Ports nach außen anbieten. Probieren Sie mit Ihrem Router noch mal die Tests aus Abschnitt 2. Sie werden feststellen, daß alles „dicht“ ist.

Allerdings verhindert der Router nicht, daß Sie sich einen Trojaner einfangen. Da Trojaner eine Verbindung von innen nach außen aufbauen und auf Antworten warten und der Router Antworten weiterleitet, wären Sie also doch wieder von außen erreichbar. Somit sind wir wieder bei Kapitel 8.

Handelsübliche Router sind mittlerweile mit einfachen Firewalls ausgestattet. Das sind Ideal-Produkte für einfache Anwendungsfälle. Natürlich müssen diese Firewalls richtig konfiguriert werden – siehe Abschnitt 6. Einfache Firewalls sind übrigens in der Tat einfach: Sie lassen meistens nur eine eingeschränkte Konfiguration zu, die den Namen „Firewall“ streng genommen nicht verdient. Router mit richtigen Firewalls sind ein gutes Stück teurer und sehr komplex in der Konfiguration, z. B. von Lancom Systems – [www.lancom-systems.de](http://www.lancom-systems.de).

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

Eines soll nicht verschwiegen werden: Der NAT-Mechanismus der Router ist nur ein Nebenprodukt. Die Hauptaufgabe eines Routers ist es nicht, Sie vor Angriffen zu schützen. Dafür gibt es Hardware Firewalls. Die Hauptaufgabe eines Routers ist, zwei verschiedene Netzwerke miteinander zu verbinden. DSL/ISDN-Router bilden dabei eine Router-Unterart, die mit Hilfe von NAT mehrere Computer mit einer einzigen Verbindung ins Internet bringt.

#### Zusammenfassung:

DSL/ISDN Router schützen Sie gegen Zugriffe (Angriffe) von außen dadurch, daß sie Ihren Rechner hinter sich selbst verstecken. Gegen Probleme (also Trojaner) von innen schützen Router im Normalfall nicht. Der Schutz ist allerdings nur ein willkommener Nebeneffekt der verwendeten Technik.

## **10. Die Rolle der Fachzeitschriften und Testmagazine:**

In der Fachzeitschrift XY wurden Personal Firewalls getestet. Ein Produkt ist „sehr gut“ getestet und wird empfohlen. Also was steht in diesem Text hier eigentlich für ein Mist – was stimmt denn nun?

Wenn Sie den Text hier aufmerksam gelesen und auch verstanden haben, können Sie sich die Frage bereits selbst beantworten, gegebenenfalls nachdem Sie auch die weiterführenden Information unter den Abschnitten 12 und 13 gelesen haben.

Aber ich sage es mal anders: Das Problem ist die Fragestellung. Die Testmagazine stellen nämlich nicht die Frage: Ist eine Desktop Firewall sinnvoll, sondern: Tut die PFW das, was auf deren Verpackung steht?

Ja, das tut sie – ohne Frage! Dabei bleiben aber die prinzipiellen Probleme der PFWs außen vor.

Außerdem wollen diese Magazine Geld verdienen. Dies tun sie, u.a. indem sie Computerprodukte testen. Da der Markt nun mal Desktop Firewalls anbietet, werden diese auch getestet.

Wenn Sie jetzt allerdings lieber einer „renommierten“ Fachzeitschrift glauben wollen, wird Sie niemand davon abhalten.

Vielleicht sollten Sie diese Frage einmal in einer Firewall-Newsgroup [40], [41] stellen. Dort werden Sie auf Menschen treffen, deren tägliches Brot es ist, mit Firewalls umzugehen. O.K., ich korrigiere mich, das sind keine Menschen, das sind wandelnde lebendige Firewalls! Das sind absolute Profis, die können Ihnen sogar erzählen, daß

---

Zum Linnegraben 46 65933 Frankfurt am Main	Telefon: +49 (069) 395955 Fax: +49 (069) 38013651 Mobil: +49 (0179) 2001336	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
---	---	--

---

im Weißdruck zur Norm für das IP Protokoll (welches für Firewalls sehr wichtig ist), der 5. Buchstabe, des 7. Wortes auf der 39. Seite 0,3% heller gedruckt wurde als der 2. Buchstabe des 29. Wortes auf Seite 11.

Die kennen sich aus!

Stellen Sie diese Frage besser nicht!

Oder besorgen Sie sich vorher einen Anwalt. Denn wenn Sie diese Frage gestellt haben, werden Sie diejenigen, die darauf antworten, wegen Beleidigung Ihrer Person anzeigen wollen. Glauben Sie nicht? – Dann lesen Sie einfach ältere Kommentare solch einer Newsgroup, die sich mit ähnlichen Fragen befassen – Sie werden sehen.

#### Zusammenfassung:

Versuchen Sie zu verstehen, wie Desktop Firewalls arbeiten, dann sind Sie in der Lage, selbst zu beurteilen, inwieweit ein Zeitschriftenartikel die Realität widerspiegelt.

## **11. Was ist sonst noch wichtig?**

- Windows 95/98 und ME, sind am stärksten durch Viren und Trojaner gefährdet. Etwas besser ist es, wenn Sie Windows NT, 2000 oder XP benutzen – allerdings nur dann, wenn Sie mit einem Benutzeraccount ohne (!) Administratorrechte arbeiten.
- Wenn Sie Linux benutzen, gilt vieles weiterhin. Allerdings haben PFWs unter Linux gänzlich andere Möglichkeiten, weil das System anders konstruiert ist. Eine PFW unter Linux ist wirkungsvoller, aber trotzdem kann auch diese nur begrenzt ausgleichen, was ihr Benutzer falsch gemacht hat. Ein falsch konfiguriertes Linuxsystem ist ebenso exponiert und angreifbar wie ein entsprechendes Windows. Einige Linux-Distributionen sind leider sträflich unsicher, wenn sie „Out-of-the-Box“ installiert werden.
- Installieren Sie regelmäßig die für Ihre Software verfügbaren Updates/Hotfixes (Fehlerkorrekturen). Diese Hotfixes schließen in der Regel Sicherheitslücken, die nach der Fertigstellung der Software entdeckt wurden. Sobald eine Sicherheitslücke entdeckt wurde, dauert es meist nur wenige Wochen, bis jemand einen automatisierten Angriff (Exploit) gegen diese Sicherheitslücke entwickelt. Wenn Ihr Computer dann nicht durch einen entsprechenden Hotfix geschützt ist, ist er in größter Gefahr. Sehr deutlich wurde dies am 12. August 2003, als der W32.Blaster/Lovesan-Wurm hunderttausende Computer befallen hatte [42], [43].

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

- Wenn Ihr Computer über ein Netzwerk mit dem Internet verbunden ist, unterlassen Sie bitte die Tests - ihr Administrator könnte darauf ziemlich ungehalten reagieren. Generell gilt: Wenn Sie nicht selbst der Administrator sind, bzw. Sie nicht für die Sicherheit ihres Computer verantwortlich zeichnen, lassen Sie dies die Verantwortlichen machen. Sie können gerne Ihren Admin fragen, wie es um die Sicherheit bestellt ist. Bedenken Sie dabei, daß ein mißtrauischer Admin (Admins sind hoffentlich immer mißtrauisch!) dies derart interpretieren könnte, daß Sie vorhaben, ins Netzwerk einzubrechen. Dies könnte ernsthafte arbeitsrechtliche Konsequenzen nach sich ziehen.
- Wenn Ihr Computer in einem Netzwerk ist, schließen Sie auf keinen Fall irgendwelche Ports, wenn Sie nicht der Administrator sind. Dies kann dazu führen, daß Sie keine Netzwerkverbindung mehr erhalten. Server oder Netzwerkdrucker können Sie dann nicht mehr benutzen.

## 12. Links zu interessanten Internetseiten zum Thema:

- <http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html>
- <http://rfc-editor.org>
- [http://www.pflock.de/computer/za\\_faq.htm](http://www.pflock.de/computer/za_faq.htm)
- <http://www.cert.dfn.de/>
- <http://cert.uni-stuttgart.de/>
- <http://home.arcor.de/nhb/pf-austricksen.html>
- <http://www.stud.tu-ilmenau.de/~traenk/dcsm.htm>
- <http://www.stud.tu-ilmenau.de/~traenk/zaweg.htm>
- <http://my-forum.netfirms.com/zone/zcode.htm>
- <http://www.securitytracker.com/alerts/2002/Aug/1005149.html>
- <http://www.team-cauchy.de/personal/>
- <http://www.bsi-fuer-buerger.de/>
- <http://www.heise.de/newsticker/data/ju-03.07.03-000/>
- <http://www.heise.de/security/news/meldung/38285/>

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

### 13. Weiterführende Informationen/Literaturnachweis:

- [1] <http://www.bsi.bund.de/faq/firewall.htm>
- [2] <http://www.iis.ruhr-uni-bochum.de/imperia/md/content/iis/praktikum/iis7.pdf>
- [3] <http://www.cert.dfn.de/dfn/berichte/db075/>
- [4] <http://www.cert.dfn.de/team/ue/fw/workshop/>
- [5] <http://grc.com/lt/leaktest.htm>
- [6] <http://www.wi1.wiso.uni-goettingen.de/pa/reco/kompetenz/schichtenmodell/1.htm>
- [7] <http://technologie.uni-duisburg.de/workshops/netzwerk/isoosi.htm>
- [8] Microsoft Windows NT Server - Version 4 – Netzwerke
- [9] Jürgen Kuri; da geht's lang; c't 6/97, Seite 380
- [10] <http://www.unibw-muenchen.de/campus/RZ/RZN/SN/9703/RZN9703.html>
- [11] siehe hierzu RFC 793 unter <http://www.rfc-editor.org/>
- [12] <http://www.iana.org/>
- [13] <http://de.wikipedia.org/wiki/Netzwerkprotokoll>
- [14] Entnommen aus: Andrew S. Tanenbaum; Computernetzwerke; 3. überarbeitete Auflage 2002; Seite 55; Pearson Studium
- [15] <http://www.zonelabs.com/>
- [16] Peter Siering; 2000 im Netz; c't 10/00, Seite 108
- [17] Karlheinz Blank, Peter Siering, Eduard Zander; Server 2000; c't 10/00, Seite 112
- [18] <http://groups.google.de/groups?q=xp+firewall+umgehen&hl=de&btnG=Google-Suche>
- [19] <http://www.trojaner-info.de/>
- [20] <http://www.heise.de/newsticker/data/pab-18.05.01-001/>
- [21] <http://www.computer-security.ch/ids/default.asp?TopicID=165>
- [22] <http://www.computer-security.ch/ids/default.asp?TopicID=164>
- [23] <http://www.ingbuero-klarmann.de/download/computerviren-information.pdf>
- [24] <http://www.trojancheck.de/>
- [25] <http://www.heise.de/ct/01/22/070/default.shtml>
- [26] Julien Oster, Florian Heinz; Die Firewall getunnelt - Fremde Pakete im Huckepack des DNS; c't 19/00, Seite 244
- [27] Martin Freiss; Alarmanlagen fürs Netz; c't 3/99, Seite 186
- [28] Bernd Rudack, Martin Freiss; Schriller die Glocken nie klingen; c't 3/99, Seite 190
- [29] Martin Freiss, Jürgen Schmidt; Einbrecher Alarm; c't 8/01, Seite 212
- [30] Jürgen Schmidt; Firewall getunnelt - Geheimer Datenaustausch über ICMP-Pakete; c't 11/97, Seite 332
- [31] <http://groups.google.de/groups?hl=de&lr=&ie=UTF-8&oe=UTF-8&group=de.soc.recht.datennetze>
- [32] <http://www.heise.de/ix/artikel/9609078/Cookies.shtml>
- [33] <http://www.techfak.uni-bielefeld.de/rechner/cookies.html>
- [34] Ralf Hüskes; Windows an der Leine - Windows Scripte: Nachfolger für Batch Dateien?; c't 6/98, Seite 310
- [35] Johannes Endres; Integrierte Surfgemeinschaft; c't 01/03, Seite 152
- [36] siehe hierzu RFC 1918 unter <http://www.rfc-editor.org/>
- [37] Jürgen Kuri; Wenn der Postmann zweimal klingelt; c't 12/96, Seite 334
- [38] <http://www.bintec-support.de/nat/nat-descr.htm>
- [39] <http://iuk.in-chemnitz.de/iall/ic/kap2/nat.htm>

---

Zum Linnegraben 46	Telefon: +49 (069) 395955	e-mail: <a href="mailto:oliver.klarmann@ingbuero-klarmann.de">oliver.klarmann@ingbuero-klarmann.de</a>
65933 Frankfurt am Main	Fax: +49 (069) 38013651	
	Mobil: +49 (0179) 2001336	

---

[40] <http://groups.google.de/groups?hl=de&lr=&ie=UTF-8&oe=UTF-8&group=de.comp.security.firewall>

[42] <http://www.heise.de/security/news/meldung/39358>

[41] <http://groups.google.de/groups?hl=de&lr=&ie=UTF-8&oe=UTF-8&group=comp.security.firewalls>

[43] <http://www.heise.de/newsticker/data/dab-12.08.03-000/>

## 14. Haftungsausschluß/Disclaimer:

Aufgrund der Schnellebigkeit und „Innovationsfreude“ der IT-Branche kann keine Gewähr für die Richtigkeit und Dauerhaftigkeit dieser Informationen gegeben werden. Es bestehen keine Haftungsansprüche gegenüber dem Autor, wenn aufgrund von Fehlern im Text Kosten entstehen. Für die Informationen der weiterführenden Links wird keine Haftung übernommen.

Es ist gestattet, dieses Skript oder Teile davon für eigene Zwecke wie Schulungen etc. einzusetzen, sofern Sie einen Hinweis auf den Autor und die Bezugsquelle lesbar anbringen.

© Dipl.-Ing. Oliver Klarmann, Frankfurt am Main 2003-2006, Personal Desktop Firewalls Version 3b