Personal Firewalls: Sinnvoll oder sinnfrei ?

Um es gleich vorweg zu nehmen - in 95% der Fälle halte ich den Einsatz einer **Personal Firewall** (im weiteren Verlauf der Beitragsfolge als PFW betitelt) für überflüssig. Kaum ein Thema im Bezug auf Internetsicherheit wird dermaßen kontrovers diskutiert und gleitet bisweilen ins Uferlose der freien Meinungsäußerung ab. Ich versuche daher trotz aller Subjektivität halbwegs sachlich und objektiv zu bleiben. Deshalb möchte ich mit etwas Grundsätzlichem zum Thema beginnen:

Grundsätzlich soll eine Firewall den eingehenden und ausgehenden Datenverkehr zwischen PC und der virtuellen Aussenwelt (Netzwerk, Internet) kontrollieren. Dies ist daher notwendig, weil es erhebliches kriminelles Potential gibt, welches aus unterschiedlichsten Gründen Zugriff auf PC's erlangen möchte. Eine Firewall ist weder zum Erkennen und Beseitigen von Viren da, noch hat sie die Aufgabe SPAM zu filtern oder Malware zu erkennen. Dies wird leider allzuoft mißverstanden. Im Prinzip ist eine Firewall ein Zugriffssystem, welches nicht auf Benutzerebene arbeitet, sondern eben auf Port- und Protokollebene, also praktisch gesehen wesentlich hardwarenaher, sofern man es technisch betrachtet. Eigentlich jedoch ist eine Firewall lediglich eine Komponente eines Sicherheitskonzeptes und nicht **das** Sicherheitskonzept selbst.

Im eigentlichen Sinn war eine Firewall quasi selbst Hardware und wurde sinnigerweise vor dem zu schützenden System eingesetzt. Ich vermute mal, dass ein findiger Geschäftsmann erkannt hat, dass eine Nachfrage nach Sicherheitsmechanismen besteht, welche für den Comsumermarkt erschwinglich wäre. Da dies nun eben nicht mit einer Hardware kostengünstig realisiert werden konnte, wurde eben die Geschichte per Software in die Tat umgesetzt.

An dieser Stelle entstand bereits der erste Widerspruch in sich:

Der Schutzmechanismus (also eine Software) befindet sich auf dem zu schützenden System. Das bedeutet in der Praxis, dass die Schadsoftware oder der "Hacker" sich bereits auf dem System befindet und der Kampf zwischen Eindringling und PFW auch dort stattfindet. Dies ist also bereits ein Risiko, das man bewußt akzeptiert, aber nur selten an den User kommuniziert.

Mein Lieblingsbeispiel in diesem Zusammenhang ist folgendes: Man stelle sich vor, im Mittelalter hätten die Rittersleut ihren Burggraben (in der Regel mit Wasser gefüllt) nicht um ihre Burg herum gebaut, sondern mitten hinein ! Selbst mit einem IQ von 2 (ein Klappspaten hat immerhin schon 4) kann man da schon ein winziges Paradoxum vermuten...

Trotzdem nehmen wir einmal an, dass das Sicherheitskonzept und die Funktionalität einer solchen PFW entsprechend ausgereift sei, dass dieser Umstand durchaus vernachlässigbar sei...

2. Personalfirewall- Tests (mal etwas anders, als man solche Tests von PC- Magazin Redaktionen gewohnt ist)

Wie arbeitet eine PFW ?

Das ist wohl weitgehend ein Geheimnis der Hersteller, aber grundsätzlich lassen sich bei der Verwendung einer PFW gewisse Dinge beobachten, die darüber Auskunft geben, wenn auch der Laie damit völlig überfordert ist. In jedem Fall schenkt der User einer Software sein volles Vertrauen und die Adminrechte, ohne zu wissen, wie zuverlässig und seriös diese Software arbeitet. Könnten die Programmierer nicht doch Fehler gemacht haben, die u.U. die PFW selbst zum potentiellen Angriffsziel macht ? Da eine PFW ja nun einmal mit sehr hohen Rechten ausgestattet ist und quasi die Schnittstelle zur Onlinewelt kontrolliert, wer garantiert dem User, dass diese Software nicht genauso wie andere Malware interessante Daten an ein entsprechendes Ziel sendet ? Die Hoffnung stirbt zuletzt, aber es gibt inzwischen genügend Beweise für solche unseriöse Sicherheitssoftware...

Um dies etwas zu verdeutlichen, habe ich mir mal verschiedene PFW's etwas näher angesehen. Dass meine Tests nicht von amtlicher Seite zertifiziert sind und die Ergebnisse auch von System zu System deutlich variieren können, ist mir durchaus bewußt. Es ist auch nicht meine Absicht, Behauptungen aufzustellen, die systemübergreifend Gültigkeit besitzen, sondern Anwendern zu verdeutlichen, was unter Umständen mit der Installation solcher Programme auf sie zukommen **könnte** (nicht zwangsläufig so sein muss). Es ist auch durchaus möglich, dass bei anderen Usern mit anderen hard- und softwaretechnischen Voraussetzungen, auch andere Testergebnisse zustande kommen könnten. Desweiteren besteht auch die Möglichkeit, dass im Laufe der Zeit, die Hersteller auf entsprechend bekannte Probleme reagieren und diese nicht mehr auftreten. Dieser Test ist also quasi eine Momentaufnahme im Zeitrahmen zwischen Juni und August 2007 und den zu dieser Zeit aktuellen Softwareversionen. Konstruktive Kritik, Anregungen oder Meinungen nehme ich gerne entgegen und arbeite u.U. nützliche Hinweise in diese Abhandlung ein. Hierzu steht speziell parallel ein kleines **Forum** bereit. Wenn ich nun im folgenden Abschnitt der jeweiligen Fan- Gemeinde der entsprechenden Software mächtig auf die "Nüsse" gehen sollte, so soll das für jene ein Anreiz sein, mit sachlichen Argumenten entsprechend zu reagieren oder mit fundierten Fakten an mich heranzutreten, anstatt in diversen Foren unqualifizierte Äusserungen zu machen. Zunächst habe ich dazu die AVG Antivirus 7.5 Version mit integrierter Firewall genommen (Anmerkung: Die Ziffern drücken keine Platzierungen aus, wie man sie gewöhlich von Tests kennt, es handelt sich lediglich um eine Aufzählung)

2. Comodo

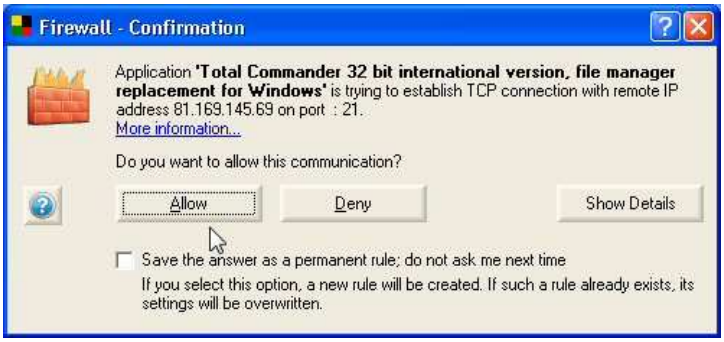
3. Sygate

4. Zonealarm Free

5. Norton Internet Security

AVG Antivirus mit integrierter Personalfirewall Version 7.5 Direktlink zum Forum

Nach der Installation, die ich im vorgegebenen Standardverfahren durchgeführt habe, ist die PFW eigentlich nicht sehr auffällig. Erst nach einer Zeit und bestimmten Aktionen des Windows- Systems meldet sich die PFW plötzlich mit einem solchen PopUp:



Ich bin mir ziemlich sicher, selbst wenn der Text in DEUTSCH zu lesen wäre, dass der durchschnittliche Computeranwender damit schon erhebliche Verständigungsprobleme hätte. Die Praxiserfahrung hat bewiesen, dass in den meisten Fällen der Applikation, die sich hier vorstellt, Durchlass gewährt wird, insbesondere, wenn der User feststellen würde, dass er in seinen Onlineaktivitäten eingeschränkt wäre. Somit ist der erste Schritt getan, die Sinnfreiheit des Einsatzes einer PFW zu bestätigen und man kann der PFW dabei nicht einmal die Schuld anlasten...

Das Programm Total Commander versucht offensichtlich mit der Außenwelt Kontakt aufzunehmen. Es wird eine IP- Adresse angezeigt und ein Port, über welchen die Kommunikation stattfinden soll. Was mit TCP/IP gemeint ist, kann ein durchschnittlicher Anwender kaum richtig verstehen. Somit dürfte die Aussage der PFW für viele Anwender wenig aussagekräftig sein. Man hat dann genau 2 Möglichkeiten und die Entscheidung bleibt allein am User haften...

Anmerkung: **Bei der Betrachtung aus Sicht eines ernstzunehmenden Sicherheitskonzeptes gilt ein System auch dann schon als infiziert, wenn eine Malware (Backdoor, Trojaner o.ä.) von innen nach außen zu kommunizieren versucht. Eine Blockade dieser Absicht durch eine PFW macht daraus kein sauberes System mehr.** In sicherheitsrelevanten Netzwerken mit verantwortungsvollen Administratoren wird ein solcher PC vom Netz genommen und in den meisten Fällen neu installiert. Somit erübrigt sich die scheinbar primäre Aufgabenstellung einer PFW, eben dieses nachhaltig zu verhindern. Das Sicherheitskonzept ist bereits unterwandert und die PFW ist von sich aus keinesfalls in der Lage, selbiges wieder herzustellen. Es ist wichtig, diesen Umstand zu berücksichtigen, wenn man von Features oder Aufgaben von PFW's redet.

In diesem Fall sollte der Total Commander über sein FTP- Modul eine Verbindung zum Webspace meines Internetproviders herstellen, was standardmäßig über Port 21 abgewickelt wird...
Ob das jedem so ersichtlich ist ? Das war jetzt noch ein einfaches Beispiel und stand in direktem Zusammenhang mit Eingaben, die von mir bewußt vorgenommen wurden...

Wer eine PFW auf seinem System, wozu auch immer einsetzen möchte, sollte sich im Klaren darüber sein, dass die Konfiguration derselben überdurchschnittliche Kenntnisse im Umgang mit Computern erfordert und natürlich auch jede Menge Zeit. Wer weder das eine noch das andere besitzt, ist eigentlich nicht derjenige, der eine solche Software einsetzen sollte. **Eine falsch konfigurierte Firewall (das betrifft natürlich auch die Hardware- Firewall) schadet mehr als sie nützt.** Zudem kann dadurch eine scheinbar vorhandene Sicherheit suggeriert werden, welche gar nicht besteht. Wer nun glaubt, dass es doch nicht so schwer sein kann, eine PFW richtig einzustellen, sollte die folgenden Schritte anhand der AVG Firewall mal genau betrachten und sich selbst mal objektiv einschätzen. Die folgenden Abbildungen zeigen lediglich nur einzelne Konfigurationsschritte ohne weitere Einstellungen vorgenommen zu haben und müssen eigentlich für alle Programme, Dienste und wer weiß was noch ebenfalls sehr präzise vorgenommen werden. Ob andere PFW's dies einfacher anbieten, kann ich nicht beurteilen, aber halte ich für kaum vorstellbar...

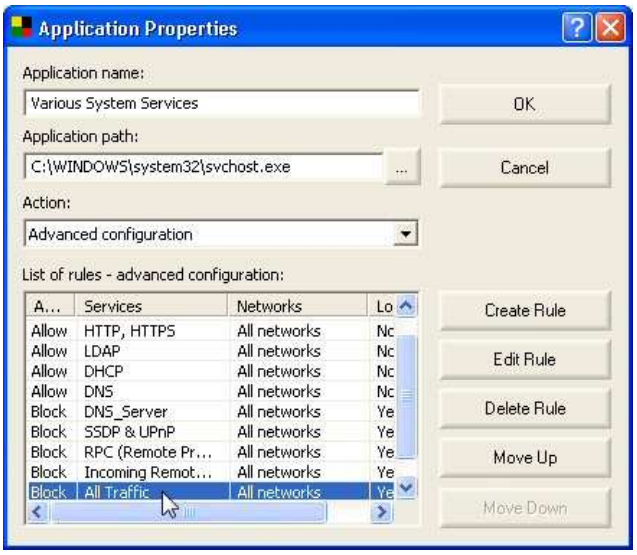
Die allgeinen Einstellungen habe ich bewußt übersprungen und bin gleich beim Menüpunkt Applications eingestiegen. Auffallend ist die festgelegte Blockierungs- bzw. Freischaltungskonfiguration der Standardinstallation, die vom Prinzip her selbsterklärend mit verständlichen Symbolen ausgestattet ist. Aber das ist auch schon alles, was im Grunde nachvollziehbar ist. "Eine DLL- Datei als Anwendung ausführen" ist offensichtlich geblockt, aber ich habe nicht die geringste Vermutung, warum das so ist ?
O.K. manche werden jetzt natürlich auch die berechtigte Frage stellen:
...und was ist eine DLL- Datei ?

Wer sich nun diese Frage wirklich stellen muss, der sollte postwendend mit der Konfiguration der PFW aufhören, die Software deinstallieren und entsprechende Verhaltensregeln im Umgang mit Computer und Internet beherzigen, da dies ganz bestimmt der bessere Weg sein wird...

Weitestgehend versteht man unter Dynamic Link Library (kurz DLL) eine Bibliothek, an der sich Programme bedienen können. Hier befinden sich die meisten Durschnittsanwender auf fremdem Terrain, welches den Softwareentwicklern und Informatikern (im weitesten Sinne) vorbehalten ist.

Andererseits ist einer anderen Anwendung der Zugang zum Internet gestattet, die bekanntermaßen die Hauptangriffsfläche für Hacker und Cracker darstellt: der Internet Explorer .
An dieser Stelle offenbart sich keineswegs, was nun mit Dingen wie Active X und Javascript möglich ist. Wenn nun also der Internet Explorer uneingeschränkt mit dem Internet kommunizieren dürfen sollte, wäre bereits damit die Funktion der Firewall in weiten Teilen unterwandert. Nun sollte auch dem Nutzer eines onlinefähigen Computers klar sein, dass Port 80 den Standardzugang eines Browsers zu einem Webserveri remoteseitig bereitstellt. Diesen Port zu blockieren, käme in vielen Fällen einer Isolierung des Users mit dem World Wide Web gleich und ist daher in der Regel nicht blockiert. Somit wird einer Firewall damit eine schwere Entscheidung abverlangt, die sie natürlich gerne an den User weitergibt, welcher sich selbst ja wohl kaum einsperren möchte...

Um noch einen Schritt weiter zu gehen, habe ich "Various System Services" als Konfigurationsopfer ausgesucht. Dieser Ausdruck ist sowohl vielsagend als auch nichtssagend und man sollte mal schauen, was sich dahinter verbirgt...



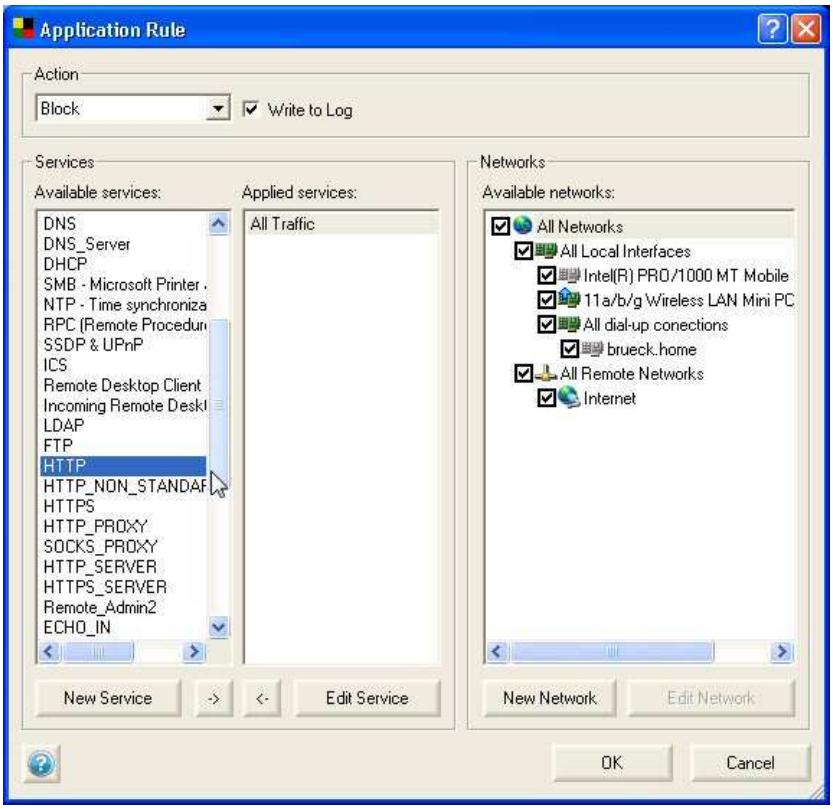
Dahinter offenbart sich die berühmt- berüchtigte Datei svchost.exe, die im Windowssystem sehr vielseitige Aufgaben hat und als Dienst dauerhaft im Windowssystem arbeitet. Dabei kann sie auch in mehreren unterschiedlichen Instanzen auftauchen und in sich weitere Prozesse steuern.

Ich persönlich muss zugeben, dass ich mir zwar schon mit speziellen IT- Tools angesehen habe, was dahinter so geschieht, aber könnte keineswegs genau erkennen, ob hier nun eine wichtige Systemdatei ausgeführt wird oder ein böser Trojaner seinem Namen alle Ehre macht. Ich hoffe (für mich selbst) dass es vielen anderen IT- Kollegen, deren Spezialgebiet nicht in der svchost.exe liegt, ebenso ergeht und kann wohl davon ausgehen, dass ein Normal- Anwender hiermit restlos überfordert ist...

...aber um nun den Einsatz einer PFW rechtfertigen zu können und zudem noch behaupten zu dürfen, dass sie richtig konfiguriert sei, macht es unumgänglich, sich damit intensiv zu beschäftigen.

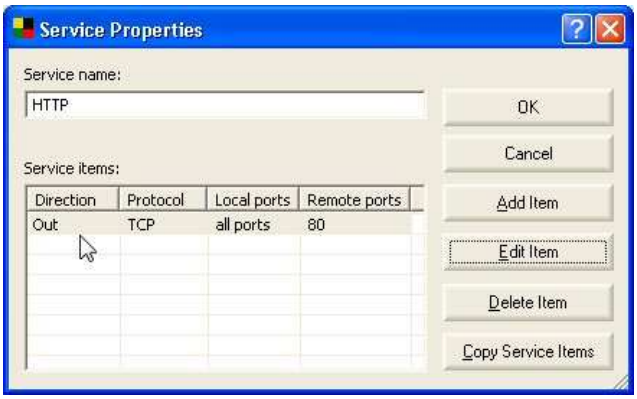
Solche Spezialausdrücke wie RPC (Remote Prozedure Call) oder DNS (Domain Name Service) sollten für den Konfigurierenden keine Fremdwörter sein. Was nun mit der Blockade von "All Traffic" gemeint ist, bringt mich wieder zum Grübeln...

Wenn "jeglicher Verkehr" blockiert sein sollte, wie funktioniert nun überhaupt noch was ? Entweder habe ich da schon wieder was falsch verstanden oder die Ausdrucksweise wurde einmal mehr sehr unglücklich gewählt. Mal sehen, ob man etwas entschlüsseln kann:

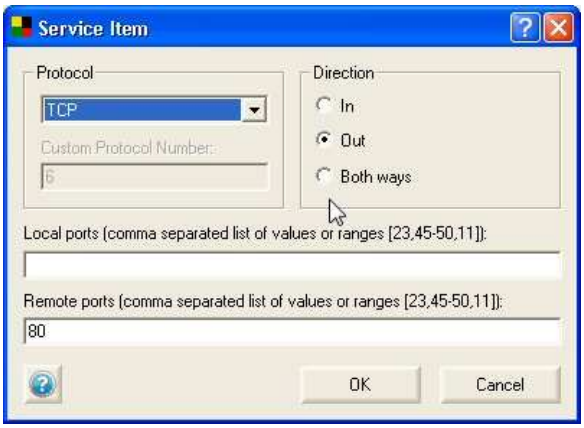


O.K. als IT- Admin kann ich mit den folgenden Dingen schon größtenteils was anfangen, allerdings weniger im Zusammenhang mit der richtigen Konfiguration dieser PFW.
Der Einfachheit halber wähle ich aus der Vielzahl der aufgeführten Protokolle
(Aber hallo - ich bin davon ausgegangen, dass der Besitzer und Anwender der PFW natürlich direkt erkannt hat, dass hier die meisten Standardprotokolle aufgelistet wurden) das HTTP- Protokoll aus, welches ja, wie bereits schon vorher mal erwähnt

über den Port 80 (standardmäßig remoteseitig) kommuniziert und für die Darstellung von Web- Inhalten im Browser zuständig ist.

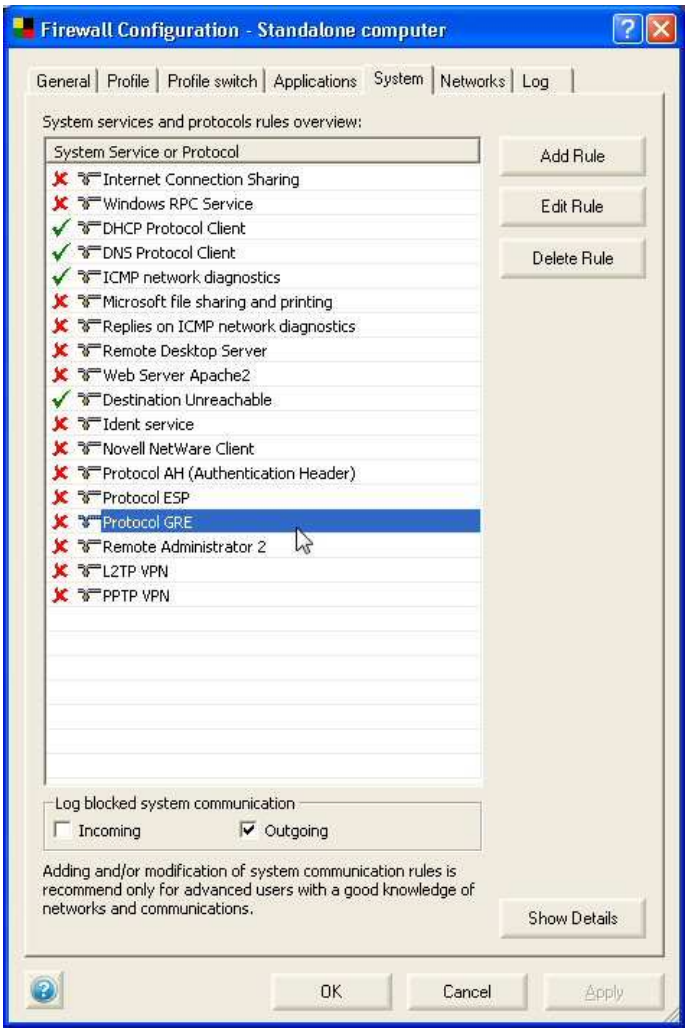


So - und nun steht der User da und fragt sich wie es weitergehen soll ? Mir jedenfals erging es im ersten Moment auch so, also keine Scheu, sich zu outen!
Soll man hier nun tatsächlich irgend etwas einstellen ? Könnte sich das nicht im Nachhinein als fataler Fehler erweisen ? Tut mir leid Leute, ich kann euch nicht helfen - ich weiß es schlicht und ergreifend auch nicht !



Der Klick auf "Edit Item" offenbart zwar neue Einstellmöglichkeiten, die aber meines Erachtens nur für IT- Administratoren interessant sein können, die auch die anderen Gegenbenheiten in der ihnen anvertrauten Netzwerkumgebung kennen und entsprechende Einstellungen machen können. Hier scheiden sich deshalb wiederum die Geister:
Im privaten Umfeld, womöglich bei einem Anwender mit ein oder zwei PC's, die genutzt werden, sind die Konfigurationshürden inzwischen dermaßen hoch gewachsen, dass die meisten längt kapituliert haben werden. Unweigerlich geht so manchem der Gedanke durch den Kopf, ob es nicht eine einfachere Art gibt, den Gefahren aus der Onlinewelt trotzen zu können ? (Gibt es - dazu aber später)!!!

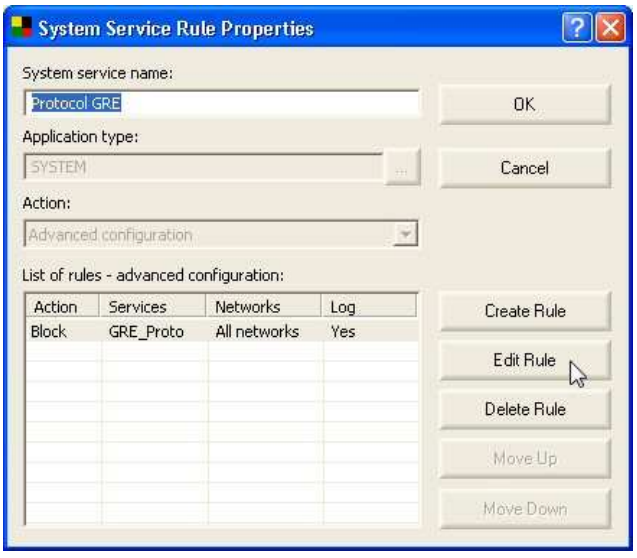
Im geschäftlichen Umfeld mit eigener IT- Abteilung wird man kaum solche Wege beschreiten. Hier werden Hardware-Lösungen bevorzugt und muss unbedingt eine PFW zum Einsatz kommen, ist diese dann serverseitig konfigurierbar. Der Aufwand, jeden einzelnen PC zu konfigurieren, ist einfach zu hoch. Selbst dass es Im- und Exportmöglichkeiten für die Einstellungen gibt, werden in einem Unternehmen mit durchdachtem Sicherheitskonzept und einer gewissen betriebswirtschaftlichen Mindestanforderung diese Art Lösung sehr schnell verwerfen...



Ich war ja noch lange nicht am Ende mit den Konfigurationsmöglichkeiten und habe im Menü Applications ja nur einen einzigen Konfigurationspunkt verfolgt, ohne wirklich eine Einstellung vorgenommen zu haben. Jetzt geht es nämlich ins nächste interessante Menü: System - wiederum vielsagend und nichtssagend:

Es wird hier zwischen Service und Protokoll keinen wirklichen Unterschied gemacht und so mancher Ausdruck ist uns noch aus dem vorhergehenden Konfigurationsmenü in Erinnerung. Was nun hier der Ausdruck "Destination unreachable" bedeuten soll, kann ich leider nicht nachvollziehen. Das ist weder ein Dienst noch ein Protokoll, aber die Entwickler haben sich dabei wohl was gedacht ? Schade dass ich ihre Gedanken dazu nicht nachvollziehen kann.

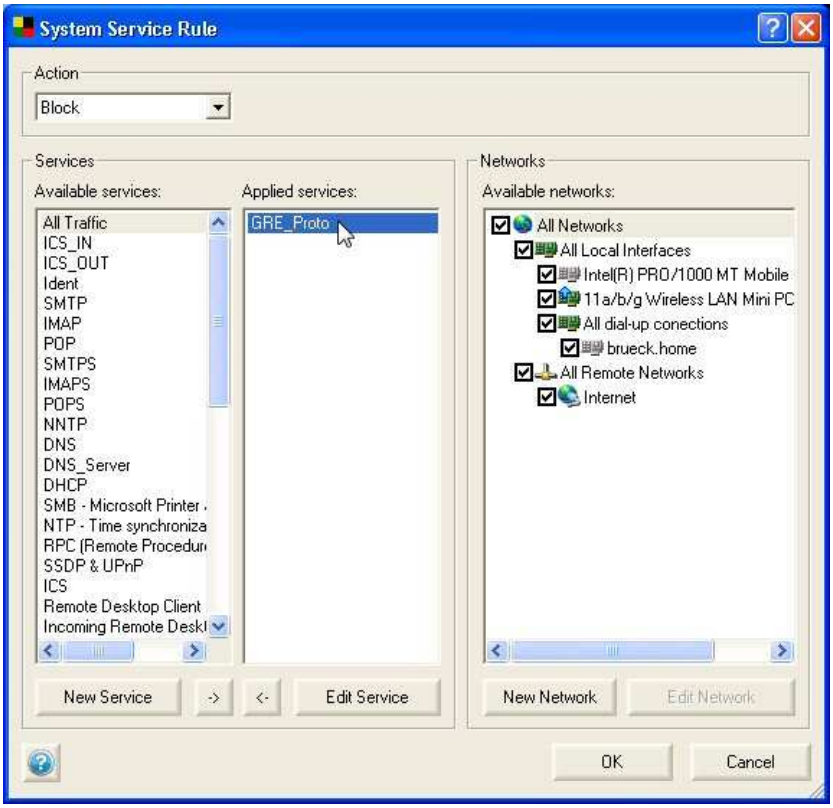
Interessanterweise gibt es in dieser Konfiguration die Möglichkeit, per Flag den eingehenden bzw. ausgehenden Verkehr des entsprechend ausgewählten Konfigurationspunktes festzulegen. Dazu ist natürlich wiederum ein fundiertes Wissen im Bereich Netzwerkprotokolle und Windows- Diensten erforderlich. Das GRE- Protokoll (Generic Routing Encapsulation) z.B. ist maßgeblich für VPN- Verbindungen (Virtual Private Network) zuständig.



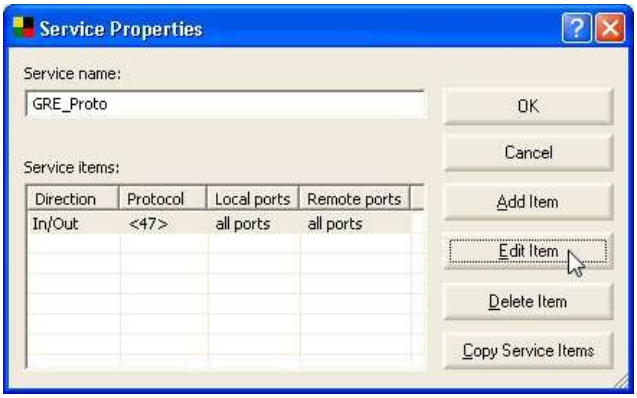
Waren wir beim HTTP- Protokoll nicht schon einmal an der gleichen Stelle ? Anscheinend sind die einzelnen Konfigurationspunkte nicht konsequent voneinander getrennt, sondern es

bestehen Querverbindungen. Das führt allerdings zu Verwirrungen, welche schnell in Fehlkonfigurationen enden können bzw. der User konfiguriert regelrecht im Kreis herum. Möglicherweise ist dies bei anderen PFW's besser gelöst...?

Jedenfalls ergibt es wenig Sinn im obigen Menü irgend welche Einstellungen vorzunehmen, wenn man nicht ansatzweise darüber bescheid weiß, wie Tunneling bei VPN- Verbindungen funktioniert.
Jetzt mag dem einem oder anderen der unberechtigte Einwand in den Sinn gekommen sein, dass man einfach nur das konfiguriert, welches man kennt und benötigt. Dieser Ansatz wäre gleichermaßen falsch wie fatal. **Ein Sicherheitskonzept wird durch das Gesamtpaket gebildet und verliert seinen Sinn, wenn man aus Unwissenheit einfach einige Teile davon unterschlägt.**



Auch hier waren wir bereits schon einmal.
Alle Wege führen anscheindend nicht allein nach Rom, wie es früher in der Antike hieß.
Der durchschnittliche User wird wohl kaum Wesentliches an der Standardkonfiguration seiner PFW verändern, aber der Schrei nach Hilfe in den einschlägigen Fachforen im Internet ist laut, wenn manche Dinge einfach nicht mehr funktionieren wollen, die zuvor ohne PFW noch tadellos ihre Dienste verrichteten.
Immer wieder wird mir in Foren vorgeworfen, dass es doch nicht mein Ernst sein könne, in solchen Fällen die Deinstallation der PFW vorzuschlagen. Sicher - alternativ dazu könnte man sich intensiv mit der Konfiguration der jeweiligen PFW auseinandersetzen, um für Freeware- Tool XYZ das Problem zu lösen. Doch wie sieht es mit Freeware- Tool ABC zwei Wochen später aus mit anderer PFW ?
Beim besten Willen - ist das sinnvoll, ganz abgesehen von der investierten Zeit ?

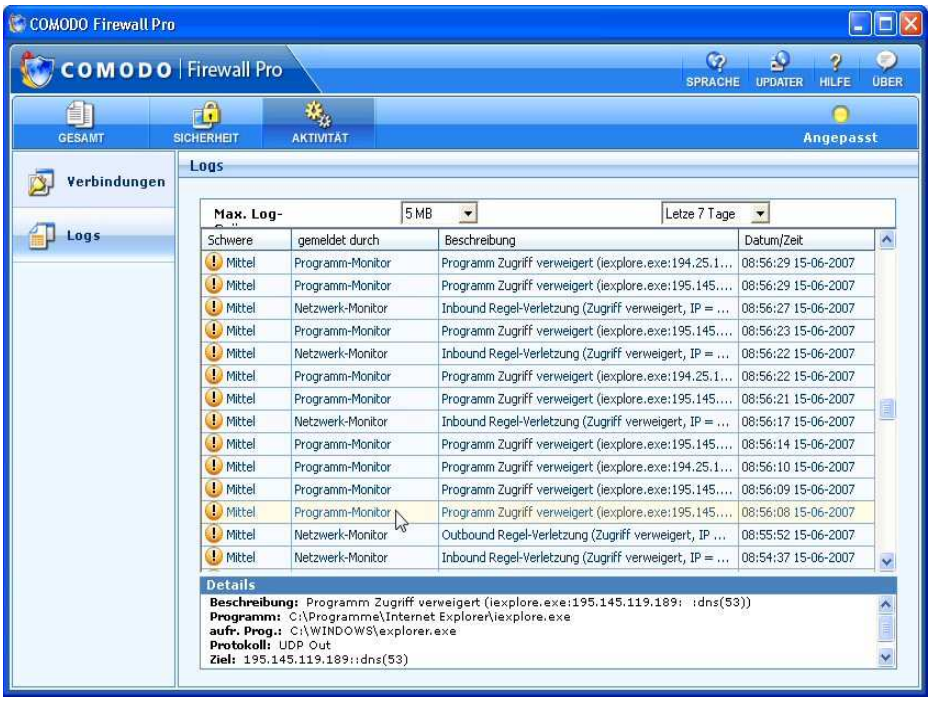


Natürlich hätte ich anstatt des GRE- Protokolls jedes andere angebotene auswählen können und hätte letztendlich vor der gleichen Entscheidung gestanden. Für mich persönlich habe ich entschieden, dass ich andere Wege beschreite, um meine Windows- PC's sauber zu halten.
Ich konnte auch erhebliche Performance- Einbußen erkennen, während die PFW installiert war, was außerdem ein schwerwiegender Grund darstellt, sich davon zu trennen. Es gibt auch andere effektive Mittel sicher online zu gehen: siehe hier

Anhand der **Comodo**- Personal Firewall habe ich eine weitere kleine Analyse versucht: Direktlink zum Forum

Nach der Installation war dies die erste Meldung, die auf dem Desktop dann zu sehen war. Was bedeutet diese Aussage nun im einzelnen ? Wie bereits erwähnt, sollte dies der Anwender, der diese Firewall einsetzt grundsätzlich wissen, da ansonsten jegliche Verwendung keinen Sinn ergibt. **avgemc.exe** : Hierbei handelt es sich um den Virenscanner von **AVG**, der auf diesem Testsystem installiert wurde. Würde man dieser Anwendung unter Verwendung des Buttons "Verweigert" die Arbeitserlaubnis entziehen, wäre das sicherlich kein guter Entschluss. Unter der fragwürdigen Bezeichnung **Fernsteuerung** ist die IP- Adresse **127.0.0.1** und der Port **10110 - TCP** aufgeführt. Dem Anwender sollte schon klar sein, dass diese IP- Adresse lediglich den sog. **Localhost**, also die eigene Maschine kennzeichnet und dass der Virenscanner über den Port 10110 mit dem Programm **services.exe** kommunizieren möchte. Es handelt sich also komplett um eine Offline- Angelegenheit und ist somit völlig unkritisch zu betrachten. Ob das jeder User so erkennen würde ?

In diesem Fall wird die Sache nun wesentlich interessanter. Dass es sich bei **iexplore.exe** um den **Microsoft Internet Explorer** handelt, sollte allgemein bekannt sein. Doch was sagt die Zeile hinter **Fernsteuerung** aus ? Als PFW- Laie kann ich daran nicht erkennen, ob dies einen Zugriff von innen nach aussen oder umgekehrt darstellt, was eigentlich doch recht wichtig sein sollte. Jedenfalls bezeichnet **Port 53** den Standardport für **DNS**-Anfragen. Als Protokoll erscheint diesmal **UDP**. All diese Umstände muss der Anwender in seine Entscheidung einbeziehen und sinnigerweise auch deren Bedeutung kennen. Nehmen wir nun mal an, der User erachtet diese Kommunikation zur oder von **IP: 195.145.119.189** als überflüssig oder gar gefährlich und "verweigert" die Kommunikation, wird er sich anschließend mit folgender Problematik auseinandersetzen müssen: **"Die Seite kann nicht angezeigt werden"** Eigentlich kennt jeder diese Fehlermeldung. Wenn dann noch unterhalb des überflüssigen Resttextes zur Fehlerbeseitung die Information steht **"Server oder DNS kann nicht gefunden werden"** ist die Sachlage klar: Man hat schlicht und ergreifend unterbunden, dass der zugehörige DNS- Server den Namen der aufgerufenen Internetseite in eine IP- Adresse auflösen konnte, was aber eine grundlegende Notwendigkeit ist, wenn man per Browser im Internet surfen möchte. Man hat sich quasi selbst ausgesperrt!

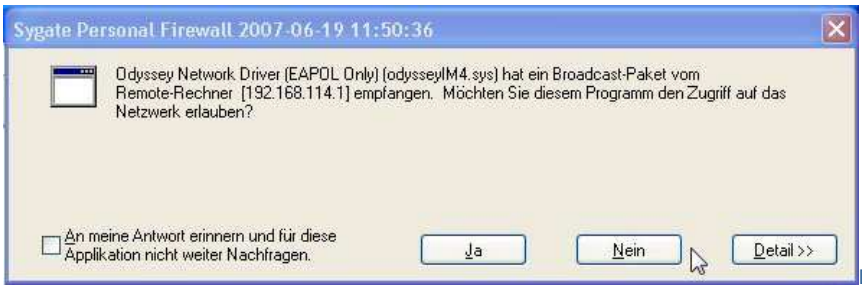


Im Log- File der Comodo- Firewall sieht die Sache dann so aus und man erkennt nun zusätzlich noch, dass es sich um eine Verbindung von innen nach aussen handelt: **UDP out**. Es ist also ungemein wichtig, dass man diese Kommunikation von der Firewall nicht blocken lassen darf, wenn man im Internet surfen möchte. Es ist also keineswegs der Versuch eines bösen "Trojaners" nach Hause telefonieren zu wollen. Jeder Benutzer einer PFW muss also genau wissen, was seine liebgewordene Personal Firewall gerade machen möchte und natürlich womit. Alles andere kann man nur als Problembeschaffungsmaßnahme ansehen.

Zum Abschluss der Excursion in die Welt der **Comodo- Firewall**, ist dann noch was interessantes erschienen, was gefährlich auszusehen scheint. "**...unter Benutzung sog. GlobalHooks, welche auch von Keyloggern zum Stehlen privater Daten benutzt werden können.**" ist in seiner Bedeutung schon ziemlich heftig. Es ist mir persönlich völlig unklar, wie diese Aussage zu deuten ist und nur der Hersteller **Jasc** könnte genaueres dazu sagen, was die Datei **JascCapture.dll** über **Port 443 - TCP** zur entsprechenden IP- Adresse kommunizieren möchte. Eigentlich habe ich nur die Funktion "Snapshot" des bekannten Bildbearbeitungsprogramms aktiviert, womit man Screenshots erstellen kann. Für mich stellt sich nun die berechtigte Frage, weshalb entweder **Paint Shop Pro** Daten aus dem System irgendwohin übertragen möchte oder ob die Aussage der **Comodo**- Firewall eine Fehlinterpretation darstellt. In beiden Fällen halte ich diese Umstände für unseriös, sofern sie zutreffen und es gilt zu klären, wer hier mit falschen Karten spielt...Es ist schon eine ziemlich schwerwiegende Anschuldigung, wenn man den Verdacht des Stehlens von Daten äußert. Andererseits wäre es im Umkehrschluss ebenfalls eine unseriöse Geschichte, wenn **Paint Shop Pro** als **Keylogger** verwendet würde. Die angegebene IP- Adresse ist jedenfalls keine öffentliche, sondern ein Gateway bzw. Router. Insofern würde diese Kommunikation wenig Sinn ergeben bzw. die Deutung für den User ist völlig unmöglich...was zu beweisen wäre!

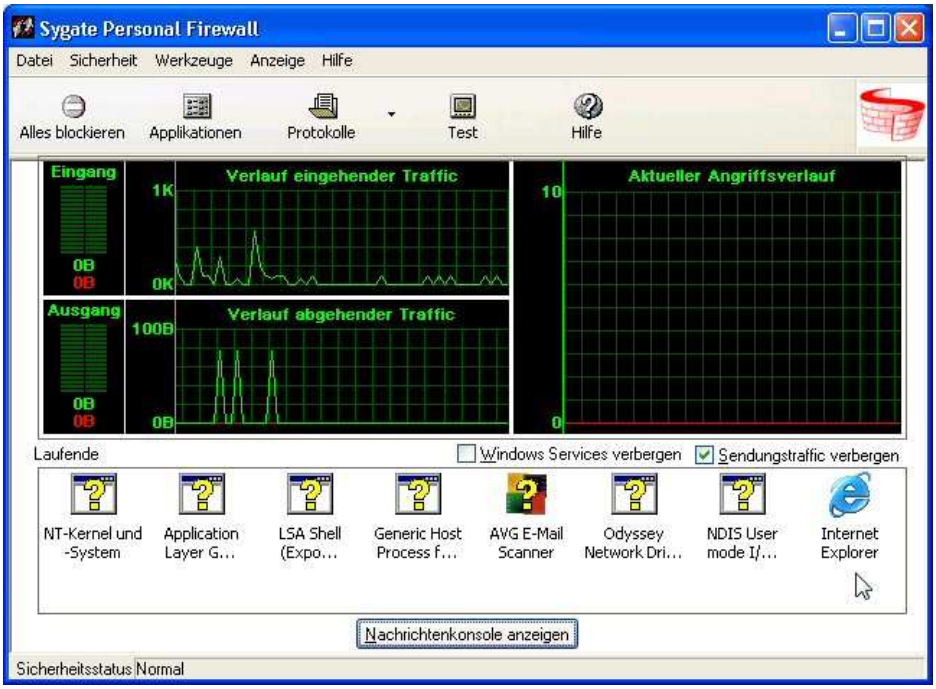
Man kann diese und ähnliche Tests (oder man könnte es auch als Versuche, die PFW zu bedienen, bezeichnen) auch auf weitere Personal Firewalls ausdehnen und daher habe ich nun auch die weit verbreitete und anscheinend beliebte **Sygate Personal Firewall** ins "Test"- Boot genommen: Direktlink zum Forum

Nach der Installation beglückten mich gleich 2 aufeinanderfolgende PopUps:

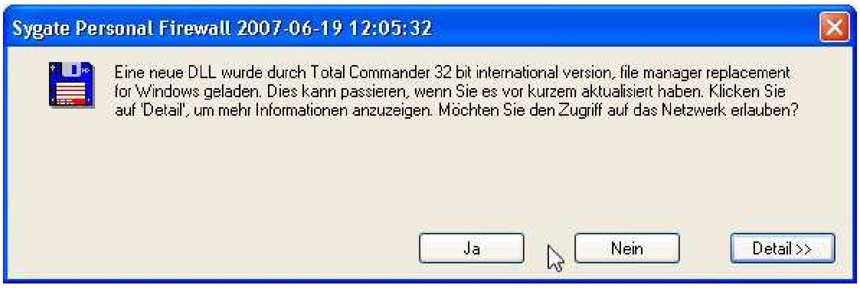


Der angebliche Remote- Rechner ist der PC selbst, auf welchem die Firewall installiert wurde. Der Zugriff bezieht sich auf den Treiber der WLAN- Netzwerkkarte und es handelt sich um irgend ein ominöses Broadcast- Paket. Nun soll bitte niemand behaupten, dass diese von der Firewall getroffenen Aussagen für jedermann verständlich sind. Dass die Netzwerkkommunikation eben über eine Netzwerkkarte (in diesem Fall ein WLAN- Adapter) stattfindet, sollte zumindest jedem Benutzer dieser Firewall nicht entgangen sein. Ob auch jeder bemerkt hat, dass der angebliche Remote- Rechner kein geringerer ist, als der PC, auf welchem die Firewall installiert wurde, was anhand der IP- Adresse rauszufinden ist, dürfte einen Großteil der Anwender schon in Verlegenheit bringen. Wer jetzt überdies hinaus noch weiß, dass ein **Broadcast** eine Standard- Anfrage vom Microsoft- Betriebssystemen ist, die quasi in Netzwerken mit Windows- Systemen ständig präsent ist und nichts anderes als einen lapidaren Rundruf darstellt, der im Prinzip allen PC's einfach mal "Guten Tag" sagt und somit deren Anwesenheit prüft, ist beinahe schon der geborene "Personal

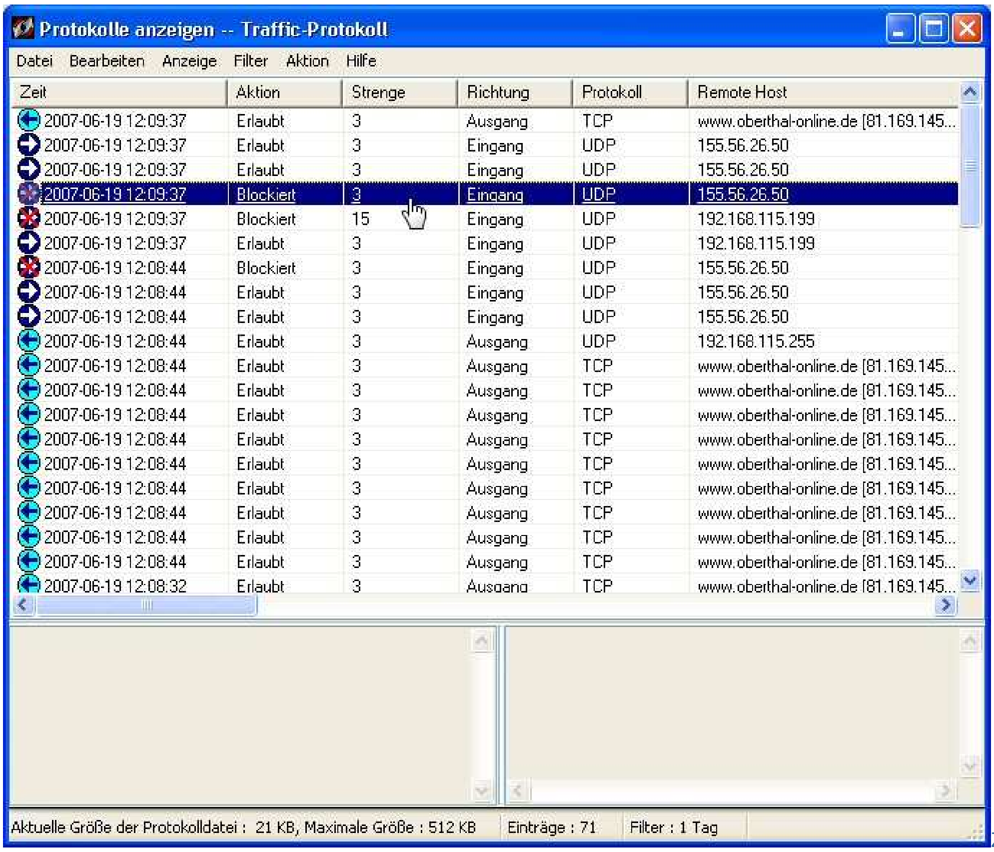
Firewall Anwender". Dass beim ersten Versuch, online zu gehen, eine Meldung kommt, ist natürlich reine Formsache und es versteht sich von selbst, dass man dem Browser natürlich diese Verbindung erlaubt. Hat man allerdings zuvor der Netzwerkkarte jegliche Verbindung verwehrt, wird dies leider nicht viel nützen. Die Zusammenhänge sind natürlich jedem User bewußt und es gibt damit auch niemals Probleme...



Diese Anzeige ist bestimmt interessant für Freaks von Koordinatensystemen oder bunten Cockpitanzeigen, aber ob jeder Firewall- User versteht, was das Dargestellte so bedeutet, darf angezweifelt werden. Jedenfalls hat der User hier die Möglichkeit, die Applikationen oder Prozesse, die mit einem Fragezeichen versehen sind, die Kommunikation nach außen zu erlauben. In diesem Beispiel ist die Auswahl noch recht überschaubar, doch habe ich bereits jetzt meine Zweifel, dass jeder User genau weiß, welche dieser Programme oder Dienste für eine reibungslose Online- Kommunikation erforderlich sind und welche eben nicht. Es handelt sich hierbei keineswegs um ein "Hütchenspiel" wo es darum geht, das Hütchen mit dem versteckten Würfel zu bestimmen - es soll eigentlich Teil eines Sicherheitskonzeptes sein...



Mit solchen PopUps dürften wohl die meisten User allmählich an ihre Verständnisgrenzen im Bezug auf Computersachverstand stoßen. Das ist keineswegs eine Schande noch wertet es eine Person ab. Hier handelt es sich um technische Details, die auch in anderen Bereichen existieren, welche auch ihre Experten haben. Auch hier zeigt sich zum wiederholten Mal, dass die richtige Benutzung einer Personal Firewall sehr viel voraussetzt. Für einen Durchschnittsanwender ohne tiefgreifende Systemkenntnisse ist dies wieder ein "Hütchenspiel"...



Zeit	Aktion	Strenge	Richtung	Protokoll	Remote Host
2007-06-19 12:09:37	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:09:37	Erlaubt	3	Eingang	UDP	155.56.26.50
2007-06-19 12:09:37	Erlaubt	3	Eingang	UDP	155.56.26.50
2007-06-19 12:09:37	Blockiert	3	Eingang	UDP	155.56.26.50
2007-06-19 12:09:37	Blockiert	15	Eingang	UDP	192.168.115.199
2007-06-19 12:09:37	Erlaubt	3	Eingang	UDP	192.168.115.199
2007-06-19 12:08:44	Blockiert	3	Eingang	UDP	155.56.26.50
2007-06-19 12:08:44	Erlaubt	3	Eingang	UDP	155.56.26.50
2007-06-19 12:08:44	Erlaubt	3	Eingang	UDP	155.56.26.50
2007-06-19 12:08:44	Erlaubt	3	Ausgang	UDP	192.168.115.255
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:44	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...
2007-06-19 12:08:32	Erlaubt	3	Ausgang	TCP	www.oberthal-online.de [81.169.145...

Zum Abschluss im Bezug auf die Sygate Firewall möchte ich noch kurz das mitlaufende Protokoll aufzeigen. In diesem Fall ist im Prinzip nichts besonderes zu erkennen. Im Grunde ist an der markierten Zeile lediglich zu erkennen, dass eingehende Zugriffe von einer bestimmten IP-Adresse über das UDP- Protokoll blockiert werden. Ob das gut und sinnvoll ist, kann ich nicht sagen, da ich eigentlich gar nicht weiß, worum es dabei geht. Vielleicht ist es ja nichts weiter als eine Broadcast- Anfrage vom WLAN- Gateway, die ich per "Hütchenspiel" im Test einfach mal blockiert habe ? Genaue Angaben liefert mir die Firewall an dieser Stelle leider nicht.

Zonealarm ist jetzt schon mehrfach in dieser Abhandlung aufgetaucht und als derzeitiger Marktführer in diesem Marktsegment soll die Personal Firewall von ZoneLabs nicht unerwähnt bleiben... Direktlink zum Forum

Als Test für **Zonealarm** habe ich mal versucht, über einen internen WLAN- Hotspot über das Internet eine Verbindung zu einem VPN- Server aufzubauen. Dies ist z.B. für Studenten oder Aussendienstler in der IT- Branche nichts ungewöhnliches. Die Personal Firewall dokumentiert dies auch recht plausibel, wenn auch ein Durchschnittsanwender schon Interpretationsschwierigkeiten bekommen dürfte. Dass **rasphone.exe** eine windowseigene Datei für Wähl- und Remotezugriffe darstellt, kann schließlich nicht jeder wissen, aber für den Anwender einer Personal Firewall sollte dies spätestens jetzt zum Lernziel gemacht werden.

Was mich bei diesem Test besonders gestört hatte, war die Tatsache, dass ich die angestrebte VPN- Verbindung nicht aufbauen konnte. Zonealarm hat mich daran gehindert, obwohl ich mir völlig bewußt war, was ich da tun möchte. Man kann das PopUp lediglich mit "OK" bestätigen, aber nicht direkt eine Verbindung aufbauen.

SmartDefense Advisor — Überblick | Technische Infos | Details | Hacker ID

Ihr Computer versucht, die IP-Adresse zu kontaktieren.

ZoneAlarm hat den ausgehenden Datenverkehr blockiert. Keine Beeinträchtigung der Sicherheit.
Ihr Computer ist sicher.

Was ist geschehen?

Die ZoneAlarm-Firewall hat ausgehenden Datenverkehr von Ihrem Computer zu Port 1723 eines Remote-Computers mit der IP-Adresse blockiert. Der Grund hierfür könnte darin bestehen, dass ein Programm auf Ihrem Computer versucht hat, eine Verbindung mit dem Internet herzustellen, bevor ZoneAlarm vollständig einsatzbereit war.

Gibt es Grund zur Besorgnis?

Nr. ZoneAlarm hat den Zugriffsversuch verhindert, so dass kein Schaden an Ihrem Computer angerichtet werden kann.

Was soll ich tun?

Klicken Sie auf **OK**, um das Meldungsfeld zu schließen. Sie erteilen dadurch keine Erlaubnis für ein- oder ausgehenden Datenstrom.

Standardmäßig ist ZoneAlarm so konfiguriert, dass das Programm beim Hochfahren des Computers automatisch gestartet wird. Um optimalen Schutz zu gewährleisten, empfehlen wir, diese Einstellung nicht zu ändern.

Falls Sie weiterhin Warnungen dieser Art erhalten, sollten Sie überprüfen, welche anderen Programme beim Hochfahren des Systems gestartet werden.

Was liegt näher als die SmartDefense Advisor "Weitere Hilfe" in Anspruch zu nehmen. Jedoch sind die dort getroffenen Aussagen wenig befriedigend, weil diese Verbindung ja bewußt iniziiert werden sollte. Ich darf zwar jede unseriöse Internetseite in der ganzen Welt ansurfen, aber den eigenen VPN- Server kann man nicht kontaktieren - jedenfalls nicht direkt.

Programme	Zugriff		Server	
	Sicher	Internet	Sicher	Internet
Adressbuch für den remote Zugriff	?	?	?	?
Application Layer Gateway Service	?	?	?	?
AVG E-Mail Scanner	?	?	?	?
firepass_test_v3_0b.exe	?	?	?	?
Generic Host Process for Win32 Se...	✓	✓	✓	✗
Google Earth	?	?	?	?
Internet Explorer	✓	✓	?	?

Es ist dazu erforderlich, dass der User die manuelle Konfiguration von Zonealarm beanspruchen muss. Das ist nicht weiter tragisch, würden sich da nicht fast schon unüberwindbare Hürden vor dem Durchschnittsuser aufstellen. Ein IT- Profi wird hier wenig Probleme haben und ein versierter Anwender kann auch unter Umständen recht zügig zum Erfolg kommen. Als ungeübter PFW- User musste ich natürlich die angebotene Hilfe- Funktion bemühen, weil ich ja schließlich erfahren wollte, was mit den Zeichen in den verschiedenen Spalten gemeint ist und natürlich was die Spalten selbst bedeuten. Ich darf an dieser Stelle behaupten, dass die integrierte Hilfe- Funktion von Zonealarm deutlich komplizierter zu bedienen ist wie die Firewall selbst. Viele User werden wohl genervt den typischen Fehler machen, hier mit den Häckchen, Kreuzen und Fragezeichen rumzuprobieren bis letzendlich alles funktioniert, was ihnen wichtig erscheint, selbst wenn nur noch grüne Häckchen zu erblicken sind.

Detailinformationen für Eintrag

Produktname	Betriebssystem Microsoft® Windows®
Dateiname	C:\WINDOWS\system32\rasphone.exe
Letzte Richtlinien...	Nicht zutreffend
Version	5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
Datum der letzten...	04.08.2004 01:58:10
Dateigröße	56 KB

Ergänzend möchte ich noch die Detailansicht anmerken, welche mir zumindest einen Zusammenhang der obigen Tabelle zu den Applikationen anzeigt. Auffällig zu anderen PFW's war für mich die Feststellung, dass außer in den PopUps keine Porteinstellungen in der manuellen Konfiguration zu finden waren (vieleicht habe ich das auch nur übersehen). Ob das nun die Konfiguration für den Laien erleichtert, sei mal dahingestellt.

Zitat: Netzwerk- und Programm-Firewall Bietet proaktiven Firewall-Schutz mit mehreren Sicherheitsebenen, die Attacken von innen und außen blockieren, Angriffe auf andere Programme verhindern und Ihren PC Hackern gegenüber unsichtbar machen.

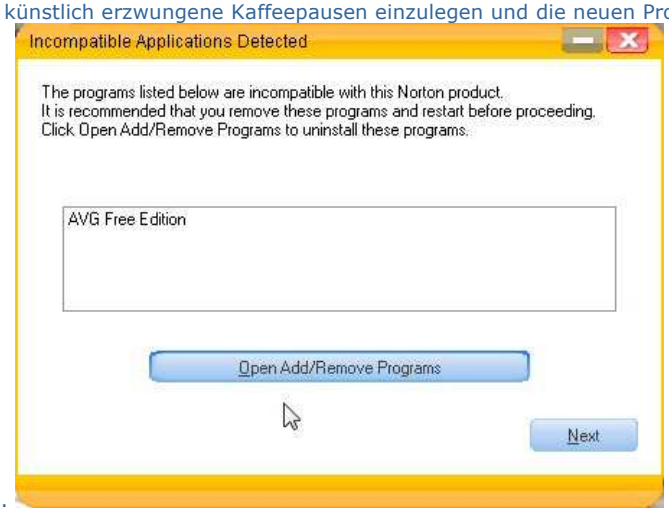
- *Die weltweit führende Firewall verhindert, dass Bedrohungen von außen oder innen den Netzwerkperimeter durchbrechen.*
- *Verhindert, dass Spyware und andere bösartige Programme Ihre persönlichen Informationen über das Internet übertragen.*
- *Sorgt mit umfassendem Stealth-Modus dafür, dass Sie im Internet völlig unsichtbar sind.*
- *Schützt Ihre Programme vor Malware.*

Quelle: ZoneLabs Homepage

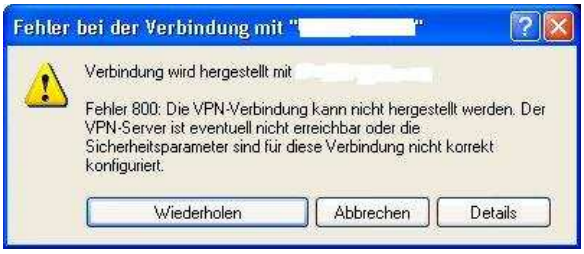
Was nun ZoneLabs selbst von Ihrer Software verspricht ist teilweise falsch und auch anmaßend. Die Realität beweißt das Gegenteil und die Marketingabteilung sollte besser etwas tiefer stapeln mit solchen Behauptungen. "**Verhindert, dass Spyware und andere bösartige Programme Ihre persönlichen Informationen über das Internet übertragen**" ist anhand der bewiesenen Sachlage, dass ZoneLabs sich selbst solcher Praktiken bedient hat(te), allein schon ein Grund, diese Software zu meiden, selbst wenn diese PFW nach eigenen Angaben die "führende" sein sollte.

Das "Beste" zum Schluss: **Norton Internet Security (2007)** Direktlink zum Forum

Nachdem ich schon einige Personal Firewalls getestet hatte, habe ich gedacht, dass der Vorreiter der sog. Security Suites nicht fehlen sollte. Die unter der Abkürzung **NIS** berühmt und berüchtigt gewordene Software, eilt der Ruf voraus, ein Windows-System so richtig nachhaltig ausbremsen zu können. Dies konnte ich nun selbst live erleben und musste etwa geschlagene 20 Minuten vom Systemstart an warten, bis die Anwendung **Paint Shop Pro 8.0** arbeitsbereit gestartet werden konnte, was zuvor noch in einem erträglichem Rahmen von 2 bis 3 Minuten geschehen ist. Als Testplattform wurde ein Laptop IBM Thinkpad T41 (512 MB RAM, 2000Mhz) verwendet. Allein der Umstand, dass **NIS** etwa 70 MB Festplattenplatz benötigt und das System mit etlichen weiteren Systemprozessen belastet, ganz zu Schweigen von Ummengen an Registry- Einträgen, die eigentlich nicht mehr überschaubar sind, ist ein vernünftiges Arbeiten kaum noch möglich. Ich hatte beinahe den Eindruck, als würde ich mit **NIS** ein eigenständiges Betriebssystem installieren, dass sich im Prinzip zur Masteranwendung des Systems erklärt hätte und alle weiteren Anwendungen nur noch beiläufig notgedrungen akzeptiert. Die Hauptaufgabe des Anwenders besteht ab sofort darin, künstlich erzwungene Kaffeepausen einzulegen und die neuen Problemstellungen, die nun durch **NIS**



auftreten, zu ergründen. Bei **NIS** gilt zudem noch das 2. biblische Gebot (Du sollst keine anderen Götter haben neben mir) und fordert den Anwender auf, andere Antivirensoftware zu entfernen. Das sollte aber das geringste der kommenden Probleme gewesen sein.



Ein Versuch der Kommunikation zu einem VPN- Server wurde kommentarlos verweigert. Auch die Änderung der Einstellungen zu dieser Sache in der der Sektion "Personal Firewall" brachten keinerlei Abhilfe. Man sieht in der Abbildung unten die verantwortliche Applikation für die VPN- Verbindung als **rasphone.exe** . Weder die Einstellung "custom" noch "allow" brachten den gewünschten Erfolg. Da leider nicht wirklich ersichtlich zu sein scheint, wie man diesbezüglich die Personal Firewall konfigurieren könnte, ist man gezwungen, ein nicht unerhebliches Sicherheitsrisiko einzugehen...und hier ist sie wieder: **die Sinnfrage** !

Erst nach vollständiger Deaktivierung der Firewall- Funktionen konnte eine Verbindung zum VPN- Server hergestellt werden. Da der Hersteller sowie diverse Tester in PC- und Online- Magazinen die unauffällige Arbeitsweise von **NIS** im Hintergrund, ohne dass der Anwender zur Interaktion aufgefordert wird, als positives Feature werten, hat der User auch kaum eine Möglichkeit, die anfallende Probematik zeitnah zu erkennen. Ich erdreiste mir zu behaupten, dass ein Laie nicht in der Lage sein wird, eine PPTP- VPN Verbindung bei aktiver **NIS**- Firewall herzustellen. Als ich dann zu Testzwecken die Warn PopUp- Anzeige aktiviert hatte, wurde ich mit Unmengen an Verbindungsanfragen überflutet. Teilweise meldeten sich **iexplore.exe** und **svchosts.exe** gleich mehrfach und der User kommt in arge Bedrängnis, ob er nun die Anfragen nach Verbindungen positiv oder negativ beurteilen soll. Wenn vielleicht bis dahin die Sicherheit noch weitgehend stabil gewesen sein sollte, so wird spätens jetzt durch die Interaktivität des Users ein Loch nach dem anderen in die Firewall gebohrt. Überläßt der User jedoch die Kontrolle gänzlich **NIS**, muss er eben gewisse Einschränkungen erdulden, sobald die Kommunikation über den üblichen bekannten Standard wie ihn **NIS** kennt, hinaus geht. Übrigens versuchte ich auch gleich ein Update zu machen, was zumindest in einem Punkt mit einem Fehler quittiert wurde und ca. weitere 15 Minuten das parallele Arbeiten mit dem PC deutlich beeinträchtigte. Wer also stolzer Besitzer dieses Sicherheitspaketes ist, braucht starke Nerven und hat wohl gute Chancen, dass jegliche Malware erst gar kein Interesse an einem solch zähflüssigen System haben wird. Der Grund für diesen Fehler ist beinahe schon deprimierend:

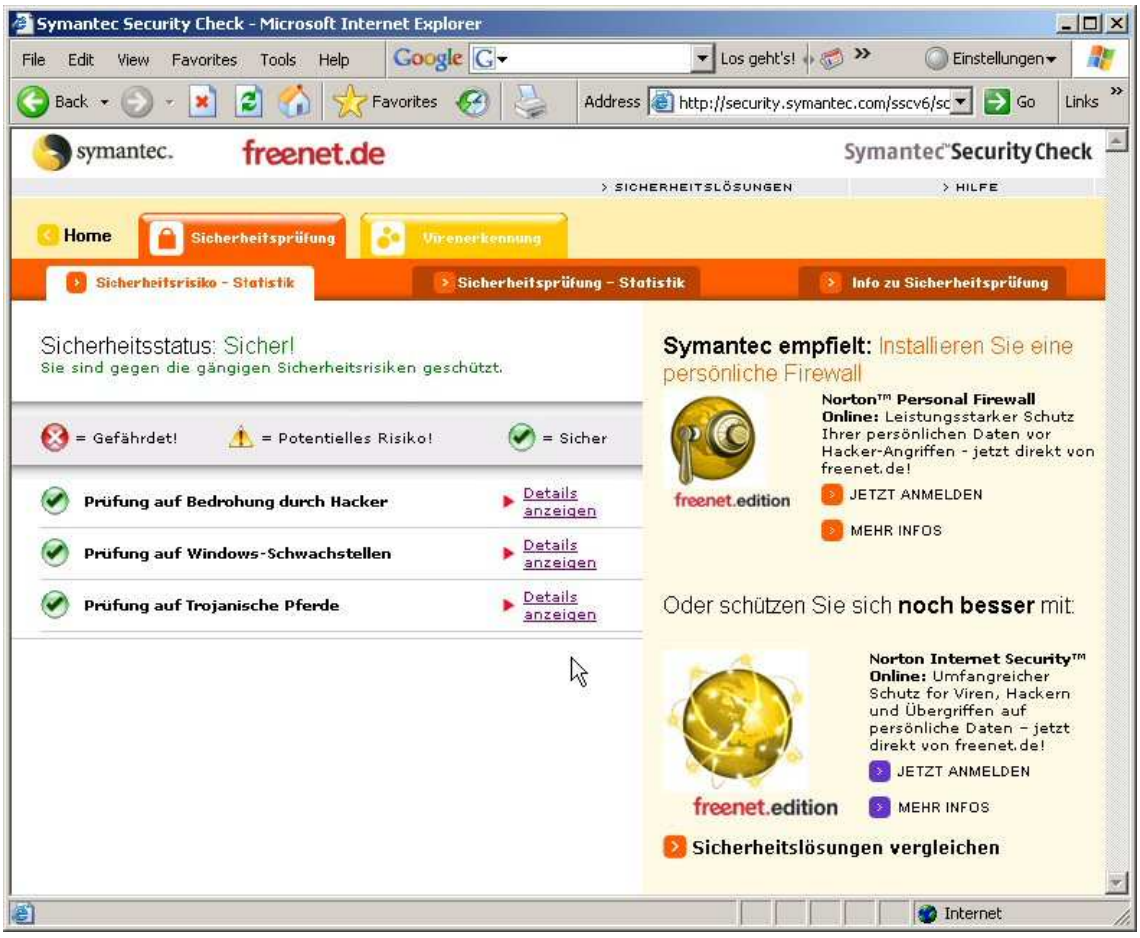
Dabei ist es weniger tragisch, dass **NIS** seine eigenen Dienste ebenso blockt wie unerkannte Programme, aber geradezu lächerlich, dass die eigene Personal Firewall die eigene Update- Funktion offensichtlich nicht erkennt...

Auf vielfachen Wunsch hin, hauptsächlich von (leider) anonymen Symantec Symphatisanten) habe ich die Installation des Paketes erneut durchgeführt. Ich habe wiederum den Laptop Thinkpad T41 (2000Mhz, 512 MB RAM) mit einer frischen Windows XP SP2 Standardinstallation und einigen Anwendungen verwendet, so wie ich ihn auch für die Tests der anderen PFW's benutzt habe. Die Installation dauerte nunmehr insgesamt mit LiveUpdate (das sich automatisch während der

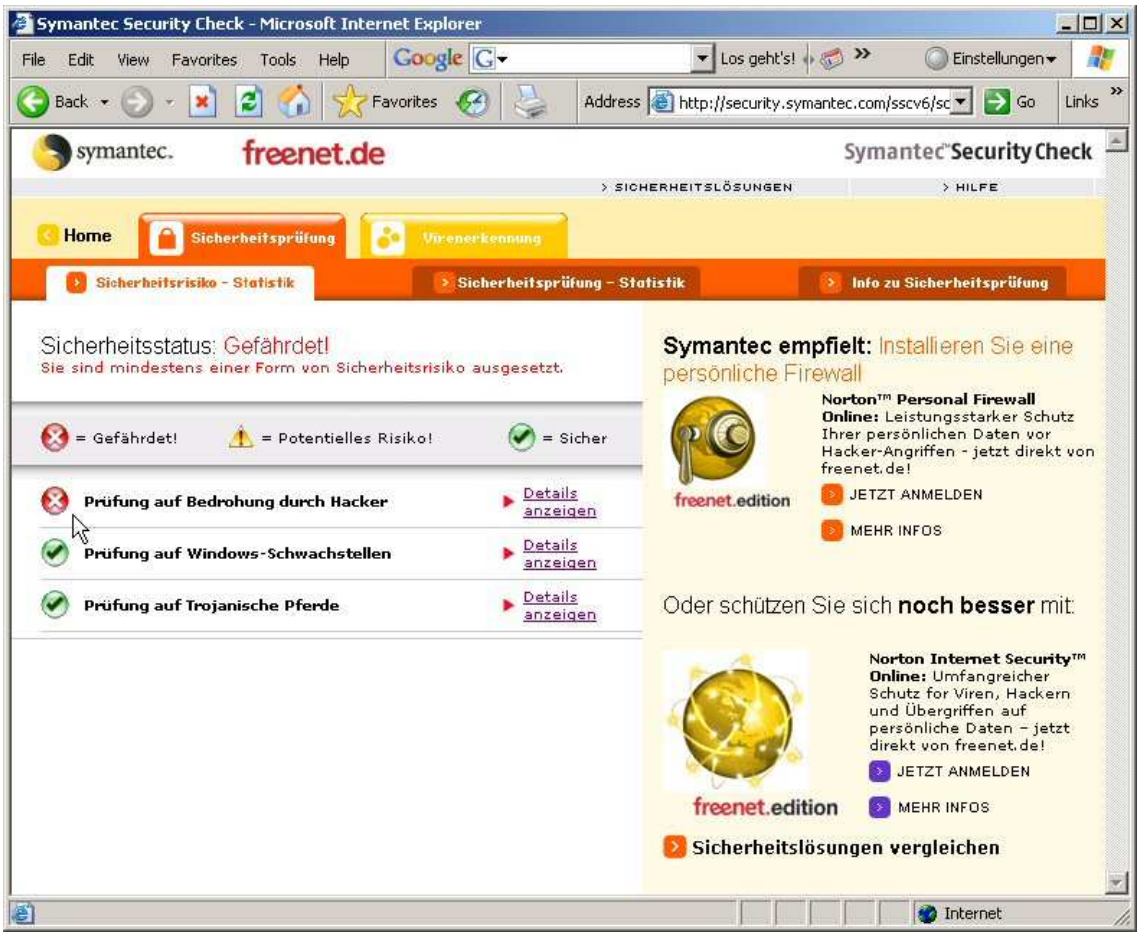
Installation meldete) immerhin 23 Minuten. Eine Breitbandverbindung zum Internet mit etwa 3000Mbit/s sollte eigentlich ausreichen, um zügig alle Updates durchzuführen. Allein für das Online- Update wurden 10 Minuten benötigt, also dauerte die reine Netto- Installationszeit auf diesem System ca. 13 Minuten. Der anschließende Start von Paintshop Pro 8 war mit ca. 1 Minute diesmal deutlich schneller und läßt damit den vorherigen Test fraglich erscheinen. Es ist natürlich mühsig, sich nun über Installationszeiten von Programmen zu unterhalten, zumal jeder individuell andere Systemvoraussetzungen vorliegen hat. Aber man kann sagen - wieder etwas dazugelernt: Ohne bedeutende Änderungen an der Testumgebung vorgenommen zu haben, war das Ergebnis zumindest in diesem einen Punkt deutlich abweichend, was mich zu der Erkenntnis bringt, dass eigentlich ein einziger Test nicht ausreicht, zumindest wenn es um Installationsgeschwindigkeiten gehen sollte. Erwischt man einen ungünstigen Zeitpunkt und das System werkelt im Hintergrund rum, kann das deutliche Unterschiede bewirken. Auf performanten Windows- Systemen sind die Resourceneinbußen natürlich weniger auffällig als auf einer leistungsschwachen Maschine und der entsprechende User muss dies berücksichtigen. Möglicherweise (da könnten Symantec Experten eher was dazu beisteuern) könnte die Problematik des ersten Testlaufes damit zusammenhängen, dass ich das LiveUpdate während der Installation übergangen habe und dies später manuell gemacht habe ? Die Installation der (überflüssigen) Yahoo- Toolbar und einer direkten Virenprüfung habe ich bei beiden Installationsläufen übergangen. Die Installation einer Security Suite sollte aber nicht so stark bewertet werden, wie die eigentliche Aufgabe der Software während des Betriebes und ich möchte mich hiermit nicht über die Maße damit beschäftigen. Wenn ja die Installation ohne große andere Probleme abläuft, ist der Zeitfaktor sicherlich für die meisten User vernachläßigbar...

Symantec beweißt Einfallsreichtum (August 2007)...

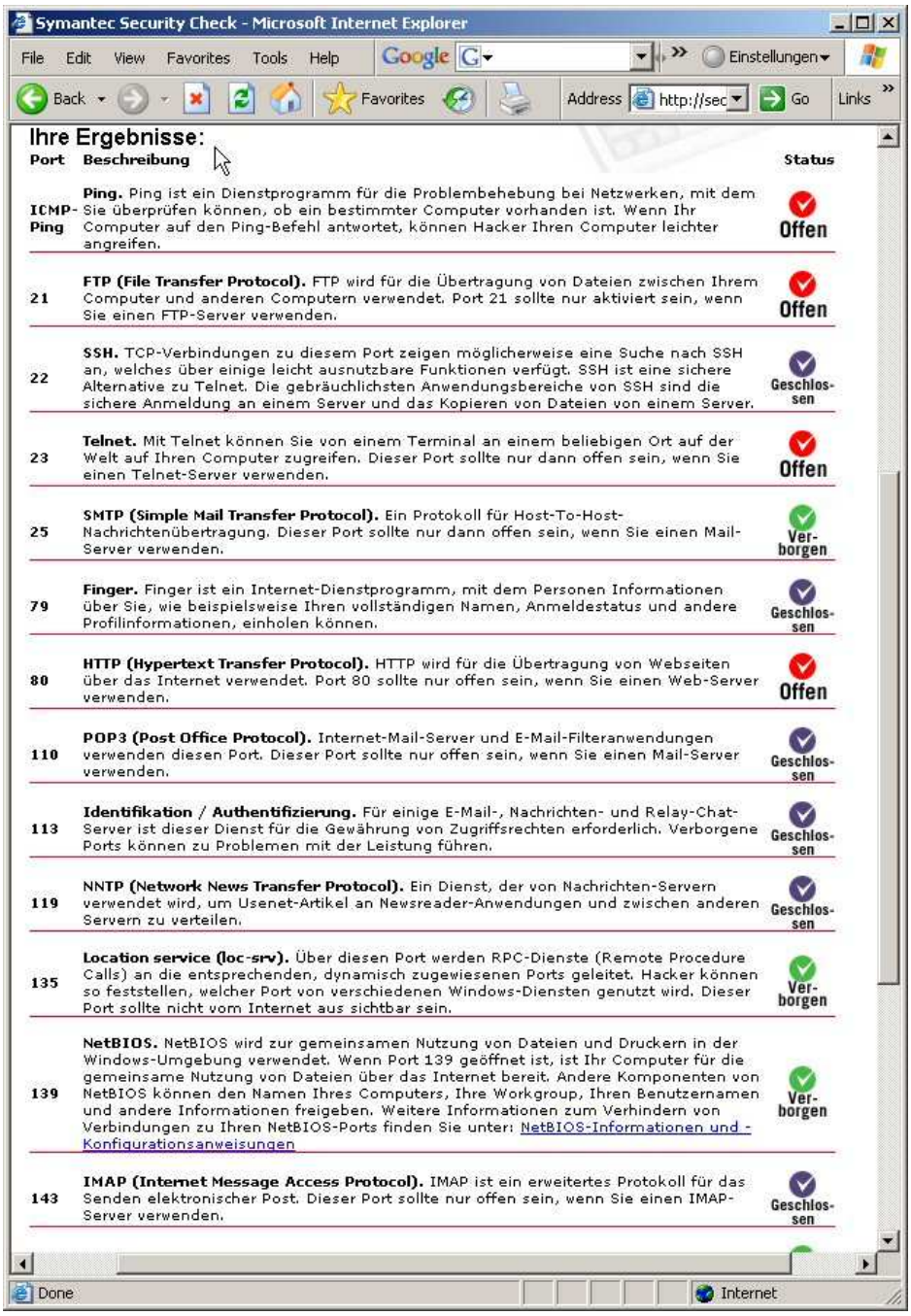
...wenn es darum geht, die eigenen Produkte zu vermarkten. Per Online- Security Scan kann ein User sein System "überprüfen" lassen: http://security.symantec.com/



O.K. dachte ich mir, teste ich auch mal das Online- (Security) Angebot von Symantec. Grundsätzlich möchte ich nicht unerwähnt lassen, dass man durch solche Online- Tests dem Testanbieter volles Vertrauen schenken muss und sich darüber im Klaren sein sollte, dass dieser dadurch u.U. alle Daten auf dem Testsystem einsehen könnte. Daher wäre ein solcher Online- Test bei mir im Normalfall eher nicht akzeptabel. Ich habe den besagten Test nun auf 2 unterschiedlichen Testsystemen durchgeführt. Zum ersten habe ich ein Windows XP- System mit vielen installierten Programmen und aktuellen Patchlevel mit zusätzlich installierter McAfee Viren- und Malware Enterprise Edition, das sich hinter einer professionellen Hardwarefirewall befindet, untersuchen lassen. Die obige Abbildung zeigt das Ergebnis, welches eigentlich eine ausreichende Sicherheit bestätigt. Unverständlicherweise empfiehlt Symantec trotzdem die Installation einer "persönlichen Firewall", natürlich vorzugsweise eines der eigenen Produkte. Ich werte dies als eindeutigen Beweis für eine marktstrategische Irreführung von potentiellen Kunden, wobei auf deren Unkenntnis gesetzt wird. Ich weiß nicht recht, was mich dazu bewegt hat, womöglich meine Skepsis gegenüber solch fragwürdigen Angeboten, aber ich führte den gleichen Test auf dem gleichen System gerade mal 5 Minuten später ein zweites Mal durch:



Die Firma Symantec könnte nun damit aber in arge Erklärungsnot geraten, denn wie bitte kann der Test unter gleichen Bedingungen, lediglich 5 Minuten später, ein anderes Ergebnis liefern ? Plötzlich ist das System gefährdet durch Hackerangriffe und Symantec rät weiterhin (standardmäßig) eine "persönliche Firewall" oder noch besser "Norton Internet Security" zu nutzen. Doch ist es sicher aufschlussreich, sich die Details anzeigen zu lassen:



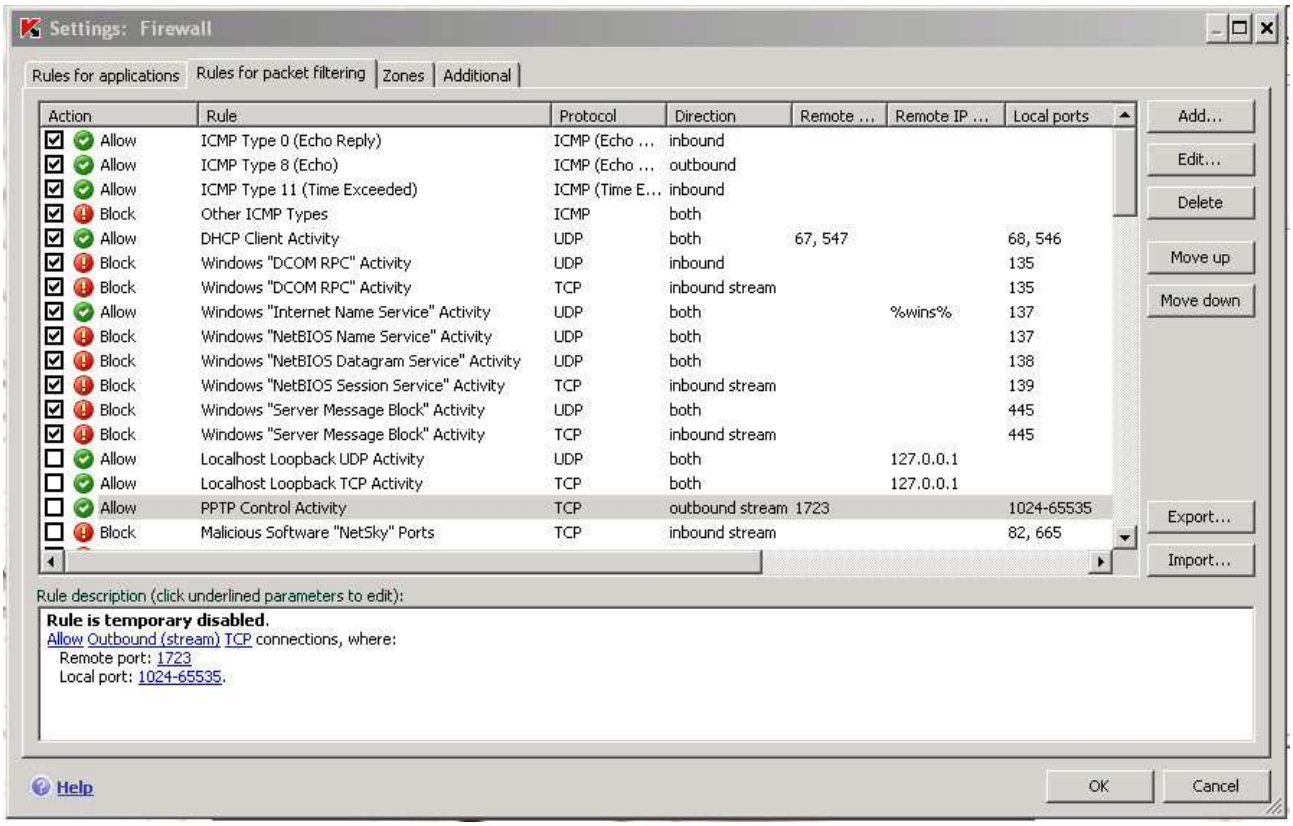
Der Ping wird plötzlich beanstandet. Dieser Befehl ist für Netzwerk- Admins ein unverzichtbares Instrument, um Probleme in Netzwerken zu analysieren. Im vorliegenden Fall, also beim verwendeten Testsystem ist ein Ping intern im Netzwerk möglich und auch sinnvoll, aber nicht von außerhalb. Diese Analyse ist **falsch**. Auf dem Testsystem ist kein FTP- Server installiert. Port 21 ist daher nicht offen. Diese Analye ist **falsch**. Telnet hingegen ist bei Bedarf offen, d.h. wenn clientseitig eine Telnet-Session zu einem Remote- System initiiert werden muss. Diese Analyse ist bedingt richtig, sollte aber in beiden Tests zum gleichen Ergebnis führen, gleich ob positiv oder negativ. Somit ist diese Aussage mehr als verwirrend, zumal zum Testzeitpunkt keine Telnet- Session eröffnet war. HTTP (Port 80) ist laut Testergebnis ebenfalls offen, obwohl kein Webserver installiert ist. Hingegen wird Port 80 remoteseitig geöffnet, wenn man per Browser auf eine Internetseite zugreift. Dieser Test ist mehr als fragwürdig und liefert auch bei anderen Online- Tests unverwertbare Ergebnisse. Wenn kein Webserver auf dem System installiert ist, ist ein angeblich offener Port 80 sowieso unbedenklich. Als Referenztest habe ich noch einen frisch installierten Laptop (Windows XP SP2 mit akuellem Patchlevel, Antivirensoftware Avira Antivir 7 Free) ohne jegliche Firewall an einen WLAN- Hotspot verbunden. Das Testergenis des Symantec- Online Scans hat mich aufs neue verblüfft:

Es wurde diesmal "firewalltechnisch" nichts bemängelt, obwohl offensichtlich und mit voller Absicht weder eine Hardware- noch eine Softwarefirewall verwendet wurde. Hingegen scheint Symantec die Avira Antivir 7 Freeware- Edition nicht als Antivirensoftware zu akzeptieren:

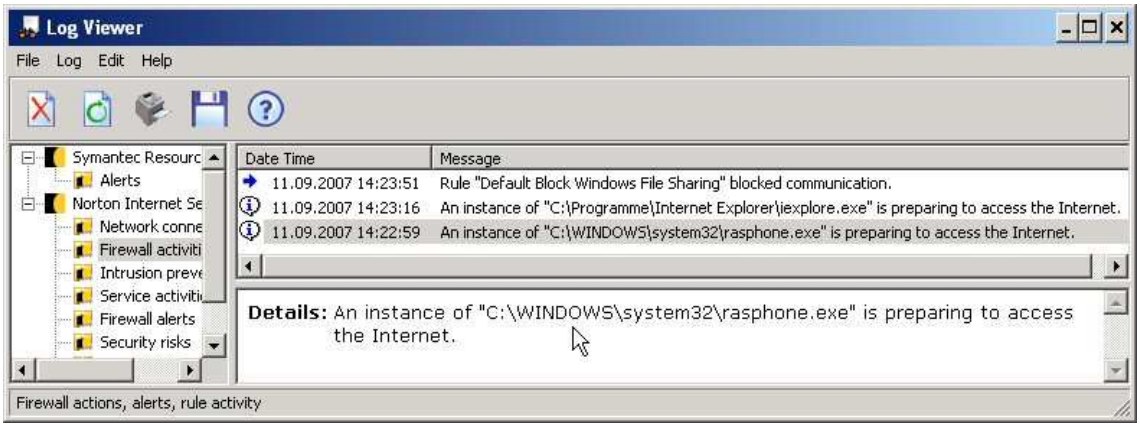
Wie aus dem Detail- Ergebnis hervorgeht, ist dem Symantec Online- Testserver offensichtlich entgangen, dass ein Konkurrenzprodukt seine Arbeit auf dem Testsystem verrichtet. Meine Frage an alle Freunde von Symantec- Produkten muss folglich lauten: Woher nehmt ihr bitte euer Vertrauen in solche Produkte (Angebote), die offensichtlich auf ganzer Linie desaströs versagen ? Anmerkung: Eine Security Suite ist nicht mit einem Online- Security Test vergleichbar und daher sollte dieser Umstand berücksichtigt werden.

Nochmal NIS - diesmal Version 2008 (Trial- Version) vs. Kasperski 7.0

Symantec hat mit der 2008er Version tatsächlich einen Quantensprung geschafft. Die Probleme mit VPN bzw. FTP wie sie die Vorgängerversion noch hatte, bereiteten im Test erfreulicherweise keine Schwierigkeiten. Auch in Sachen Performance hat Symantec dazugelernt, das muss man neidlos zugestehen. So kann diese Suite nunmehr mit dem Konkurrenzprodukt **Kasperski 7.0** in etwa wieder gleichziehen. Ich führe Kasperski 7.0 deshalb an, weil ich diese Suite zwar auch kurz angetestet hatte, aber keine offensichtlichen Mängel feststellen konnte. Ein ausführlicher Testbericht kann somit entfallen und ich beschränke mich mit einem Vergleich dieser beiden Produkte:

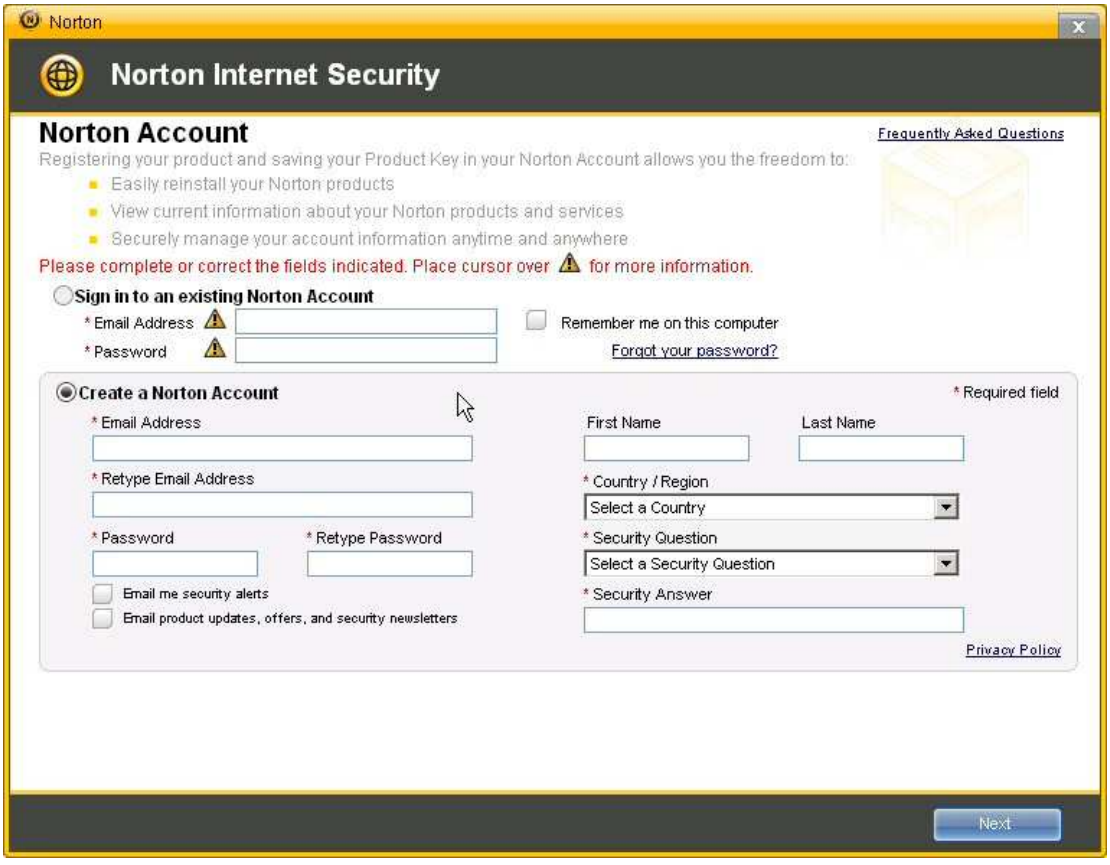


So stellt Kaspersky 7.0 die initiierte VPN- Verbindung dar und hat diese anstandslos akzeptiert.



Bei **NIS 2008** sieht so aus. Auch hier wurde die VPN- Verbindung ohne weitere Konfiguration akzeptiert. Die entsprechenden Log- Files werden zwar nach wie vor von Laien nicht interpretierbar sein, aber der Umstand, dass die Benutzerfreundlichkeit dahingehend deutlich verbessert wurde, läßt dies verschmerzen.

Kaspersky's Hauptproblem scheint die Update- Funktionalität zu sein. Hiermit hatte ich im Test einige Probleme.



Bei **NIS 2008** störte mich hauptsächlich, dass Symantec nun auch für Trial- Versionen eine Registrierung verlangt. Hier besteht zwar Spielraum für Manipulation, aber es müßte wirklich nicht sein. An dieser Stelle konnte ich aber auch einen Fehler provuzieren. Besteht nämlich keine Online- Verbindung, wenn man mit dem "Next"- Button weiter machen möchte, kann man die komplette Installation durcheinander bringen. Im Testfall war ein Reboot nötig, um die Installation erneut vorzunehmen. Damit hat Symantec sich völlig unnötigerweise ein Problem beschert.

Fazit (NIS 2008 & Kaspersky 7.0) : Von den getesteten Security- Produkten konnten diese beiden am meisten überzeugen. Dies führe ich darauf zurück, dass für den Laien die geringsten Konfigurationsprobleme auftreten. Dennoch überzeugt mich das alles nicht davon, dass man auf eine Personal Firewall bzw. Security Suite nicht verzichten könnte.

Geht's auch ohne Personalfirewall: Alles eine Frage des Konzeptes

Emailanhänge niemals öffnen, wenn diese aus unbekannten Quellen stammen!
Emails von scheinbar vertrauenswürdigen Quellen trotz allem kritisch begutachten, gegebenenfalls nachfragen, wenn

Zweifel bestehen sollten, denn auch Emailadressen lassen sich fälschen!
Emailanhänge mit mehrfach kombinierten Dateinamensendungen (pdf.exe) o.ä. niemals öffnen!
Den Besuch fragwürdiger und unseriöser Internetpräsenzen vermeiden!
Nicht auf alles "klicken" was auf dem Monitor erscheint, wenn man nicht genau weiß, was auf einen zukommt!
Sog. Online- Tauschbörsen sehr vorsichtig begutachten, bestenfalls meiden!
Das Windowssystem sollte immer auf dem aktuellen Patchlevel gehalten werden!
Antivirensoftware sollte immer aktuell sein und auch aktiv das System überwachen!
Bei der Installation von Freeware sollte man genau lesen und beachten, was evt. noch zusätzlich als Adware mitinstalliert wird!
Nach Möglichkeit nicht mit einem User, der administrative Rechte besitzt, online gehen, was das Risiko heimlicher Installationen erheblich reduziert!
Firewalls richtig konfigurieren (lassen), wenn möglich, Hardwarelösungen den sog. Desktop- Firewalls vorziehen!
Desktop- Firewalls unbedingt korrekt konfigurieren, da eine falsch eingestellte Firewall u.U. eine scheinbare Sicherheit vortäuscht!
Linux (Knoppix, Ubuntu) oder Windows PE von Live- CD nutzen!

Darüberhinaus werden PFW's von Menschen programmiert, denen Fehler unterlaufen können, deren Auswirkungen gar nicht abschätzbar sind. Nicht selten werden neben den bekannten Patches von Microsoft auch immer wieder Bugfixes vieler anderer Softwareprodukte angeboten, wozu auch nicht selten sog. Sicherheits- Suites gehören. Allein dies bestätigt, dass man sein Vertrauen u.U. einem Produkt schenkt, welches selber nicht richtig funktioniert. Und wer kann übrigens seine Hand dafür ins Feuer legen, dass ein solches Programm wie eine Personal Firewall nicht mißbraucht werden kann, ob vom Hersteller selbst oder unbewußt durch Dritte, die Schwachstellen darin für eigene Zwecke ausnutzen ? Wer bereits einen DSL- Router besitzt, hat meist schon einen Firewall- Grundschutz, der im Zusammenspiel mit Virenscanner und umsichtigem Surfverhalten eigentlich völlig ausreichen dürfte. Wozu braucht man nun bitte schön noch zusätzlich eine Personal Firewall ?

Wichtige Links zum Thema "Internet Sicherheit"

Wikipedia zum Thema

Live Demo des Chaos Computer Clubs

Wie Personal Firewalls ausgetrickst werden!

Interessante Ausführungen von Alexander Böhm

geniales Video über Datentransfer

Sicherheitslücken bei Personalfirewalls (Jörg-Olaf Schäfers)

Timo Kehler's Sinn und Unsinn von Personal Firewalls

Lutz Donnerhacke's Firewall Kompendium

Universität Münster (Rainer Perske's Beschwerde- Management)

Sehr verständliche Abhandlung von Olaf Lukas

Kompromittierung unvermeidbar ? - auch für Laien lesenswerte Abhandlung von Malte J. Wetz

Wie mache ich meinen PC sicher ? - Umfassende Abhandlung zum Thema PC- Sicherheit von Bernd Homberg

Es ist darüber hinaus auch interessant in einer Suchmaschine nach dem Begriff "Personal Firewall" suchen zu lassen. Man findet entweder kommerzielle Angebote, die darauf abzielen, Kunden für das jeweilige Produkt überzeugen zu wollen, indem sie die Unverzichtbarkeit ihres Produktes im Zusammenhang mit Internetsicherheit demonstrieren oder eben Artikel, meist privat iniziiert, von meines Erachtens fast ausschließlich Experten, die mehr oder weniger auf die Gefahren des Einsatzes von Personal Firewalls hinweisen.

Dann findet man auch einige Tests, meist von den gängigen Online- Redaktionen diverser Computer- Magazine, deren Priorität im Verkauf ihrer Printmedien liegt und dafür gerne aktuelle und interessante Themen aufgreifen. Ob da eine gewisse Subjektivität beim Testen im Spiel ist, darf vermutet werden, wenn man bedenkt, dass die Hersteller von diesen Sicherheitspaketen wiederum mehr oder weniger Werbepartner dieser Magazine sind. In verschiedenen Online- Foren einiger dieser Online- Magazine wurde ich nach meinen Statements zum Thema inzwischen gebannt, weil ich angeblich Werbung betreiben würde, was laut Forenregeln untersagt sei. Sehr merkwürdig, dass die Verlinkung zu diesem Forumsbeitrag als Werbung gewertet wird, während gleichzeitig andere Links zu Download- und Bezugsquellen diverser Anbieter unzensiert bleiben. Daher habe ich eigens ein separates Forum eingerichtet, wo ich nicht der Willkür anderer ausgeliefert bin.
Mir ist bewußt, dass in manchen Foren diese Diskussionen weitergeführt werden, aber es würde mich auch freuen, wenn welche hier in die Diskussion einsteigen würden - ganz gleich welche Meinung sie vertreten, sie wird akzeptiert und eine User-Verbannung oder Sperrung wegen Verlinkung auf sachbezogene Websites ist auch nicht zu befürchten: Forum (Personal Firewalls)

hier geht's weiter Dokument wird sonst zu lang!