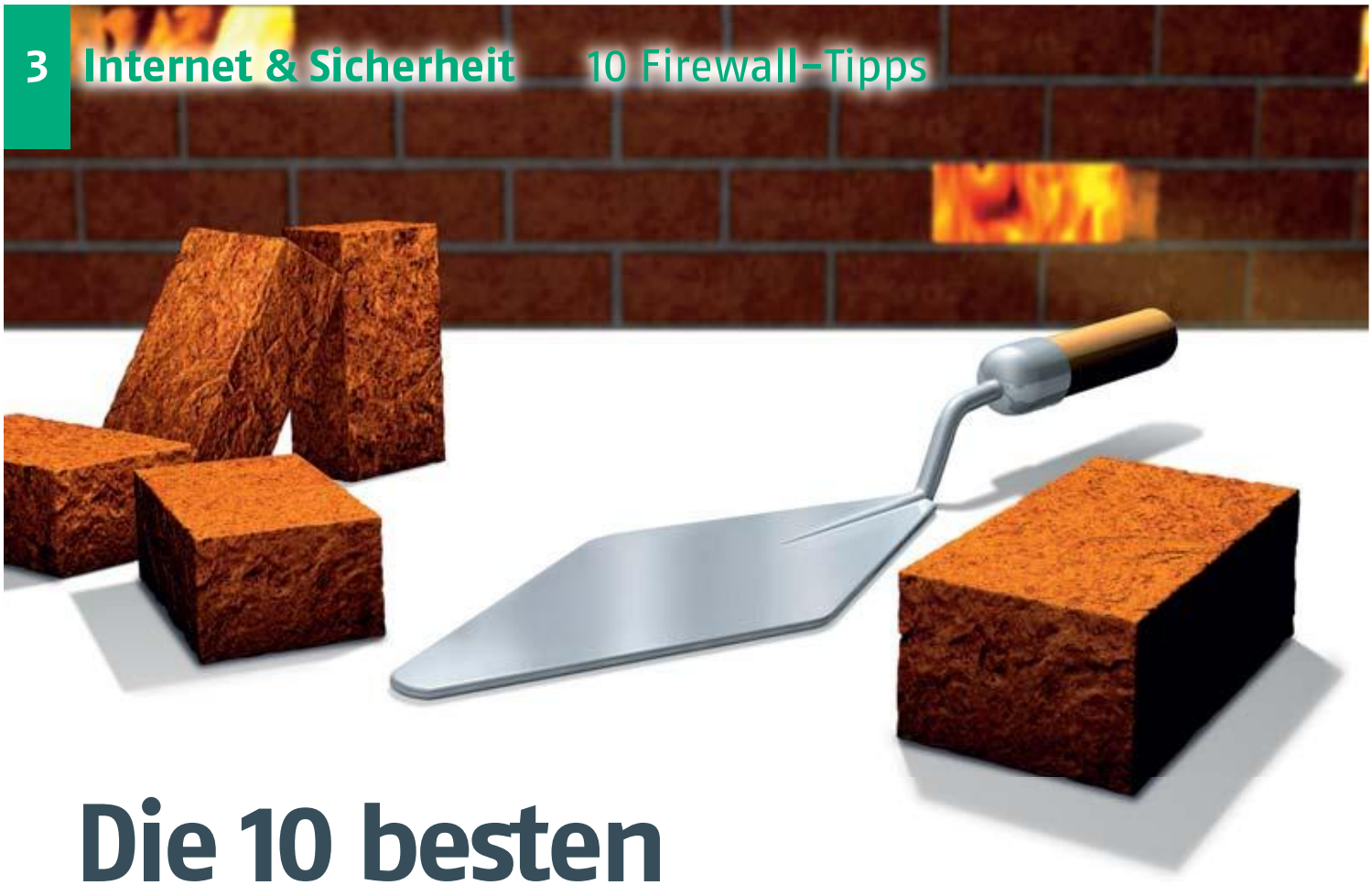


Die 10 besten Firewall-Tipps

Mit einer Desktop-Firewall schützen Sie Ihren Rechner effektiv vor Angriffen aus dem Internet. Allerdings darf beim Konfigurieren kein Fehler passieren. Mit unserer Schritt-für-Schritt-Anleitung machen Sie Ihr System bombensicher.

Von **Arne Arnold**

Eigentlich machen Sie alles richtig: Sie halten Ihr Windows auf dem neuesten Stand, Sie setzen Antiviren-Software ein. Da kann kaum noch etwas passieren ... Falsch. Ständig werden Sicherheitslücken aufgedeckt und neue Schädlinge verbreitet, die der Virenscanner noch nicht kennt. Für eine Infektion reicht es schon aus, wenn Ihr Rechner mit dem Internet verbunden ist – unabhängig davon, welchen Browser Sie verwenden oder welche Web-Seiten Sie besuchen. Denn die Schädlinge durchforsten das Internet automatisch nach verwundbaren Rechnern.

Desktop-Firewall

Schotten dicht: Darum brauchen Sie eine Firewall

Eine Firewall bietet Schutz gegen fiesen Code. Sie blockt alle unerwünschten Anfragen aus dem Internet ab und sperrt damit die Schädlinge aus. Das gelingt ihr auch bei Windows-Sicherheitslücken, für die noch keine Updates bereit stehen.

Wenn Sie eine Software-Lösung einsetzen, benachrichtigt diese Sie jedes Mal, wenn ein Programm online gehen will, dem Sie das nicht ausdrücklich erlaubt haben. Sie bekommen damit zunächst mal einen genauen Überblick, welche Online-Aktivitäten sich auf Ihrem Rechner abspielen.

Vor allem aber ist diese Funktion das letzte Bollwerk: Sollte sich ein Schädling oder Spionage-Programm am Antiviren-Tool vorbeigeschmuggelt haben, werden Sie darauf aufmerksam, sobald es Kontakt mit dem Internet herstellen will.

Gute Leistung gibt's nur mit Training

So lange Ihre Firewall nicht weiß, was sie erlauben und was sie blockieren soll, über-

schüttet sie Sie mit Fragen. Und die können fortgeschrittene Anwender strapazieren und Einsteiger abschrecken. Denn Sie müssen beispielsweise entscheiden, ob das Programm Svchost.EXE ins Internet senden darf oder nicht. In der ersten Phase sind Geduld und Sorgfalt gefordert. Wer nämlich entnervt bei der x-ten Frage „Darf das Programm XYZ Daten ins Netz senden?", mal schnell auf „Ja" klickt, schafft womöglich einem Trojaner freie Bahn. Und wer bei der manuellen Konfiguration der Firewall einen Fehler macht, der verliert den Schutz vor Angriffen aus dem Internet. Das kann schneller geschehen als gedacht, denn keine Desktop-Firewall ist wirklich einfach zu bedienen.

Freeware oder Bezahl-Software: Eine Frage des Komforts

Im großen Angebot an Desktop-Firewalls finden sich kostenlose Tools und Kaufprogramme. Welche leisten mehr?

Bei kostenpflichtigen Firewalls zahlen Sie für einige Extras: Das wertvollste ist sicher eine Liste, in der bereits viele Programme stehen, die gefahrlos online gehen dürfen. Das erspart es Ihnen, eine Menge kryptischer Fragen zu beantworten. Die Hersteller hochwertiger Firewalls beziehen viele Anwendungen und auch Änderungen an den Windows-Komponenten in ihre Updates mit ein. Außerdem besitzen diese Tools Prüfmechanismen, die über einen einfachen Check von Pfad und Name hinausreichen. Die Lernphase ist bei solchen Produkten deutlich kürzer. Andere Bezahlprogramme kennen allerdings nur ein paar Windows-Systemdateien.

Sicher & bequem: Diese Fähigkeiten guter Kauf-Software bedeuten durchaus ein Plus an Sicherheit. Das Risiko falscher Entscheidungen wird reduziert. Und wenn die Firewall den Anwender nur mit wenigen wichtigen Fragen stört, wird er sich für diese auch mehr Zeit nehmen und nicht vorschnell und vielleicht gar fahrlässig auf „Zulassen" klicken.

Das Sicherheitspaket mit der besten Vorabkonfiguration und den wenigsten Fragen ist übrigens **Norton Internet Security 2007.** Der Trend bei den kostenpflichtigen Firewalls geht übrigens in Richtung Komplettlösung inklusive Antiviren-Software und einiger Zusatz-Tools. So bietet etwa Kaspersky seine Firewall nur noch im Paket **Kaspersky Internet Security** an.

Von Symantec ist nur noch die Version 2006 einzeln erhältlich (Programmlisten werden aktualisiert). Die neue Version der Firewall aber gibt's nur noch im Rahmen des Sicherheitspakets Norton Internet Security 2007. Empfehlenswerte Gesamtlösungen finden Sie in unserem Test „6 Internet-Sicherheitspakete" in der PC-WELT 12/2006, ab Seite 86 (auch auf CD).

Gratis für Fortgeschrittene: Wenn Sie bereit sind, etwas mehr Zeit in die Konfiguration Ihrer Firewall zu investieren, dann genügt eine Freeware dennoch voll und ganz. Sie verzichten damit zwar auf eine fertige Positivliste und ein paar Zusatzfunktionen. Wenn Sie Ihr Tool aber sorgfältig einrichten, kommen Sie auf dasselbe hohe Sicherheitsniveau. Wir geben Ihnen Tipps für die optimale Konfiguration.

Empfehlenswerte Freeware-Tools sind **Zone Alarm Free** (gut geeignet für Einsteiger) und **Comodo Firewall.** Sie finden beide Programme auf CD. Das englischsprachige Comodo richtet sich eher an Profis, die sich auch für Protokollregeln interessieren. Von Zone Alarm haben wir übrigens zusätzlich die allerneueste Version auf CD gepackt. Sie liegt bisher nur in englischer Sprache vor.

Einen Test von fünf Freeware-Firewalls und wichtige Informationen über die Firewall in Windows Vista finden Sie in der PC-WELT 2/2007 ab Seite 74 (auch auf CD).

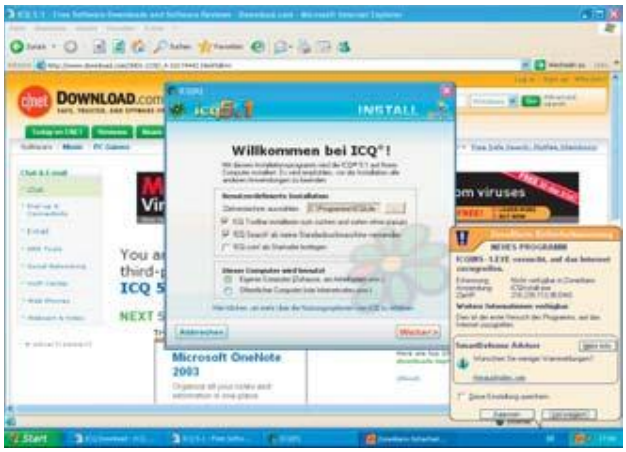
Mit unserer Schritt-für-Schritt-Anleitung klicken Sie sich sicher durch Installation und Konfiguration einer Firewall.

Überblick Firewall-Tipps

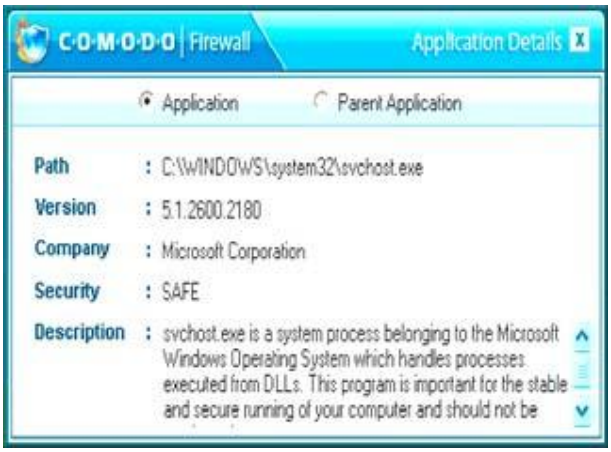
Überblick: Empfehlenswerte Sicherheits-Tools

Programm	Kategorie	Win-Betriebssysteme	Internet (Download)	Preis	Seite
CD **Antivir Personal Edition Classic 7.03**	Antiviren-Tool	98/ME, NT 4, 2000, XP	www.free-av.de (14 MB)	privat: gratis	98
CD **Comodo Firewall Pro 2.4** 1)	Firewall	2000, XP	www.comodogroup.com (8 MB)	gratis	97
Kaspersky Internet Security 6.0	Internet-Sicherheitspaket	98/ME, NT 4, 2000, XP	www.kaspersky.de	40 Euro	97
Norton Internet Security 2007	Internet-Sicherheitspaket	2000, XP	www.symantec.de	60 Euro	97
CD **pcwProcess**	Prozess-Tool	ME, 2000, XP	www.pcwelt.de/bc4 (4 KB)	gratis	99
CD **Zone Alarm 6.5 Free**	Firewall	2000, XP	www.zonelabs.com (14 MB)	privat: gratis	97
CD **Zone Alarm 7.0 Free** 1)	Firewall	2000, XP	www.zonelabs.com (38 MB)	privat: gratis	97

CD auf CD und unter www.pcwelt.de 1) englischsprachig



Meldungen: Im Trainingsmodus informiert eine Firewall über jedes Tool, das eine Verbindung mit dem Internet aufbauen will (Punkt 2)



Mit Pfad: Eine Firewall – hier Comodo – sollte zusätzlich zum Programmnamen einer Anwendung den Pfad anzeigen (Punkt 3)

Firewall-Tipps

1. Scannen, optimieren – und erst dann installieren

Bevor Sie eine (neue) Firewall installieren, sollten Sie sicherstellen, dass Ihr System so sauber und sicher wie möglich ist. Dann geht das Training problemlos vonstatten.

Windows-Updates: Ihr System sollte stets über die neuesten Windows-Patches verfügen. Wenn die automatische Update-Funktion aktiviert ist, werden diese ohne Ihr Zutun heruntergeladen und installiert. Bei Vista erreichen Sie das über „Systemsteuerung, Windows-Update". Wenn Sie diese Option nicht nutzen, können Sie über http://update.microsoft.com prüfen, auf welchem Stand Ihr System ist. Bequem ist auch die automatische Update-Prüfung von Windows. Unter Windows 2000 und XP können Sie sich über „Systemsteuerung, Automatische Updates" benachrichtigen lassen, sobald neue Flicken bereitstehen

Achtung: Wenn Sie online gehen – auch wenn Sie das nur für das Update tun –, sollte zumindest eine einfache Firewall aktiv sein. Basisschutz bieten die entsprechenden Module in in Windows XP SP 2 oder Vista. Sie aktivieren sie über „Systemsteuerung, Windows-Firewall".

Virenschutz: Eine Firewall soll Trojaner und Würmer an schädlichen Aktionen hindern – eine Antiviren-Software soll dafür sorgen, dass sie sich gar nicht erst einnisten. Dieses unverzichtbare Tool muss deshalb immer auf dem neuesten Stand sein. Nutzen Sie also die Update-Funktion. Mit den aktuellen Virensignaturen starten Sie einen manuellen Scan über das gesamte System. Eine empfehlenswerte, kostenlose Antiviren-Software ist **Antivir PE Classic** (auf CD).

Wenn Sie ganz sichergehen und eine zweite Meinung einholen möchten, nutzen Sie einen Online-Virenscanner. Dazu eignet sich etwa der englischsprachige Dienst unter www.bitdefender.de.

Benutzerrechte: Für den Online-Check müssen Sie als Administrator angemeldet sein. Sonst aber gilt: Surfen Sie ausschließlich mit Benutzerrechten. Denn wer als Admin im Netz unterwegs ist, lebt gefährlich. Nicht nur Sie haben dann das Recht, Änderungen an der Windows-Konfiguration vorzunehmen – sondern auch schädlicher Code, der es doch durch die Abwehr schafft. Ein Konto mit eingeschränkten Rechten erstellen Sie über „Systemsteuerung, Benutzerkonten" (Windows 2000, XP, Vista).

Achtung: Achten Sie darauf, nicht versehentlich das Admin-Konto zu löschen. Sonst können Sie unter anderem keine Programme mehr installieren.

Desktop-Firewall installieren: Generell sollten Sie nur ein solches Tool aktiv schalten, da sich zwei Firewalls gegenseitig behindern. Das gilt auch für die Firewalls von Windows XP und Vista.

Gute Tools deaktivieren das systemeigene Firewall-Programm bei der Installation automatisch. Das gilt etwa für die beiden Gratisprodukte Zone Alarm und Comodo. Bei anderen Programmen müssen Sie die Windows-Firewall vor der Installation selbst abschalten.

Die Installation läuft üblicherweise über einen Setup-Assistenten – das ist bequem. In der Regel ist am Schluss ein Neustart erforderlich.

Zone Alarm bietet ein Lernvideo, das in die Bedienung einführen soll. Dieses funktionierte allerdings in der zu Redaktionsschluss aktuellen deutschsprachigen Version 6.5 737 nicht auf unseren PCs. Eine englischsprachige Version des Videos können Sie sich über www.pcwelt.de/17f ansehen.

Nach der Installation sind alle Ports dicht. Von außen – aus dem Internet – lässt sich der PC nicht mehr erfolgreich angreifen.

Tipp: Die kostenlose Version von Zone Alarm fragt gegen Ende der Installation, ob Sie das Tool zu Testzwecken für ein paar Wochen mit den Funktionen der Pro-Version starten wollen. Wir empfehlen, diesen Modus zu nutzen. Dann liefert Ihnen das Tool schon etliche Regeln für bekannte Programme. Diese Regeln bleiben Ihnen auch erhalten, wenn die Firewall später in den Freeware-Modus wechselt.

2. Firewall-Training: Gezielt verbieten und erlauben

Ihre Desktop-Firewall sollte auf jeden Fall einen Trainingsmodus bieten. Auf die Tools in der Tabelle auf Seite 97 trifft das durchweg zu. Training bedeutet: Sobald ein Programm eine Verbindung ins Internet aufbauen will, fragt die Firewall, ob Sie das zulassen. Sie können jeweils einzeln erlauben beziehungsweise verbieten – oder gleich eine Regel festlegen und einen Prozess für die Zukunft zulassen oder blockieren.

Die erste Zeit nach der Installation Ihrer Firewall werden eine Menge Fragen auf Sie

einprasseln, wenn Sie online gehen. Nach dem gründlichen Virenscan sollte es sich dabei nicht mehr um gefährliche Programme handeln. Dennoch sollten Sie sich jede Anfrage anschauen und gegebenenfalls genauer unter die Lupe nehmen (Punkt 3).

Am Anfang kann das Training tatsächlich nerven. So meldet etwa Zone Alarm Free alle sieben Module des Antivirenprogramms Antivir PE Classic einzeln. Wer sich das ersparen will, muss auf eine kostenpflichtige Firewall umsatteln (siehe Seite 97).

Übrigens: Bei einigen Firewalls lässt sich der Trainingsmodus auch abstellen. Alle Verbindungsversuche nach draußen werden dann einfach ohne Meldung geblockt. Dahinter steckt folgender Gedanke: Hat der Anwender ein paar Tage nach der Installation der Firewall alle Online-Programme bereits einmal genutzt und entsprechende Regeln eingerichtet, hat kein neues Tool mehr online zu gehen. Das hat allerdings einen Haken: Wenn Sie den Trainingsmodus abstellen, müssen Sie nach dem Installieren einer neuen Anwendung daran denken, entweder manuell die Rechte zu vergeben oder den Trainingsmodus wieder zu aktivieren. Sonst läuft die Software nicht oder nur fehlerhaft.

3. Lizenz zum Online-Gehen: Meist schnell erteilt

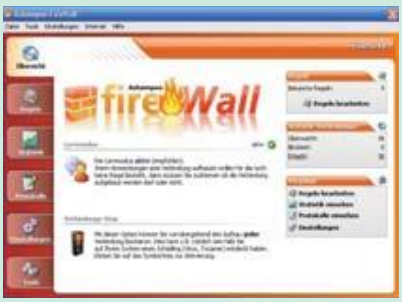
Die Entscheidung, ob ein Programm raustelefonieren darf, lässt sich häufig recht leicht beantworten. Wenn Sie etwa Ihr Mailprogramm Thunderbird zum ersten Mal starten, dann ist es nur logisch, dass Ihre Firewall fragen wird, ob Thunderbird.EXE online gehen darf. Wichtig ist, dass es sich dabei wirklich um das eben gestartete Programm handelt. Das kontrollieren Sie über den Speicherort, also die Pfadangabe und den Namen.

Pfad prüfen: Die Firewall Comodo gibt diesen Pfad bei der Warnmeldung mit an, sobald Sie darin auf den Programmnamen klicken. Zone Alarm Free tut das allerdings nicht – der Hersteller bietet diese sinnvolle Funktion nur bei der Pro-Version. Lösen lässt sich das Problem auf diese Weise: Im Zweifelsfall wählen Sie erst einmal „Verweigern". Öffnen Sie dann das Hauptprogramm von Zone Alarm Free mit einem Doppelklick auf das Symbol im Systray, und gehen Sie auf „Programmeinstellungen, Programme". Dort markieren Sie das eben gemeldete Tool. Unten unter „Dateiname" sehen Sie dann den kompletten Pfad. Wollen Sie dem Tool nun eine dauerhafte Erlaubnis erteilen, dann klicken Sie in der entsprechenden Zeile in die Spalte unter „Zugriff, Internet" und wählen „Zulassen". Dort können Sie sich auch für „Sperren" und „Fragen" entscheiden.

4. Schwierige Fälle: Prüfen Sie, um welchen Prozess es geht

Ab und an meldet sich die Firewall aber auch, ohne dass der Grund gleich ersichtlich ist. Wenn Sie den Programmnamen samt Pfad nicht sicher zuordnen können, sollten Sie misstrauisch sein und die Online-Verbindung zunächst weder erlauben noch verbieten. Recherchieren Sie erst, um was es genau geht. Besonders bequem geht das mit dem PC-WELT-Tool **pcwProcess** (auf CD).

PC WELT SUPERGUIDE FIREWALLS



Können kostenlose Firewalls Attacken zuverlässig abwehren? Ja. Ob auch die Bedienung überzeugt, lesen Sie im Superguide

Computer & Technik

5 Gratis-Firewalls gegen Vista

Wir haben getestet, welche kostenlose Firewall zuverlässig Attacken abwehrt und sich gut bedienen lässt. Im Test hatten wir auch die Firewall von Windows Vista. Lesen Sie, für wen das Bordmittel ausreichend ist.

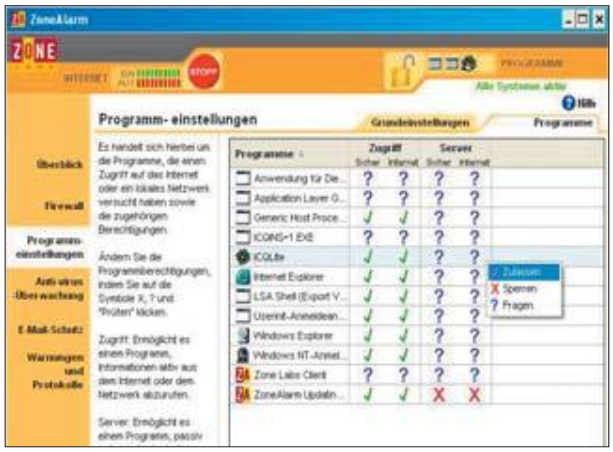
IT-Professionals

IT-Security wird zu wenig geschult

Viele Firmen ignorieren die Gefahren der Cyber-Kriminalität und qualifizieren ihre Mitarbeiter in Sachen IT-Sicherheit zu wenig.

Diesen Artikel finden Sie auf CD/DVD Dieses Video finden Sie auf DVD Diesen Artikel finden Sie im E-Paper

Dateitausch: Für den Empfang einer Datei müssen Sie Server-Rechte in der Firewall vergeben und in ICQ zustimmen (Punkt 6)



Mit links: Bei Zone Alarm aktivieren Sie das Kontextmenü für die Online-Erlaubnis mit der linken Maustaste (Punkt 7)

Sie müssen es nicht installieren. Nach dem Start zeigt es sofort alle laufenden Programme an. In der Liste erscheint also auch jenes, das die Firewall gerade meldet. Über den Button „PC-WELT" werden Sie mit unserer Prozessdatenbank verbunden und können dort nachsehen, ob die Sache harmlos ist oder nicht. Die Datenbank umfasst bereits mehrere hundert Einträge. Sie können übrigens mithelfen, sie zu erweitern – das geht nach einer kurzen Anmeldung. Läuft bei Ihnen ein Tool, das dort fehlt, über das Sie aber schon mehr herausgefunden haben, dann tragen Sie es doch auf der Website ein. Damit helfen Sie den anderen PC-WELT-Lesern.

Wenn Sie Infos zu einem Programm brauchen, das noch nicht verzeichnet ist, können Sie direkt in pcwProcess eine Web-Suche starten – per Klick auf den Button „Google".

Sollten Sie noch nicht genug Informationen haben, können Sie es noch bei zwei weiteren Datenbanken versuchen. Sie erreichen sie über www.pcwelt.de/223 (englischsprachig) und www.reger24.de/processes.php (zum großen Teil ebenfalls englischsprachig).

5. Vorsicht, Falle! Schädlinge tarnen sich als Tools

Die Antiviren-Software sollte zwar Würmer, Trojaner und Viren melden, doch wenn diese Schädlinge ganz neu und gut getarnt sind, bleibt sie stumm. Sobald die Programme allerdings online gehen wollen, warnt die Firewall. Jetzt heißt es: Vorsicht! Denn viele Malware-Programmierer tarnen ihre Erzeugnisse als Windows-Systemprogramme. Entweder haben sie denselben Namen, etwa Svchost.EXE, stecken aber in einem anderen Ordner als das Original. Oder die Schadprogramme heißen ein klein wenig anders – beispielsweise Svchosts.EXE. Mit Hilfe einer Prozessdatenbank klären Sie, ob Sie Freund oder Feind vor sich haben (Punkt 4).

Die Systemdatei Svchost.EXE liegt unter Windows XP übrigens im Windows-Ordner System32, also meist in C:\Windows\System32.

6. Spezialfall: Tools mit Server-Ambitionen

Die meisten Programme wollen nur eine einfache Verbindung zum Internet – etwa der Browser. Er fordert einzelne Web-Seiten an und bekommt diese dann zugestellt. Die Firewall lässt die Seiten aus dem Internet passieren, denn sie wurden ja zuvor angefordert.

Eine paar Programmen – etwa Chat- oder VoIP-Tools – genügt das aber nicht. Damit sie vollständig funktionieren, müssen sie auch Daten empfangen können, die sie vorher nicht bestellt haben. Das aber muss die Firewall wissen, denn sie wirft für gewöhnlich alle Daten weg, die ohne vorherige Anforderung aus dem Internet eintreffen – und zwar ohne jede Information an den Anwender.

Beispiel: Sie nutzen ICQ, um mit anderen ICQ-Anwendern zu chatten. Der Dienst von ICQ übernimmt hier die Koordination. Anders sieht es aber aus, wenn ihnen jemand eine Datei über das Tool sendet. Diese bekommen Sie direkt vom anderen ICQ-Anwender.

Damit das Tool die nicht angeforderten Daten auch empfangen kann, macht es einen Port auf und bietet sich selbst als Server an. Diese Aktion muss aber über die Firewall erlaubt sein. Sollten Schädlingsprogrammierer gerade ein noch ungestopftes Sicherheitsloch im Chat-Tool entdeckt haben, bedeutet diese Erlaubnis allerdings ein Risiko.

Gratis: Online-Sicherheitstests

Haben Sie Ihren Rechner per Firewall gegen Angriffe aus dem Internet abgedichtet, können Sie den Erfolg Ihrer Maßnahmen mit Hilfe eines Online-Checks überprüfen. Wir stellen Ihnen zwei kostenlose Angebote vor.

Grc.com: Einen guten, englischsprachigen Test für Ihre Firewall finden Sie unter www.grc.com. Folgen Sie dem Link „Shields Up". Sie haben nach einem Klick auf „Proceed" die Wahl zwischen sieben Testszenarien. Darunter ist eins, bei dem Sie die zu prüfenden Ports selbst auswählen.

Symantec: Der Hersteller von Sicherheits-Tools bietet einen informativen Scan, den Sie über www.pcwelt.de/d8b erreichen. Das Unternehmen profitiert von diesem Gratis-Service: Findet der Scan ein Sicherheitsproblem, schlägt die Site vor, dieses mit einem Tool von Symantec zu beheben. Natürlich lässt sich dazu aber auch ein Programm eines anderen Herstellern einsetzen.

7. Server-Rechte erteilen und verweigern

Einige Firewalls, etwa Zone Alarm Free und Comodo, erkennen automatisch, wenn ein Programm Server-Rechte benötigt, und fragen Sie eigens um Erlaubnis. Oft ist klar, warum ein Tool als Server arbeiten möchte, – etwa wenn Sie einen FTP-Server einsetzen. Beim Beispiel ICQ leuchten die Server-Ambitionen nicht jedem sofort ein – oder sind schlicht nicht erwünscht.

Sind Sie im Zweifel, sagen Sie zunächst mal Nein. Wenn das Tool dann nicht wie erwartet arbeitet, sollten Sie in der Hilfe oder auf der Hersteller-Website nachsehen, ob es Server-Rechte benötigt. Lautet die Antwort ja, müssen Sie diese nachträglich manuell zuweisen. Bei etlichen Firewalls wird Ihnen das durch die unübersichtliche Bedienerführung sehr schwer gemacht.

Zone Alarm kann hier mit seiner einfachen Handhabung punkten. Unter „Programmeinstellungen, Programme" klicken Sie mit der linken Maustaste auf die Zeile unter „Server" und wählen „Zulassen".

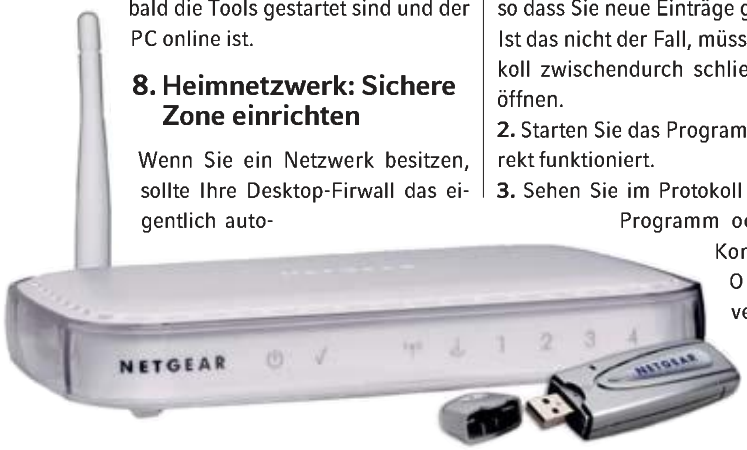
Bei Comodo markieren Sie unter „Application Monitor" das Programm und wählen „Edit". Auf der Registerkarte „General" ändern Sie „Direction" von „Out" auf „In/Out".

Generell gilt: Sie sollten Programmen nur Server-Rechte zugestehen, wenn Sie auch die entsprechenden Funktionen nutzen wollen. Sicherheits-Updates für diese Tools sollten Sie umgehend einspielen. Denn wenn sie eine Online-Sicherheitslücke haben, ist der Rechner von außen angreifbar, sobald die Tools gestartet sind und der PC online ist.

8. Heimnetzwerk: Sichere Zone einrichten

Wenn Sie ein Netzwerk besitzen, sollte Ihre Desktop-Firwall das eigentlich automatisch erkennen. Doch das klappt oft nicht. Die Folge: Die Firewall stuft die anderen PCs im Netz wie Rechner im Internet ein und blockt etwa den Zugriff auf die Dateien der PCs. Lösen lässt sich das Problem auf einem Umweg: Tragen Sie das Netzwerk in der Firewall als vertrauenswürdige Zone ein.

In Zone Alarm wählen Sie dazu „Firewall, Zonen". Klicken Sie auf „Hinzufügen, IP-Bereich", und geben Sie den Bereich der internen IP-Adressen ein, den Sie für Ihr Netzwerk nutzen. Haben Sie die Daten nicht zur Hand, probieren Sie es mit dem Bereich von 192.168.0.1 bis 192.168.255.255. Von den Adressbereichen, die für private Netzwerke reserviert sind, wird dieser am häufigsten genutzt. Im Internet kommen diese Adressen nicht vor. Oder Sie geben in der Kommandozeile „ipconfig" ein – dann bekommen Sie die Daten. Als „Beschreibung" tippen Sie zum Beispiel „Heimnetz" ein.



Hardware-Firewalls: Die kleinen Kisten bieten einen guten Schutz vor Angriffen (Punkt 10)

9. Fehlersuche: So finden Sie heraus, wo es hakt

Sollte ein Online-Programm nicht so funktionieren wie erwartet, dann kann das an der Desktop-Firewall liegen. Eventuell haben Sie einem Modul den Online-Zugriff verboten, das diesen dringend benötigt, oder die Firewall hat das Programm von sich aus blockiert.

Bei der Fehlersuche hilft Ihnen das Protokoll der Firewall. Sie verrät Ihnen, welche Online-Aktionen stattgefunden haben – und welche blockiert wurden. So geht's:

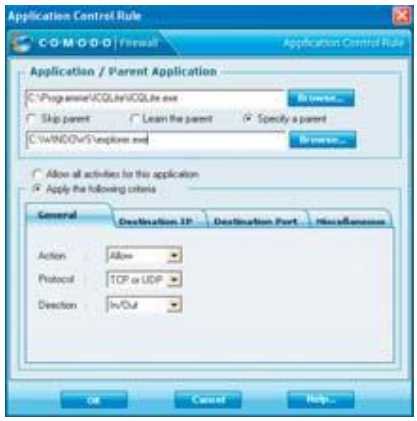
1. Öffnen Sie das Protokoll. Bei den meisten Firewalls wird dieses dynamisch aktualisiert, so dass Sie neue Einträge gleich entdecken. Ist das nicht der Fall, müssen Sie das Protokoll zwischendurch schließen und wieder öffnen.

2. Starten Sie das Programm, das nicht korrekt funktioniert.

3. Sehen Sie im Protokoll nach: Wird dem Programm oder einer seiner Komponenten der Online-Zugang verweigert, fehlt dem Modul eine entsprechende Berechtigung.

4. Vergeben Sie in der Firewall die fehlende Berechtigung.

In Zone Alarm finden Sie das Protokoll unter „Warnungen und Protokolle, Protokollanzeige", kontrollieren Sie sowohl die Anzeige unter „Meldungstyp, Programm" als auch unter „Meldungstyp, Firewall". Die Berechtigung für ein Programm ändern Sie unter „Programmeinstellung, Programme".



Server-Rechte: Bei der Firewall Comodo sehen diese als Regel so aus (Punkt 7)

In Comodo finden Sie das Protokoll unter „Activity, Logs". Außerdem lohnt sich auch ein Blick unter „Activity, Connections". Im einen Punkt finden Sie Infos zu den Programmen, im anderen zu den Verbindungsversuchen. Berechtigungen ändern Sie unter „Summary, Application Monitor".

Übrigens: In Comodo sollten sich nur fortgeschrittene Anwender an die Konfiguration unter „Network Monitor" wagen. Denn dort kann man schnell mal ungewollt Online-Verbindungen kappen.

10. Hardware-Firewalls: Die perfekte Ergänzung

Hardware-Firewalls bieten einen tollen zusätzlichen Schutz gegen Gefahren aus dem Internet. Anders als Desktop-Firewalls sind sie kaum anfällig gegen Angriffe auf Sicherheitslücken in Software. Mit nur einem Gerät lassen sich mehrere Rechner auf einmal schützen. Das reduziert den Konfigurationsaufwand bei einem größeren Netzwerk erheblich. Zudem arbeiten sie unabhängig von den Betriebssystemen der PCs im Netzwerk. Einfache Hardware-Firewalls gibt's mittlerweile beim Abschluss eines neuen DSL-Vertrags günstig mit dazu. Sie sind oft bereits im DSL-Modem integriert. Wie Sie diese Firewall konfigurieren, erfahren Sie im Special zum Thema Netzwerke in der PC-WELT 3/2006 ab Seite 113 (auch auf CD). Darin erhalten Sie auch viele weitere wertvolle Infos.