Special: Was Firewalls wirklich taugen

Firewall-Fakten

Eine Firewall soll Ihren PC vor Angriffen aus dem Internet schützen. Das gelingt ihr aber nur, wenn sie richtig konfiguriert ist. Wir geben Tipps, wie Sie die Software am besten einstellen.

Das Geschäft mit der Angst floriert. Das beweisen Massen an One-Click-Schutz-Tools für den PC. Doch schützt eine Firewall Ihren PC vor allen Gefahren? Glauben Sie das nicht! Diese Tools können weniger, als man ihnen nachsagt. Mit dem richtigen Wissen schützen Sie Ihr System sogar ganz ohne Wächster-Tools!

In diesem Ratgeber-Special lesen Sie, inwieweit Personal Firewalls Einzelplatz-PCs oder kleine Netzwerke vor Angriffen aus dem Internet schützen und ob die Produkte ihren Marketing-Aussagen gerecht werden können. Wir verraten, wo Ihre Firewall nichts nützt, und geben Tipps, wie Sie wirklich sicher sind. Außerdem erfahren Sie, wie gut die Windows-Firewall schützt, welche Gratis-Firewall empfehlenswert ist, wie Sie die Tools richtig konfigurieren, was ein DSL-Router als Firewall taugt, warum eine Desktop-Firewall eine gute Ergänzung zu DSL-Routern ist und wie Sie die Sicherheit Ihrer Firewall und damit Ihres Rechners testen können.

Die Inhalte im Überblick:

10 Regeln für ein sicheres System ohne Schutz-Tools

SICHER OHNE SCHUTZ

Das Geschäft mit der Angst floriert. Das beweisen Massen an One-Click-Schutz-Tools für den PC. Mit unseren 10 Regeln schützen Sie Ihr System effektiv – ohne Wächter-Tools. Denn Wissen ist immer der beste Schutz.

Von **Christian Löbering**

DAS THEMA SICHERHEIT IST EINE GELDMASCHINE, Paranoia ein Geschäftsmodell. Susi-Sorglos-Schutz-Tools für den Privat-PC haben einen großen Markt und vermitteln dem Verbraucher das Gefühl, dass absolute Sicherheit käuflich ist und zudem kaum weitere Einschränkungen mit sich bringt. Beide Annahmen sind falsch: Absolute Sicherheit ist eine Illusion, ein vernünftig geschütztes System allerdings keineswegs. Im Gegenzug bedeutet Schutz aber auch immer, auf Freiheiten zu verzichten. Wenn Sie die Tür offen lassen, kann die beste Alarmanlage der Welt nichts gegen Einbrecher ausrichten.

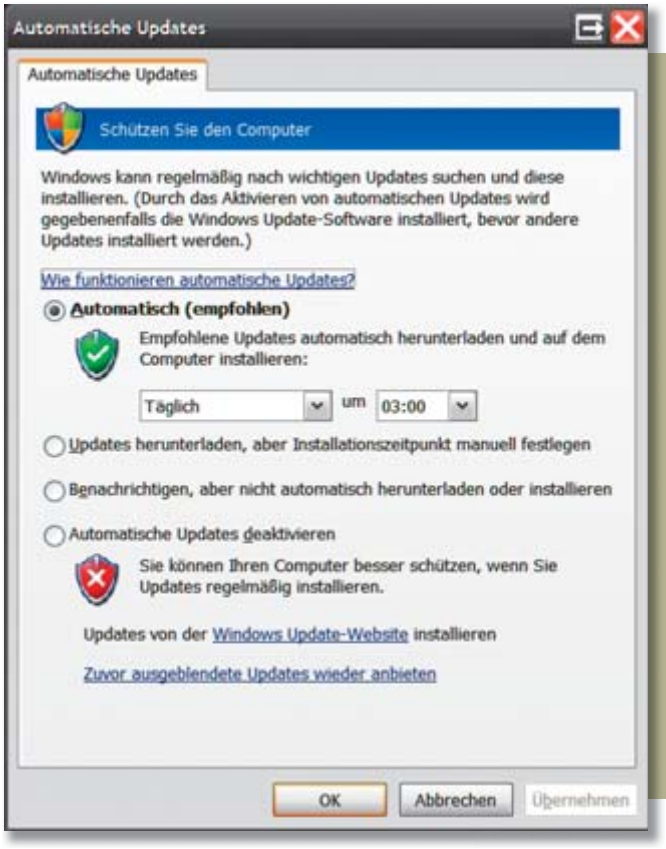
Sowohl die Hersteller von Schutz-Software als auch die Medien schüren Angst vor – unsichtbaren, virtuellen – Bösewichtern, die dem ehrlichen Anwender ans System, die persönlichen Daten und vor allem ans Geld wollen. Malware-Entwicklern haftet dabei meist der Ruf von Hexenmeistern an, die scheinbar unmögliche Tricks anwenden, mit denen sie den arglosen Benutzer prellen. Zugegeben – es wird viel Hirnschmalz in Malware- und Phishing-Attacken investiert. Trotzdem gibt es nur eine Handvoll Prinzipien, nach denen die Angriffe seit Jahren verlaufen. Wer diese Strategien kennt und versteht, kann getrost auf zusätzliche Schutz-Software wie Desktop-Firewalls, Virenwächter, Mailscanner oder Ähnliches verzichten.

10 Grundregeln: Ausschlaggebend ist dabei vor allem ein verantwortungsvoller Umgang mit dem PC, gerade wenn er per Internet mit der ganzen Welt verbunden ist. Die Leitsätze dafür haben wir im Folgenden in

DIE 10 GEBOTE

1. Aktualisieren Sie Ihr **System** regelmäßig
2. Aktualisieren Sie Ihre **Software** zuverlässig
3. Setzen Sie eine **Router-Firewall** ein
4. Arbeiten und surfen Sie als **eingeschränkter** Benutzer
5. Öffnen Sie **keine** Mailanhänge von unbekannten Absendern
6. Lassen Sie sich beim Surfen **nicht täuschen**
7. Vergeben Sie stets verschiedene **sichere Kennwörter**
8. Empfangen Sie Mails **nur** als Plain-Text
9. Installieren Sie **keine** Tools aus unbekannten Quellen
10. Nutzen Sie immer **NTFS-Rechte**

Form von 10 Grundregeln zusammengefasst. Wenn Sie diese verinnerlicht haben und ausnahmslos anwenden, ist Ihr System unter Windows 2000, XP und Vista mindestens genauso gut geschützt wie durch den Einsatz eines Spezial-Tools. Die positiven Nebeneffekte dabei: Sie müssen sich nicht blind auf eine Software verlassen, die selbst fehlerhaft sein kann und deren Funktionalität nicht transparent ist. Außerdem nehmen Sie der Malware ihren Schrecken. Ein Blick auf die Angriffs-Strategien zeigt recht schnell, dass auch hier nur mit Wasser gekocht wird.



Automatische Updates: Sicherheitslücken im System zu schließen verringert die Angriffsfläche für Malware massiv. Lassen Sie Ihr Windows deshalb stets automatisch aktualisieren (Punkt 1)

1. Aktualisieren Sie Ihr System regelmäßig

Entwickler von Malware möchten viele Rechner erreichen. Deshalb entwickeln sie ihren Code für möglichst populäre Systeme. Derzeit sind das vorwiegend die aktuellen Windows-NT-Versionen (2000, XP und Vista). Falls Sie eine davon nutzen, stehen Sie im Fadenkreuz der Viren-Industrie und sollten das System stets mit allen nötigen Sicherheits-Updates versorgen. Am einfachsten geht das über „Automatische Updates“ in der Systemsteuerung (Vista: „Systemsteuerung, Windows Update). Damit werden regelmäßig alle wichtigen neuen Updates heruntergeladen und installiert.

Update-Archiv: Im Fall einer Neu-Installation starten Sie aber wieder mit null Patches, da das automatische Update die Setup-Dateien nicht aufbewahrt. Die Folge: Ihr System ist beim ersten Besuch im Netz ungeschützt und fängt sich mit einiger Wahrscheinlichkeit eine Malware ein, auch wenn Sie nur **www.windowsupdate.com** aufsuchen. Mit unserem **pcwUltimateLoader** legen Sie ganz leicht ein Update-Archiv an, das Sie bei einer Neu-Installation aufspielen können, bevor Sie das erste Mal ins Netz gehen. Wie Sie das Tool optimal nutzen, lesen Sie in unserer Anleitung unter **www.pcwelt.de/ult**.

2. Aktualisieren Sie Ihre Software zuverlässig

Je mehr Software Sie auf Ihrem Windows-Rechner installiert haben, desto größer ist das Risiko einer Sicherheitslücke. Denn jedes Tool kann selbst fehlerhaft sein oder Bugs im System verursachen. Deshalb sollten Sie zum einen nur Programme einrichten, die Sie wirklich brauchen, und den Rest radikal ausmisten. Zum anderen sollten Sie darauf achten, dass die installierte Software auf dem neuesten Stand ist.

Einige Anwendungen – etwa Firefox oder Thunderbird – besitzen eine eigene automatische Update-Funktion. Bei vielen anderen müssen Sie in regelmäßigen Abständen auf der jeweiligen Website nach Aktualisierungen Ausschau halten.

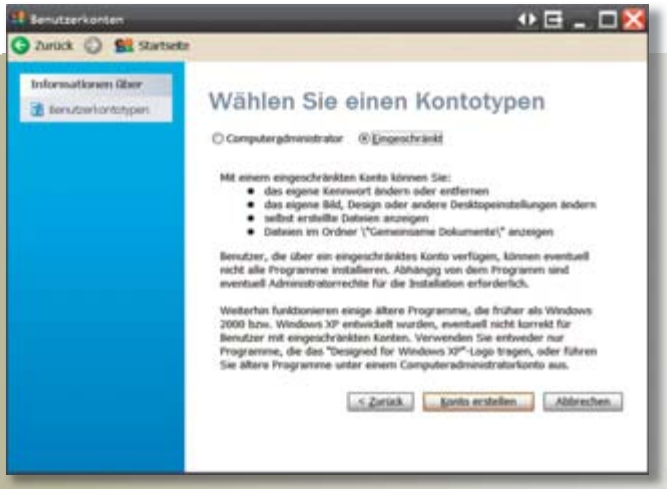
Alternative: Erleichtern Sie sich das Leben, indem Sie eine Software wie **Update Star** einsetzen. Nachdem Sie das Tool aufgespielt haben, macht es eine Inventur aller installierten Anwendungen. Nach einem Klick auf „Updates suchen“ gleicht Update Star Ihre Software-Liste mit einer eigenen Datenbank im Internet ab und liefert eine Aufstellung derjenigen Tools, für die ein Update verfügbar ist. Anschließend klicken Sie auf „Programmliste“, laden sich die neueren Versionen über die jeweiligen „Download“-Schaltflächen herunter und installieren sie. ›

GEGEN DIE ANGST-INDUSTRIE Kostenlose Tools

Name	Beschreibung	Win-Systeme	Download (Größe)	Seite
Keepass 1.09 [1]	Sichere Passwörter verwalten und erstellen	2000, XP, Vista	**http://keepass.info/** (920 KB)	86
Password Hasher 1.0.4 [1]	Firefox-Erweiterung zum Erstellen von Passwörtern	[2]	**http://wijjo.com/passhash** (59 KB)	86
pcwUltimateLoader 1.08	Update-Manager für Windows und Office	2000, XP, Vista	**www.pcwelt-praxis.de/downloads** (725 MB)	83
pcwXPProme 1.0	Aus XP Home mach (fast) Pro	XP Home	**www.pcwelt-praxis.de/downloads** (48 KB)	87
Sudown 2.21 [1]	Mehr Rechte für einzelne Programmaufrufe	XP	**http://sudown.sourceforge.net** (402 KB)	84
Update Star 1.1	Update-Manager für Software	2000, XP, Vista	**http://www.updatestar.com/** (3,81 MB)	83

1) englischsprachig, 2) Firefox ab Version 1.5

Software-Update: Alte Software ist ein Sicherheitsrisiko. Sparen Sie an installierten Tools, aber aktualisieren Sie diese regelmäßig (Punkt 2)



Sicher im Netz: Arbeiten und surfen Sie mit einem eingeschränkten Benutzerkonto, so kann Malware kaum Schaden anrichten (Punkt 4)

3. Setzen Sie eine Router-Firewall ein

Eine Desktop-Firewall ist nichts anderes als eine Anwendung, die den Netzwerkverkehr überwacht und Datenpakete aussortiert, die nicht den definierten Regeln genügen. Das Problem dabei: Die Firewall-Anwendung läuft auf demselben System, das sie schützen soll. Weist das System oder die Schutz-Software eine Sicherheitslücke auf, kann der Schutz nicht gewährleistet werden. Es ist so, als würde eine Stadt auf eine Feuerwehr verzichten und stattdessen in jedem Wohnblock einen vorlauten Mini-Jobber mit einem Eimer Wasser abstellen.

Hardware-Firewall: Viel sicherer ist es, wenn Sie eine Firewall nutzen, die auf einem anderen System läuft, etwa auf Ihrem DSL-Router. Angreifende Malware kommt so mit Ihrem System überhaupt nicht in Berührung. Wenn Sie über eine solche Firewall surfen, schicken Sie Datenpakete über den Router an die gewünschte Website. Der Router speichert für jedes Paket eine gewisse Zeit die Quell- und Ziel-IP, das verwendete Protokoll und ob eine Antwort erwartet wird. Nur wenn die Website in dieser Zeit ein Paket zurückschickt, das den Kriterien entspricht, wird es durchgelassen. Aus diesem Grund können bei der Firewall meist auch alle Ports geschlossen bleiben. Viele DSL-Router verfügen über eine Firewall, die häufig standardmäßig aktiv ist.

4. Arbeiten und surfen Sie als eingeschränkter Benutzer

Windows 2000, XP und Vista verfügen über konfigurierbare NTFS-Rechte. Indem Sie diese richtig einsetzen, halten Sie schon die meiste Malware ab. Der Trick dabei: Zusätzlich zu Ihrem normalen Admin-Konto legen Sie ein eingeschränktes Konto an, über das Sie im Idealfall arbeiten und surfen. Das bietet den Vorteil, dass keine Malware, die in diesem Kontext ausgeführt wird, in das System eingreifen darf. Nur wenigen Schädlingen gelang bisher eine „Privilegien Eskalation" – also, sich trotz eingeschränkter Rechte per Sicherheitslücke den Admin-Zugriff zu ergaunern. Dagegen hilft es aber, System und Software regelmäßig zu patchen (Punkte 1 und 2).

Für ein Plus an Komfort: Wenn Ihnen das Arbeiten als eingeschränkter Benutzer zu unbequem ist, können Sie ein Tool wie **Sudown** nutzen. Damit weisen Sie gewünschten Benutzern die Gruppe „Sudoers" zu. Sobald Sie oder eine Software eine Aktion ausführen, die nach Admin-Rechten verlangt, werden Sie aufgefordert, Ihr Kennwort einzugeben. Erscheint der Kennwort-Dialog, ohne dass Sie irgend etwas getan haben, deutet das möglicherweise darauf hin, dass sich eine Malware auf Ihrem System einschleichen will. Sie wird aber nicht ausgeführt, wenn Sie es nicht explizit erlauben. Wie das englischsprachige Tool funktioniert, lesen Sie im Online-Tipp „Admin-Arbeiten sicher erledigen" auf Seite 169.

5. Öffnen Sie keine Mailanhänge von unbekannten Absendern

Das schwächste Glied in der Sicherheitskette und daher das beliebteste Angriffsziel von Malware ist der Benutzer des Rechners. Eine alte, aber immer noch wirkungsvolle Methode ist das Versenden von Mails mit manipulierten Anhängen. Wenn Sie den Anhang öffnen, starten Sie die Malware. Deshalb lautet die eiserne Regel: Öffnen Sie keine unbekannten Mailanhänge, und sorgen Sie dafür, dass Ihr Mail-Client es auch nicht automatisch tut. Kommt unerwartete Post mit Anhang von einem Bekannten, einer Bank oder der Telefongesellschaft, nutzen Sie einen zweiten Kanal (zum Beispiel ICQ oder Telefon), um sich zu vergewissern, dass alles seine Ordnung hat. Mails von Fremden, auch wenn sie vorgeben, von einem bekannten Unternehmen zu stammen, sollten Sie immer löschen.

Achtung, Risiko: Auch wenn der Anhang einer Mail harmlos erscheint, kann sich dahinter durchaus etwas Bösartiges verbergen. So erscheint beispielsweise eine Datei mit einem Namen wie Rechnung.PDF<Zeilenumbruch>.PIF in Ihrem Mail-Client etwa nur als „Rechnung.PDF", weil der Zeilenumbruch und die Endung PIF nicht angezeigt werden. Wenn sie dann auch noch aus einer scheinbar sicheren Quelle stammt, ist die Neigung zum Klicken schon recht groß. Trotzdem dürfen Sie die Datei keinesfalls öffnen, denn durch die Endung PIF ist sie ausführbar und enthält wahrscheinlich Malware.

„Arbeiten und surfen Sie nur in einem Konto mit eingeschränkten Rechten"

Achtung vor Datendieben: Akzeptieren Sie beim Surfen niemals ein Zertifikat, dessen Zertifizierungsstelle unbekannt ist (Punkt 6)

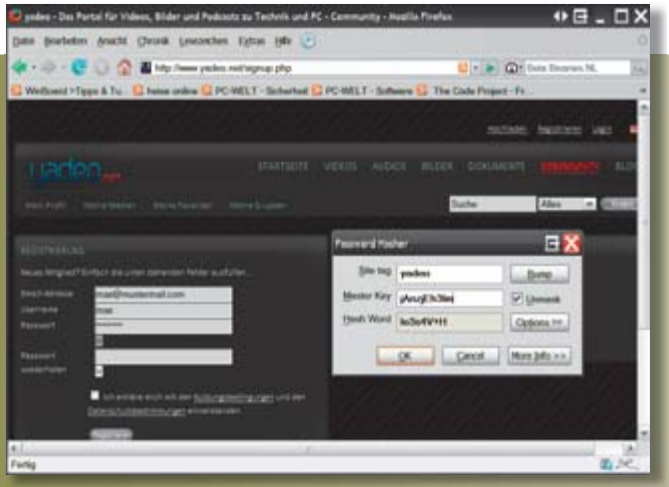
6. Lassen Sie sich beim Surfen nicht täuschen

Eine relativ neue Masche, Malware auf Privat-PCs zu platzieren oder persönliche Daten zu ergaunern, ist das Typosquatting. Wenn Sie sich bei der Eingabe einer URL vertippen oder eine falsche Top-Level-Domain eingeben, landen Sie möglicherweise auf einer speziell präparierten Seite. Diese sieht zwar auf den ersten Blick aus wie die gewünschte, fordert Sie jedoch auf, etwas herunterzuladen oder persönliche Daten einzugeben.

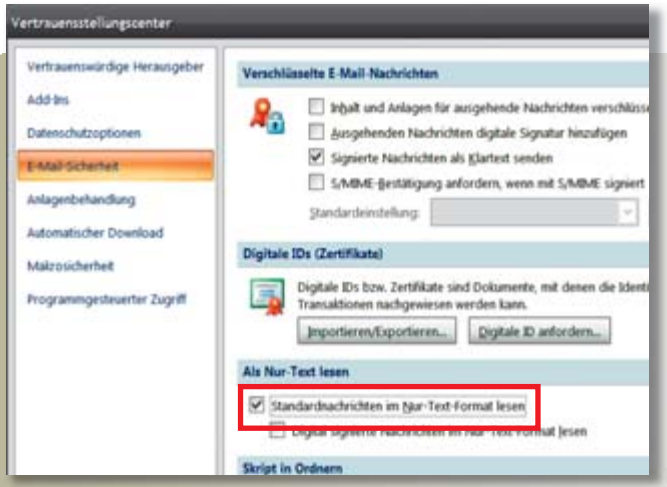
Ähnliches kann passieren, wenn Kriminelle populäre Web-2.0-Seiten hacken. Unlängst wurde zum Beispiel das Hintergrundbild des Myspace-Profils von Alicia Keys so manipuliert, dass ein versehentlicher Klick darauf Sie auf einen Malware-Server umgelenkt hätte. Der Fehler wurde beseitigt, jedoch wird das Prinzip weiterhin genutzt.

SSL & Zertifikate: Wer mit eingeschränkten Benutzerrechten unterwegs ist (siehe Punkt 4), muss in der Regel zumindest nicht den Befall durch Malware befürchten. Allerdings schützt Sie das nicht davor, vertrauliche Informationen preiszugeben. Grundsätzlich gilt: Geben Sie vertrauliche Infos ausschließlich in Formulare mit verschlüsselter Verbindung ein (etwa SSL), und achten Sie davor akkurat auf Zertifikats-Fehler. Die verschlüsselte Verbindung erkennen Sie im Firefox oder IE daran, dass die Adresszeile sich gelb verfärbt und die URL mit „https://“ beginnt.

Praktisch alle Banken und Online-Shops sind bei einer der vielen Stammzertifizierungsstellen (etwa Verisign) registriert, so dass Sie nicht explizit bestätigen müssen, dass Sie die Verbindung aufbauen wollen. Erscheint die Nachfrage dennoch, sollten Sie in jedem Fall den Text der Dialogbox sehr genau lesen. Ist das Zertifikat abgelaufen, können Sie davon ausgehen, dass Sie zumindest auf der korrekten Website sind. Allerdings arbeitet die IT-Abteilung dieser Firma hier nicht besonders sauber, und Sie sollten sparsam mit der Eingabe vertraulicher Daten umgehen, wenn Sie das Zertifikat akzeptieren sollten. Stimmt der Name der Site nicht mit dem des Zertifikats überein, sollten Sie genau schauen, worin der Unterschied besteht, und das Zertifikat gegebenenfalls ablehnen. Fehlt hingegen die Zertifizierungsstelle komplett, sollten Sie das Zertifikat auf jeden Fall ablehnen. ›



Sichere Kennwörter: Mit Password Hasher erzeugen Sie viele komplexe Passwörter, müssen sich aber nur eines merken (Punkt 7)



Keine HTML-Mails: Empfangen Sie Mails nur als Text. So vermeiden Sie Fehl-Klicks auf Links, die auf verseuchte Seiten führen (Punkt 8)

7. Vergeben Sie stets verschiedene sichere Kennwörter

Für die Sicherheit Ihres lokalen Rechners ist es zwingend erforderlich, dass Sie für jedes Benutzerkonto ein eigenes sicheres Kennwort vergeben. Am bequemsten geht das für den angemeldeten Benutzer über „Systemsteuerung, Benutzerkonten“. Besonders wichtig ist jedoch das vordefinierte Administrator-Konto, das etwa bei XP Home standardmäßig kein Kennwort besitzt. Sie sollten diesen Mangel in jedem Fall beseitigen, indem Sie aus einem Konto mit Admin-Rechten in einem Kommandozeilen-Fenster (Cmd.EXE) den Befehl

```
net user Administrator <KW>
```

eingeben. Statt „<KW>“ wählen Sie als Kennwort eine möglichst komplexe Zeichenfolge, die mindestens aus Groß- und Kleinbuchstaben und Zahlen besteht.

Auch die Sicherheit Ihrer Daten im Web steht und fällt mit der Vielfalt und Qualität der Kennwörter, die Sie für die einzelnen Seiten vergeben haben. Verwenden Sie bei Amazon, Ebay & Co. keinesfalls dasselbe Kennwort wie fürs Online-Banking oder Ihr Aktiendepot und auch nicht dasjenige Ihres lokalen Benutzerkontos.

Allerdings kann sich kaum jemand so viele komplexe alphanumerische Passwörter merken, wie er eigentlich braucht. Viele Benutzer greifen deshalb häufig auf Muster zurück. Das Problem bei durchnummerierten Kennwörtern oder Kennwörtern, die aus dem Namen und Geburtstag der Katze bestehen, ist jedoch, dass sie per Wörterbuch-Attacke schnell geknackt werden.

Passwort-Generator: Für deutlich mehr Sicherheit ohne Gedächtnistraining können Sie zum Beispiel die Firefox-Erweiterung **Password Hasher** verwenden. Dieses englischsprachige Tool erzeugt aus einem Domänen-Namen und einem von Ihnen zuvor definierten Master-Kennwort ein sicheres Passwort für eine Website. So müssen Sie sich nur ein einziges Kennwort merken, profitieren aber dennoch von der Sicherheit vieler unterschiedlicher Kennwörter. Wie Sie das Tool einsetzen, lesen Sie im Tipp „Automatisch sichere Passwörter generieren“ auf Seite 170.

Passwort-Datenbank: Alternativ können Sie das englischsprachige Tool **Keepass** nutzen, um Ihre Kennwörter in einer verschlüsselten Datenbank abzuspeichern. Lassen Sie sie jedoch keinesfalls auf Ihrer Festplatte liegen, sondern nutzen Sie das Tool von einem USB-Stick.

„Die Sicherheit Ihrer Daten steht und fällt mit der Qualität der Kennwörter“

8. Empfangen Sie Mails nur als Plain-Text

Nicht nur der Browser kann HTML-Seiten anzeigen, auch im Mail-Client werden HTML-Mails standardmäßig geparst, also interpretiert, und angezeigt. Falls Sie die Grundregeln 1 bis 4 befolgen, liegt das Risiko auch hier eher beim Datenklau als beim Einnisten einer Malware. Der „Header“ und somit auch der Absender einer Mail kann leicht gefälscht werden, somit liefert das keinen gültigen Hinweis darauf, ob es sich etwa um eine Phishing-Mail handelt. HTML-Mails können so gestaltet werden, dass sie wie offizielle Schreiben anmuten, und zusätzlich können darin enthaltene Links maskiert werden.

Sicherer ist es, Sie lassen sich alle Mails immer nur als reinen Text anzeigen. So sehen Sie direkt, wo ein Link hinführt, und riskieren keinen versehentlichen Klick. Außerdem geraten Sie nicht in Versuchung, etwa ein HTML-Formular auszufüllen, denn das sollten Sie keinesfalls tun.

So geht's: In Thunderbird finden Sie die entsprechende Option unter „Ansicht, Nachrichtentext, Reiner Text“. Bei Outlook Express aktivieren Sie unter „Extras, Optionen, Lesen“ die Klickbox neben „Alle Nachrichten als Nur-Text lesen“.

Bei Outlook ist es komplizierter. In der Version 2002 (XP) müssen Sie zunächst Regedit starten. Dann öffnen Sie den Schlüssel „Hkey_Current_User\Software\Microsoft\Office\10.0\Outlook\Options\Mail\“, legen einen neuen Dword-Eintrag „ReadAsPlain“ an, und geben ihm den Wert „1“. Unter Outlook 2003 gibt es eine Option auf der Oberfläche. Wählen Sie „Extras, Optionen, Einstellungen, Email-Optionen“, und aktivieren Sie die Klickbox neben „Standardnachrichten im Nur-Text-Format lesen“. Bei Outlook 2007 wählen Sie „Extras, Vertrauensstellungscenter, E-Mail-Sicherheit“ und aktivieren die Klickbox neben „Standardnachrichten im Nur-Text-Format lesen“.

Zugriff verweigern: Über die Registerkarte „Sicherheit“ können Sie im Explorer NTFS-Rechte für Datei und Ordner vergeben (Punkt 10)

9. Installieren Sie keine Tools aus unbekannten Quellen

Die 4. Regel (siehe oben) wird außer Kraft gesetzt, sobald Sie eine Software installieren, die dafür Admin-Rechte verlangt. Achten Sie deshalb genau darauf, woher die Software stammt, bevor Sie sie einrichten. Bei populären Tools sollte die Herstellerseite grundsätzlich immer die erste Wahl sein (zum Beispiel Microsoft, Adobe …), da hier eine nachträgliche Manipulation der Pakete eher unwahrscheinlich ist. Alternativ können Sie natürlich auch jede Software aus den Download-Archiven von **www.pcwelt.de** und **www.pcwelt-praxis.de** installieren. Vermeiden sollten Sie allzu vielversprechende Freeware dubioser Herkunft, für deren Unbedenklichkeit Sie keine Bestätigung aus zuverlässiger Quelle finden können.

10. Nutzen Sie immer NTFS-Rechte

Ein eingeschränktes Konto (siehe Punkt 4) verfügt über keinerlei Schreibrechte im Windows-Ordner. Somit ist es auch nicht möglich, Systemdateien zu manipulieren. Sie können die NTFS-Rechte aber auch nutzen, um Ihre eigenen Dokumente zu schützen.

Pro-Funktionen für XP Home: Unter XP Home fehlt die Registerkarte, auf der Sie NTFS-Rechte über den Explorer vergeben können. Mit **pcwXPProme** können Sie sie nachrüsten. Rufen Sie unser Tool dazu einfach per Doppelklick auf. Im Ordner von pcwXPProme wird die Datei ProductOptions.ORG angelegt. Bewahren Sie diese Datei gut auf, da das Tool ohne sie den Urzustand nicht wiederherstellen kann.

Nach einem Neustart können Sie wie unter XP Pro oder Vista mit der rechten Maustaste auf eine Datei oder einen Ordner klicken, „Eigenschaften“ wählen und über die Registerkarte „Sicherheit“ Zugriffsrechte für das Objekt vergeben. So verhindern Sie, dass bestimmte Benutzer Ihres Systems auf das Objekt zugreifen.

Vertrauliches verschlüsseln: Da NTFS-Rechte von anderen Administratoren Ihres Systems immer überschrieben werden können, sollten Sie besonders vertrauliche Dateien besser mit der EFS-Verschlüsselung schützen. Klicken Sie dazu mit der rechten Maustaste auf die Datei oder den Ordner, und wählen Sie „Eigenschaften“. Auf der Registerkarte „Allgemein“ gehen Sie auf „Erweitert“ und aktivieren „Inhalt verschlüsseln, um Daten zu schützen“.

Was Firewalls wirklich taugen

DIE WAHRHEIT ÜBER FIREWALLS

Personal Firewalls sollen Einzelplatz-PCs oder kleine Netzwerke vor Angriffen aus dem Internet schützen. Lesen Sie, ob die Produkte ihren Marketing-Aussagen gerecht werden können.

Von **Ramon Schwenk**

Als Internet-Nutzer sind Sie den Begehrlichkeiten von Hackern und Unternehmen ausgesetzt. Erstere machen sich einen Spaß daraus, fremde Rechner auszuspähen, zu verändern oder einfach nur zum Absturz zu bringen. Letztere wollen vor allem mehr Informationen über den potenziellen Kunden erlangen, um ihr Marketing effizienter zu gestalten. Als Schutzmaßnahme gegen dererlei Angriffe auf Ihre informelle Selbstbestimmung kommen Personal Firewalls ins Spiel, die Teilfunktionen einer Firmen-Firewall auf den Desktop übertragen.

Der Markt für Personal Firewalls – eine andere Bezeichnung lautet Desktop-Firewalls – ist seit Jahren umkämpft: Neben Klassikern wie Outpost Firewall Pro oder Zone Alarm gibt es vielversprechende Neuerscheinungen wie Commodo Firewall. Als Wundermittel gegen allfällige Bedrohungen der Rechnersicherheit sind Personal Firewalls aber nicht zu verstehen. Dennoch haben sich die Schutzprogramme heute weitgehend durchgesetzt, denn sie bieten ein beachtliches Repertoire an Abwehrmöglichkeiten. Doch Einsteiger und weniger versierte Anwender finden kaum Antworten auf grundlegende Aspekte zu Personal Firewalls. Wir haben die wichtigsten Fragen und kompakte Antworten in diesem Ratgeber für Sie gebündelt.

1. Firewall – was ist darunter zu verstehen?

Eine Firewall trennt zwei Netzwerke voneinander, zum Beispiel ein Firmennetzwerk, ein kleines Heimnetzwerk oder einen Einzelplatz-PC (inneres Netzwerk) vom Internet (äußeres Netzwerk). Die Anwender im inneren Netzwerk können etwa im Web surfen und Mail nutzen, vom äußeren Netzwerk gelangt aber niemand auf die Computer des inneren Netzwerks. Es gibt Hard- und Software-Firewalls, wobei sich letztere nicht zuletzt aufgrund günstiger Preise und etlicher Zusatzfunktionen durchsetzen.

2. Welche Gründe sprechen für den Einsatz einer Firewall?

Es gibt mehrere gute Gründe für den Betrieb einer Personal Firewall:

- um falsch konfigurierte PCs zu schützen
- um Trojaner und Viren zu erkennen, sobald sie aktiv werden
- um versteckt arbeitende Spy- und Adware zu identifizieren
- um etwas über die Sicherheit von PCs in Netzwerken zu erfahren

Eine falsche Rechnerkonfiguration betrifft besonders nach außen sichtbare Netzwerkfreigaben und aus Unwissenheit des Anwenders installierte Server-Software wie etwa einen im Hintergrund arbeitenden

Web- oder FTP-Server bei Windows 2000, XP oder Vista. Eine Personal Firewall blockiert diese Dienste.

Trojaner und Viren werden erkannt, da sie eine Verbindung ins Internet aufbauen müssen oder auf eine solche warten. Heimliche Verbindungsversuche am Anwender vorbei sollten von einer guten Personal Firewall zuverlässig erkannt werden. Von vielen Ad- und Spyware-Varianten geht zwar keine wirkliche Gefahr aus – sie versenden nur unbemerkt Informationen vom Anwender-PC ins Internet. Dennoch ist es sinnvoll, die Schnüffel- und Werbemodule wirkungslos zu machen.

Eine Firewall macht in jedem Fall Arbeit: Den Meldungen des Tools sollten Sie so lange nachgehen, bis Sie wissen, was sie bedeuten: Handbücher zu wälzen, Support-Seiten zu studieren und Diskussionsforen zu lesen hilft beim Verständnis.

3. Welche Desktop-Firewall soll ich verwenden?

Diese Frage ist nicht leicht zu beantworten. Die in Windows XP SP2 enthaltene Desktop-Firewall ist veraltet und checkt keine eingehenden Verbindungsversuche. Besser sieht es bei Windows Vista aus, doch auch hier haben Sie über die Datenkommunikation einiger syteminterner Prozesse keine Kontrollmöglichkeit.

Die meisten Firewall-Tools von Drittherstellern bieten eine gute Basisschutzwirkung und reichen für einen Einzelplatzrechner oder ein kleines Netzwerk allemal aus. Es ist wichtig zu verstehen, wie das Produkt funktioniert, um sich nicht in falscher Sicherheit zu wiegen.

Einfach zu bedienende Personal Firewalls wie Zone Alarm sind für Anwender empfehlenswert, die sich nicht zu sehr mit Netzwerksicherheit beschäftigen möchten, ihren PC aber dennoch einigermaßen schützen wollen. Komplexere Produkte wie Outpost oder Norton Internet Security bieten mehr Konfigurationsmöglichkeiten, erfordern jedoch auch einen höheren Wissensstand.

4. Wie kann ich prüfen, ob mein Rechner sicher ist?

Personal Firewalls blockieren Ports, über die Verbindungen in das Internet hergestellt werden, und umgekehrt. Um zu prüfen, ob die Ports offen, geschlossen oder blockiert sind, verwenden Sie einen Portscanner. Wer einen Einzelplatzrechner hat, nutzt am besten einen Online-Portscanner, der die kritischen Port-Bereiche untersucht. Crossnet bietet zum Beispiel einen Online-Portscanner unter der Adresse **www.port-scan.de** an. Die Tests von PC Flank (**www.pcflank.com**) scannen verschiedene Port-Bereiche, die von typischen Diensten wie HTTP oder FTP, aber auch von Trojanern genutzt werden, und melden den Zustand der Ports. Ein offener Port kann für eine Verbindungsaufnahme aus dem Internet genutzt werden – er stellt eine Tür in Ihren Rechner dar. Auch geschlossene Ports melden einem potenziellen Eindringling: Hier ist etwas. Der sicherste Zustand ist der Stealth-Zustand.

ÜBERBLICK Firewall-Ratgeber

INHALT SEITE

Ein Port im Stealth-Zustand gibt überhaupt keine Antwort, jede Anfrage wird kommentarlos verworfen. PC Flank wie auch die Testseite unter der Adresse **www.grc.com** prüfen Ports auf den Stealth-Zustand. Bei GRC wählen Sie „ShieldsUP!“ und folgen den englischsprachigen Anweisungen.

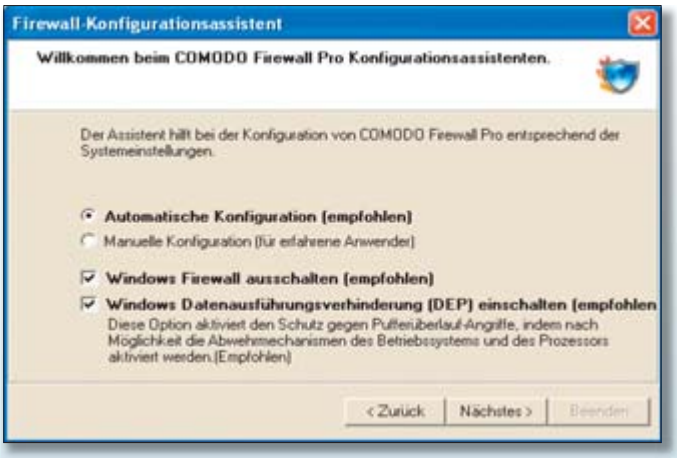
Verschiedene Online-Scans können jedoch unterschiedliche Ergebnisse liefern. Dann sollten Sie zunächst die Seriosität der Seiten abwägen. Testseiten von Firewall-Herstellern verfolgen möglicherweise bestimmte unternehmenspolitische Ziele, unabhängige Seiten eher nicht. Auch gibt es fehlerhafte Testseiten. Unstimmigkeiten müssen Sie jedenfalls klären.

›

Regeln: Die Firewall meldet alle Kommunikationsversuche, fragt um Erlaubnis und legt anhand Ihrer Antworten ein Regelwerk an (Punkt 2)

Online-Portscan: Mit Hilfe eines Web-Scanners kontrollieren Sie, welche Informationskanäle Ihr PC ins Internet offen hält (Punkt 4)

Auch im Netzwerk: Die meisten Firewall-Programme bieten Grundfunktionen, die auch den Netzwerkverkehr kontrollieren (Punkt 6)



Nur ein Wächter: Gute Firewall-Installationsprogramme deaktivieren die Windows-Firewall während des Setups automatisch (Punkt 8)

5. Ich habe offene Ports. Ist mein Rechner angreifbar?

Ja. Wer Dienste wie Web- oder FTP-Server im Internet anbietet, läuft immer Gefahr, dass diese kompromittiert werden. Nahezu ständig werden Fehler in Server-Software gefunden, die verschiedenste Angriffe erlauben. Als Gegenmaßnahme bleibt nur die Installation der jeweils neuesten Sicherheits-Patches der Hersteller. Zu den gefährlichen Ports gehört Port 139, der für die Freigaben in Windows-Netzwerken (Netbios-Netzwerken) zuständig ist. Dieser Port sollte auf der Internet-Schnittstelle grundsätzlich unsichtbar sein.

Zum Testen eignen sich Online-Scanner, die aber nur kleine Ausschnitte aus dem gesamten Port-Bereich – meistens nur einige Wellknown Ports sowie einige wenige typische Trojaner-Ports – testen. Verbindungen auf Ports größer als 1023 werden häufig nicht erfasst. Dort befindet sich die Spielwiese der Backdoors und Trojaner. Ein- und ausgehende Verbindungen auf solchen Ports sollten von der Firewall erkannt werden. Verlassen kann man sich jedoch nicht darauf. Alle aktiven Sockets (IP-Adressen und Port-Nummern) kann man leicht mit dem Kommandozeilen-Befehl „netstat -an“ anzeigen lassen. Das Problem dabei: Verbindungen können schnell geöffnet und auch wieder geschlossen werden. Wenn man nicht innerhalb dieses Zeitfensters den Netstat-Befehl ausführt, bleibt die Verbindung unerkannt.

6. Kann ich eine Personal Firewall auch im Netz einsetzen?

Ja. Die meisten Produkte bieten inzwischen LAN-Unterstützung. Wichtig ist die Unterscheidung zwischen interner Netzwerkanbindung ins LAN und externer Internet-Verbindung. Im Idealfall lässt sich die Firewall für beide Schnittstellen unterschiedlich konfigurieren. Die meisten Personal Firewalls bieten diese Unterscheidung jedoch nicht, sondern erlauben stattdessen die Angabe von vertrauten IP-Adressen, -Bereichen oder Subnetzen. Das eigene Netzwerk sollte immer mit privaten IP-Adressen konfiguriert sein (zum Beispiel 192.168.x.x), die dann in der Firewall als vertrauenswürdig („trusted“) eingetragen werden. Der Zugriff auf solche Adressen über das Internet funktioniert nicht, da sie nicht geroutet werden.

Ist bereits ein Netzwerk eingerichtet und wird später eine Firewall dazugeschaltet, müssen die im LAN benötigten Dienste in der Firewall freigeschaltet werden.

7. Warum funktioniert das Netzwerk mit der Firewall nicht mehr?

Eine Personal Firewall macht das, was sie machen soll: Sie blockiert Dienste und Verbindungen, und zwar alle. Ein- und ausgehende Verbindungen müssen erst explizit erlaubt werden, damit etwas funktioniert. Meistens funktionieren nach der Installation einer Personal Firewall die Freigaben im Netzwerk nicht mehr, dann ist so zu verfahren wie in der vorhergehenden Antwort beschrieben. Auch typische Client-Verbindungen wie ICQ müssen erst in der Personal Firewall freigeschaltet werden.

Betroffen sind grundsätzlich alle Internet-Anwendungen, auch News- und FTP-Clients, Online-Spiele, Filesharing-Tools oder Instant-Messenger-Programme und so weiter. Der Betrieb solcher Tools in einem

PERSONAL FIREWALLS Die richtigen Einstellungen

Mit der bloßen Installation einer Personal Firewall auf allen Arbeitsstationen im lokalen Netzwerk ist es nicht getan. Die Firewall darf nämlich nicht einfach alles abblocken, sondern muss differenzieren. Dafür verwenden die Tools vor allem einen Anwendungsfilter, der die Internet- Verbindung von Anwendungsprogrammen überwacht. Zwar bieten die meisten Firewalls bereits nach der Installation ein gewisses Grundmaß an Sicherheit. Viele der heute verfügbaren Personal Firewalls erkennen zudem bereits häufig die auf dem Rechner installierten Programme und legen automatisch entsprechende Filterregeln an. Dennoch ist an vielen Ecken und Enden noch immer Handarbeit nötig, wenn Sie auf maximale Sicherheit aus sind.

Für die Firewall müssen Sie Regeln erstellen und pflegen. Damit alle Ihre Anwendungen funktionieren und Sie zugleich unerwünschte Internet-Zugriffe – etwa von Viren und Trojanern – unterbinden, benötigen Sie ein sorgfältig abgestimmtes Regelwerk. Die Regeln legen Sie fest, und Sie bestimmen auch, inwieweit Anwendungen auf Ihrem Rechner Verbindungen nach außen aufbauen dürfen.

Die Konfiguration der Filterregeln ist oft kompliziert. Das gilt besonders bei Programmen mit umfangreichen Konfigurationsmöglichkeiten. Als für den Einsatz auf Einzelplatz-PCs und in kleinen Netzwerken hilfreich erweist sich die Nutzung von Assistenten, die ausführliche Erklärungen geben.

Netzwerk kann durchaus problematisch sein: Die Personal Firewall muss all diese Verbindungen unterstützen.

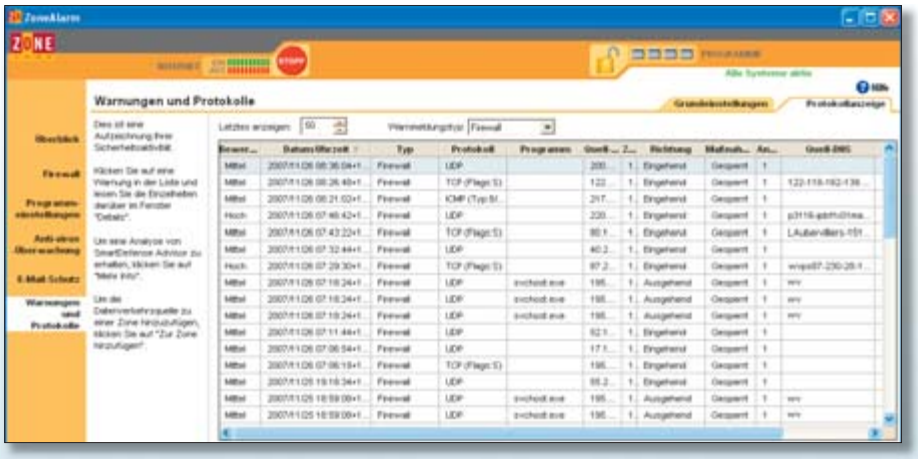
8. Bringt eine zweite Personal Firewall mehr Sicherheit?

Nein. Firewall-Programme klinken sich auf der Ebene der Netzwerkkartentreiber ein und filtern dort den Datenverkehr. Je mehr Prozesse dort eingreifen, desto höher ist die Gefahr von Abstürzen. Eine Firewall reicht normalerweise aus, um den gewünschten Sicherheitsgrad zu erreichen. Zwei Desktop-Firewalls behindern sich gegenseitig.

9. Was bedeuten die Meldungen über Angriffe?

Das sind in den meisten Fällen Fehlalarme. Einige Personal Firewalls geben bei fast jedem ankommenden Datenpaket eine Meldung aus. In der Regel handelt es sich dabei um Portscans oder im Internet übliche zufällig erfolgte Verbindungsversuche.

Das Firewall-Protokoll gibt Auskunft über Art und Häufigkeit von Verbindungsversuchen. Allerdings sind viele Logdateien schlecht lesbar, manche zeigen nicht einmal die fernen IP-Adressen an, so dass eine Zurückverfolgung unmöglich ist. Einige Firewalls liefern zu jedem vermeintlichen Angriff Links ins Web, wo sich Infos über die Art des Verbindungsversuchs nachlesen lassen. Die hektische Betriebsamkeit mancher Personal Firewall soll nur einreden: Ich passe auf und war eine gute Wahl.



Umfangreiches Aktivitätsprotokoll: Nicht alle Einträge, die eine Firewall meldet und in der Protokolldatei festhält, weisen auf tatsächlich erfolgte Angriffe hin (Punkt 10)

10. Mein Rechner wird angegriffen – was soll ich tun?

Ruhe bewahren! Die Feststellung, ob Ihr Rechner tatsächlich attackiert oder gehackt wird oder nicht, ist extrem schwer zu treffen. In den Logdateien werden meist die IP-Adressen angezeigt, die Verbindungsversuche unternommen haben. Längst nicht alle davon sind Einbruchsversuche. Ein reiner Port-Scan ist noch kein Einbruch, sondern durchaus üblich. Wer immer online und aktiv im Internet ist, kann mit häufigen Scans rechnen. Wichtig ist, welcher Port gescannt wurde. Auch das steht im Protokoll. Scans auf den so bezeichneten Well-known Ports sind immer verdächtig. Werden die Ports 21, 25 und 80 gescannt, ist ein Einbruchsversuch wahrscheinlich.

11. Wie lässt sich ein Angreifer zurückverfolgen?

Wird ein Angreifer vermutet, können Sie seine IP-Adresse mit Tools wie dem englischsprachigen Visual Route (für Win XP und Vista, Download und unter **www.visualroute.com**; Lite-Version für Privatnutzer gratis) ausfindig machen.

Neben dem Standpunkt seines Einwahl-Routers ist der Besitzer der IP-Adresse leicht ausfindig zu machen. Eine Abfrage seiner IP-Adresse bei **http://www.ripe.net/perl/whois** liefert seinen Namen und den Provider. Mit diesen Infos senden Sie eine Mail an den Provider. Meistens wird dieser allerdings nichts unternehmen, es sei denn, ein Einbruch ist nachgewiesen, etwa durch sich häufende Beschwerden.

FIREWALL-SCHUTZ Hardware oder Software?

Damit Angreifer aus dem Internet nicht auf Ihren Rechner und PCs in Ihrem Netzwerk zugreifen können, kämpft eine Firewall an zwei Fronten: Sie blockt unberechtigte Zugriffe von außen ab und verhindert den nicht autorisierten Datenversand von innen.

Firewalls gibt es als Hardware (Firewall-Box oder -PC) und als Software (Personal Firewall, Desktop-Firewall), die Sie auf allen am Netzwerk angeschlossenen Computern installieren müssen. Professionellen Anwendern steht zudem die Möglichkeit offen, einen eigenen Firewall-Rechner einzusetzen, beispielsweise auf Basis einer speziell konfigurierten Linux-Distribution. Er lässt sich sogar als virtuelles System aufsetzen.

Bei einer Hardware-Firewall handelt es sich um eine kleine Box mit eigener Stromversorgung und mindestens zwei Netzwerkanschlüssen, die Sie zwischen Ihrem Netzwerk-Hub oder -Switch und Ihrem Internet-Gateway – beispielsweise einem DSL-Router – anschließen.

Allerdings kann eine Hardware-Firewall nicht verhindern, dass Programme ungewollt Verbindungen ins Internet aufbauen. Die Geräte bieten neben einer Firewall für alle am Netz angeschlossenen PCs meist auch weitere Funktionen – etwa einen Netzwerkzugang über ein Virtual Private Network, einen vorkonfigurierten DHCP-Server oder einen Printserver. Die Vorteile von Hardware-Firewalls: Sie fangen Hacker-Angriffe ohne Rückfragen beim Anwender selbständig ab und arbeiten nach einmaliger Einrichtung über ihren Browser unabhängig von den Arbeitsplatz- PCs.

Professionelle Hardware-Firewalls sind vorwiegend für Firmen konzipiert und daher meist recht teuer. So kostet zum Beispiel eine Einsteigerlösungen rund 600 Euro. Dazu kommt in der Regel noch ein Support-Vertrag, der mit monatlichen oder jährlichen Kosten zu Buche schlägt. Wenn Sie den großen Funktionsumfang einer vollwertigen Hardware-Firewall nicht benötigen, sind Sie mit einem ISDN- beziehungsweise DSL-Router mit einer integrierten Hardware-Firewall besser beraten.

Eine Software-Firewall bietet sich für einzelne Windows-PCs und Mini-Netzwerke an. Eine Software-Firewall schottet den PC nach außen ab, bemerkt aber auch Verbindungsaufnahmen vom jeweiligen Rechner ins Internet – diese sind typisch für Trojaner oder Spyware. Einfach zu bedienen sind etwa das englischsprachige **Zone Alarm** oder **PC Tools Firewall Plus** . Beide Programme laufen unter allen Windows-Versionen und sind für den privaten Einsatz kostenlos.

Tipps für einen sicheren PC – Schutz-Tools auf CD DVD

Firewall – Das steckt dahinter

Tools können weniger, als man ihnen nachsagt. Wir verraten, wo Ihre Firewall nichts nützt, und geben Tipps, wie Sie wirklich sicher sind.

Von **Arne Arnold** und **Benjamin Schischka**

Mythos 1 Mit einer Firewall bin ich vor Internet-Gefahren sicher

Wer glaubt, mit einer Firewall allein genug für die Sicherheit getan zu haben, der irrt sich. Ganz im Gegenteil: Ein Anwender kann sich dadurch in falscher Sicherheit wiegen und leichtsinnigerweise in Ecken des Internets vorwagen, die er normalerweise nie ansurfen würde.

Tatsächlich filtert die Firewall nur den Netzwerkverkehr. DVD- und USB-Laufwerke bleiben nicht zu unterschätzende Einfallstore. Das beweist der Wurm Conficker, der sich über diese Medien erstaunlich rasant verbreitet hat. Die Firewall ist außerdem machtlos gegen klassische Vireninfektionen: Wenn ein Schädling heruntergeladen und gestartet wurde, kann er sich im Internet Explorer einnisten und mit der Online-Berechtigung des Tools die Firewall austricksen.

Konsequenz: Ergänzen Sie Ihre Firewall unbedingt mit einer Antiviren-Software, etwa dem kostenlosen **Antivir Personal Free 9.0** (für Windows XP, Vista und 7, unter *www.free-av.de*). Runden Sie den Schutz des PCs durch regelmäßige Updates aller Programme und durch kritisches Anwenderverhalten ab.

Mythos 2 Der Stealth-Modus macht mich unsichtbar

Der Stealth-Modus, der in manchen Firewalls integriert ist, suggeriert Unsichtbarkeit und damit völligen Schutz vor Angreifern. Die Realität sieht anders aus: Der Stealth-Modus schweigt zwar bei Ping-Anfragen. Aber wenn ein Hacker keine Antwort auf seine Anfrage bekommt, weiß er, dass dort ein Rechner existieren muss, der seine Anfrage verworfen hat. Denn wenn sich kein PC hinter einer bestimmten IP-Adresse befindet, antwortet die entsprechende Netzwerkstelle mit „Destination unreachable“ („Ziel nicht erreichbar“).

Konsequenz: Schalten Sie den Stealth-Modus in der Firewall ab.

Mythos 3 Hardware-Firewall ist besser als Software-Firewall

Genau genommen ist die Unterscheidung zwischen Hardware- und Software-Firewall falsch. Denn auch auf einer Hardware-Firewall läuft Software. Meist ist das ein Linux-basiertes Betriebssystem mit einem Paketfilter. Wie jedes andere System kann auch dieses Sicherheitslücken haben und angreifbar sein. Tatsächlich mussten schon mehrere Anbieter einer Hardware-Firewall Updates bereitstellen, da ihre Betriebssysteme gefährliche Lücken hatten.

Die Stärke von Hardware-Firewalls liegt woanders: Sie arbeiten im Gegensatz zu einer Desktop-Firewall völlig getrennt vom PC. Sie kommen damit der Anforderung an eine Firewall, zwei Netzwerke zu trennen, besser nach (siehe Kasten).

Konsequenz: Den besten Schutz bekommen Sie durch die Kombination aus Hardware-Firewall (etwa per DSL-Router) und Desktop-Firewall (etwa **Zone Alarm Free**, Version 7.0 für Win XP unter *www.zonealarm.com*).

Mythos 4 Eine aktive Firewall muss dauernd Angriffe melden

Viele Desktop-Firewalls melden per Popup, wenn sie Datenpakete verwerfen, die ankommen, ohne dass sie zuvor von einem Programm angefordert wurden. Die Popups erscheinen als Warnung, teils sogar mit Signalton.

Doch diese Warnungen sind fast immer überflüssig: In den meisten Fällen sind die gemeldeten Pakete nur die Antworten auf Anfragen, die eins Ihrer Tools – etwa der Browser – generiert hat, die der Firewall aber entgangen sind. Wer sich zudem für eine Online-Verbindung neu einwählt, bekommt eine IP-Adresse, die eventuell kurz zuvor an einen anderen PC vergeben war und an die noch Pakete gesendet werden.

Außerdem: Hacker durchsuchen das Internet laufend automatisiert nach verwundbaren Rechnern. Sie überprüfen per Ping, welche Rechner eingehende Verbindungen zulassen, indem sie ganze IP-Adressbereiche scannen. Genauso gehen etliche Würmer vor. Auch solche Scans lösen bei einer mitteilungsfreudigen Firewall eine Warnung aus.

Konsequenz: Deaktivieren Sie die Meldungen – meist bietet die Firewall diese Option an.

Mythos 5 Geschlossene Ports erhöhen die Sicherheit

Grundsätzlich bedeuten weniger offene Ports weniger Angriffsfläche. Es gibt aber eine Methode, mit der sich geschlossene Ports umgehen lassen: Beim so genannten Tunneln schickt der Anwender über einen offenen Port dienstfremde Daten, die eigentlich nicht für die Übertragung über diesen Port vorgesehen sind. Um den Netzwerkdienst des Ports auszutricksen, hat der Anwender die Daten vorher in dessen Format konvertiert.

Dazu ein Beispiel: Fast immer ist der Port 80 für das HTTP-Protokoll offen. Über einen solchen HTTP-Tunnel lassen sich auch FTP-Daten austauschen, obwohl der FTP-Port (21) geschlossen ist. Die FTP-Daten wurden dafür in ein HTTP-Protokoll eingebettet. Besonders beliebt fürs Tunneln sind Verbindungen über HTTPS (Hypertext Transfer Protocol Secure). Die darin integrierte Verschlüsselung verhindert, dass die Firewall die verschickten Daten bewerten und eventuell abblocken kann. Viele Filesharing-Programme, mit denen sich Musik, Filme und andere Dateien übers Internet tauschen lassen, tunneln die Daten über Port 80, da ihr Standard-Port in vielen Firmen blockiert ist.

Allerdings müssen für einen Tunnel beide Seiten der Verbindung entsprechend konfiguriert sein. Ist auf einem PC keine Tunnel-Software aktiv, kann ein Angreifer von außen diese Lücke nicht nutzen.

Konsequenz: Mit der Firewall die Ports dicht zu machen ist in jedem Fall sinnvoll. Wichtiger ist aber, dass Sie keine Online-Programme – etwa einen FTP-Server – laufen haben, die Sie nicht benötigen. Die Tools aber, die Sie brauchen, sollten Sie stets mit Updates versorgen.

FIREWALL-FAKTEN Das leisten die Programme wirklich

So arbeitet eine Firewall: Sie trennt zwei Netzwerke

Eine Firewall trennt zwei Systeme voneinander. Bei Privatanwendern sieht das in der Regel so aus: Auf der einen Seite befindet sich das Internet, auf der anderen der eigene PC. Die Firewall platziert sich dazwischen: entweder in Form eines DSL-Routers, etwa der verbreiteten Fritzbox, oder als Desktop-Firewall auf dem PC selbst. Idealerweise ist beides vorhanden – die Schutzfunktionen von Hardware-Box und Desktop-Firewall ergänzen sich.

Darum brauchen Sie eine Firewall: Nur so bleiben Würmer draußen

Eine Firewall bietet Schutz gegen gefährlichen Code. Sie blockt alle unerwünschten Anfragen aus dem Internet ab und sperrt damit die Schädlinge aus, etwa Würmer. Das gelingt ihr auch bei Windows-Sicherheitslücken, für die noch keine Updates bereitstehen. Eine Desktop-Firewall, die direkt auf Ihrem PC läuft, arbeitet zudem als Anwendungsfilter – das heißt: Sie benachrichtigt Sie jedesmal, wenn ein Programm online gehen will, dem Sie das zuvor nicht ausdrücklich erlaubt haben. Vor allem aber ist diese Funktion das letzte Bollwerk: Sollte sich ein Schad- oder Spionageprogramm am Antiviren-Tool vorbeigeschmuggelt haben, werden Sie darauf aufmerksam, sobald es Kontakt mit dem Internet herstellen will.

Schwächen einer Firewall: Viren hebeln den Schutz aus

Es tauchen immer wieder Schädlinge auf, die den Schutz umgehen und hintenherum Daten ins Internet senden. Beispielsweise nehmen die Viren mit den Rechten des Internet Explorers Verbindung zum Web auf. Andere Viren können die Firewall komplett beenden und löschen, um anschließend ungestört Daten ins Internet zu senden.

Testen Sie Ihre Firewall

Firewall-Tipps

Eine Firewall soll Ihren PC vor Angriffen aus dem Internet schützen. Das gelingt ihr aber nur, wenn sie richtig konfiguriert ist. Wir geben Tipps, wie Sie die Software am besten einstellen.

Von **Arne Arnold**

Eine Desktop-Firewall hat eine eindeutige Aufgabe: Sie lässt erwünschte Datenpakete passieren, und unerwünschte blockt sie ab. Doch woher weiß das Programm, was erwünscht ist und was nicht? Es hört auf die Befehle des Anwenders – also auf Ihre.

Wenn Sie etwa eine typische Tauschbörsen-Software starten, dann geben Sie zumindest einen Ordner Ihres PCs auch allen anderen Anwendern dieses Dienstes frei. Das Verzeichnis ist von jedem Rechner im Internet aus erreichbar. Es ist also entscheidend, dass Sie Ihre Firewall richtig einstellen und bedienen. Die Firewall folgt außerdem mitgebrachten Regeln. Stets aktiv und wahrscheinlich die wichtigste Regel ist: Die Annahme von unaufgefordert zugesandten Datenpaketen aus dem Internet wird verweigert. Auf diese Weise schützt eine Firewall auch vor den gefürchteten „Wurmlücken" in Windows. Schließlich protokolliert eine Desktop-Firewall auch, welche Anwendung wann Daten versendet. Das verschafft einen guten Überblick über den Netzwerkverkehr auf Ihrem Rechner.

In diesem Artikel geben wir Ihnen 20 Tipps, wie Sie Desktop- und Hardware-Firewalls richtig testen und konfigurieren.

TIPP 1 Kontrollieren Sie die Windows-Firewall

Die Windows-Firewall genügt als Schutz gegen Angriffe aus dem Internet vollkommen. Wenn Sie keine zusätzliche Desktop-Firewall nutzen wollen, verwenden Sie das Bordmittel von Windows. Ab der Version XP mit Service Pack 2 ist das Tool standardmäßig eingeschaltet.

Achtung: Wenn Sie irgendwann eine ältere Desktop-Firewall installiert hatten, hat diese die Windows-Firewall bei der De-Installation wahrscheinlich nicht wieder eingeschaltet. Kontrollieren Sie, ob das Bordmittel aktiv ist: Das geht unter „Systemsteuerung, Windows Firewall". Sollten Sie aber eine Desktop-Firewall installiert haben, so darf nur diese aktiv sein. Die Windows Firewall muss vom Installations-Assistenten deaktiviert worden sein. Ob das wirklich geschehen ist, überprüfen Sie an derselben Stelle: „Systemsteuerung, Windows Firewall".

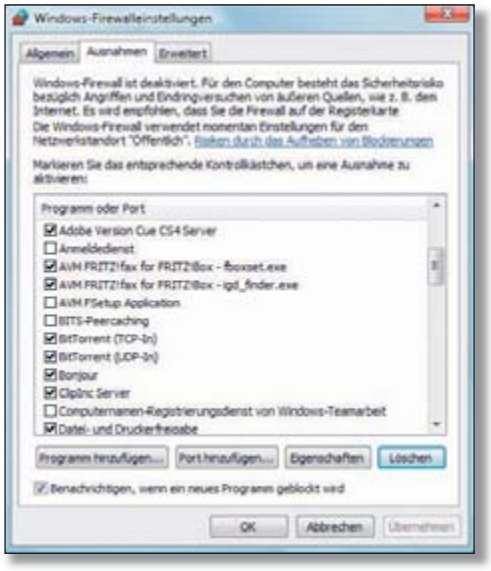
QUICK-CHECK für Ihre Firewall

- **Prüfen Sie im Windows-Sicherheits-Center,** ob überhaupt eine Desktop-Firewall aktiv ist: Das geht unter „Systemsteuerung, Sicherheitscenter".
- **Kontrollieren Sie im Sicherheitscenter,** dass nur eine Firewall aktiv ist.
- **Wenn Sie eine Desktop-Firewall installiert haben,** prüfen Sie, welche Programme die Erlaubnis haben, online zu gehen und welche als Server arbeiten dürfen.
- **Checken Sie,** ob nur erwünschte Ausnahmen in der Windows-Firewall eingetragen sind: Das geht unter „Systemsteuerung, Windows-Firewall".
- **Scannen Sie Ihren PC** mit einem Online-Dienst auf offene Ports (Online-Türen): *www.pcwelt.de/c5a*. Je weniger Sie finden, desto besser.

TIPP 2 Kontrollieren Sie Freigaben in der Windows-Firewall

Nach außen ist Ihr Rechner durch die Windows-Firewall abgeschottet. Denn sie verwirft alle Datenpakete, die unaufgefordert ankommen. Aber: Sie lässt alle Pakete durch, die an Programme auf der Ausnahmenliste gesendet werden. Diese Liste sollten Sie regelmäßig kontrollieren, um sicher zu sein, dass dort nur erwünschte Tools stehen. Das geht über „Systemsteuerung, Windows Firewall, Ausnahmen“ (XP) oder „Systemsteuerung, Windows Firewall, Programme durch die Windows-Firewall kommunizieren lassen“ (Vista).

Was die „Ausnahmen“ genau bedeuten, erfahren Sie im Tipp 9. Sollten auf dieser Liste Namen auftauchen, die Ihnen nichts sagen, markieren Sie diese und schauen sich unter „Eigenschaften“ den Pfad und den Dateinamen an. Mit Hilfe von Tipp 8 finden Sie schnell heraus, was das Programm macht. In der Regel ist es unproblematisch, Tools von der Ausnahmeliste zu entfernen (Häkchen entfernen). Sollte ein Online-Tool danach nicht mehr richtig arbeiten, setzen Sie das Häkchen wieder.

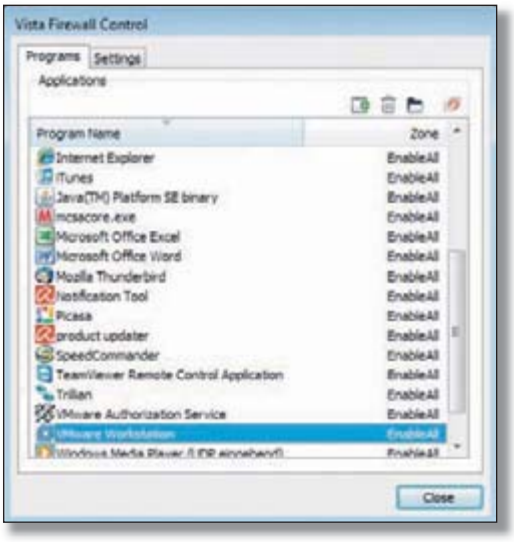


TIPP 3 Windows-XP-Firewall mit Tipps von Microsoft einstellen

Die Firewall von Windows XP bietet nicht gerade viele Einstellmöglichkeiten. Wer sie dennoch einsetzen möchte, findet bei Microsoft selbst eine ausführliche Anleitung – über *www.pcwelt.de/3b6*. Wenn Sie die Firewall nicht nur auf einem PC konfigurieren wollen, sondern auf vielen in gleicher Weise, geht das am besten über eine Konfigurationsdatei (Netfw.inf). Diese kopieren Sie mit den gewünschten Regeln auf jeden PC, und schon ist die Firewall entsprechend konfiguriert. Eine genaue Anleitung gibt's über *www.pcwelt.de/22b*.

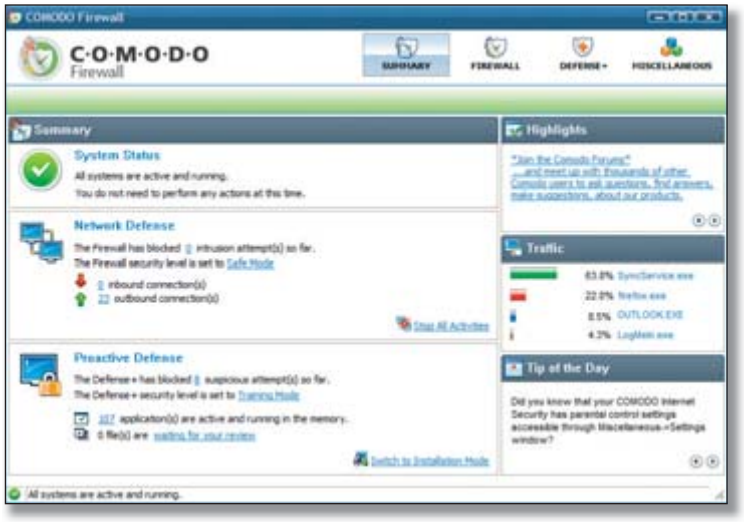
TIPP 4 Die Vista-Firewall als Zwei-Wege-Firewall nutzen

Neu in Windows Vista ist eine Zwei-Wege-Firewall. Diese ist anders als bei XP auch in der Lage, den ausgehenden Datenverkehr zu regulieren. Aber Achtung: Wenn Sie diese Option einschalten, müssen Sie manuell jedes einzelne Programm eintragen. Eine mühselige Aufgabe, bei der man schnell ein wichtiges Tool vergisst, etwa den Updater des Antiviren-Programms.



Die komfortable Lösung: Das kostenlose **Vista Firewall Control** ist eine Ergänzung zu der in Windows Vista eingebauten Firewall. Nach der Installation meldet das Tool jede Anwendung, die Daten ins Internet senden will – so, wie man es von anderen Desktop-Firewalls her kennt. Auf diese Weise gelingt die Konfiguration Schritt für Schritt.

Wenn Vista Firewall Control ein Programm meldet, das Zugriff aufs Internet fordert, können Sie mit „Enable All“ und „Disable All“ für dieses Programm den gesamten Datenverkehr erlauben beziehungsweise verbieten. Eine Beschränkung auf den nur ein- oder ausgehenden Verkehr ist ebenfalls möglich.



TIPP 5 So finden Sie die beste kostenlose Desktop-Firewall

Wenn Ihnen die Firewall von Windows zu wenig bietet, sollten Sie eine kostenlose Desktop-Firewall installieren. In den vergangenen Jahren hat in Tests meist **Zone Alarm Free** am besten abgeschnitten. Wer dennoch eine Alternative sucht: Einfach in der Bedienung ist etwa die **Ashampoo Firewall Free**, schlicht ist das Tool **Vista Firewall Control** (Tipp 4). Profis können sich die gute, aber komplizierte Firewall in der Suite **Comodo Internet Security** ansehen.

TIPP 6 Das darf eine gute Desktop-Firewall kosten

Wer mit einer kostenlosen Firewall nicht glücklich wird, schielt vielleicht auf ein Bezahl-Tool, etwa **Zone Alarm Pro** (www.*zonealarm.com*), **Online Armor** oder **Outpost Firewall Pro** (*www.agnitum.de*). Wir raten allerdings davon ab, lediglich eine Desktop-Firewall allein zu kaufen. Wenn Sie Geld ausgeben wollen, investieren Sie lieber in eine komplette Sicherheits-Suite, die außer der Firewall auch einen Virenschutz bietet. Empfehlenswert sind beispielsweise die Suiten von **Norton** und **G-Data** . Die Die Vollversionen kosten laut Hersteller zwischen 25 und 40 Euro im Elektromarkt, bei Online-Versendern gibt's die Tools teils deutlich billiger.

GRATIS-FIREWALLS Diese Tools schotten ab (zu Tipp 5)

Programm	Internet	Windows
Ashampoo Firewall Free	*www.ashampoo.com*	XP
Comodo Internet Security 1)	*www.comodo.com*	XP, Vista
Jetico Personal Firewall 1)	*www.jetico.com*	XP, Vista
Online Armor Personal Firewall 1)	*www.tallemu.com*	XP, Vista
PC Tools Firewall Plus	*www.pctools.com*	XP, Vista
Sunbelt Personal Firewall	*www.sunbeltsoftware.com*	XP, Vista
Webroot Desktop Firewall 1) 2)	*www.webroot.com*	XP, Vista
Vista Firewall Control 1)	*www.sphinx-soft.com*	Vista
Zone Alarm Free	*www.zonealarm.com*	XP, Vista

1) englischsprachig 2) derzeit gratis

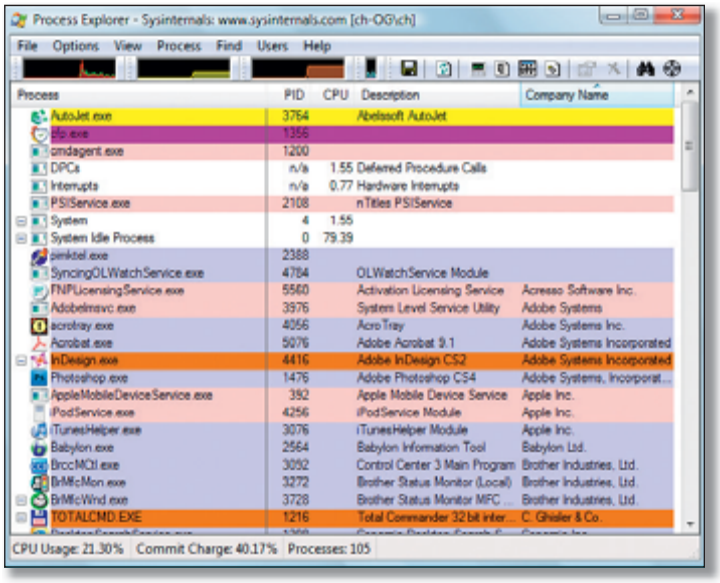
TIPP 7 Pro-Funktionen von Zone Alarm kostenlos nutzen

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 konfiguriert das Tool automatisch Regeln für etliche bekannte Programme. Diese Regeln bleiben Ihnen erhalten, wenn die Firewall später in den Freeware-Modus wechselt. So sparen Sie sich eine Menge Konfigurationsaufwand.

TIPP 8 So schätzen Sie Meldungen der Firewall richtig ein

Eine Gratis-Firewall wird Sie immer wieder mal fragen, ob ein bestimmtes Programm online gehen darf. Dazu zeigt es zumindest den Namen der Programmdatei an, meist aber auch den kompletten Pfad zur Datei. Sind Sie sich nicht sicher, ob es sich bei dem Programm um eine harmlose, legitime Anwendung handelt, hilft unser Prozessmanager **Process Explorer** weiter.

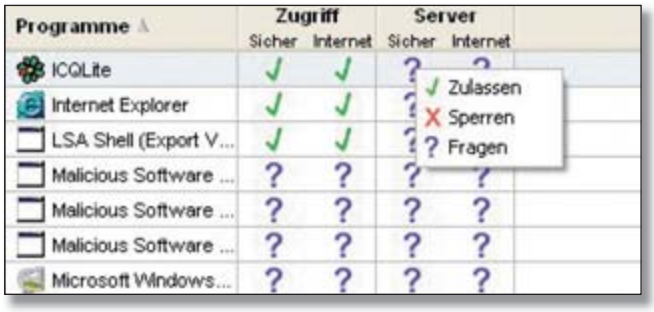
Sie müssen das Tool nicht installieren. Nach dem Start zeigt es alle aktiven Programme an. Den Programmnamen können Sie dann auf *www.pcwelt.de/b10* in unserer Prozessdatenbank suchen. Wenn er dabei ist, erhalten Sie entsprechende Infos zur Anwendung; wenn nicht, geben Sie den Namen in Google ein. Sie dürfen übrigens unsere Datenbank (ein Wiki) erweitern.



TIPP 9 Achtung! Seien Sie sparsam mit Server-Rechten für Tools

Programme, die auf das Internet zugreifen, lassen sich in zwei Gruppen einteilen: Tools, die nur Client-Rechte benötigen, und solche, die (auch) als Server arbeiten. Client-Tools empfangen nur Datenpakete, die sie zuvor angefordert haben. Beispielsweise der Browser, der die Website *www.pcwelt.de* angefordert hat.

Für andere Tools sind Server-Rechte erforderlich, da sie unangeforderte Datenpakete empfangen wollen. Dafür öffnen die Tools selbst einen Port des PCs für Zugriffe aus dem Internet. Oft ist klar, warum ein Tool als Server arbeiten möchte – etwa wenn Sie einen FTP-Server einsetzen. Ein offener Port alleine ist noch keine Sicherheitslücke. Erst wenn der Dienst, der dahinter aktiv ist, einen Bug hat, ist der PC über diesen Port und den Bug angreifbar. Je weniger Programme also Server-Rechte in der Firewall besitzen und einen Port geöffnet haben, desto besser.



TIPP 10 So erteilen Sie Server-Rechte, wenn es nötig ist

Die meisten Firewalls erkennen automatisch, wenn ein Programm Server-Rechte benötigt (Tipp 9), und fragen Sie eigens um Erlaubnis. Sind Sie im Zweifel, ob Sie dem Tool das erlauben wollen, sagen Sie zunächst mal „Nein“. Wenn das Tool dann nicht wie erwartet arbeitet, vergeben Sie die Server-Rechte nachträglich.

Server-Rechte – so geht's: In Zone Alarm etwa finden Sie die Optionen unter „Programmeinstellungen, Programme“. Klicken Sie mit der linken Maustaste auf die Zeile unter „Server“, und wählen Sie „Zulassen“. Bei anderen Firewalls findet sich das Regelwerk an ähnlicher Stelle.

QUICK-TIPPS für Ihre Firewall

- **Gibt's mal Probleme** mit einer Online-Anwendung, dann schauen Sie im Regelwerk der Desktop-Firewall nach, ob die jeweilige Anwendung dort verboten ist.
- **Installieren Sie Updates** für Ihre Desktop-Firewall, um Bugs und Sicherheitslücken zu beseitigen.
- **Vergewissern Sie sich**, dass Ihr Antiviren-Programm und das zugehörige Update-Modul Zugriff aufs Internet haben, sonst kann sich das Tool keine Infos über neue Viren holen und Ihren Computer nicht mehr schützen.
- **Wenn Sie ein DSL-Modem mit Router haben,** dann verwenden Sie es auch wirklich als Router und nicht als Modem (Handbuch), da Sie nur so von den Schutzfunktionen des Geräts profitieren.

TIPP 11 Fehler finden, wenn es mit Online-Programmen hapert

Sollte ein Online-Programm nicht so funktionieren wie erwartet, dann kann das an der Desktop-Firewall liegen. Keine gute Idee ist es, die Firewall einfach auszuschalten, denn dann sind Sie unter Umständen von außen angreifbar. Stattdessen sollten Sie sich auf die Fehlersuche begeben. Das gelingt meist sehr gut über die Protokollfunktion in der Firewall.

1. Öffnen Sie das Protokoll. Bei den meisten Firewalls wird das Protokoll laufend aktualisiert, so dass Sie neue Einträge gleich entdecken.

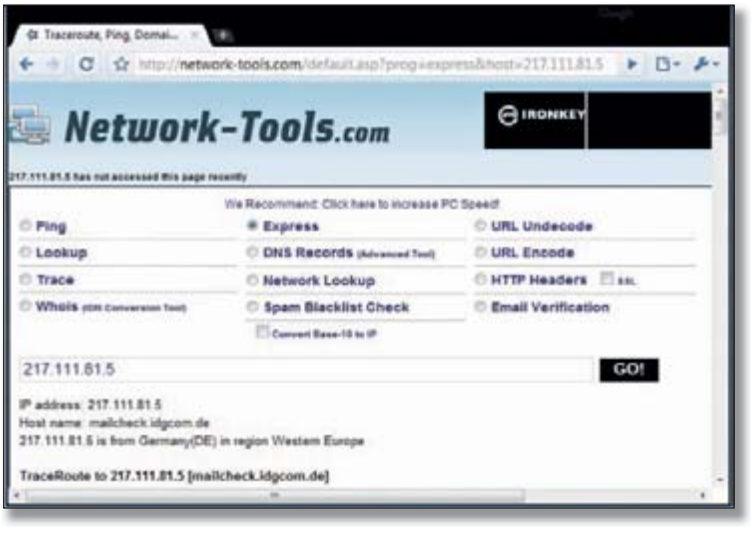
2. Starten Sie das Programm, das nicht korrekt funktioniert.

3. Achten Sie auf die Angaben im Protokoll. Wird dort dem Programm oder einer Komponente davon verboten, online zu gehen, dann fehlt eine entsprechende Berechtigung.

4. Vergeben Sie in der Programmliste 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 die unter „Meldungstyp, Firewall". Die Berechtigung für ein Online-Programm ändern Sie unter „Programmeinstellung, Programme".

TIPP 12 Den Unsichtbarkeitsmodus können Sie sich sparen

Einige Desktop-Firewalls werben immer noch damit, dass sie einen Rechner unsichtbar machen können. Das ist Unsinn. Denn um zu signalisieren, dass eine bestimmte IP-Adresse nicht vergeben ist – sich dort also auch kein PC befindet –, muss die davor befindliche Netzwerkstelle die ICMP-Meldung 3 ausgeben (Destination Unreachable). Beim PC ist das der Internet-Provider. ICMP steht für Internet Control Message Protocol. Eine Firewall hat aber keinerlei Einfluss auf den Internet Service Provider. Sie kann die ICMP-Anfrage, ob dort ein PC ist, nur verwerfen. Da das aber bei ICMP nicht vorgesehen ist, kann ein Angreifer folgern, dass sich auf der angesprochenen IP-Adresse etwas befinden muss, das die Anfrage verworfen hat. Den Unsichtbarkeitsmodus (Stealth-Modus) können Sie sich getrost sparen. Innerhalb eines privaten Netzwerks stört er gar bei einer möglichen Fehlersuche.



TIPP 13 So finden Sie den Anbieter zu einer IP-Adresse

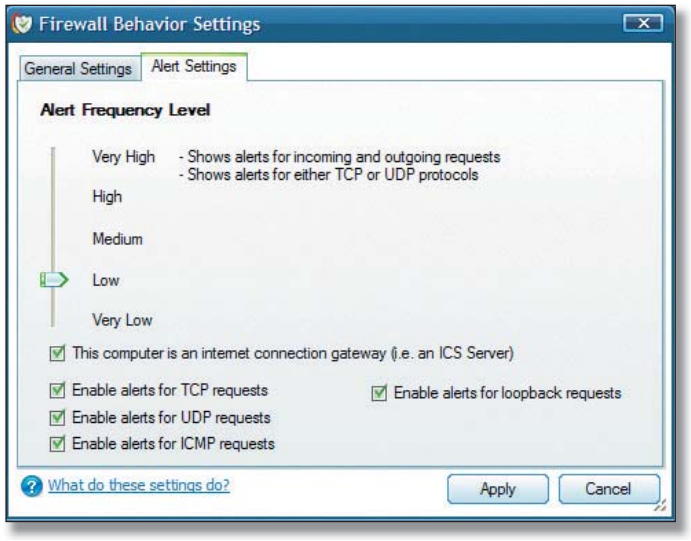
Im Protokoll Ihrer Firewall können Sie sich Verbindungen zu einer bestimmten IP-Adresse nicht erklären. Dann sollten Sie auf der sehr nützlichen Site *http://network-tools.com* die IP-Adresse eingeben und auf „Go" klicken. Voreingestellt ist die Option „Express", die per Whois und anderen Netzwerk-Tools Infos über die IP holt. Wenn es sich um eine dynamisch verteilte IP-Adresse handelt, erfahren Sie zumindest, welcher Internet-Service-Provider die IP-Adresse vergibt. Gehört die IP-Adresse zu einer Website, zeigt Ihnen der Dienst den Namen der Site an – etwa *www.pcwelt.de*. Auch liefert der Dienst den Eigentümer der Site plus viele weitere Informationen.

TIPP 14 Diese Warnungen der Firewall können Sie ignorieren

Viele Desktop-Firewalls melden per Pop-up, wenn sie Datenpakete verwerfen, die ankommen, ohne dass sie zuvor von einem Programm angefordert wurden. Diese Pop-ups sind fast immer überflüssig, und Sie können sie abschalten – meist bietet die Firewall diese Option an.

Darum sind die Warnungen überflüssig: In den meisten Fällen sind die gemeldeten Pakete nur die Antworten auf Anfragen, die eines Ihrer Tools – etwa der Browser – generiert hat, was der Firewall aber entging. Und wer sich für eine Online-Verbindung neu einwählt, bekommt eine IP-Adresse, die eventuell kurz zuvor an einen anderen PC vergeben war und an die noch Pakete gesendet werden.

Außerdem: Hacker durchsuchen das Internet laufend automatisiert nach verwundbaren Rechnern. Sie überprüfen, welche Rechner eingehende Verbindungen zulassen, indem sie ganze IP-Adressbereiche scannen. Auf dieselbe Weise gehen etliche Würmer vor. Auch solche Scans lösen bei einer mitteilungsfreudigen Firewall eine Meldung aus.



TIPP 15 Eine Desktop-Firewall als Ergänzung zum DSL-Router

Die meisten DSL-Router blocken Angriffe aus dem Internet ab. Doch sie informieren den Nutzer nicht über Anwendungen, die vom PC aus Daten ins Internet senden. Kurz: Alles was vom PC aus mit dem Web reden will, darf das – selbst Trojaner, Bots und andere Schädlinge. Darum ist eine Desktop-Firewall (siehe Tipp 5) eine gute Ergänzung zu dem Schutz durch einen DSL-Router.

TIPP 16 Vor- und Nachteile von DSL-Routern

Das bringt ein Router: Hardware-Firewalls beziehungsweise DSL-Router bieten einen guten zusätzlichen Schutz gegen Gefahren aus dem Internet. Da sie getrennt vom Arbeitsrechner laufen, sind sie selber weniger für Angriffe anfällig. Sie können also zuverlässig alle unaufgeforderten Sendungen aus dem Internet verwerfen.

Nachteile eines Routers: Auch auf einem DSL-Router läuft ein Betriebssystem, das gegen Angriffe nicht gefeit ist, meist Linux.

Es gab bereits Angriffe per Javascript und den Browser des Anwenders, ebenso Angriffe per Flash-Dateien sowie Angriffe durch einen Wurm mit dem Namen Psyb0t, der manche DSL-Router mit dem System Mipsel in ein Botnet zieht (Infos über *www.pcwelt.de/31a*). Entsprechende Attacken sind bislang aber noch selten und meist nur bei Routern mit schwachen Passwörtern möglich.

TIPP 17 NAT im DSL-Router ist nur fast ein ausreichender Schutz

Network Address Translation (NAT) ist keine Firewall-Funktion, sondern die Aufgabe eines Routers. Er erhält bei der Einwahl ins Internet eine öffentliche IP-Adresse vom Provider. Alle PCs hinter dem Router haben eine private IP-Adresse. Fordert ein PC etwa eine Website aus dem Internet an, gibt NAT die Anforderung ans Web weiter.

Anschließend erhält NAT die Site und leitet sie an den PC. Bei der Anforderung tauscht die Funktion die private IP-Adresse des Rechners gegen die öffentliche des Routers aus – und beim Liefern an den PC umgekehrt. Das hat zur Folge, dass die IP-Adresse des PCs im Internet gar nicht auftaucht, was ihn für IP-Angriffe unempfindlich macht. NAT ist somit ein sehr zuverlässiger Schutz gegen viele verbreitete Gefahren im Internet.

Aber: Es gibt eine – wenn auch eher theoretische – Angriffsart, die NAT überrumpeln würde. Erreicht den Router ein nicht angefordertes Paket für eine vorhandene Adresse, etwa die häufig genutzte private Adresse 192.168.0.1, so versuchen einfache Modelle, irgendwie den passenden Port zu erraten und das Paket zuzustellen.

TIPP 18 Gefährliche Angriffe auf DSL-Router abwehren

Die Nachteile beziehungsweise Schwächen eines DSL-Routers (Tipp 16) können Sie durch die folgenden Maßnahmen zur Gänze ausgleichen.

1. Installieren Sie regelmäßig Updates für Ihren DSL-Router. Sie erhalten damit nicht nur neue Funktionen, sondern schließen auch Sicherheitslücken.

2. Falls Sie Universal Plug and Play (UPnP) nicht benötigen, deaktivieren Sie diese Funktion in Ihrem DSL-Router.

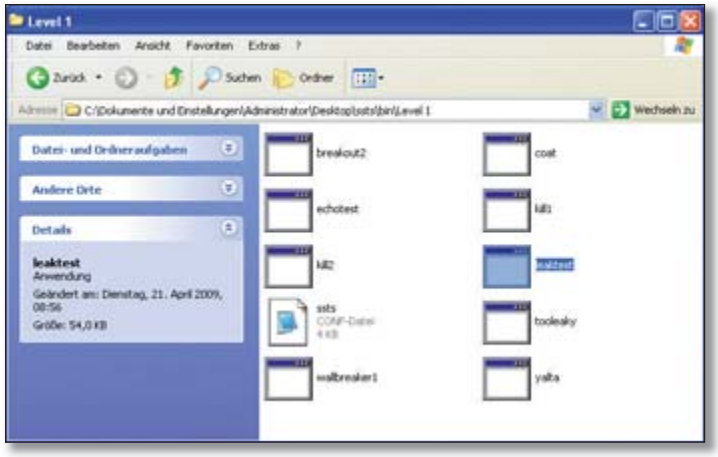
3. Ändern Sie unbedingt das voreingestellte Passwort, da sich sonst Angreifer über Sicherheitslücken von außen einloggen können. Dieser Punkt ist nur dann nicht relevant, wenn Ihr DSL-Router mit einem individuellem Passwort kommt. Das ist etwa bei der Fritzbox und den Geräten von T-Home der Fall.

4. Führen Sie vor dem Ändern des Passworts ein Reset durch. Folgen Sie dazu den Anweisungen im Handbuch. Sollte der Router vorher von einem Angreifer manipuliert worden sein, wird dies dadurch rückgängig gemacht.

TIPP 19 Nur für Profis: Testprogramme für Firewalls

Für absolute Profis gibt's im Internet die „Security Software Testing Suite" (über *www.pcwelt.de/320*, für Windows XP und Vista, gratis). Das ist eine Sammlung von einigen Dutzend Befehlszeilen-Tools, die es auf Desktop-Firewalls abgesehen haben. Zunächst müssen Sie die Konfigurationsdatei ssts.conf an Ihre Bedürfnisse und an die zu testende Firewall anpassen und darin die Bestimmungen akzeptieren (in der vorletzten Zeile).

Achtung: Verwenden Sie die Tool-Sammlung zur Sicherheit nicht auf einem Produktivsystem, sondern ausschließlich auf reinen Test-PCs.



TIPP 20 So testen Sie Ihre Firewall auf offene Ports (Online-Türen)

Ein Online-Check Ihrer Firewall zeigt Ihnen, ob Ihr System nach außen komplett geschützt ist. Gut ist etwa der Dienst Shields Up (über *www.pcwelt.de/d6a*). Sie können dort aus sieben Szenarien auswählen – darunter eines, bei dem Sie selbst die zu prüfenden Ports bestimmen. Der Test ist englischsprachig, er zeigt geschlossene Ports als „Closed", offene als „Open" und unsichtbar gemachte als „Stealth" (siehe Tipp 12). Zum Testergebnis hinzu bekommen Sie einige nützliche Informationen zu Ihrem System.

Einen deutschsprachigen Portscan bietet die Firma Symantec (über *www.pcwelt.de/c5a*). Hier können Sie zwar nicht die Ports festlegen, doch der Dienst prüft bereits in seiner Standardeinstellung sehr gründlich. Mögliche Warnungen zu Sicherheitslücken sollten Sie aber genau studieren. Denn natürlich will Symantec in erster Linie seine Produkte verkaufen und bewertet eine Schwachstelle im System möglicherweise stärker als nötig. Insgesamt ist der Test aber verlässlich.

Achtung: Wenn Sie einen DSL-Router oder eine Hardware-Firewall einsetzen, dann werden bei dem Scan nicht die Ports Ihres Rechners getestet, sondern die des DSL-Routers. Diese sollten allerdings ebenfalls geschlossen sein.

FIREWALL Das zeichnet ein gutes Programm aus

Sicherheit: Eine Firewall sollte alle Angriffsversuche auf den Rechner verhindern. Dabei spielt es keine Rolle, ob die Angriffe von außen oder von innen kommen. Ein Tool muss etwa Backdoor-Programme erkennen und den Regeln sowie Filtern entsprechend behandeln. Der Selbstschutz muss Manipulationen an der Regelliste und das Deaktivieren des Tools blockieren. Auch müssen sich die Tools gegen das Löschen der eigenen Programmdateien schützen.

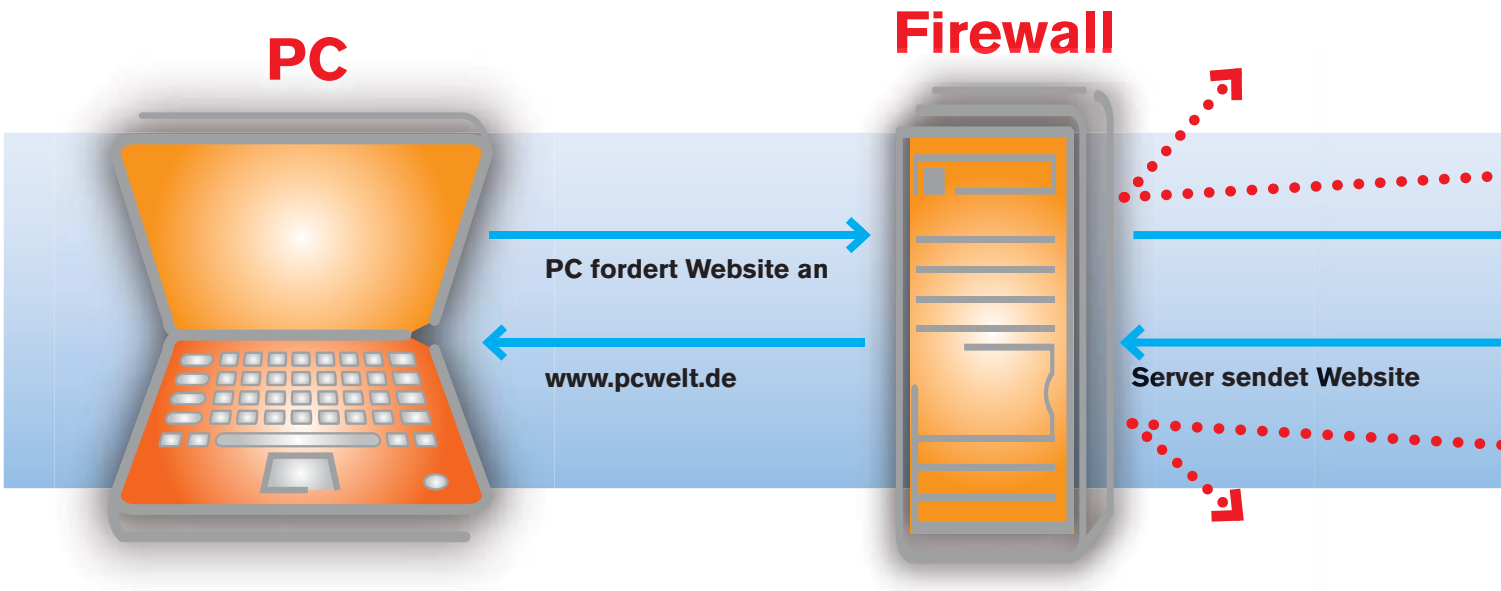
Funktionen: Eine Firewall muss den Nutzer über Programme informieren, die eine Verbindung zum Internet aufzubauen versuchen. Die Anwendungen sollten sich in Listen einordnen lassen, über die man festlegt, ob die Programme online gehen dürfen oder nicht. Assistenten sollten mit einfachen Erklärungen helfen.

Bedienung: Als Sicherheits-Software greift eine Firewall tief in das System ein. Aus diesem Grund ist es unverzichtbar, dass sie eine klare Benutzerführung bietet, die Fehler ausschließt.

Systemanforderungen: Wichtig sind auch die von der Firewall geforderte Prozessorleistung sowie der benötigte Platz auf Festplatte.

So ist Ihr Rechner geschützt

Firewalls im Test



Fünf kostenlose Firewalls mussten in unserem Härtetest zeigen, ob sie einen Rechner wirklich schützen. Hier erfahren Sie die Ergebnisse – und wie Sie Ihren PC am besten gegen aktuelle Bedrohungen absichern.

Von **Arne Arnold**

Der Virus auf Ihrem Rechner verschickt heimlich Spam mit Werbung für Viagra, führt Angriffe auf Websites protibetischer Organisationen aus und protokolliert nebenbei alle Ihre Online-Passwörter. Eingefangen haben Sie sich den Schädling auf einer an sich harmlosen Website, die aber von Hackern gekapert wurde. Ihr Antiviren-Tool hat den Schädling nicht gemeldet, da seine Programmierer ihn ganz neu entwickelt hatten und nur 100 Exemplare davon unter die Leute brachten, bevor sie sein Aussehen total veränderten.

Dieses Szenario muss Sie nicht zwangsläufig betreffen, doch es findet täglich tausendfach statt. Dabei ist es recht einfach, so einen Schädling zu stoppen. Und das, nachdem das Antiviren-Programm versagt hat. Sie benötigen dafür eine Firewall. Wir erklären hier, was man von einem solchen Schutzprogramm generell erwarten kann.

„Die Firewall springt ein, wenn das Antiviren-Programm versagt hat“

Und wir berichten detailliert über die Leistungen von aktuellen Firewalls. Dazu mussten fünf kostenlose Tools unter härtesten Bedingungen in einem Test zeigen, was sie können. Wie wir testen, erfahren Sie im Kasten auf Seite 73. Einer Übersicht aller Testergebnisse finden Sie auf Seite 74.

HIER LESEN SIE ...

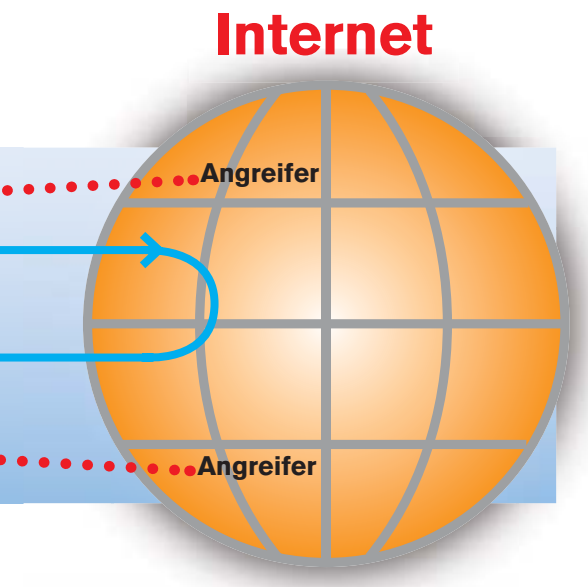
- **wozu** eine Firewall gut ist
- **welche** Firewall für wen die richtige ist
- **wie** Sie das Tool richtig bedienen
- **welche** Vorteile eine Hardware-Firewall hat
- **wie** Sie einen DSL-Router richtig anschließen und konfigurieren

Firewall-Trends

Mehr Angriffe über Websites

Desktop-Firewalls sind Programme, die Sie auf Ihrem PC installieren, um den Rechner gegen Angriffe von außen und auch von innen zu schützen. In den letzten Jahren gab es zwar kaum Attacken aus dem Internet auf die Online-Türen (Ports) von Privat-PCs. Dafür gibts einen einfachen Grund: Die Angreifer haben schon lange keinen Fehler mehr in Windows gefunden, der den Rechner ohne Interaktion des Anwenders angreifbar macht.

Stattdessen finden Kriminelle aber haufenweise Sicherheitslücken in Internet Ex-



CHECKLISTE FIREWALLS Das müssen Sie beachten

Mit diesen Tipps machen Sie Ihren PC in wenigen Minuten sicher vor Angriffen aus dem Internet und hindern unbekannte Viren daran, Daten ins Web zu senden.

✔ **Minimalanforderung**
Prüfen Sie, ob wenigstens die Windows Firewall aktiv ist („Systemsteuerung, Sicherheit, Windows-Firewall"). Sie ist besser als ihr Ruf, denn sie schützt zumindest vor Angriffen von außen. Gegen unbekannte Viren und andere Schädlinge richtet sie aber nichts aus.

✔ **Virencheck zuerst**
Bevor Sie eine Desktop-Firewall einrichten, sollten Sie mit einem Virenscanner und einem Online-Virenscanner – etwa *www.infected ornot.com* – den PC komplett durchsuchen lassen. So können Sie nach der Installation mit gutem Gefühl vorhandenen Programmen in der Firewall Online-Zugriff gewähren. Meist müssen Sie am Anfang sehr viele Regeln erstellen.

✔ **Es kann nur eine geben**
Installieren Sie niemals zwei Desktop-Firewalls auf einem System. Die Tools klinken sich mit eigenen Netzwerktreibern in den Datenverkehr ein. Wenn das zwei Tools machen, gibt's oft Probleme.

✔ **Nur mit Updates**
Auch für Desktop-Firewalls gibt's regelmäßig Updates, die Sie unbedingt einspielen sollten. **Achtung:** Oft ändert sich die Versionsnummer nicht, sondern nur die Build-Nummer. Das ist auf der Website des Herstellers meist nicht ersichtlich. Nutzen Sie also am besten die Update-Funktion der Firewall.

✔ **In die Karten gucken**
Machen Sie sich mit dem Regelwerk der Firewall vertraut. Denn wenn mal eine Online-Anwendung nicht richtig funktioniert, kann das an einem Verbot in den Firewall-Regeln liegen, die Sie dann korrigieren müssen.

plorer, Firefox und anderen Anwendungen, über die sie sehr einfach einen PC verseuchen können. Entsprechend verbreiten die Angreifer ihren Schadcode hauptsächlich über Websites.

Firewalls schützen nicht gegen die Browser-Lücken – doch sie sind deswegen keineswegs überflüssig geworden. Erstens gibt es etliche andere Anwendungen, die einen PC von außen angreifbar machen. Zweitens benutzt man sinnvollerweise den Sicherheitsgurt im Auto auch dann, wenn man ein paar Jahre lang keinen Unfall hatte.

Firewalls werden immer wichtiger

Die Desktop-Firewall kontrolliert außerdem jedes Programm, das online gehen will. Sie meldet den Prozess dem Anwender. Der muss dann ausdrücklich erlauben, dass das Programm mit dem Internet Kontakt aufnimmt (Anwendungsfilter). Damit ist die Firewall das letzte Bollwerk: Sollte sich ein Schädling oder ein Spionageprogramm am Antiviren-Tool vorbeigeschmuggelt haben, werden Sie darauf aufmerksam, sobald der Code online gehen will. Da es immer öfter Viren und andere Schädlinge gibt, die von Antiviren-Programmen erst mal nicht gemeldet werden, gewinnt die Firewall immens an Bedeutung.

Pro-Versionen lohnen sich kaum

Im Test haben wir fünf kostenlose Firewalls. Jede davon gibt es auch in einer Pro-Version zu kaufen. Dafür bekommt man mehr Funktionen und meist besseren Support. Die zusätzlichen Funktionen sind bei den meisten Firewalls ganz nett, aber unserer Meinung nach nicht ihr Geld wert. Eine Ausnahme ist hier Zone Alarm, das in der Pro-Version automatisch Regeln für die meisten Anwendungen erstellt. So wird die Entscheidung, ob eine Anwendung online ›

PC-WELT-EMPFEHLUNG

Unser Testsieger ist Zone Alarm Free. Das Tool zeigte Top-Ergebnisse bei den Sicherheitstests. Fortgeschrittene Anwender können es schnell richtig bedienen.

Auf Platz 2 landet die englischsprachige Software **Comodo Firewall Pro**. Sie bietet umfassende Sicherheitsfunktionen, ist aber äußerst komplex in der Bedienung. Wir empfehlen diese Firewall wirklich nur Profis.

Im Test hatten wir auch die beliebte **Fritzbox 7270** in ihrer Eigenschaft als Firewall. Sie lief außer Konkurrenz, hat aber deutlich gezeigt, dass ein DSL-Router sehr guten Schutz vor Angriffen aus dem Internet bietet.

Platz 1: Zone Alarm Firewall Free bringt Top-Sicherheit

Platz 2: Comodo Firewall Pro ist für Profis eine interessante Alternative

Tipp: Die Fritzbox als DSL-Router bietet einen hervorragenden Außenschutz - andere DSL-Router übrigens auch

gehen darf, nicht dem Anwender überlassen, sondern die Sicherheits-Software übernimmt sie selbst.

Generell lohnt sich die Anschaffung einer kostenpflichtigen Firewall nicht. Der Grund: Eine Firewall sollte gut mit den anderen Sicherheits-Tools zusammenarbeiten, etwa dem Antiviren-Programm. Darum ist es sinnvoll – wenn man Geld für Sicherheits-Software ausgeben möchte –, in eine komplette Suite zu investieren und nicht in die Pro-Version einer Firewall. Suiten gibts von G-Data, Kaspersky, Symantec und vielen anderen. Eine Liste von Sicherheitspaketen finden Sie unter *www.pcwelt.de/avh*.

Vorteile eines DSL-Routers

Wer bei einem Internet-Provider einen Vertrag für einen DSL-Anschluss abschließt, erhält oft einen DSL-Router kostenlos dazu. Diese Geräte bieten für Ihren PC einen sehr guten Schutz gegen Angriffe aus dem Internet. Denn Ihr Rechner befindet sich vom Internet aus gesehen hinter dem Router – er ist somit für einen Angreifer nicht sichtbar und nicht direkt ansprechbar. Der PC besitzt keine öffentliche IP-Adresse, er ist nicht Teil des Internets. Die für die Kommunikation unabdingbare IP-Adresse hat sich der DSL-Router geben lassen. Datenpakete leitet jeweils der Router an den PC beziehungsweise ins Internet weiter. Und standardmäßig gibt er dabei nur die jeweils vom PC angefragten Daten weiter.

Nachteile eines DSL-Routers

Wer den DSL-Router als alleinige Firewall nutzen will, hat ein Problem. Denn er muss im Router nicht nur den eingehenden Datenverkehr filtern lassen, sondern auch den ausgehenden. Für Browser und Mailprogramm sind die nötigen Einstellungen (offene Ports) zwar meist schon werkseitig beim Routerhersteller vorgenommen, doch für jede weitere Anwendung müssten Sie manuell Ports im Router öffnen. Das ist äußerst unkomfortabel. Darum erlauben etliche Router den kompletten ausgehenden Datenverkehr – ohne Filterung. Das ist auch bei der beliebten Fritzbox der Fall. Es empfiehlt sich somit die Kombination aus DSL-Router und Desktop-Firewall. Der Router blockt Angriffe aus dem Internet, die Firewall meldet Programme, die vom PC aus Daten ins Internet senden wollen.

„Wer ein Sicherheits-Tool kaufen will, sollte zu einer kompletten Suite greifen“

Testergebnisse

Die PC-WELT hat fünf kostenlose Desktop-Firewalls unter die Lupe genommen. Außerdem haben wir den beliebten DSL-Router Fritzbox 7270 mitgetestet. Wir wollten wissen, ob Anwender mit einem solchen Gerät auf eine Desktop-Firewall verzichten können.

Der Test hat gezeigt, dass alle Firewalls beim Außenschutz gut sind. Sie blocken gefährliche Datenpakete aus dem Internet zuverlässig ab. Unterschiedlich agieren die Firewalls beim **Blockieren von Anfragen aus dem lokalen Netzwerk**. Ashampoo Firewall Free und Vista Firewall Control erlauben standardmäßig den Zugriff auf freigegebene Ordner. Uns gefällt aber die Strategie der anderen Tools besser, die nach ihrer Installation den Zugriff auf freigegebene Ordner erst einmal unterbinden.

Innenschutz

Schwächen fanden wir beim Selbstschutz-Test. Dabei versuchten wir, die Firewall zu deaktivieren und zu löschen. Beides müssen

KURZANLEITUNG DSL-Router in 5 Minuten anschließen

Ein DSL-Router bietet viele Vorteile: Er schützt gegen Angriffe aus dem Internet, verwaltet die DSL-Einwahl und verbindet weitere Geräte mit dem PC. Hier erfahren Sie, wie Sie einen DSL-Router richtig anschließen.

1. DSL-Router verkabeln

Die meisten DSL-Router bieten viele Anschlussmöglichkeiten. Hier zeigen wir die absolut nötigen Schritte. Über die „DSL“- oder „WAN“-Schnittstelle verbinden Sie das Gerät mit Ihrer DSL-Buchse. Darüber läuft der Kontakt nach außen ins Internet – meist zeigt ein LED-Lämpchen an, dass die Verbindung steht. Die „LAN“-Buchsen des Routers dienen zum Anschluss des PCs über ein Netzwerkkabel. Für beide Verbindungen sollten dem Gerät Kabel beiliegen. Verwechseln Sie die Kabel nicht! Denken Sie auch an das Stromkabel für den Router.

2. Kontakt zum Router herstellen

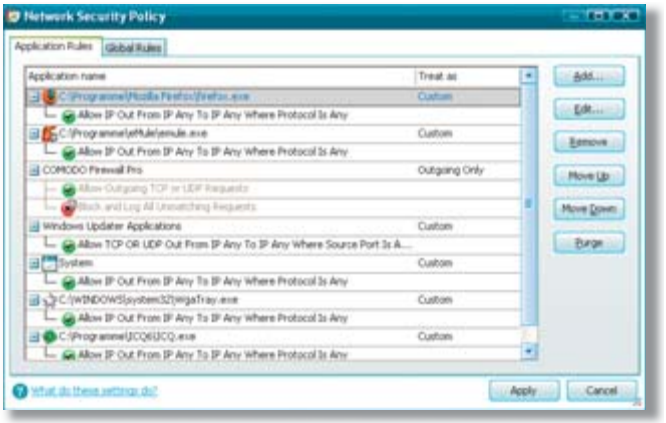
Windows XP und Vista sind standardmäßig so konfiguriert, dass sich der PC per DHCP (Dynamic Host Configuration Protocol) automatisch eine IP-Adresse zuweisen lässt. Die Konfiguration des DSL-Routers erfolgt über einen Webbrowser. Sie geben die Adresse des DSL-Routers in die Adressleiste des Browsers ein. Oft verbringt man beim Anschluss eines DSL-Routers eine Menge Zeit mit dem Suchen nach der richtigen Adresse. Im Idealfall steht sie groß in der Anleitung zum Gerät. Bei der Fritzbox heißt sie etwa *http://fritz.box*, gängig ist zudem *http://192.168.0.1*.

Nun fehlt noch der Log-in, denn aus Gründen der Sicherheit sind die meisten DSL-Router passwortgeschützt. In der Werkseinstellung erfragen viele Router nur einen Standard-Benutzernamen und ein Passwort wie „admin“ oder „supervisor“. Beides steht in der Installationsanleitung des jeweiligen Routers. Später sollten Sie das vorgegebene Passwort ändern.

3. DSL-Anschluss konfigurieren

Im Router-Menü geben Sie nun noch die Log-in-Daten fürs Internet ein, die Sie von Ihrem DSL-Provider erhalten haben. In der Regel steht Ihnen dafür ein Einrichtungsassistent zur Seite.

DSL-Anschluss konfigurieren: Per Assistent führt Sie der Router durch Konfiguration und Einrichtung Ihres DSL-Anschlusses (Schritt 3)



Nix für Anfänger: Das Regelwerk einer Firewall ist zwar kein Hexenwerk, doch für die richtige Konfiguration benötigt man schon einige Kenntnisse

die Tools verhindern, da etliche **Viren das Schutzprogramm so außer Gefecht zu setzen versuchen**. Ashampoo Firewall Free, Vista Firewall Control und Fritz DSL-Protect – die der Fritzbox beigefügte Desktop-Firewall – bestanden diesen Test nicht. Dementsprechend verdienen diese Tools keine Empfehlung.

Schwach schnitten fast alle Produkte bei einem weiteren Sicherheitstest ab: Sie ließen **Programme mit gestohlenen Online-Rechten** passieren. Bei dem Test hat ein Anwender einer Anwendung, zum Beispiel einem FTP-Client, per Firewall-Regel erlaubt, online zu gehen. Nun überschreibt ein Schadcode gleichnamig die EXE-Datei der FTP-Clients und versucht, mit dem Internet Kontakt aufzunehmen. Eine Firewall, die sich lediglich den Dateinamen und den Speicherort einer Anwendung in ihrer Regelliste gemerkt hat, wird den Schadcode nicht aufhalten können. Nur Sicherheits-Tools, die einen Fingerabdruck der Datei genommen haben, etwa einen Hash-Wert, erkennen den Trick. Erschreckend: Nur Zone Alarm und Fritz DSL-Protect haben diesen Test bestanden. Alle anderen Tools versagten.

Bedienung

Kostenlose Desktop-Firewalls sind nach wie vor anspruchsvolle Tools, die den Anwender immer wieder vor Herausforderungen stellen. Für absolute Einsteiger sind diese Firewalls nichts. Ein Beispiel für schwierige Bedienung liefert sogar unser Testsieger Zone Alarm Free. Lädt man das Tool herunter und startet unter Vista die Installation in einem eingeschränkten Benutzerkonto, kommt erwartungsgemäß die Aufforderung, ein Admin-Passwort einzugeben. Tippt man dieses ein, bricht die Installation mit einer banalen Fehlermeldung ab. Lösen lässt sich das Problem, indem man das Tool unter einem Administratorkonto installiert.

Hat man solche Hürden der Installation genommen, wollen die kostenlosen Firewalls vom Anwender wissen, welche EXE-Dateien online gehen dürfen und welche nicht. Erfahrene Anwender haben eine gute Chance, hier die richtigen Entscheidungen zu treffen, Einsteiger dagegen kaum.

Gewinner und Verlierer

Auf den ersten Platz in unserem Firewall-Vergleichstest schafft es wieder das bekannte **Zone Alarm Free**. Das Programm zeigte die beste Sicherheitsleistung, und die Bedienerführung ist in Ordnung.

Auf den zweiten Platz kommt **Comodo Firewall Pro**. Bei den Sicherheitstests war das Tool in einem Fall schlechter als Zone Alarm. Die Konfiguration der Firewall ist kompliziert, da sie sehr viele Einstellmöglichkeiten bietet. Und: Comodo Firewall gibt's nur englischsprachig, was die Bedienung für viele Anwender noch erschwert. Auf der anderen Seite bietet Comodo tiefgreifende Schutzfunktionen. So überwacht das Tool auch die Registry und meldet verdächtige Änderungen. Comodo empfiehlt sich also für Profis, die eine kostenlose Firewall mit vielen Einstellmöglichkeiten suchen. Einsteigern raten wir von diesem Tool ab.

Den dritten Platz erringt die **Sunbelt Personal Firewall Free**. Anders als in der Vorversion besteht sie nun auch die Tests beim Selbstschutz. Anwender, die Sunbelt 4.5 oder älter bereits einsetzen, sollten unbedingt auf Version 4.6 aktualisieren.

Auf Platz vier und fünf landen **Vista Firewall Control** und **Ashampoo Firewall Free**. Beide hatten Schwächen im Sicherheitstest. ›

Platz 1

Beliebt und bewährt: Zone Alarm überzeugte bei den Sicherheitstests

Zone Alarm: Der Testsieger

Der Klassiker unter den kostenlosen Firewalls – **Zone Alarm Free** – hat es wieder auf den ersten Platz geschafft. Das liegt allerdings nicht daran, dass Zone Alarm ein exorbitant gutes Tool ist, sondern viel mehr daran, dass alle anderen Gratis-Firewalls schlechter abschneiden. Die Bedienung von Zone Alarm ist zumindest für fortgeschrittene Anwender kein großes Problem.

Sicherheit: Zone Alarm hat alle Tests ohne Probleme bestanden.

Tipp: Zone Alarm lässt sich für die ersten vier Wochen als Pro-Version nutzen. Das Angebot sollten Sie annehmen (bei der Installation) – denn dann erstellt die Firewall fast alle Regeln automatisch.

Fazit: Zone Alarm zeigte bei der Sicherheit eine Top-Leistung und schaffte es damit auf den ersten Platz.

Platz 2

Für Profis: Comodo ist bei der Konfiguration sehr kompliziert

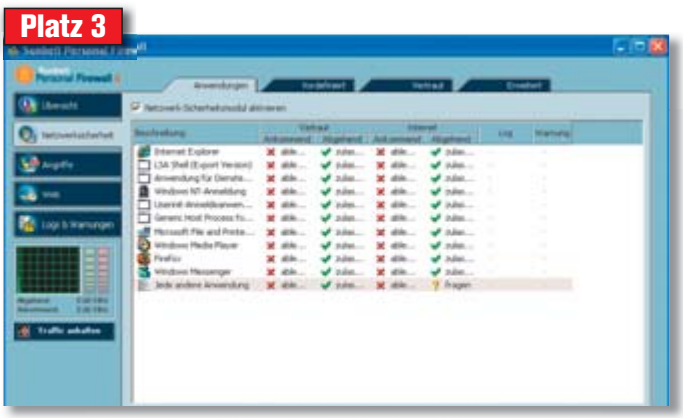
Comodo Firewall Pro: Komplizierte Bedienung

Das englischsprachige Tool **Comodo Firewall Pro** bietet umfangreiche Schutzfunktionen, wie es sie sonst nur bei kostenpflichtigen Firewalls gibt. Das Tool patzte aber bei einem Sicherheitstest und verpasst deshalb eine Spitzennote.

Sicherheit: Comodo hat ein Programm online gehen lassen, das sich das Recht für den Online-Zugriff von einem anderen Tool gestohlen hat. Die weiteren Sicherheitstests bestand das Tool. Sehr gut gefällt uns die Zusatzfunktion Defense. Sie überwacht den PC im Hinblick auf Änderungen am Dateisystem und an der Registry.

Fazit: Comodo bietet Top-Funktionen und eine gute Sicherheitsleistung. Das Tool ist wegen seiner komplizierten Bedienung aber nur für fortgeschrittene Anwender empfehlenswert.

Platz 3



Schlägt sich wacker: Die Firewall von Sunbelt kommt auf den 3. Platz

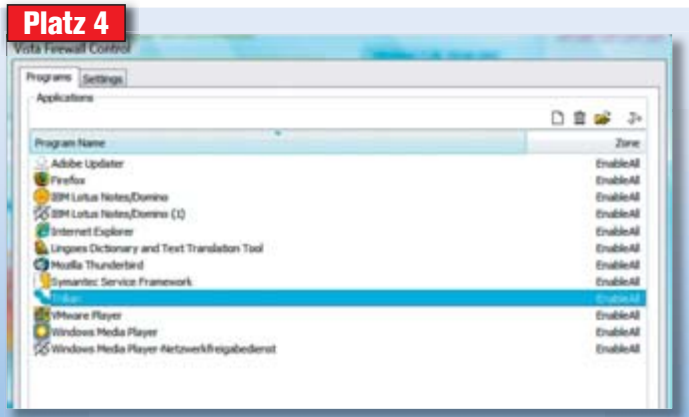
Sunbelt Personal Firewall: Zufriedenstellende Leistung

Die erste Hürde muss man mit der **Sunbelt Personal Firewall** gleich bei der Installation nehmen. Wer hier den voreingestellten „Simple Mode“ belässt, erhält eine Firewall, die jeden Datenverkehr nach draußen zulässt.

Sicherheit: Das Tool bestand die meisten Tests. Gut: Die alte Version 4.5 konnten wir im Selbstschutztest sehr einfach deaktivieren. Hier hat der Hersteller in Version 4.6 nachgebessert. Allerdings blockte die Firewall keine Programme, die mit geklauten Rechten online gingen, und sie stoppte nur 6 der 10 Trojaner.

Fazit: Sunbelt Personal Firewall lieferte bei den Sicherheitstests ein mittelmäßiges bis gutes Ergebnis.

Platz 4



Gute Idee: Das Tool will die Vista-Firewall ergänzen – hat aber Schwächen

Vista Firewall Control: Spartanisch

Das Tool **Vista Firewall Control** ist eine Ergänzung zu der in Windows Vista eingebauten Firewall. Das ist eine gute Idee, da das Bordmittel zuverlässig und ressourcenschonend gegen Angriffe von außen schützt. Den ausgehenden Datenverkehr lässt die Windows-Firewall in der Standardeinstellung ungehindert passieren. Vista Firewall Control will dieses Manko beheben.

Sicherheit: Wir konnten das kleine Utility Vista Firewall Control recht einfach abschießen. Zudem blockte es keine Programme, die das Recht, online zu gehen, geklaut hatten. Die Schwächen beim Schutz im lokalen Netz sind unschön, aber nicht zu arg.

Fazit: Das schlanke Tool Vista Firewall Control passt gut zur Vista-Firewall, hat aber eine Schwäche beim Selbstschutz.

Platz 5

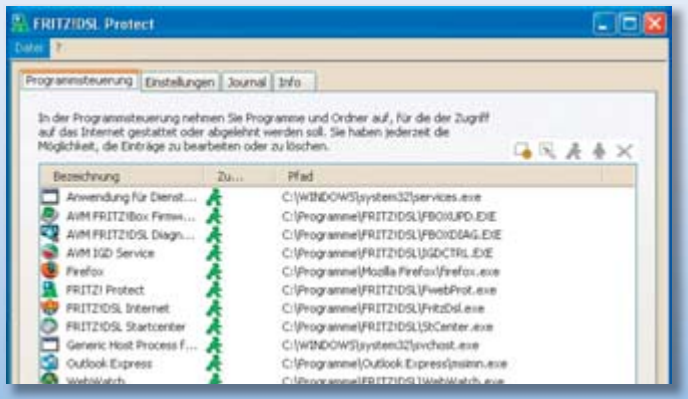
Fehler im System: Ashampoo ließ die Firewall von XP aktiviert

Ashampoo Firewall Free: Verbesserter Schutz

Die Freeware **Ashampoo Firewall Free** muss man spätestens nach 10 Tagen kostenlos per Mailadresse registrieren. Das zog ein Abo für den Ashampoo-Newsletter nach sich.

Sicherheit: Die Ashampoo Firewall ließ die Windows-XP-Firewall aktiviert. Es war dann auch die Windows-Firewall, die den Zugriff auf die aktiven Backdoor-Programme des Testrechners verhinderte (Backdoor-Test I und II). Deaktiviert man die Windows-Firewall – da man glaubt, man habe ja ein neues Tool –, lässt sich der PC über die Backdoors fernsteuern. Auf freigegebene Ordner ließ sich vom internen Netzwerk aus zugreifen.

Fazit: Die Ashampoo Firewall Free bietet zwar eine übersichtliche Bedienerführung, überzeugte aber bei den Sicherheitstests nicht.



Fritzbox mit Fritz-Software: Zum DSL-Router gibt's eine Desktop-Firewall

Fritzbox 7270: Außer Konkurrenz

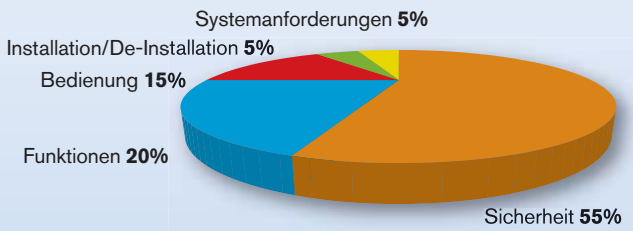
Die Fritzbox lief in diesem Test außer Konkurrenz, da ein DSL-Router systembedingt andere Schutzqualitäten hat.

Sicherheit: Beim Außenschutz dichtete die Fritzbox den PC perfekt gegen Internet-Angriffe ab. Weil die Box in der Standardeinstellung alle Daten vom PC ins Internet durchlässt, kann auch die Kommunikation von Backdoor-Programmen passieren. Die mitgelieferte Firewall Fritz DSL Protect gleicht dies aber voll aus. Das Tool hat zudem einen Vorteil: Gewährt man einer Anwendung Server-Rechte, dem öffnet Fritz DSL Protect den passenden Port auch in der Fritz Box. Schlecht: Das Tool besitzt keinen Selbstschutz.

Fazit: Die Fritzbox bringt einen sehr guten Außenschutz mit. Gegen Angriffe von innen braucht man eine Desktop-Firewall.

DESKTOP-FIREWALLS Wie wir testen

Die PC-WELT prüft Firewalls nach fünf Kriterien und gewichtet für die Endnote so:



Eine Firewall sollte alle Angriffsversuche auf den Rechner verhindern, egal, ob die Angriffe von außen oder von innen kommen.

Beim Außenschutz testen wir mit mehreren Port-Scannern, ob die Datenwege des PCs von außen dicht sind und sich keine für einen Angriff nützlichen Infos, etwa über das Betriebssystem, ermitteln lassen. Danach führen wir auf die PCs drei DoS-Angiffe (Denial of Service) durch.

Beim Innenschutz muss die Firewall etwa ein Backdoor-Programm, das sich heimlich ins System geschlichen hat, erkennen und seine Kommunikation blockieren (Backdoor-Tests). Auch starten wir 10 Backdoor-Programme, die bereits vor der Installation der Firewall auf dem System waren. Das Sicherheits-Tool muss auch deren Kommunikation mit dem Internet verhindern.

Der Selbstschutz muss Manipulationen an der Regelliste und das Deaktivieren des Tools blockieren. Auch müssen sich die Tools gegen das Löschen ihrer Programmdateien schützen.

Die Tests im Bereich Sicherheit haben für uns die Spezialisten Guido Habicht und Maik Morgenstern von Sicherheitslabor AV-Test (*www.av-test.de*) durchgeführt.

Funktionen

Eine Firewall muss den Nutzer über Programme informieren, die eine Verbindung zum Internet aufzubauen versuchen. Die Anwendungen sollten sich in Listen einordnen lassen, über die man festlegt, ob die Programme online gehen dürfen oder nicht. Assistenten sollten mit einfachen Erklärungen helfen, die richtige Entscheidung zu treffen.

Bedienung

Als Sicherheits-Software greift eine Firewall tief in das System ein. Aus diesem Grund ist es unverzichtbar, dass sie eine klare Benutzerführung bietet, die Fehler bei der Nutzung oder Konfiguration ausschließt. Deshalb sollten alle Meldungen, Bezeichnungen und Beschreibungen auch für weniger erfahrene Anwender verständlich sein. Die Programme sollten aber nur wichtige Ereignisse anzeigen und den Anwender nicht mit überflüssigen Meldungen nerven.

Installation/De-Installation

Neben der einfachen Installation, die mit wenigen Abfragen auskommen sollte, spielt auch die De-Installation eine Rolle. Das Programm sollte sich restlos vom System entfernen lassen, inklusive aller durch die Software angelegten Registry-Schlüssel.

Systemanforderungen

Viele Programme entpuppen sich beim Einsatz als wahre Speicherfresser. Wichtige Punkte sind auch die geforderte Prozessorleistung sowie der benötigte Festplattenplatz.

›

FÜNF DESKTOP-FIREWALLS IM ÜBERBLICK Die Testergebnisse

PRODUKT	Zone Alarm Firewall 7.0 Free	Comodo Firewall Pro 3.0	Sunbelt Personal Firewall 4.6 Free	Vista Firewall Control 2.0	Ashampoo Firewall Free 1.2	Fritzbox 7270 / Fritz DSL Protect 2.04 (Desktop-Firewall)
Anbieter	Check Point	Comodo	Sunbelt Software	Sphinx Software	Ashampoo	AVM
Internet	*http://zonealarm.com*	*http://comodo.com*	*http://sunbelt-software.com*	*www.sphinx-soft.com*	*http://ashampoo.com*	*www.avm.de*
Preis	gratis	gratis	gratis	gratis	gratis	175 Euro / gratis
Platzierung	1	2	3	4	5	außer Konkurrenz
Gesamtnote	●●●●○	●●●●○	●●●◐○	●●●◐○	●●●◐○	außer Konkurrenz
BEWERTUNG						
Sicherheit (55%)	90	85	80	80	75	90
Funktionen (20%)	85	90	85	75	85	85
Bedienung (15%)	85	80	85	90	85	80
Installation / De-Installation (5%)	85	85	85	85	85	85
Systemanforderungen (5%)	90	90	90	85	85	90
TECHNISCHE DATEN / FUNKTIONEN						
Windows	2000, XP, Vista	XP, Vista	2000, XP, Vista	Vista	2000, XP	n.a. / XP, Vista
Sprache	Deutsch	Englisch	Deutsch	Englisch	Deutsch	Deutsch
Plattenplatz	36 MB	65 MB	16 MB	2 MB	13 MB	n.a. / 14 MB
Anwendungsfilter	ja	ja	ja	ja	ja	nein / ja
hat Regeln für System-Programme	ja	ja	ja	ja	ja	n.a. / nein
erstellt automatisch Regeln	nein	teilweise	nein	nein	nein	n.a. / nein
detailliertes Protokoll	ja	ja	ja	ja	ja	ja / ja
Warnungen per Pop-up	ja	ja	ja	ja	ja	n.a. / ja
automatisches Internet-Update	ja	ja	ja	nein	ja	nein / nein
Filter für Mailanhänge	ja	nein	nein	nein	nein	nein / nein
Hinweis auf Windows-Updates	nein	nein	nein	nein	nein	n.a. / nein
Innenschutz						
Selbstschutz: Verhindert die Deaktivierung der Firewall	ja	ja	ja	nein	ja	n.a. / nein
Selbstschutz: Verhindert das Löschen der Firewall	ja	ja	ja	ja	nein	n.a. / nein
blockt Programme mit geklauten Rechten ab	ja	nein	nein	nein	nein	n.a. / ja
Backdoor-Test I	ja	ja	ja	ja	ja (durch die Windows Firewall, die aktiv bleibt)	n.a. / ja
Backdoor-Test II	ja	ja	ja	ja	ja (durch die Windows Firewall, die aktiv bleibt)	n.a. / ja
blockiert aktive Trojaner (xx von 10)	10	10	6	10	10	0 / 10
Außenschutz						
blockt Portscans ab	ja	ja	ja	ja	ja	ja[1] / n.a.
blockt Stealth-Portscans ab	ja	ja	ja	ja	ja	ja[1] / n.a.
Betriebssystem nicht ermittelbar	ja	ja	ja	ja	ja	ja[1] / n.a.
blockt Zugriffe auf freigegebene Ordner	ja	ja	ja	nein	nein	n.a. / ja
blockiert Nachrichten an den Windows-Nachrichtendienst	ja	ja	ja	n.a.	nein	n.a. / ja
wehrt DoS-Angriffe ab	ja	ja	ja	ja	ja	ja / n.a.

Wir testen in Zusammenarbeit mit AV-Test (www.av-test.org) n.a.= nicht anwendbar [1] Ein Port der Fritzbox war offen, was für den PC aber keine Gefahr darstellte.