AVG Whitepaper

Göttingen, den 28. Juni 2005

AVG Anti-Virus plus Firewall

Firewall? Was ist das?

Wer seinen PC mit dem Internet verbindet, öffnet damit ein virtuelles Tor zur großen weiten Welt. Was vielen nicht bewusst ist: Durch dieses Tor kommt nicht nur der Benutzer hinaus, sondern auch Fremde herein. Der PC steht plötzlich nicht mehr in eher sicheren Städten wie Berlin, München, Göttingen oder Wuppertal - er steht mitten in den kriminellen Orten dieser Welt. Orte, die man besser nicht betreten sollte. Im Internet gibt es keine abgegrenzten Orte. Im Internet sind die Kriminellen überall.

Wer heute ins Internet geht, kann davon ausgehen, dass er innerhalb der ersten halben Stunde angegriffen wird. Ich habe gerade mal in den Log-Dateien meiner Firewall nachgeschaut: Heute kam der erste Angriff nach vier Minuten.

Wer seinen PC mit dem Internet verbindet, öffnet damit eine Tür, durch die ständig Daten hin und her wandern. Der Benutzer schickt eine Web-Adresse hinaus ins Netz und erhält im Gegenzug eine Internet-Seite. Das Dumme daran ist, dass die eigentlichen Bytes unsichtbar sind. Man bekommt nur den Teil zu sehen, den der Browser auf dem Bildschirm darstellt. Was sonst noch an Daten durch die Internet-Leitung wuselt, bekommt man gar nicht mit - und das kann eine ganze Menge sein.

Eine Firewall überwacht diese Daten und schlägt Alarm, wenn etwas Verdächtiges dabei ist. Und damit sind nicht Viren gemeint, sondern Einbrecher. Um Computerviren kümmert sich das Antivirenprogramm AVG 7. Firewalls wurden ursprünglich entwickelt, um Einbrüche in Computersysteme zu verhindern. Das tun sie auch immer noch, aber Firewalls können heute weit mehr. Das müssen sie auch, denn die Zeiten sind vorbei, als ein paar einsame Hacker bei Cola und Zigaretten im Internet an den virtuellen Türen rüttelten. Heute gehen die Hacker lieber ins Kino und lassen automatisierte Programme die Arbeit machen. Für die Firewall bedeutet die Automatisierung der Hacker, dass es viel mehr Angriffe in immer kürzerer Zeit gibt. Die Firewall findet in den beobachteten Daten immer mehr Verdächtiges.

Aber die Hacker haben nicht nur die Anzahl der Angriffe massiv erhöht. Sie irritieren die Sicherheitsbranche auch damit, dass sie sich nicht mehr an herkömmliche Einteilungen halten. Früher gab es Hacker und Virenautoren, Computerviren, Würmer und Trojaner. Heute gibt es Hacker, die gleichzeitig Virenautoren sind. Und sie schreiben Programme, die gleichzeitig als Virus, Wurm, Einbruchswerkzeug und Trojaner funktionieren. Die alten Einteilungen funktionieren nicht mehr.

Da die Angreifer Viren- und Hackertechniken verbinden, ist es sinnvoll, das auch auf Abwehrseite zu tun. Grisoft hat sich deshalb entschieden, sein bewährtes Antivirenprogramm, AVG 7, um eine Firewall-Komponente zu ergänzen.

Wenn ein Computerwurm durch eine Sicherheitslücke in den PC gelangt ist, so kann das Antivirenprogramm, AVG 7, ihn entdecken - aber eben erst, wenn er drin ist. Die Firewall dagegen kann bereits den Versuch, den PC zu infizieren, abblocken. Das gilt aber nicht für alle Infektionswege. Erst die Kombination von Antivirenprogramm und Firewall schützt den Computer komplett (Wenn auch nicht hundertprozentig, denn hundertprozentige Sicherheit ist leider prinzipiell unmöglich).

Ein Beispiel

Nehmen wir an, ein Hacker will Ihren PC infizieren. Natürlich nicht nur Ihren, sondern möglichst viele. Er will die Computer fernsteuern, um damit Spam zu verschicken, Passwörter zu knacken oder dergleichen.
Er schreibt also einen Trojaner, der sich per eMail-Anhang verschickt, sich auf vielen PCs installiert und dann wieder Kontakt zu seinem Schöpfer aufnimmt, um auf Befehle zu warten.

Wenn der Benutzer den eMail-Anhang mit dem brandneuen Trojaner ausführt, dann wird dieser installiert. Als eMail-Anhang ist der Trojaner PC ganz legal in den PC gelangt. Die Firewall kann nur schützen, wenn

ein Programm versucht, auf illegale Weise in den PC zu kommen. Und das Antivirenprogramm hat in diesem Beispiel versagt, weil der Trojaner zu neu war - es kannte ihn noch nicht.

Der PC ist nun infiziert. Trotzdem hat der Angreifer sein Ziel nicht erreicht. Der Trojaner hat sich auftragsgemäß installiert und wartet auf die Befehle, mit denen der Angreifer den PC fernsteuert und missbraucht. Aber diese Befehle kommen nie an. Denn die Firewall verhindert, dass der Angreifer auf die Hintertür des Trojaners zugreift.

Statt dessen schlägt die Firewall Alarm, weil der Trojaner auf nicht genehmigte Weise versucht, mit dem Internet zu kommunizieren. Weder das Eindringen noch die Installation des Schädlings konnten in diesem Beispiel verhindert werden. Trotzdem wird der vom Angreifer beabsichtigte Schaden abgewendet, weil die Firewall die Fernsteuerung des Rechners unterbindet.

Zudem erfährt der Benutzer durch den Alarm der Firewall, dass da etwas nicht stimmt. Die Grisoft-Firewall zum Beispiel zeigt dann ein Fenster an, in der der Benutzer gefragt wird, ob er die Kommunikation erlauben will oder nicht. Ein Klick auf "Details anzeigen" enthüllt, wo der Trojaner gespeichert ist und wie seine Programmdatei heißt. Der Benutzer kann den Trojaner löschen, der Angriff ist abgewehrt.

Technik

Die Firewall überwacht also die ein- und ausgehenden Daten auf dem PC auf unerwünschte Kommunikation. Wie macht sie das eigentlich?

Wenn Sie eine Internet-Seite sehen wollen, dann geben Sie im Browser deren Adresse ein, zum Beispiel www.grisoft.de. Der Computer schaut im Internet-Adressbuch DNS nach, wo der entsprechende Computer zu finden ist und kontaktiert ihn mit Hilfe einer Zahlenkombination, der IP-Adresse. In diesem Beispiel lautet die IP-Adresse 193.86.103.19. IP-Adressen sind die Hausnummern des Internet. Jeder Computer, der mit dem Internet verbunden ist, hat so eine Adresse. Zusätzlich zu diesen Hausnummern gibt es noch Zimmernummern. Das Zimmer, in dem die Web-Seiten aufbewahrt werden, hat zum Beispiel auf jedem Computer die Nummer 80. Sie können diese Nummer an die Internet-Adresse anhängen: 193.86.103.19:80 oder www.grisoft.de:80. Das ist in dem Fall nicht nötig, weil der Browser ohnehin weiß, dass er Web-Seiten in Zimmer 80 findet. In anderen Fällen kann es aber nötig sein, eine Zimmernummer anzugeben, zum Beispiel wenn ein Server einen Dienst aus Sicherheitsgründen unter einer unüblichen Nummer anbietet.

Die Hausnummern im Internet heißen IP-Adressen, die Zimmernummern heißen Port-Nummern oder kurz Ports. Viele Ports sind Standardprotokollen wie SMTP für Mail oder HTTP für das Web zugeordnet. Jedes Protokoll dient einem bestimmten Zweck und wird von bestimmten Programmen benutzt. Ein eMail-Programm wie Outlook zum Beispiel holt vom POP3-Server unter Port 110 die eMails ab. Weitere Beispiele:

Port	Protokoll	Zweck	Programmbeispiel
7	ICMP	Netzwerkdiagnose	Ping
20,21	FTP	Dateien übertragen	FileZilla
23	Telnet	Fernwartung	Telnet
25	SMTP	Mail-Versand	Outlook
53	DNS	Internet-Adressbuch	Viele Programme
80	HTTP	Webseiten übertragen	Internet Explorer
110	POP3	Mail-Empfang	Outlook
119	NNTP	Online-Foren	Outlook Express

Neben den Standard-Ports gibt es noch jede Menge freie Ports, deren Verwendung nicht normiert ist. Einige davon werden immer von den selben Programmen benutzt, weil das so Sitte ist, andere können ganz beliebig verwendet werden. Die Firewall überwacht nun, auf welche Ports Ihres Computers jemand von außen zuzugreifen versucht. Und umgekehrt. Bei Zugriffen von innen nach außen überwacht sie zudem,

welches Programm auf dem PC den Zugriff auslöst. Und dann tut sie etwas sehr einfaches und sinnvolles: Sie fragt nämlich den Benutzer, ob er diesen Internet-Zugriff will oder nicht.

Das ist eine einfache aber wirksame Filtertechnik. Wenn es einem Angreifer gelungen sein sollte, ein Fernsteuerungsprogramm auf Ihrem PC zu installieren, dann muss er anschließend den Kontakt herstellen. Egal, wie herum er es versucht, die Firewall wird es bemerken.

- Der Hacker kann versuchen, von außen zuzugreifen - er wird abgeblockt und der Angriff gemeldet.
- Oder sein Trojaner versucht, sich bei Herrchen zu melden - das Ergebnis ist dasselbe.

Viele Trojaner kommunizieren nicht auf Standard-Ports sondern auf freien Portnummern. Andere versuchen sich zu tarnen, indem sie Standard-Ports zweckentfremden. Eine personal Firewall erkennt beides. Die freie Portnummer wird blockiert, weil sie überhaupt nicht benutzt werden sollte. Und der Trojaner-Zugriff auf den Standard-Port wird verhindert, weil der Trojaner nicht zu den Programmen gehört, denen der Zugriff darauf erlaubt ist.

Auf diese Weise lässt sich die Verbreitung der meisten aktuellen Viren und Würmer unterbinden. Denn die meisten versenden sich selbst per eMail und greifen dabei mit einem eigenen Programmmodul auf den SMTP-Port Nr 25 für den eMail-Versand zu. Das erlaubt die Firewall aber nur Outlook (oder dem Mailprogramm, das der Benutzer eingestellt hat). Allein diese einfache Maßnahme könnte die Virenflut im Internet um mindestens die Hälfte eindämmen.

Ports sperren

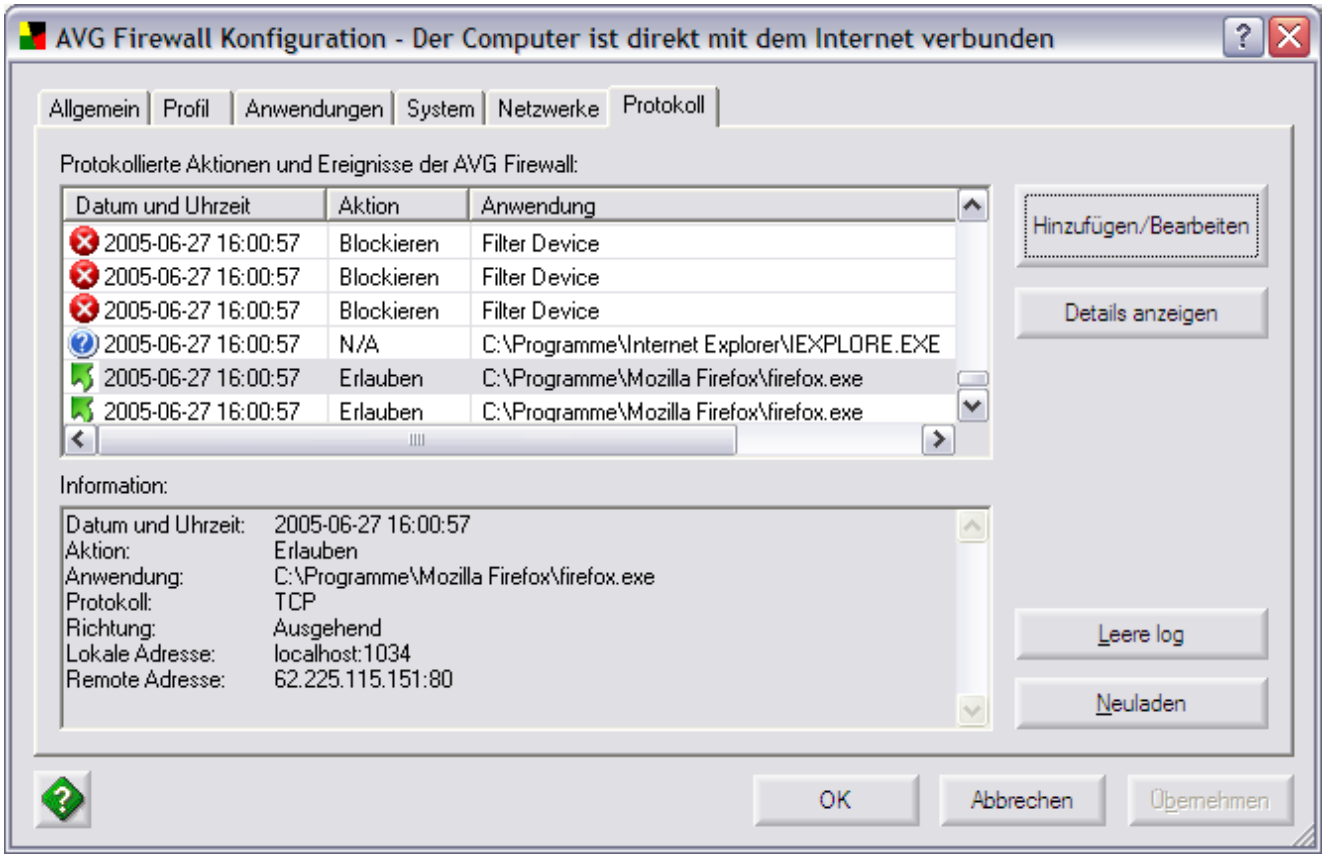
Statt ein aufwändiges Filterprogramm laufen zu lassen, könnte man statt dessen Ports einfach für jeden Zugriff sperren. Das wäre aber nur für Ports sinnvoll, die nie benutzt werden. Da man aber mit dem Internet arbeiten will, muss man die Ports, die man dafür braucht, freigeben. Und die Firewall kontrolliert, dass nur die Programme zugreifen, die das auch dürfen.

Firewall-Modi

Wie sicher eine Firewall ist, hängt sehr von ihrer Konfiguration ab. Professionelle Firewalls werden von Spezialisten anhand komplizierter Regeln konfiguriert. Die Personal Firewalls machen es den Benutzern leichter. Sie werden mit einer restriktiven Voreinstellung ausgeliefert, in der bis auf wenige Standard-Anwendungen auf ebenso wenigen Standard-Ports alles gesperrt ist. Im Dialog mit dem Benutzer lernt die Firewall dann nach und nach, welche Arten von Internet-Kommunikation der Benutzer zusätzlich freigeben möchte. Auf diese Weise entsteht Schritt für Schritt ein Regelwerk für den Internet-Verkehr, das genau auf die Bedürfnisse des Benutzers zugeschnitten ist.

In Firmennetzen gibt es typischerweise Fileserver, auf denen Dateien gespeichert werden und Datenbankserver für zentrale Informationen. Die Zugriffe auf diese Ressourcen werden von der Firewall ebenfalls bemerkt und müssen vom Anwender freigeschaltet werden - aber nur einmal.

Zusätzlich gibt es die Möglichkeit, die Firewall ganz abzuschalten. Das kann nötig sein, um größere Downloads zu beenden oder aufwendige Internet-Anwendungen zu nutzen. Die Firewall sollte aber nur im Ausnahmefall komplett deaktiviert werden.



Das Protokoll der Firewall zeigt die Behandlung eingehender und ausgehender Netzwerkzugriffe.

Spyware und Adware

Viele Leute da draußen im Netz versuchen, private Daten auszuspähen um sie zu Geld zu machen. Einige tun das sogar legal, weil sie den Benutzer offiziell darauf hinweisen, dass ein Spionageprogramm installiert wird.

Wie das geht? Ganz einfach. Man spricht nicht von Spionage sondern von Adware. Der Benutzer bekommt als Gegenleistung eine kostenlose Software wie zum Beispiel das eMail-Programm Eudora oder den Video-Codec DivX. Finanziert werden die Gratisprogramme durch Werbung. Und damit die den Benutzer möglichst wenig nervt, wird sie auf seine Bedürfnisse zugeschnitten. Das ist doch nett, oder?

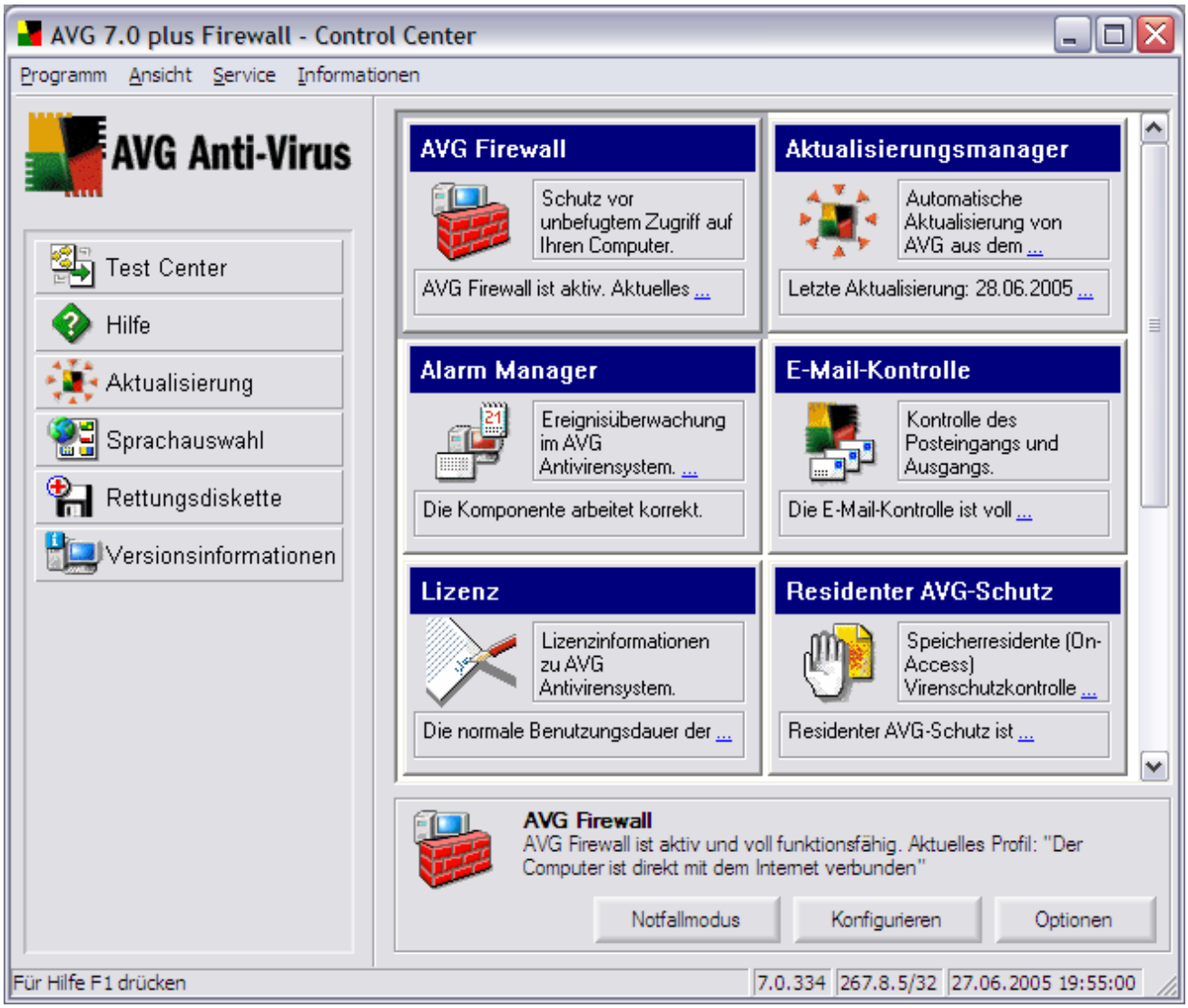
"Wenn schon Werbung, dann wenigstens welche, die mich interessiert", werden viele denken. Die Sache hat nur einen Haken - Sie ahnen es - man muss sich ausspionieren lassen.

Inwieweit Adware mit den deutschen und europäischen Regelungen zum Verbraucher- und Datenschutz kompatibel ist, muss hier außen vor bleiben. Die Grenze zu illegalen Spionageprogrammen ist teilweise fließend. Eindeutig verboten sind jedoch Programme, die sich als Trojaner ohne Wissen des Benutzers installieren.

Aber egal, wie ein Programm rechtlich zu bewerten ist: ohne Firewall kann jedes Spyware-Programm ungefragt Daten ins Internet senden. Mit Firewall bestimmt der Benutzer, welches Programm das darf.

Fazit:

Eine Firewall ist eine notwendige und sinnvolle Ergänzung zum Antivirenprogramm, AVG 7. Zusammen bieten beide wesentlich mehr Schutz, es werden mehr unterschiedliche Angriffe unterbunden. Zusätzliche Sicherheitsmaßnahmen wie Updates und Datensicherungen sind aber außerdem nötig. Und absolute Sicherheit gibt es leider trotz allem nicht.



Control-Center von AVG Anti-Virus plus Firewall

Redakteur: **Harald Schlüter; www.drs13.de**
Autor: **Achim Wagenknecht**