

Die kostenlose Ashampoo Firewall 1.10 auf dem Prüfstand

Kategorie : software

Veröffentlicht von [Chefkoch](#) am 27.10.2006

"Der Ashampoo a-Man hat wieder zugeschlagen" steht auf der Internetseite von Ashampoo und damit wurde die kostenlose Firewall in den Medien kräftig beworben. Auch wir haben darüber berichtet.

"JEDER PC auf dieser Welt soll sicher sein" steht da und wir wollten wissen, ob die Ashampoo Personal Firewall dem gerecht wird. So hat es diese Firewall also in unser Testcenter geschafft und wurde einem zweiwöchigen Praxistest unterzogen.

Ob eine Softwarefirewall nun geeignet ist, einen PC dauerhaft zu schützen, ist häufig genug Grund für endlose Diskussionen. Es gibt Anwendungsfälle, in denen eine Softwarefirewall durchaus Sinn macht. Trotzdem ist die Kritik, dass durch die zusätzliche Software auch zusätzliche Angriffsflächen geschaffen werden, durchaus berechtigt.

An eine Softwarefirewall müssen aus Sicherheitsgründen hohe Anforderungen gestellt werden. Ob die Ashampoo Firewall dem gerecht wird?

Versprochene Eigenschaften

Während der Testphase haben wir uns vorsichtshalber nochmal die versprochenen Produkteigenschaften durchgelesen. Kein Zweifel, steht auf der Internetseite doch: Eine Firewall schützt nicht nur vor Attacken aus dem Internet, sondern schlägt auch Alarm, sobald eines der eigenen Programme heimlich versucht, "nach Hause zu telefonieren" und Daten ins Internet zu senden. [...] Die Ashampoo FireWall tritt an, um die aktive Internet-Verbindung zu überwachen, so dass Viren und Spyware-Programme automatisch ausgebremst werden. So wird auch effektiv verhindert, dass Trojanische Pferde den Rechner in einen Zombie-PC verwandeln, der unbemerkt Millionen Spam-Mails in die ganze Welt versendet.

Der vollständige Text ist auf der [Ashampoo Website](#) nachzulesen.

Um ganz sicher zu gehen, haben wir nochmal einen Blick in die Dokumentation geworfen: "*Erkennt und blockiert Anwendungen welche z.B. durch Virusbefall verändert wurden.*"

Warum wir uns dessen nochmal versichert haben, wird im Verlauf des Testberichtes geklärt werden. Eins steht fest, ein großer Teil der versprochenen Produkteigenschaften werden sicher eingehalten. Aber trotzdem patzt Ashampoo an einer entscheidenden Stelle.

Die Installation

Die Installation ist einfach gehalten und gelingt jedem Anwender auf Anhieb. Für die kostenlose Nutzung erhält man auf der Internetseite den Produktkey, für den man sich in einen Newsverteiler eintragen muss. Während der Testzeit erhielten wir genau eine Mail von Ashampoo. Zudem kann man sich aus dem Newsverteiler wieder austragen.

Nach der Installation arbeitet die Firewall standardmäßig im Lernmodus, bei dem Regeln für Programme, die das Internet ansprechen, erstellt werden können.

Die Dokumentation

Ein Handbuch gibt es nicht, dafür aber eine sehr umfangreiche Hilfe, die das Handbuch durchaus ersetzt und alle wichtigen Fragen beantwortet. Viel mehr braucht man dazu nicht sagen, hier kann Ashampoo deutlich punkten. Hinzu kommt, dass die Oberfläche in der Tat übersichtlich und selbsterklärend ist. Hier wurde nicht zuviel versprochen.

Du kommst hier nicht rein



Kleine Übersicht mit Statistik. Nun wenden wir uns den Aufgaben einer Personal Firewall zu. Dazu gehen wir auch ein bisschen auf die Angriffsarten ein, denen die Firewall standhalten sollte.

Einem direkten Angriff aus dem Internet geht meist ein anderer Prozess voraus. Ein potentieller Angreifer muss wissen, dass Sie online sind und muss dann ermitteln, welche IP-Adresse Ihnen zugewiesen wurde und welche Ports geöffnet sind. Hier wird es spannend, denn damit das Internet funktioniert, müssen Sie natürlich Ihre IP-Adresse nach Außen publik machen. Firewalls müssen hier entscheiden, welche Anfragen aus dem Internet erwünscht sind und welche nicht. Baut Ihr Browser eine Verbindung zu einer Internetseite auf, so ist hier Datenverkehr erwünscht. Versucht ein Angreifer durch wahlloses Pinggen einen (Ihren) PC zu finden, so ist das unerwünscht und die Firewall sollte diesen Ping nicht beantworten.

Auf diese Weise sieht der Angreifer Ihren Rechner nicht im Internet und er kommt auch nicht auf die Idee, an Ihre Tür zu klopfen. Oftmals sind solche Pings aber keine Angriffe, sondern "Keep Alives" z.B. von Filesharingservern. Trotzdem werden Sie als Angriff gewertet und geblockt.

Lange Rede kurzer Sinn: jede Firewall sollte diese Disziplin beherrschen, auch die von Ashampoo. In unseren Tests konnten wir auch nichts Gegenteiliges feststellen. Die erste Hürde hat der Kandidat also schon genommen.

Doch sehen wir der Wahrheit ins Auge, dieser Weg des Angriffs ist veraltet und kann zudem auch durch andere Maßnahmen vermieden werden. So können entweder manuell oder mit einem Tool (z.B. von <http://www.dingens.org/>) alle kritischen Windowsdienste deaktiviert werden. Das Ergebnis ist ähnlich.

Angriffe finden mittlerweile von innen statt, z.B. durch Trojaner die Backdoors (Hintertüren) einrichten. Sie kommunizieren mit dem Internet, laden zusätzlichen Programmcode nach und richten Serverdienste ein, über die Ihr Rechner z.B. für SPAM-Transfer missbraucht werden kann. Die Programmierer von Trojanern suchen unterschiedliche Wege, ihre Schädlinge zu verbreiten. Zwei davon sind derzeit recht aktiv. Sie erhalten eine E-Mail und werden aufgefordert den Dateianhang zu öffnen oder Sie werden dazu verleitet eine präparierte Internetseite zu öffnen. Durch Sicherheitslücken in der Software und im System wird so schadhafter Code (z.B. Trojaner)

eingeschleust. Diese versuchen dann eine Verbindung mit dem Internet aufzubauen.

An dieser Stelle greift eine Personal Firewall ein. Sie überwacht die Prozesse, die mit dem Internet kommunizieren wollen und fragt bei dem Benutzer um Erlaubnis. Damit für Standardanwendungen nicht ständig die Sicherheitsmeldungen bestätigt werden müssen, kann der Benutzer entsprechende Regeln definieren. Auch bei Ashampoo ist das so. Sie können für jedes Programm, das auf das Internet zugreifen möchte Regeln erstellen, die entweder alle Ports zulassen oder nur einige Wenige. Dazu müssen Sie lediglich "Regel anlegen / Nicht mehr nachfragen" bestätigen und die gewünschte Aktion anklicken. Hier verhält sich die Ashampoo Firewall genauso wie viele Andere auch. Trojaner tricksen diese Regeln aus, indem Sie sich auf vorhandene Prozesse aufsetzen. Ein IExplorer ist z.B. auf jedem Windowssystem installiert und die Wahrscheinlichkeit ist groß, dass dieser auch mit dem Internet kommunizieren darf.

Hängen Trojaner eigenen Programmcode an den IExporer an, können diese also mit den gleichen Rechten wie dieser agieren. Um das zu verhindern wird in der Regel von der Firewall beim Anlegen der Regel auch eine CPrüfsumme (Hash) zum Programm angelegt und jedesmal verglichen. Ändert sich dieser Hash, sollte die Firewall den Internetzugang sperren und den Benutzer darauf hinweisen. Wurde zum Beispiel der Browser aktualisiert, so kann der Benutzer dann die Regel erneuern. Ist ein Trojaner Grund für die Hash-Änderung, kann der gewarnte Benutzer nun weitere Schritte einleiten.

Hinweis: Bitte beachten Sie, dass die oben beschriebene Angriffsweise weit verbreitet ist und mittlerweile zur üblichen Praxis geworden ist. Sie ist nicht fiktiv, sondern wird von Virenautoren sogar bevorzugt.

Auch Ashampoo speichert den Hash Wert, patzt aber trotzdem an dieser Stelle. Aufgefallen ist uns dies als erstes beim Upgrade von Firefox 1.5.6 auf die Version 2.0, wobei sich nicht nur die Versionsnummer ändert, sondern auch erheblich der Programmcode. Ashampoo hat nicht gezögert und ihm Zugang gewährt. Für eine Firewall, die verspricht, Trojanern den Zugang in das Internet zu verwehren, gehört es aber sicher zu den Pflichtaufgaben den Benutzer auf solche Änderungen hinzuweisen. Nachfolgende Leaktests haben dieses Verhalten bestätigt und es war problemlos möglich, die Firewall zu durchtunneln. Ein Trojaner hätte hier leichtes Spiel.

Eine weitere Variante des Trojanerangriffs ist das Deaktivieren von Sicherheitssoftware wie Virens Scanner und Personal Firewall. Unsere Möglichkeiten sind hier eingeschränkt. Es ist uns nicht gelungen, den Firewallprozess im laufenden Betrieb zu beenden. Unsere Versuche, die Firewall beim Booten zu löschen oder den Programmstart zu verhindern verliefen zwar erfolgreich, aber der Internetzugang ist dann gesperrt. Unsere Testmöglichkeiten waren damit erschöpft, aber wo ein Wille ist ist auch ein Weg. Das Deaktivieren der Sicherheitssoftware ist der Pferdefuß Ihres Systems und die Programmierer von Trojanern sind darauf spezialisiert, genau das vorzunehmen. Für unseren Test allerdings hat Ashampoo hier erstmal bestanden.

Updates

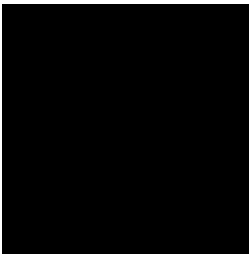
Wie häufig Ashampoo die kostenlose Firewall aktualisieren wird, können wir nicht beurteilen. Sie bietet aber die Möglichkeit, über die Programmoberfläche nach aktuellen Updates zu suchen. Leider lässt sich das nicht automatisieren und dafür kassiert Ashampoo einen weiteren Minuspunkt.

Installation

98%
Updatemöglichkeit
70%
Funktion *
30%
Bedienung
98%
Handbuch/Hilfe
89%

Gesamt
69% * die Funktion haben wir doppelt gewichtet

Fazit



Die Ashampoo Firewall kommt schick daher, leider konnte sie aber die versprochenen Produkteigenschaften nicht einhalten. Fairer Weise muss man sagen, dass die Jagd auf Trojaner eigentlich einer anderen Softwarefamilie zgedacht ist, die Schädlinge bereits im Vorfeld ausschalten sollte.

Aber versprochen ist versprochen. Schlüpft ein Trojaner durch die Maschen des Antivirenprogrammes, so gelingt es ihm ohne Weiteres z.B. Tastaturanschläge, Anwendungsdaten, Screenshots usw. ins Internet zu senden. Von anderen Aktionen einmal ganz abgesehen. Auch andere Softwarefirewalls schneiden bei den Leaktests nicht immer gut ab, bieten aber meist mehr Schutz, als es die Ashampoo Firewall vermochte.

Eine Empfehlung möchten wir für die Ashampoo Firewall nicht abgeben und jeder sollte ganz genau für sich prüfen, ob er sein System ihr anvertraut. (hri)