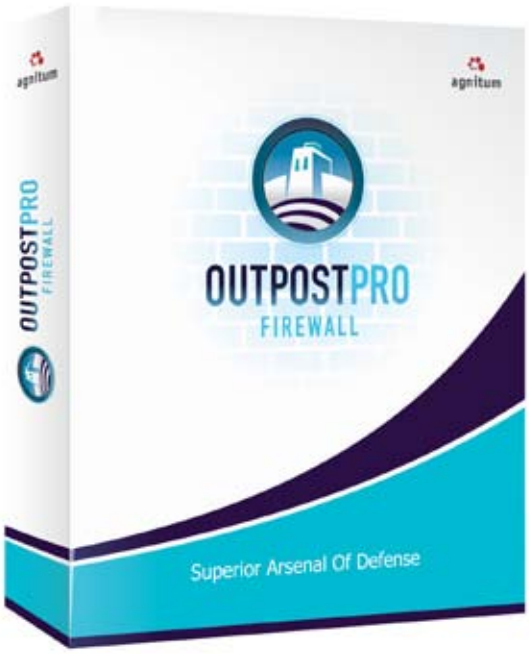
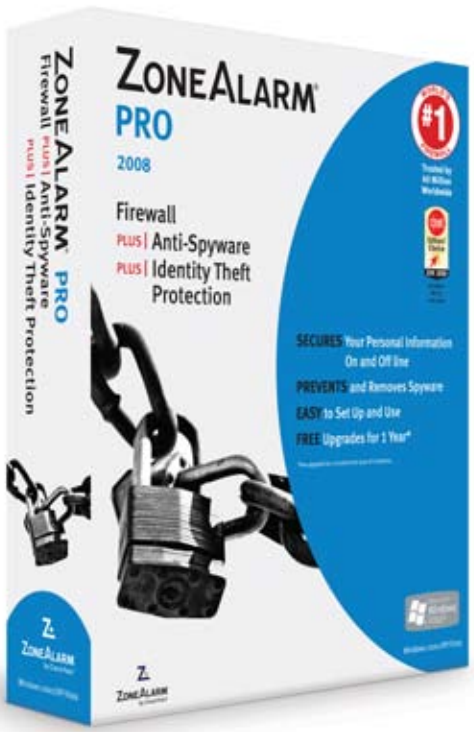
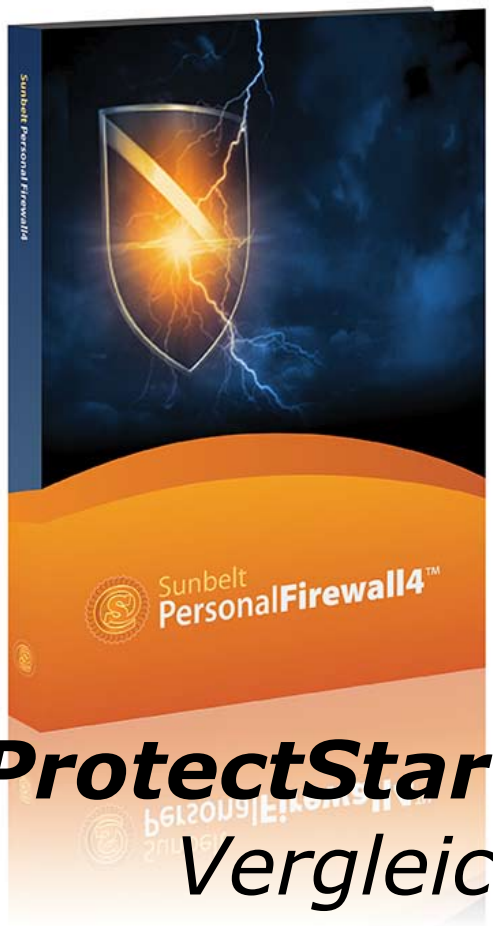






ProtectStar ™ TestLab

Vergleichstest: Personal Firewalls 2008 / 2009

ProtectStar™ TestLab
Vergleichstest - Personal Firewalls 2008 / 2009

INHALTSVERZEICHNIS:

Getestete Produkte und Versionen

Hersteller	Produktname	Release (Version)
Agnitum	Outpost Firewall 2009	6.5.2356.316.0603
CA	CA Personal Firewall 2008	10.0.0.157
Iolo	Personal Firewall	1.5.2
Jetico	Personal Firewall V2	2.0.2.4.2264
Netgate Tech.	Fort Knox Personal Firewall 2008	n/a
Norman	Norman Personal Firewall	n/a
Sunbelt Soft.	Personal Firewall 4 (Full)	4.6.1839.0
ZoneLabs	Zone Alarm Pro	7.1.254.000

n/a = keine Angabe, da im Programm selbst nicht angezeigt

A.) Allgemeine Erläuterung der Testverfahren

Getestet wurde sowohl unter **Labor- als auch realen Bedingungen.** Im Bereich der **SICHERHEIT** lag der Fokus auf dem äußeren und inneren Schutz der Personal Firewalls. Das Hauptaugenmerk waren die werkseitigen Einstellungen, also Auslieferungszustand der jeweiligen Produkte.

„Äußerer Schutz“ bedeutet, dass die Sicherheitsüberprüfung mit einem direkt an das Internet angeschlossenen Rechner (PC / Laptop) erfolgte; z. B. Direktanschluß des PC / Laptops am DSL-Modem (nicht via Router/Hardware-Firewall).

„Innerer Schutz“ bedeutet, die Durchführung von Sicherheitstests der Personal Firewall, wenn der entsprechende Rechner im LAN eingebunden ist. Ein LAN (bspw. Heim- oder Firmennetzwerk) gilt als vertrauenswürdige Zone und wird daher von vielen Personal Firewalls nur mit niedrigeren Sicherheitseinstellungen überwacht. In diesem Bereich soll also analysiert werden, was passieren könnte, wenn ein LAN-Rechner bereits verseucht ist, oder ein Gast-Computer als Hacker-Computer agiert.

Im Bereich der **Benutzerfreundlichkeit** waren es Installation, Deinstallation, Verständlichkeit der Meldungen und die individuellen Einstellungs- und Konfigurationsmöglichkeiten; sowohl während der Installation als auch danach. Weitere Augenmerke lagen auf Handbuch (teilweise im Lieferumfang als gedruckte Version enthalten) und dessen Verständlichkeit, der Onlinehilfe und FAQs.

Im Segment **Performance** standen für die Personal Firewalls eine Vielzahl unterschiedlicher Rechnersysteme zur Verfügung.

Ausstattungsmerkmale der Testrechner von – bis):
Betriebssystem:
Windows XP mit SP 3 und/oder
Windows Vista mit SP1

CPU:
566MHz [Single Core] – 2.400 MHz [Quad-Core] (Durchschnitt: 1.8GHz Dual Core)

Ram:
256–4.096 MB SD-Ram und DDR-Ram (Durchschnitt: 1024 MB DDR-Ram)

Festplatte:
10–1.000 GB, IDE und S-ATA
(Durchschnitt: 120 GB S-ATA Festplatte)

Preis- /Ausstattungs-verhältnis

Wie stehen Preis und Ausstattung einer Personal Firewall zueinander? Also welche zusätzlichen Softwaremodule wie bspw. Anti-Spyware Scanner werden dem Anwender ausgeliefert sowie die Anzahl der enthaltenen Lizenzen. Zudem wurde der Preisunterschied zwischen einer Box- und Downloadversion beim Hersteller gegenüber – sofern verfügbar - dem „Straßenpreis“ am Beispiel des Onlineversandhauses Amazon verglichen.

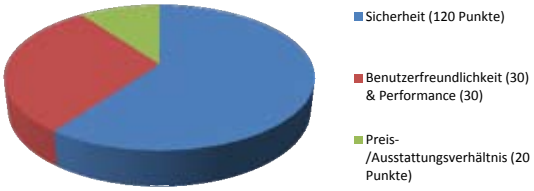
B.) Bewertungskriterien

Bei allen getesteten Personal Firewalls handelt es sich ausschließlich um Sicherheitslösungen, die dem Anwender Schutz vor modernen Gefahren wie Hackerangriffen oder Denial of Service (DoS) Attacken, uvm. versprechen und vor allem auch gewährleisten sollten. Hauptaugenmerk muss daher zwangsläufig auf die enthaltenen Schutzfunktionen der jeweiligen Personal Firewall gelegt werden.

Sowohl die **Benutzerfreundlichkeit** als auch die **Performance** sind neben der Sicherheit vor allem in der Praxis essentiell. Aus diesem Grund sollen sich beide Bereiche zu jeweils gleichen Teilen in der Bewertung widerspiegeln.
Weniger essentiell für die Sicherheit eines Produktes, aber dennoch erwähnenswert ist der Testbereich **Preis-/Ausstattungsverhältnis**. Obwohl es immer weniger reine Personal Firewall Einzelplatzlösungen gibt – das Produkt ist immer weiter verdrängt worden und ist zwischenzeitlich Bestandteil von Internet Security Suite – werden zusätzliche Schutzkomponenten wie beispielsweise Anti-Spywarescanner in die Personal Firewall integriert. Zudem sollte eine moderne Personal Firewall – im Vergleich zu Konkurrenzprodukten - unabhängig von ihrem höheren oder niedrigeren

Verkaufspreis einen **maximalen Schutz** gewährleisten. Hier soll der Anwender zunächst nicht durch zusätzliche Features oder die Zugabe von weiteren Lizenzen zum Kauf maßgeblich beeinflusst werden. Auf der anderen Seite jedoch ergeben sich besondere Preisvorteile für den Anwender.

Aus den genannten Gründen wird sich das Preis-/Ausstattungsverhältnis zu **zehn Prozent** in der Gesamtbewertung wiederfinden. Das ProtectStar™ TestLab hat sich daher zu folgendem Punktesystem aus insgesamt **200 Punkten** als Bewertungsgrundlage entschieden:



Von den insgesamt **200** Punkten ist der größte Teil mit **120** Punkten an den Bereich der **Sicherheit** zu vergeben. Diese 120 Punkte werden so aufgeteilt, dass maximal 60 Punkte für den äußeren Schutz der Firewall zu vergeben sind und 50 Punkte für den inneren Schutz. Weitere 10 Punkte für sonstige Sicherheitsfunktionen wie zum Beispiel die Qualität der Warnmeldungen, Log-Dateien, Intrusion Prevention Systeme, Hostprotection, usw.

Für die beiden Testbereiche **Benutzerfreundlichkeit** und **Performance** können insgesamt **60** Punkte vergeben werden. Jeder Bereich kann dabei maximal **30 Punkte** erhalten. Zuletzt können insgesamt **20** Punkte für den Testbereich **Preis-/ Ausstattungsverhältnis** an die Produkte vergeben werden.

C.) SICHERHEIT DER ÄUSSERE SCHUTZ

Jede durch das ProtectStar™ TestLab bewertete Personal Firewall überwacht **ein- und ausgehende** Verbindungen überwacht. Analysiert wurden die Produkte in erster Linie in den Werkseinstellungen, also in den jeweiligen Konfigurationen des Auslieferungszustandes.Die Personal Firewalls sind – wie bereits in „Allgemeine Erläuterung der Testverfahren“ erwähnt – auf zweierlei Weise analysiert worden: Zum einen der **äußere Schutz** (Angreifer -> Internet -> Testrechner) der Schutzmauer und zum anderen der **innere Schutz** (Angreifer -> LAN -> Testrechner).

Die Firewalls haben in den Durchläufen bezüglich des äußeren Schutzes, alle zum Testzeitpunkt bekannten **15.133** differenten **Angriffs- und Sicherheitstests** erfolgreich bestanden (Stand: August 2008).

Fehlerhaft zeigte sich die **Iolo Personal Firewall**. Eventuell weißt die Software Kompatibilitätsprobleme mit diversen Windows-Netzwerktreibern auf. Getestet wurden die aktuell bekannten **Denial of Service** (DoS)-Angriffsarten, sowie die **Schwachstellen** in Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und Sicherheitschecks.

Zur Anwendung kamen jeweils die verschiedenen Gefahrenstufen (Low, Medium, High) im Bereich der **DoS-Angriffe,** beispielsweise im „Microsoft SMS Client“, „ping of death“, „RPC DCOM Interface DoS“, „MS RPC Services null pointer reference DoS“ und „WinLogon. exe DoS“, uvm.

Aus den Bereichen **Microsoft Bulletins-** und **Windows-Angriffe** gehörten z. B. „Buffer Overrun in Messenger Service (828035)“, „Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)“, „Windows Network Manager Privilege Elevation (Q326886)“, „Checks for MS HOTFIX for snmp buffer overruns“,uvm.
In der **Grundeinstellung** prüften standardisierte Portscans nach geöffneten TCP- und UDP- Ports. Die Scanrange umfasste alle Ports (0 – 65535). Im **zweiten Schritt** wurde die Firewall einem SYN-Portscan (half-open) - dem so genannten Stealth-Scan - unterzogen.

Darüber hinaus waren die Personal Firewalls 33 **speziellen Angriffsvariationen** für **Firewalls** ausgesetzt. Alle Personal Firewalls wehrten die Angriffe **erfolgreich** ab. Im Rahmen der durchgeführten Portscans (tcp-connect und syn/half-open) fanden sich **keine** geöffneten Ports und **keine** unnötigen Dienste, die für gewöhnlich zu Sicherheitsproblemen führen. Sowohl durch die **automatisch** ablaufenden Testreihen des hardwarebasierenden **ProtectStar™ Security-Scanners**, der zusätzlich **10957** (Stand: August 2008) weitere Sicherheitstests und Angriffstaktiken auf die Firewalls ausführte, als auch durch die **manuell** durchgeführten Prüfungen konnten **keine** Schwachstellen oder Sicherheitsrisiken festgestellt werden.

Den **dreistündigen** Dauer-**Penetrationstest** absolvierten alle Personal Firewalls ebenfalls **erfolgreich**, ohne nennenswerte Performanceverluste. Bis auf die **Iolo Personal Firewall**, zeigte **kein** anderes Produkt im Bereich des **äußeren Schutzes** irgendwelche Mängel oder Sicherheitsrisiken. Lediglich die Warnhinweise, Logdateien und Pop-Ups, welche dem Anwender während der Angriffsphase angezeigt werden, könnten bei einigen Produkten wie von CA, Iolo und Netgate Tech. verbessert oder die Angriffe entsprechend ihrer Priorität sortiert werden. Zum Beispiel stellt ein Portscan im eigentlichen Sinn keinen Angriff dar und der Benutzer sollte nur dann über einen Portscan informiert werden, wenn er seine Herkunft aus der vertrauenswürdigen Zone hat.

In dem Bereich der Warnhinweise/ Alarmmeldungen zeigten sich die Personal Firewall von **Agnitum**, **Sunbelt** und **ZoneLabs** bereits in den Werkseinstellungen **vorbildlich**. Besonders lobenswert im Bereich der Konfiguration sind die Personal Firewalls von **Agnitum**, **Jetico**, **Sunbelt** und **ZoneLabs**. Bei diesen Produkten lassen sich größtenteils individuellen Einstellungen bis in das **kleinste Detail** vornehmen. Allerdings sollte der Anwender ausreichend **Erfahrung und Wissen** bezüglich IT-Sicherheit mitbringen, bevor manuell Firewallregeln erstellt oder bestehende modifiziert werden.

Auch die **Norman Personal Firewall** erfüllt nahezu spielend durch einen hilfreichen **Regelassistent** individuelle Wünsche

des Anwenders. Nützlich wäre es, wenn die Personal Firewall künftig **mehr Angriffstechniken** erkennen und dem Benutzer melden würden. Die Mehrheit der analysierten Produkte – bis auf Ausnahme von **Agnitum**, **Sunbelt** und **ZoneLabs** - beschränkte sich in diesem Bereich lediglich auf das Melden von entdeckten Portscans. Spezielle Brute-Force Attacken und DoS-Angriffe sind zwar geblockt

worden, der Anwender erhielt über die Art des Angriffs jedoch keine Meldung; selbst dann wenn dieser Angriff permanent über eine Stunde andauerte. Anwendern wird empfohlen, die Logdateien manuell auf etwaige Ungereimtheiten und Angriffe hin zu überprüfen, da die Firewalls oftmals in den Werkseinstellungen so konfiguriert sind, dass sie wenig Angriffe via Pop-Up melden, wohl aber die Attacken in die Reportdatei (Log) schreiben.

DER INNERE SCHUTZ

Der vorhergehende Test zeigte, dass nahezu alle Personal Firewalls **ausreichend Schutz** gegen Angriffe aus dem Internet – einer nicht sicheren Zone - bieten. Wie sieht es aber aus, wenn ein oder mehrere Computersysteme direkt aus der „vertrauenswürdigen Zone“ – wie zum Beispiel dem Intranet/LAN oder Heim- und Firmen- Netzwerk - angegriffen werden?

In zunehmendem Maße gibt es in den Haushalten mehr und mehr vernetzte Computer. Sei es nun für Spiele der Kinder oder als Home-Office der Eltern. Zudem gewinnt die computergestützte Steuerung der Haustechnik zunehmend an Bedeutung. Die Schutzlösungen werden im Kinderzimmer oftmals ausgeschaltet, da sie die Performance von Onlinespielen beeinträchtigen können. Während dieser Zeitspanne sind die Computer nahezu allen Hackerangriffen, Würmern, Viren und Trojaner schutzlos ausgeliefert und könnten dann ggf. andere Computer im Haushalt „infizieren“.

Außerdem kommt es – sowohl im Home Office als auch im Business Bereich - immer wieder dazu, dass sich ein Gastcomputer mit dem eigenen Netzwerk verbinden möchte. Sei es nur ein Freund oder Bekannter, der bei seinem Besuch beispielsweise nur kurz seine E-Mails abrufen möchte. Was würde geschehen, wenn dieser Gastrechner bereits mit einem Wurm oder Trojaner infiziert wäre? Würden die anderen „geschützten“ Computer im LAN dadurch beeinträchtigt werden? Die Sicherheitsexperten des ProtectStar™ TestLab analysierten daher die Personal Firewalls in deren Werkeinstellungen und verfügbaren Sicherheitskonfigurationen bezüglich der Schutzwirkungen im LAN**.** Getestet wurden die aktuell bekannten DoS-Angriffsarten, sowie bekannte **Schwachstellen** in Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und andere Sicherheitschecks.

Einige Produkte zeigten hier **verschiedene Schwächen**; ganz im Gegensatz zu der sonst guten äußeren Schutzwirkung. Um den zunehmenden Forderungen nach mehr Benutzerfreundlichkeit gerecht zu werden, konfigurieren einige Hersteller ihre Personal Firewalls bereits in den Werkseinstellungen für die vertrauenswürdige(n) Zone(n). Die Computer sind dadurch in der Lage zwischen den Netzwerk-Computern Dateien auszutauschen, gemeinsame Drucker zu verwenden, oder auf freigegebene Order und Dateien zuzugreifen, ohne das der Anwender manuelle Konfigurationen vornehmen muss.

Aus diesem Grund sind bei den Firewalls oftmals die Ports (tcp) **135** (msrpc), **139** (netbios-ssn) und **445** (microsoft-ds) **unzureichend geschützt**.

Diese Eigenschaft weisen vor allem die Lösungen von **Iolo**, **Jetico** und **Norman** auf. Probleme gab es während den Testreihen stets mit **Iolo Personal Firewall**. Es schien, als würde das Produkt schlichtweg keine Attacken im Bereich der Testreihen des inneren Schutzes blockieren, selbst wenn die Konfiguration das interne Netzwerk als nicht-sichere Zone behandeln soll. Die Software selbst zeigte jedoch dem Benutzer an, dass die Firewall eingeschaltet ist, blockierte jedoch keinerlei Angriffe. Ob es sich hier um ein generelles Treiberproblem der Software in Bezug auf bestimmte Netzwerkkarten unter Windows Vista oder es sich um einen generellen Bug handelt ist nicht analysiert worden.

Ausnahmefälle im Bereich der **inneren Schutzwirkung** der Personal Firewalls bilden die Produkte von **CA**, **Jetico** und **ZoneLabs**. Bei diesen Lösungen kann der Anwender jeweils während der Installation oder danach auswählen, ob der PC mit anderen Computern im LAN kommunizieren soll oder nicht. Dementsprechend werden die genannten Ports von der Firewall entweder geschützt oder offen gelassen.

Stets positive Resultate zeigten die beiden Personal Firewalls der Hersteller **Agnitum** und **Sunbelt Software**, da die integrierten **Intrusion Prevention** Schutzmodule bei diesen Firewalls in den Werkseinstellungen besonders auf Angriffe aus der vertrauenswürdigen Zone konfiguriert sind. So werden bei diesen Produkten selbst dann Angriffe erfolgreich blockiert, wenn der Anwender beispielsweise sein Heimnetzwerk als „sichere Zone“ konfiguriert um gemeinsam Dateien und Drucker im Netzwerk zu verwenden.

Die genannten Produkte von **Agnitum, CA, Jetico, Sunbelt** und **ZoneLabs** zeigen sich hier also **vorbildlich.** Andere Hersteller sollten diese Möglichkeit ebenfalls in Erwägung ziehen. Dies erlaubt dem

unerfahrenen Benutzer, sich nachträgliche manuelle Portsperrungen zu ersparen. Erwähnenswert ist jedoch, dass es sich bei der „Portfreigabe im LAN“ im eigentlichen Sinne nicht um Sicherheitsrisiken im klassischen Sinne handelt. Lediglich erfahrene Internet-Sicherheitsspezialisten könnten aufgrund der offenen Ports verschiedene Informationen erhalten, welche als Grundlage für weitere gezielte Angriffe dienen könnten. Zum Beispiel resultieren daraus Gefährdungen wie **TCP Sequence prediction** und **IP ID FIELD Prediction Vulnerability**.

Dies bedeutet, dass der TCP/IP Stack nicht vollständig geschützt ist. Im Ernstfall hätte das zur Folge, dass ein Angreifer die Sequenz-Nummer vorhersagen bzw. erraten, und somit bestehende Verbindungen manipulieren könnte. Zudem lassen sich Informationen wie Domain Name, MAC-Adresse, Rechnername, uvm. erlangen, womit ein Angreifer weitere spezifische Angriffe ausführen könnte. Vorausgesetzt natürlich, der Angreifer befindet sich innerhalb der vertrauenswürdigen Zone und verfügt über das notwendige Know-How.

Es ist ratsam, dass sich der Anwender nicht auf die „Sicherheits-(schiebe)regler“ der Personal Firewalls verlässt, denn es ist eine **irrige Annahme**, dass sich offene Ports, die für das vertrauenswürdige Netzwerk freigegeben sind, durch die **Erhöhung der Sicherheitsstufe** schließen lassen. Hier sollte immer manuell durch den Benutzer kontrolliert werden, ob die Netbios-Ports auch durch die Firewall geschützt werden, sofern diese nicht benötigt werden. Einen **Pluspunkt** erhalten im Bereich der „inneren Schutzwirkung“ die Lösungen von Agnitum, CA, Jetico, Sunbelt Software und ZoneLabs aufgrund guter Warnmeldungen und Logdateien sowie benutzerfreundlicher Userinteraktions-Meldungen.

Zu bemängeln ist, dass einige Firewalls den Anwender zwar darüber benachrichtigen (via Pop-Up), wenn ein Angriff aus dem Internet gegen seinen Computer durchgeführte wurde, nicht aber wenn Angriffe ihre Herkunft aus dem LAN haben. Nachstehende Tabelle zeigt die gefundenen Gefährdungen (äußerer und innerer Schutz) im Überblick:

Angriffe direkt via Internet
(geordnet nach Gefahrenlevel + Anzahl gefundener Risiken)

Angriffe direkt via LAN
(geordnet nach Gefahrenlevel + Anzahl gefundener Risiken)

Hersteller	High / Medium / Low	Sonstiges	High	Medium	Low	Sonstiges
Agnitum	0	-	0 / 0	0 / 0	0 / 0	A*, C*
CA	0	-	0 / 4	0 / 4	0 / 13	C*
Iolo	0[2]	-	1[2]/1[2]	2[2]/2[2]	10[2]/10[2]	[2]
Jetico	0	-	0 / 1	0 / 4	0 / 13	A*, C*
Netgate Tech.	0	-	0 / 0	1 / 2	3 / 9	C*
Norman	0	-	1 / 1	2 / 4	5 / 10	C*
Sunbelt Soft.	0	-	0 / 0	0 / 0	0 /1	A*, B*, C*
ZoneLabs	0	-	0 / 2	0 / 2	0 / 13	C*

Legende:

A*	Firewall zeigte sich widerstandsfähig gegen die durchgeführten Attacken
B*	1x „Low Level“ Sicherheitsrisiko aufgrund von „Remote system answers to PING command“
C*	Zeigt den Unterschied wenn das vertrauenswürdige Netzwerk (LAN) durch die Firewall blockiert bzw. erlaubt wird (xx / yy).
D*	Hilfreiche Logdateien und Warn-PopUps während der Angriffe
[2]	Resultate mögl. fehlerhaft, da Probleme während des Betriebs der Software

Stand:	**Juli 2008**
Anzahl Angriffe (Internet):	15133 + 10957 **= 26090**
Anzahl Angriffe (LAN):	**10957**
Produkt analysiert in:	**Werkseinstellungen**

EMPFEHLUNGEN VON PROTECTSTAR™

Zu den durchgeführten Testreihen bezüglich Sicherheit der überprüften Personal Firewall, spricht das ProtectStar™ TestLab folgende Empfehlungen aus:

Um die Sicherheit einer Personal Firewall zu erhöhen, sollte jedes Produkt mit einem **Passwortschutz** vom Anwender versehen werden. Alle getesteten Firewalls weisen eine solche Funktion auf, die jedoch in den Werkseinstellungen deaktiviert ist.

Die Passwort-Funktion sollte vom Benutzer aktiviert und mit einem Passwort aus mindestens acht Zeichen, bestehend aus Buchstaben, Zahlen und Sonderzeichen versehen werden (vgl.: http://www.protectstar-research.com/de.informationen-passworter.html). Dies verhindert, dass die Schutzsoftware deaktiviert, manipuliert oder sogar deinstalliert werden kann.

Personal Firewalls sind in der Regel in den Werkseinstellungen ausreichend auf die Bedürfnisse des Endanwenders

eingestellt. Sollte der Benutzer jedoch die Personal Firewall manuell auf den sogenannten „**Lernmodus**“ oder „**Trainingsmodus**“ umstellen so sollte er sich gerade nach dem ersten Neustart – also nach der Installation - des Computers ausreichend Zeit nehmen, die Vielzahl an Warnmeldungen, über Programme und Dienste die versuchen eine Verbindung in das Internet aufzubauen, zu studieren.

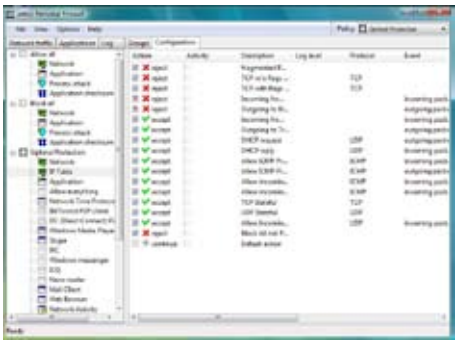
Sofern der Anwender ein **(Heim-) Netzwerk** betreibt und in diesem keine freigegebenen Ordner, Dateien, Drucker, usw. mit anderen Computern eines Netzwerkes teilen möchte, so sollten entsprechend die Netbios-Dienste (Port 139, 443, usw.) ggf. manuell blockiert werden. Die Personal Firewall **Outpost Firewall Pro 2009** von **Agnitum** und die **Iolo Personal Firewall** deaktivieren die Windows-Firewall **nicht** automatisch. Hier wird empfohlen die Windows-Firewall nach der Installation manuell zu deaktivieren. Einen Dual-Betrieb beider Firewalls wird abgeraten.

D.) BENUTZER-FREUNDLICHKEIT

Bezüglich der Benutzerfreundlichkeit sind dem ProtectStar™ TestLab folgende Eigenschaften aufgefallen: Die getesteten Personal Firewalls zeigen sich im Bereich der Benutzerfreundlichkeit als sehr gut bis gut. Außerdem helfen in den meisten Fällen bereits während der Installation nützliche Assistenten/Wizards das Produkt entsprechend einzustellen, um während des Betriebs die Interaktion mit dem Benutzer gering zu halten. Sei es durch die Aktivierung des „Trainingsmodus“ oder durch das generieren von automatischen Regeln durch die Personal Firewall selbst.

Für **fortgeschrittene Benutzer** fällt kein Produkt aus dem Rahmen. Für Anwender, die sich weniger mit Konfigurationsmöglichkeiten, Warnmeldungen und erweiterten Einstellungen auseinandersetzen möchten, sollten die **Jetico Personal Firewall v2** eher umgehen. Gerade nach der Installation des Produktes fragt die Firewall den Anwender nach der Kontrolle von ausgehenden Verbindungen von seinem Computer, die je nach individuellem Schutzbedürfnis entweder „immer erlaubt“, „einmal erlaubt“, „immer blockiert“ oder „einmal blockieren“ möchte oder aber auch zu jeder Verbindung eine eigene erweiterte Regel erstellen kann. Nach der Installation der **Jetico Firewall** sind so zwanzig und mehr Meldungen an den Benutzer keine Seltenheit. Sobald jedoch diese Regeln entsprechend bestätigt worden sind, arbeitet das Produkt sehr zuverlässig und überzeugt durch fortschrittliche und detailierte Einstellungsmöglichkeiten und umfangreiche Reportdateien, welche jedoch vor allem nur von technisch versierten Benutzern analysiert werden können.

Die **Outpost Firewall PRO 2009** von **Agnitum** bietet sowohl erfahrenen als auch weniger technisch versierten Anwendern starke Einstellungs- und Konfigurationsmöglichkeiten im Bereich der Firewall, Reports, Hostschutz und der Angriffserkennung. Die Angriffserkennung



via Pop-Up ist sehr gut umgesetzt worden und informiert den Benutzer umfassend bei Sicherheitsverletzungen. Der „Auto-Learn Mode“ arbeitete während der Testreihen sehr zuverlässig. Das Hauptmenü ist einfach und übersichtlich gehalten, so dass der Anwender alle Einstellungen schnell erreichen kann. Fortgeschrittene Anwender werden an den Einstellungsmöglichkeiten ihre Freude finden. Der Benutzer hat außerdem die Möglichkeit, das Produkt während der Installation bereits vor zu konfigurieren, in dem er im „Configuration Wizard“ entweder „Advanced“ oder „Normal“ auswählt. Jede Option ist ausreichend erläutert.

Die **CA Personal Firewall 2008** zeigt sich vor allem gegenüber Heimanwendern, die schnell und ohne Umstände ihre Firewall

durch Sicherheitsregler konfigurieren möchten, vorbildlich. Individuelle Einstellungen können dann über den Button „Expertenregeln“ bzw. über „Erweitert…“ im Hauptmenü der Firewall vorgenommen werden. Die Software unterteilt zudem anschaulich die Sicherheitsebenen für die „sichere Zone“ und „eingeschränkte Zone“. Das bereits während der Testreihen erwähnte Problemprodukt - die **Iolo Personal Firewall** – zeigt sich in Sachen der Benutzerfreundlichkeit von einer positiven Seite, auch wenn das Hauptmenü überladen scheint.

Benutzer können nach der Installation mit Hilfe eines wizardähnlichen Programms genau festlegen, welche Arbeitsprogramme wie SkyPE, AOL, Apple iTunes, World of Warcraft, uvm. der Anwender verwendet. Entsprechend werden diese Programme durch die Iolo Firewall freigegeben bzw. bei Nichtauswahl blockiert. Auch kann der Benutzer festlegen, ob er im Bezug auf die „innere Sicherheit“ seinen Dateien und Drucker mit anderen Netzwerkteilnehmern teilen möchte. Auch hier werden (theoretisch) dann die Netbios-Ports unter Windows blockiert, was sich jedoch in unserem Test nicht bestätigte aufgrund der genannten Problematik.

Die **Norman Personal Firewall** zeichnet sich vor allem durch hilfreiche

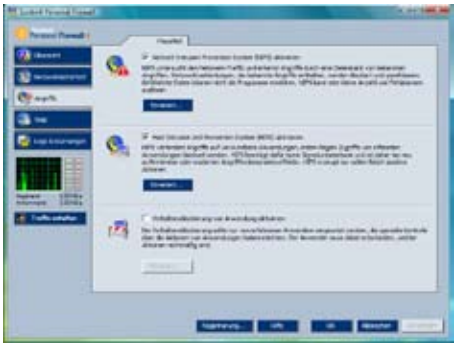
und gut erläuterte Installations- und Konfigurationsassistenten aus. Sie erleichtern dem Benutzer die Firewall nach seinen Bedürfnissen einzustellen oder spielend neue Firewallregeln zu erstellen. Im ersten Schritt bereits fragt das Produkt bereits nach der persönlichen Erfahrungsstufe („unerfahrener Benutzer“ oder „erfahrener Benutzer“) des Anwenders. Ebenso können während der Installation bei Bedarf durch aktivieren von Kontrollkästchen die Windows-Dateifreigabe und Netzwerkdrucker freigegeben oder blockiert werden.

Die Logdateien sind jedoch unter „Support-Center“ sehr versteckt. Auch warnte das Programm den Benutzer während der durchgeführten Angriffe nur äußerst minimal oder überhaupt nicht. Eher Geschmackssache ist das Hauptmenü der **FortKnox Personal Firewall 2008** von **Netbelt Technologies**. Zwar kann während der Installation das Benutzermenü (GUI) farblich angepasst werden, dennoch zeigte sich die Software im Bereich der Ästhetik eher minimalistisch. Anstatt einer Übersicht über Einstellungen und abgewehrte Angriffe, zeigt sich das Menü dem Anwender zunächst in Form einer Live-Statistik in schwarzem Hintergrund. Zwar kann der Benutzer unproblematisch und neue Regeln erstellen oder bestehende Konfigurationen an seine Wünsche anpassen, dennoch überzeugt die Firewall in diesem Testbereich - im Gegensatz zu den Konkurrenzprodukten – wenig.

Die **Personal Firewall 4** (Full) des amerikanischen Unternehmens **Sunbelt Software** ist in Sachen der Benutzerfreundlichkeit der **Testsieger** dieses Vergleichstests; dicht gefolgt von der Outpost Firewall PRO 2009 des russischen Herstellers Agnitum.

Im Übrigen ist die Sunbelt Personal Firewall (SPF) auf Grundlage der Kerio Personal Firewall (KPF) entstanden, nach dem Sunbelt Software das Produkt von Kerio gekauft hat.

Die Firewall von **Sunbelt** ist sowohl für den erfahrenen als auch typischen Heimanwender gleichermaßen geeignet. Das Benutzermenü zeigt sich gut durchdacht und Dank der Übersichtlichkeit können alle Einstellungen – sei es im Bereich der Firewallregeln, des Network Intrusion Prevention Systems (NIPS), des Host Intrusion Prevention Systems (HIPS), Verhaltensblockierung von Anwendungen, uvm. leicht vorgenommen werden. Das HIPS kann zum Beispiel auf das Schutzbedürfnis des Benutzers so angepasst werden, dass es vor Pufferüberlauf und/oder Codeinjektion schützt. Ebenso kann während der Installation des Produktes ausgewählt werden, ob die Firewall im „Simple (No popup mode)“ oder im „Advanced (Learning mode)“ betrieben werden soll. Die Reportdateien sind informativ und übersichtlich nach Kategorien wie HIPS, NIPS, Web, uvm. sortiert.



ZoneAlarm Pro von **ZoneLabs** (Check Point) stellt sich besonders für Heimanwender in zeitgemäßem Design dar. Die Installation der Software wird durch einen Assistenten geleitet. Nach dem obligatorischen Neustart des Systems bietet sich dem Anwender die Möglichkeit, im Rahmen eines Schulungsvideos die grundlegenden Funktionen der Software zu erlernen. Sobald die Software nach dem Neustart geladen ist, werden bereits laufende Programme und Installationen erkannt. Hier ist die Firewall jedoch auch auf die Zusammenarbeit mit dem Benutzer angewiesen.

Die erweiterte Konfiguration erfordert kurze Einarbeitung des Anwenders, da nicht alle Dialoge sofort zu erkennen sind. Neben der Navigation im linken Teil der Sicherheitslösung die jeweiligen Untermenus oben rechts angesteuert werden. Ein über dreihundertseitiges Handbuch, das dem Anwender in digitaler Form zu Verfügung steht, stellt eine sehr brauchbare Hilfe dar. Es unterstützt

den Benutzer nicht nur bei möglichen Problemen, sondern steht ihm auch durch viele nützliche Hinweise für die tägliche Arbeit mit der Software zur Seite.

E.) PERFORMANCE

Personal Firewalls beanspruchen Prozessorleistung und auch die Datenübertragungsgeschwindigkeit kann verringert werden. Zusätzlich integrierte Schutzmodule wie ein Anti-Spyware Scanner, der beispielsweise in den Lösungen von Agnitum und ZoneLabs integriert ist, bieten dem Benutzer auf der einen Seite ein **höheres Maß an Sicherheit** und **Benutzerfreundlichkeit**, auf der anderen Seite jedoch wird aufgrund der zusätzlichen Schutzkomponente der Prozessor stärker **ausgelastet**. Alle getesteten Personal Firewalls hinterließen einen durchweg **positiven Eindruck** im Bereich der Performance. Keines der Produkte fiel gravierend aus dem Testrahmen. Lediglich die **Jetico Personal Firewall v2** zeigte sich bis zur endgültigen Konfiguration mit leichten, aber nicht gravierenden Performanceeinbußen.
Jedes Produkt arbeitete bei den durchgeführten Testreihen **schnell** und **zuverlässig**.

Es konnten keine Leistungseinbußen oder Mängel bei der System-Performance festgestellt werden. Selbst während des **mehrstündigen** Dauer-Penetrationstest konnte weiterhin unter minimalen Leistungseinbußen mit den Personal Firewall gearbeitet werden. Der Datendurchsatz ist stets als **gut** zu bewerten. Auch konnten kaum Geschwindigkeitseinbußen zum Beispiel bei Internetanwendungen bei den Lösungenvon Agnitum und ZoneLabs registriert werden. Obwohl beide eine weitere Schutzkomponente – den Anti-Spywarescanner – integriert haben. Zu beachten ist jedoch, dass die gute Performanceeigenschaften hauptsächlich von den Konfigurationen des Anwenders und seiner Computergeschwindigkeit, Betriebssystem und Arbeitsspeicher abhängig sind. Vor allem auf älteren Computersystemen unter Windows Vista mit 1024 Megabyte Hauptspeicher kommt es dann zu Verzögerungen in der Performance, wenn die Schutzebenen der Firewall manuell auf „Hoch/High“ eingestellt worden sind.

F.) PREIS-/AUSSTATTUNGS-VERHÄLTNIS

Bei der Beurteilung des Preis-/Ausstattungsverhältnisses fällt zunächst auf, dass zwischen den empfohlenen Preisen der Hersteller bzw. den von den Herstellern betriebenen Onlineshops und den Verkaufspreisen von Amazon (zum Großteil inkl. kostenloser Lieferung) teilweise Unterschiede bestehen. Ein Preisverglich lohnt daher immer. Auch kostet beispielsweise ZoneAlarm PRO in den USA US$ 39,95 (~EUR 25,00) und in Europa EUR 39,95 (~ US$63.00).

	Preis (Box)	*Preis (Download)*	*Amazon-preis*	*Lizenzen*	zusätzliche Software	*PUNKTE* max. 20	*Bewertung*
Agnitum	---	39,95	---	3x	Anti-Spyware	***20***	***excellent***
CA	---	59,99*	---	3x	---	***15***	***befried.***
Iolo	39,95	39,95	24,99	3x	---	***18***	***sehr gut***
Jetico	---	39,95	---	1x	---	***16***	***gut***
Netgate Tech.	---	29,95	---	1x	---	***17***	***gut***
Sunbelt Soft.	---	29,95	---	3x	---	***18***	***sehr gut***
ZoneLabs	39,95	39,95	37,99	1x	Anti-Spyware	***17***	***sehr gut***

*Preise umgerechnet in US$

G.) FAZIT

Bevor nun das finale Ergebnis dieses Vergleichstest bekannt wird, sollten zunächst einige wesentliche Erkenntnisse erwähnt werden:

Es ist aufgefallen, dass die klassischen Personal Firewalls auf dem IT-Markt immer mehr durch Internet Security Suiten verdrängt werden. Wo vor einigen Jahren noch nahezu jeder Hersteller wie beispielsweise McAfee und Symantec eine Einzelplatzlösung ihrer Firewall anboten, sind die Produkte zwischenzeitlich in die jeweils hauseigenen Internet Security Suiten integriert worden. Interessenten müssen sich daher verstärkt auf einem kleineren Markt nach einem passenden Produkt umsehen. Auf der anderen Seite zeigt sich jedoch, dass sich auf diesem Markt dennoch Experten in Sachen Personal Firewalls befinden. Preislich gesehen sind die Einzelplatzlösungen im Vergleich zu den Security Suiten teuer. Zurückschrecken sollten Interessenten dennoch nicht, denn eine gut gewählte Kombination von Einzelplatzlösungen kann immer noch preiswerter und besser sein, als eine Suite.

Der Hauptanforderung an Personal Firewalls - an erster Stelle den Schutz vor Angriffen aus einem externen Netzwerk – sind die Firewalls in jeder Hinsicht gewachsen. Alle getesteten Personal

Firewalls zeigen sich im Bereich der äußeren Sicherheit, Benutzerfreundlichkeit und Performance als sehr gut bis gut. Die Zeiten, bei denen die Anwender noch Schwierigkeiten und Verständnisprobleme bei der Konfiguration hatten, scheinen vorbei zu sein. Im laufenden Arbeitsbetrieb sind die meisten Produkte auf modernen Computersystemen kaum bemerkbar. Lediglich die Firewall von Jetico hat einige „Anfangsschwierigkeiten" aufgrund der zu bestätigenden ein- und ausgehenden Verbindungsregeln nach der Installation. Aber auch diese verschwinden nach getaner Konfiguration. Das Produkt von Agnitum zeigt nur dann Beeinträchtigungen im Bereich der Performance, sobald manuell alle Sicherheitskonfigurationen auf „Hoch/High" eingestellt werden. Aus dem Testrahmen fällt das Produkt des Herstellers Iolo. Obwohl sich die Firewall problemlos und benutzerfreundlich installieren ließ und auch gute Ergebnisse im Bereich des äußeren Schutzes zeigte, wies sie jedoch Mängel im Bereich des inneren Schutzes auf. Ob es sich dabei um Treiberprobleme mit den verwendeten Netzwerkkarten oder um Programmierfehler handelt ist derzeit nicht bekannt. Allerdings würde sich in der überprüften Testsituation der ahnungslose Benutzer in falscher Sicherheit wiegen, da die Iolo Firewall scheinbar betriebsbereit ist, aber keine Angriffe erkennt und blockiert. Der Hersteller wird über die Vorfälle informiert und das Produkt in einem künftigen Test nochmals analysiert.

Die beiden Testsieger im Bereich der Benutzerfreundlichkeit sowie des Preis-/ Ausstattungsverhältnis sind die Personal Firewalls von Agnitum und Sunbelt Software. Aber auch die Lösung von Norman kann aufgrund seines optisch ansprechenden und benutzerfreundlichen Konfigurationsassistenten an dieser Stelle erwähnt werden. Allerdings patzt Norman im Bereich der inneren Sicherheit, der Konfigurationsmöglichkeiten und den Reportdateien. Wertet man die Testreihen bezüglich Sicherheit, Benutzerfreundlichkeit, Performance und Preis- / Ausstattungsverhältnis gemäß den festgelegten Bewertungskriterien (Vgl. B – Bewertungskriterien) aus, so werden im Detail folgende Punkte erzielt:

HERSTELLER	SICHERHEIT (Außen/Innen./ Sonst.)	BENUTZERFREUND. & PERFORMANCE	PREIS-/ AUSSTATTUNG	PUNKTE	%
Agnitum	60 / 50 / 09	29 / 28	20	196	98,00%
CA	60 / 47 / 08	29 / 28	15	187	93,50%
Iolo	(60) / (00) / (00)	25 / 29	18	(132)	66,00%
Jetico	60 / 48 / 09	25 / 27	16	185	92,50%
Netgate Tech.	60 / 46 / 06	24 / 29	17	182	91,00%
Norman	60 / 45 / 07	28 / 29	14	183	91,50%
Sunbelt Soft.	60 / 50 / 09	30 / 28	18	195	97,50%
ZoneLabs	60 / 48 / 10	28 / 28	17	191	95,50%

Tabelle: Vergebene Punkte in den Testbereichen (Vgl. C.: Bewertungskriterien)

Nach dem Punktebewertungssystem können die verfügbaren Platzierungen wie folgt vergeben werden:

1. Platz mit **196** Punkten an:
Agnitum Outpost Firewall PRO 2009

2. Platz mit **195** Punkten an:
Sunbelt Personal Firewall 4 (Full)

3. Platz mit **191** Punkten an:
ZoneAlarm PRO 7

4. Platz mit **187** Punkten an:
CA Personal Firewall 2008

5. Platz mit **185** Punkten an:
Jetico Personal Firewall v2

6. Platz mit **183** Punkten an:
Norman Personal Firewall

7. Platz mit **182** Punkten an:
Netgate FortKnox Firewall 2008

8. Platz mit **132** Punkten an:
Iolo Personal Firewall

Der **Testsieger** dieses Vergleichstests ist das Produkt **Outpost Firewall PRO 2009** des Herstellers **Agnitum**, dicht gefolgt von der **Sunbelt Software Personal Firewall 4 (Full)**.

Aufgrund der äußerst knappen und nah zusammenliegenden Punkteplatzierung - mit einer Differenz von lediglich einem Punkt - hat sich das ProtectStar™ TestLab dazu entschieden, die beiden Erstplatzierten Personal Firewalls mit dem **ProtectStar™ AWARD 2008** auszuzeichnen.

Empfehlung

Ein Punktebewertungssystem wie in **G.) Fazit** aufgeführt, ist jedoch nicht für jede Anwendergruppe hilfreich. Je nach Kenntnisstand des Benutzers und Ausstattung des Computers/Notebooks sind für ihn andere Entscheidungskriterien relevant.

Sowohl für den erfahrenen als auch weniger technisch versierten Anwender – sei es im Home- oder auch Businessbereich – kann das ProtectStar™ TestLab die Personal Firewall **ZoneAlarm PRO 7** von **ZoneLabs**. empfehlen. Die Firewall zeichnet sich durch eine robuste Sicherheit sowie guten und verlässlichen Warnmeldungen aus. Der integrierte Anti-Spyware Scanner rundet ZoneAlarm PRO 7 zudem ab.

Das Produkt wird mit der Sicherheitsempfehlung **ProtectStar™ Excellent Security** ausgezeichnet.

Anregungen, Kritik und Spenden

Das ProtectStar™ TestLab, als auch AV Comparatives arbeiten strikt unabhängig. Die hier durchgeführten Testanalysen, die Aufbereitung und Ausarbeitung der Testresultate, Design des Testberichts, Übersetzungen, Publizierungen, usw. wurden ausschließlich von der ProtectStar™, Inc. finanziert. Die im Testbericht genannten Hersteller stellten für die Testreihen lediglich die benötigten und notwendigen Testversionen bzw. Lizenzen bereit.

Um die Testreihen in Zukunft weiter verbessern zu können, dankt das ProtectStar™ TestLab jeder Art von Anregung und Kritik seiner Leserinnen und Leser. Teilen Sie uns bitte mit, was Ihnen besonders gut gefallen hat und welcher Test für Sie hätte ausführlicher behandelt werden können. Könnten künftig weitere Testkriterien integriert werden, die im aktuellen Testbericht vergessen wurden?

Sofern Ihnen der Testbericht gefallen und Ihnen bei einer möglichen Kaufentscheidung geholfen hat oder Sie durch ergänzendes Expertenwissen im Bereich der IT-Sicherheit Neues erfahren konnten, so würden wir Ihnen für **Ihre Unterstützung** für die wohltätige und international tätige **ProtectStar™ Foundation** sehr danken. Ihre Unterstützung kommt gemeinnützigen Hilfsprojekten auf der ganzen Welt in den Bereichen Bildung, Gesundheit, Armut und IT-Sicherheit für Schulen zugute.

Weitere Informationen über die gemeinnützige **ProtectStar™ Foundation** erhalten Sie unter:

www.protectstar-foundation.org

Copyright

Kontakt

Corporate Headquarter:
ProtectStar, Inc.
444 Brickell Avenue
Suite 51103
Miami, FL 33131
USA
Phone: +1 888 218 4123
Fax : +1 888 218 8505
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org

European Headquarter:
ProtectStar, Inc.
Test Lab
Daws House
33-35 Daws Lane
London NW7 4SD
UK

Phone: +44 20 8906 6651
Fax : +44 20 8906 6611
e-Mail: testcenter@protectstar.com
Web : www.protectstar-testlab.org