



ProtectStar™ - Vergleichstest Internet Security Suites 2008

INHALTSVERZEICHNIS:

Seite 2	Inhaltsverzeichnis
Seite 3	A.) Getestete Produkte und Versionen
	B.) Hintergrundinformationen
	C.) Allgemeine Erläuterung der Testverfahren
Seite 4	D.) Bewertungskriterien
Seite 5	E.) Test: SICHERHEIT
	DIE FIREWALL – der äußere Schutz DIE FIREWALL – der innere Schutz DIE MALWAREERKENNUNG
Seite 9	F.) Test: BENUTZERFREUNDLICHKEIT
Seite 12	G.) Test: PERFORMANCE
Seite 14	H.) Test: PREIS-/AUSSTATTUNGSVERHÄLTNIS
Seite 15	I.) FAZIT
Seite 16	J.) FAZIT II (Empfehlungen)
Seite 17	Anregungen, Kritik und Spenden
	Kontakt & Copyright



A.) Getestete Produkte und Versionen

Hersteller	Produktname	Größe Setupdatei	Release (Version)
Agnitum	OutpostPro Security Suite 2008	30,4 MB	6.0.2225.232.0465
Avira	Premium Security Suite 2008	18,8 MB	7.06.00.168
BitDefender	Internet Security 2008	41,8 MB	n/a
BullGuard	BullGuard 8.0	30,4 MB	n/a
ESET	Smart Security 3.0	18,0 MB	3.0.621
F-Secure	Internet Security 2008	81,9 MB	n/a
G DATA	Internet Security 2008	201,8 MB	18.0.7295.201
Kaspersky	Internet Security 7.0	28,9 MB	7.0.1.321
McAfee	Internet Security 2008	38,7 MB	n/a
Microsoft	Live OneCare 2.0	n/a	2.0.2500.14
Panda	Internet Security 2008	50,0 MB	12.00.00
Symantec	Norton Internet Security 2008	61,5 MB	n/a
Trend Micro	Internet Security 2008	88,3 MB	16.00.1645

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

B.) Hintergrundinformationen

In regelmäßigen Abständen erhält das ProtectStar™ TestLab (www.protectstar-testlab.org) immer wieder Anfragen bezüglich sicherer und moderner Schutzlösungen für IT- und Kommunikationssysteme aller Art. Vermehrt sind es Hinweise von IT-Verantwortlichen, die veröffentlichte Testresultate in Fachforen und Zeitschriften als irritierend und verwirrend bemängeln.

Dem Endanwender ist es ein Rätsel, aus welchen Gründen beispielsweise die „Security Suite A“ auf Platz Nummer Eins (von zehn und mehr Plätzen) des einen Magazins gewählt wird, während eine andere Fachzeitschrift das Produkt eher als „durchschnittlich“ bewertet und auf den siebten oder achten Platz setzt. Auch sind die Testverfahren bei Benutzerfreundlichkeit, Performance oder den Sicherheitstests der Firewalls mehr als diffus oder werden gar nicht behandelt.

Bei der Bestimmung von Viren-erkennungsraten scheinen die Anwender im Allgemeinen zufriedener zu sein. Aber auch in diesem Bereich wird oftmals eine gewisse Ungenauigkeit oder Verallgemeinerung bemängelt, da sich ein Vergleichstest oft nur auf die Erkennung von Malware der Produkte kümmert.

Aufgrund des zunehmenden Interesses an übersichtlichen und aussagekräftigen Testergebnissen sah sich ProtectStar™ veranlasst, einen Vergleichstest aktueller Internet Security Suites durchzuführen. Das Hauptaugenmerk der Testreihen lag dabei auf den Sicherheitseinstellungen der Produkte im Auslieferungszustand (Standardeinstellung nach der Installation). Gefragt war also:

wie gut ist die Sicherheit der Suite, nach der Installation und ohne weitere Konfiguration?

sind die Hinweise bezüglich Programmwarnungen und Hinweise für den Anwender verständlich?

gibt es Einschränkungen in der Systemperformance?

Im Test waren insgesamt **dreizehn** aktuell auf dem IT-Sicherheitsmarkt verfügbare **Internet Security Suites**. Für die Zukunft plant das ProtectStar™ TestLab alle weltweit verfügbaren Suites miteinander zu vergleichen. Die bei diesem Test nicht zur Verfügung gestandenen Suites wie zum Beispiel von avast!, AVG, Norman, Sophos, Trustport, ZoneAlarm, uvm. werden daher im nächsten Vergleichstest berücksichtigt.

C.) Allgemeine Erläuterung der Testverfahren

Getestet wurde sowohl unter **Laborals auch realen Bedingungen**. Im Bereich der **SICHERHEIT** lag der Fokus auf dem äußeren und inneren Schutz der integrierten Personal Firewall. Das Hauptaugenmerk waren die werkseitigen Einstellungen, also Auslieferungszustand der jeweiligen Security Suite. „**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, o.ä.).

„**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. Die umfangreichen Bestimmungen und Analysen der Viren- bzw. Malwareerkennungsraten der Engines in den getesteten Internet Security

Suiten wurden in Kooperation mit AV-Comparatives (www.av-comparatives.org) durchgeführt. Der in diesem Bereich verwendete Begriff „Malware“ beinhaltet sowohl Viren, Würmer, Trojaner, etc. 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 Augenmerkmale lagen auf Handbuch (teilweise im Lieferumfang als gedruckte Version enthalten) und dessen Verständlichkeit, der Onlinehilfe und FAQs.

Fragen nach der Verfügbarkeit einer Boot-CD (Rettungs-CD/DVD) oder der Möglichkeit selbst eine Rettungs-CD erstellen zu können runden diesen Themenblock ab. Im Segment **PERFORMANCE** standen für die dreizehn Internet Security Suiten eine Vielzahl unterschiedlicher Rechnersysteme zur Verfügung.

Ausstattungsmerkmale der Testrechner (von – bis):

Betriebssystem:

Windows XP mit Service Pack 2 und / oder Windows Vista

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)

Außerhalb der Reihe fanden Bewertungen statt, ob die Produkte nach den Herstellerangaben bezüglich Mindestvoraussetzungen der Systeme auch benutzergerecht verwendet werden können.

PREIS-/AUSSTATTUNGSVERHÄLTNIS: Wie stehen Preis und Ausstattung einer Security Suite zueinander? Also welche zusätzlichen Softwaremodule wie bspw. Backup, Tuning, etc. dem Anwender ausgeliefert werden und die Anzahl der enthaltenen Lizenzen. Außerdem wurde der Preisunterschied zwischen einer Box- und Downloadversion beim Hersteller gegenüber dem sog. „Straßenpreis“ am Beispiel des Onlineversandhauses Amazon verglichen.

D.) Bewertungskriterien

Bei allen dreizehn getesteten Internet Security Suiten handelt es sich ausschließlich um Sicherheitslösungen, die dem Anwender ausgezeichneten Schutz vor modernen Gefahren wie Hackern, Viren, Rootkits, Keyloggern, Phishing- und Pharming-Angriffen, uvm. versprechen und vor allem auch gewährleisten sollen. Da es sich um **Sicherheitsprodukte** handelt, muss das Hauptaugenmerk zwangsläufig auch auf die enthaltenen Schutzfunktionen der jeweiligen Security Suiten 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**. Eine moderne Internet Security Suite sollte – im Vergleich zu Konkurrenzprodukten - unabhängig von ihrem höheren oder niedrigeren Verkaufspreis einen maximalen Schutz gewährleisten. Hier soll der Anwender zunächst nicht durch zusätzliche Features wie Tuning- und Backup-Programmen oder die Zugabe von weiteren Lizenzen zum Kauf maßgeblich beeinflusst werden. Auf der anderen Seite jedoch ergeben sich besondere Preisvorteile für den Anwender, wenn er durch den Kauf einer Internet Security Suite kein separates

Backupprogramm mehr erwerben muss, wenn eine gleichwertige Speicherlösung bereits in dem Produkt enthalten ist. Ähnliches gilt für Programme im Bereich Systemoptimierung und Kindersicherung. 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:



- Sicherheit (100 P.)
- Benutzerfreundlichkeit (40 P.)+ Performance (40 P.)
- Preis-/Ausstattungsverhältnis (20 P.)



E.) Test: SICHERHEIT

1.) DIE FIREWALL – der äußere Schutz

Jede durch das ProtectStar™ TestLab bewertete Security Suite enthält eine integrierte Firewall bzw. Personal Firewall, die **ein- und ausgehende** Verbindungen überwacht. Analysiert wurden die Personal Firewalls 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 in den Security Suites integrierten Firewalls haben in den Durchläufen bezüglich des äußeren Schutzes, alle zum Testzeitpunkt bekannten **14.037** unterschiedlichen **Angriffs- und Sicherheitstests** erfolgreich bestanden (Stand: Februar 2008).

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“, „WINS Code Execution (870763)“, „Vulnerability in NetDDE Could Allow Code Execution“ und „MS Task Scheduler vulnerability“, uvm. dazu. 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 und hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **10257** (Stand: Februar 2008) weitere Sicherheitstests und Angriffstaktiken auf die Firewalls ausführte, als auch durch die **manuell** durchgeführten Prüfungen konnten **keine** Schwachstellen oder Sicherheitsrisiken festgestellt werden.

Den **mehrständigen** Dauer-**Penetrationstest** absolvierten die Firewalls ebenfalls **erfolgreich**, ohne nennenswerte Performanceverluste. **Keine** Security Suite zeigte 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 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 Security Suites von **Agnitum**, **BullGuard** und **Symantec** bereits in



den Werkseinstellungen **vorbildlich**. Besonders lobenswert im Bereich der Konfigurationsmöglichkeiten sind die integrierten Firewalls der Security Suites von **Agnitum** und **BullGuard**. Bei beiden Produkten – vor allem bei **BullGuard** – lassen sich Einstellungen bis in das **kleinste Detail** vornehmen. Allerdings sollte der Anwender ausreichend Erfahrung und Wissen bezüglich IT-Sicherheit mitbringen, bevor er manuell die Regeln modifiziert oder neu definiert.

Wünschenswert wäre es jedoch, wenn die Schutzsuiten in Zukunft **mehr Angriffstechniken** erkennen und dem Benutzer melden würden. Die Mehrheit der analysierten Security Suites beschränkte sich in diesem Bereich lediglich auf das Melden von entdeckten Portscans. Spezielle Brute-Force Attacken und Denial of Service 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.

2.) DIE FIREWALL – der innere Schutz

Der vorhergehende Test zeigte, dass alle in den Security Suites integrierten Personal Firewalls **ausreichend Schutz** gegen Angriffe aus dem Internet bieten. Wie sieht es aber aus, wenn ein oder mehrere Computersysteme direkt aus der „vertrauenswürdigen Zone“ – dem LAN – 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 bezüglich der Schutzwirkungen im LAN mit unterschiedlichen **Angriffs- und Sicherheitstests**. Getestet wurden die aktuell bekannten **Denial of Service (DoS)**-Angriffsarten, sowie die **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 Firewalls bereits in den Werkeinstellungen für das LAN bzw. vertrauenswürdigen Zone. 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 dass der Anwender manuelle Konfigurationen vornehmen muss. Aus diesem Grund sind bei den in den Security Suites integrierten Firewalls verschiedener Hersteller beispielsweise die Ports (tcp) **135 (msrpc)**, **139 (netbios-ssn)** und **445 (microsoft-ds)** **unzureichend geschützt**.

Diese Eigenschaft weisen die Lösungen von G DATA, Kaspersky, McAfee und Trend Micro auf. Einen Ausnahmefall bilden die Lösungen von BitDefender, ESET, Microsoft und Symantec: Bei „**BitDefender Internet Security 2008**“, „**ESET Smart Security 3.0**“, „**Microsoft Live OneCare 2.0**“ und „**Norton Internet Security 2008**“ können die Benutzer jeweils nach der Installation des Produktes auswählen, ob der PC mit anderen Computern im LAN kommunizieren soll oder nicht. Dementsprechend werden die genannten tcp-Ports von der Firewall entweder geschützt oder offen gelassen. Die vier genannten Security Suites von **BitDefender**, **ESET**, **Microsoft** und **Symantec** 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.

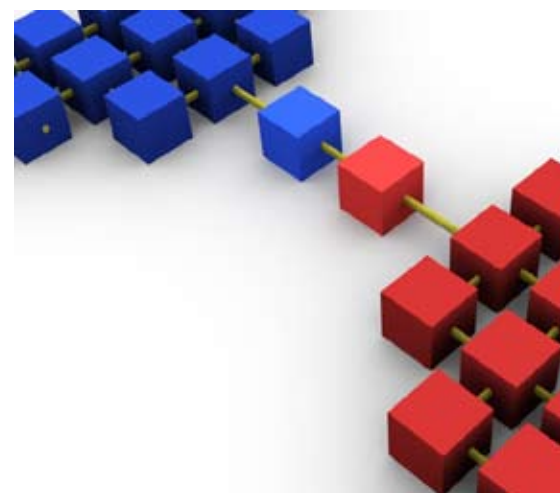
Erwähnenswert ist jedoch, dass es sich bei der „Portfreigabe im LAN“ im eigentlichen Sinne nicht um Sicherheitsrisiken im klassischen Sinne handelt. Lediglich erfahrene Internet-Sicherheitsspezialisten könnten aufgrund der offenen Ports verschiedene Informationen erhalten, welche als Grundlage für weitere 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, usw. erlangen, womit ein Angreifer weitere spezifische Angriffe ausführen könnte. Vorausgesetzt natürlich, der Angreifer befindet sich innerhalb der vertrauenswürdigen Zone (LAN) und verfügt über das notwendige Know-How. Über diese Erkenntnis haben wir beispielsweise den Hersteller **G DATA** informiert.

Man teilte uns mit, dass das Verhalten der G DATA Firewall „so gewollt“ ist. Zudem informierte uns ein Techniker von G DATA darüber, dass sofern „*ein Anwender eine DFÜ-Verbindung (also ohne Router) benutzt, so wird der Regelsatz 'direkte Verbindung mit dem Internet' automatisch ausgewählt. In diesem Fall ist von außen kein offener Port zu sehen. In einem Firmen-Netzwerk kann man mit diesem Regelsatz vernünftig arbeiten, da z.B. Netzwerk-Laufwerke, durch Login-Script mit eingebunden werden, nicht funktionieren.*

Im Bereich 'Netzwerke' kann man für jedes Netzwerk einen entsprechenden Regelsatz zuordnen, falls man mit der Standard-Einstellung nicht zufrieden ist“. Die Sicherheitsexperten des **ProtectStar™ TestLab** können die Antwort von **G DATA** bestätigen, für zu Recht erklären und ebenso auf die anderen Lösungen wie von Kaspersky,





McAfee und Trend Micro - bei denen diese Eigenschaft ebenfalls auftritt – anwenden. Dennoch zeigte sich durch Hinzuziehen von externen ProtectStar™-Testpersonen verschiedenen Erfahrungsstandes, dass die in den Security Suites vorhandenen „Sicherheits-(schiebe)regler der Firewalls“ dann zum Teil Verständnisprobleme mit sich bringen:

Es ist eine irriige Annahme, dass sich offene Ports, die für das vertrauenswürdige Netzwerk freigegeben sind, durch die Erhöhung der Sicherheitsstufe schließen lassen. Sowohl bei der Suite von **G DATA**, **Kaspersky**, **McAfee** als auch **Trend Micro** waren diese Ports auch dann noch im LAN offen, nachdem man die Sicherheitsstufe auf „maximale/höchste Sicherheit“ hochstellte.

Die oben genannte Gefährdungen - **TCP Sequence prediction** und **IP ID FIELD Prediction Vulnerability** - weisen in den Werkseinstellungen **nicht** die Produkte von Agnitum, Avira, BitDefender, Eset, F-Secure, Microsoft, Panda Security und Symantec auf. Einen **Pluspunkt** erhalten im Bereich der „inneren Schutzwirkung der Firewalls“ die Lösungen von Agnitum, BullGuard, BitDefender, Kaspersky, Symantec und Trend Micro, aufgrund guter Warnmeldungen und Logdateien. Einen weiteren **zusätzlichen Pluspunkt** erhalten die Suites von **BullGuard** und **Trend Micro** für die sehr detaillierten Warnmeldungen und benutzerfreundlicher Userinteraktions-Meldungen. Zu bemängeln ist, dass einige Security Suites den Anwender zwar darüber

benachrichtigen (via Pop-Up), wenn ein Angriff aus dem Internet gegen seinen Computer durchgeführt wurde, nicht aber wenn Angriffe ihre Herkunft aus dem LAN haben. Das ist bei den Suites von Eset, G DATA, McAfee, Microsoft und Trend Micro aufgefallen.

Bei diesen Produkten wurde lediglich ein Eintrag in die Logdateien vollzogen; und das selbst dann, als die Sicherheitsstufe der Firewalls auf „maximale/höchste Sicherheit“ gestellt wurde.

Nachstehende Tabelle zeigt die bei den Security Suites 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	High	Medium	Low	Sonstiges
Agnitum	0	0	0	0	A*, G*
Avira	0	0	0	1	B*
BitDefender	0	0	0 / 0	0 / 0	E*
BullGuard	0	0	0	0	A*, G*
ESET	0	0	0 / 3	0 / 9	C*
F-Secure	0	0	0	0	-
G DATA	0	0	3	7	D*
Kaspersky	0	0	3	9	-
McAfee	0	0	3	9	-
Microsoft	0	0	0 / 3	0 / 7	E*
Panda	0	0	0	0	-
Symantec	0	0	0	0	-
Trend Micro	0	0	3	7	F*, G*

Stand:
Februar 2008

Anzahl Angriffe (Internet):
14.037 + 10.257 = **24.294**

Anzahl Angriffe (LAN):
10.257

Produkt analysiert in:
Werkseinstellungen

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 zwischen der Option „Strict Control“ und „Allow Sharing“, welche nach der Installation ausgewählt werden kann.
- D* Sicherheitsschieberegler der Firewall zeigt nach Betätigung verschiedener Sicherheitslevels keinerlei Unterschiede zwischen Werkseinstellung und „Höchster Sicherheit“.
- E* Zeigt den Unterschied zwischen der Option „Öffentlicher Bereich“ und „Home- oder Workzone“, welche nach der Installation ausgewählt werden kann.
- F* Sicherheitsschieberegler der Firewall zeigt nach Betätigung verschiedener Sicherheitslevels keinerlei Unterschiede zwischen Werkseinstellung und „Höchster Sicherheitsstufe“ / „Maximal“ bei Angriffen aus dem LAN
- G* Hilfreiche Logdateien und Warn-PopUps während der Angriffe

3.) Die MALWAREERKENNUNG

In Kooperation mit dem unabhängigen und renommierten Testcenter AV-Comparatives (www.av-comparatives.org), wurden die Malwareerkennungsraten in den dreizehn getesteten Security Suites integrierten Malwarescannern analysiert.

Um eine genaue Erkennungsrate bestimmen zu können wurden alle Security Suites an einem Tag aktualisiert und dann „eingefroren“, so dass eine weitere automatische Aktualisierung der Produkte nicht mehr möglich war. Zudem sind die Produkte optimal konfiguriert worden, damit möglichst alle Schädlinge erkannt werden konnten. Wichtig ist an dieser Stelle zu nennen, dass ausschließlich der signaturbasierte und heuristische Schutz (on-demand/on-access) der Malwarescanner überprüft worden ist. Einige Produkte bieten weitere

Schutzmechanismen an, die beispielsweise ein Virus an seinem Verhalten erkennen (proaktiver Schutz), wenn dieser bereits vom Anwender ausgeführt wurde. Proaktive Schutztechniken wurden nicht analysiert!

Das Malware-Testset bestand aus insgesamt **1.683.364** Samples, welche von jedem integrierten Malwarescanner untersucht würde. Im Detail bestand das Testset aus Windows Viren (**149.202**), Macro Viren (**95.059**), Script Viren (**14.284**), Würmer (**190.952**), Backdoors/Bots (**400.986**), Trojaner (**817.043**) und anderen Schädlingen (**15.838**). Zu nennen ist, dass Agnitum auf die Malwareengine von VirusBuster und BullGuard auf die Engine von BitDefender basiert. Im Einzelnen ergaben sich daraus folgende Resultate:

Pos	Hersteller	erkannte Samples / Erkennung in %
1.	Avira	1.676.963 99,6%
2.	G Data	1.675.358 99,5%
3.	Kaspersky	1.653.991 98,3%
4.	Trend Micro	1.649.191 98,0%
5.	Symantec	1.644.006 97,7%
6.	Eset	1.643.957 97,7%
7.	F-Secure	1.641.228 97,5%
8.	BitDef. & BullGuard	1.624.123 96,5%
9.	McAfee	1.598.078 94,9%
10.	Microsoft	1.580.981 93,9%
11.	Panda Security	1.439.175 85,5%
12.	Agnitum	1.273.142 75,6%

4.) SICHERHEITSEMPFEHLUNGEN VON PROTECTSTAR™

Zu den durchgeführten Testreihen bezüglich Sicherheit der überprüften Security Suites, spricht das ProtectStar™ TestLab einige allgemeine Empfehlungen aus:

Um die Sicherheit einer Security Suite zu erhöhen, sollte jede Lösung mit einem **Passwortschutz** vom Anwender versehen werden. Alle getesteten Produkte 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.: www.protectstar-research.com/de/informationen-passworte.html). Dies verhindert, dass die vollständige Suite oder Teilprodukte wie Anti-Virens Scanner, Personal Firewall, usw. deaktiviert oder sogar deinstalliert werden können. Einige in den Security Suites integrierten Personal Firewalls sind in den Werkseinstellungen größtenteils gut auf die Bedürfnisse des Endanwenders ein-

gestellt. Sollte der Benutzer jedoch die Personal Firewall manuell auf den sogenannten „Lernmodus“ oder „Trainingsmodus“ umstellen (bspw. bei Agnitum und Kaspersky), 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.

Hier wird oftmals schnell „Verbindung blockieren“ angeklickt, was dann wiederum zu weiteren Problemen führt, wenn zum Beispiel der automatische Updatedienst von Windows blockiert wurde. Sofern der Anwender ein (**Heim-)Netzwerk** betreibt und in diesem keine freigegebenen Ordner, Dateien, Drucker, usw. mit anderen Computern des Netzwerkes teilen möchte, so sollte er entsprechend die Netbios-Dienste (bspw. Port 139, 443, usw.) blockieren. Dies müsste bei den Suites von G DATA, Kaspersky und McAfee **manuell** vollzogen werden. Bei den Suites von Agnitum, BitDefender, BullGuard, Eset, Microsoft und

Symantec sollte **nach der Installation** „Mein Computer befindet sich in einem öffentlichen Netzwerk“ o.ä. ausgewählt werden.

Die Security Suites von **Agnitum** und **BullGuard** deaktivieren die Windows-Firewall **nicht** automatisch. Zwar gibt das Programm **BullGuard** dem Anwender nach der Installation eine ausführliche Nachricht darüber, dass die Windows-Firewall vom Benutzer deaktiviert werden sollte. Dennoch geriet dies bei vielen Testpersonen schnell in Vergessenheit. Einen Dual-Betrieb beider Firewalls wird abgeraten.

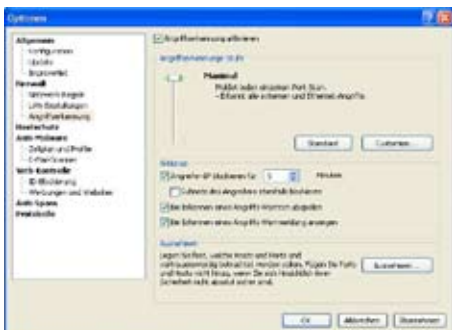
Der Benutzer sollte wissen, dass der Betrieb einer Personal Firewall zusätzliche Prozessorleistung beansprucht und auch die Datenübertragungsgeschwindigkeit verringern kann, sofern größere bzw. große Datenmengen überwacht werden. Zum Beispiel zeigt sich dieses Phänomen bei Online-Computerspielen. Aus diesem Grund schalten einige Gamer ihre Schutzsoftware oftmals während eines Online-Spiels ab.

AVIRA, BitDefender und **G DATA** bieten in ihren Produkten den sog. „**Gaming-modus**“ an, der die genannten Probleme größtenteils durch spezielle Konfigurationseinstellungen an der Firewall und des Malwarescanners unterbinden soll.

F.) TEST: BENUTZER-FREUNDLICHKEIT

Bezüglich der Benutzerfreundlichkeit, sind dem ProtectStar™ TestLab folgende Eigenschaften aufgefallen:

Agnitum OutpostPRO Security Suite 2008 bietet erfahrenen 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 bei möglichen Sicherheitsverletzungen.



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; technisch weniger versierte Benutzer können sich jedoch schnell in der Flut der Warnmeldungen frustriert fühlen, sofern sie die Werkzeugeinstellungen der Suite ändern.

AVIRA Premium Security Suite 2008 bietet Anwendern ausführliche und gute Logdateien bezüglich gefundener Malware. Mit Hilfe des „Expertenmodus“ kann die Suite an individuelle Anwenderwünsche

umfassend angepasst und konfiguriert werden. Die Konfigurationsmöglichkeiten der integrierten Firewall sind für die meisten Anwender ausreichend, jedoch nicht so ausführlich wie beispielsweise bei BullGuard oder Agnitum.



Die Benutzeroberfläche ist übersichtlich doch im Gegensatz zu den anderen Lösungen nicht gerade modern gehalten. Das Update ist auf 24 Stunden eingestellt und sollte vom Anwender nach der Installation auf 1-3 Stunde(n) geändert werden. Eine Bootfähige CD ist nicht vorhanden und kann auch nicht erstellt werden. Allerdings soll dies in der kommenden Version 8.0 (2. Quartal 2008) vorhanden sein.

BitDefender Internet Security 2008 tritt dem Benutzer als eine moderne Lösung mit Personal Firewall, Malwarescanner, Kindersicherung, Anti-Spam und einer Lizenz für den Mobile Antivirens scanner entgegen. Gewöhnungsbedürftig ist allerdings das Hauptmenü der neuen Version 2008: BitDefender hat die



Oberfläche durch vier Buttons neu gestaltet, was eine vereinfachte Handhabung der Security Suite mit sich bringen soll. Es ist zwar korrekt, dass der Benutzer einen schnellen Überblick über den aktuellen Schutzstatus erhält, allerdings vermissen die Testpersonen eine gewohnte Oberfläche mit Einstellungsmöglichkeiten. Diese sind erst nach einer kurzen Suchphase des Benutzers zu finden.

Der Benutzer sollte ausführlichere Warnmeldungen über Attacken aus dem Internet und/oder der vertrauenswürdigen Zone (LAN) im Auslieferungszustand erhalten, ohne erst manuell die entsprechenden Einstellungen vorzunehmen.

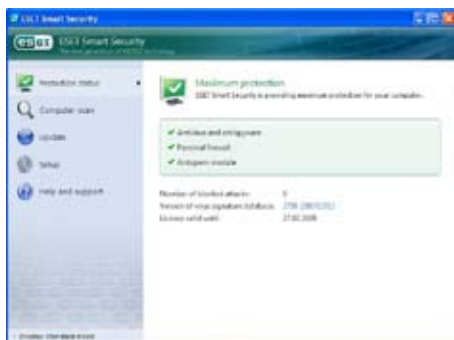
BullGuard 8.0 ist in einigen Ländern noch teilweise unbekannt. Dennoch muss sich die Suite keineswegs vor den bekannten Lösungen verstecken. Bezüglich der Benutzerfreundlichkeit ist den Testern aufgefallen, dass die Konfigurationseinstellungen aufgrund des



übersichtlichen Hauptmenü zwar schnell und einfach zu handhaben sind, allerdings müssen Aktionen wie zum Beispiel „Malware-Scan des Arbeitsplatzes“, usw. in einem separaten Menü/Tab gestartet werden. Dies wird zumindest bei Anwendern, die in der Vergangenheit Lösungen anderer Hersteller verwendet haben, zunächst ungewohnt erscheinen. Die Warnmeldungen über Angriffe aus dem Internet und/oder LAN sind vorbildlich dargestellt und sehr detailliert. Ein http-Scanner, welcher unerwünschte

und gefährliche Inhalte aus Webseiten filtert, gibt es nicht. Ebenso ist keine bootfähige Notfall-CD vorhanden oder kann vom Anwender erstellt werden. Eine benutzerdefinierte Installation ist nicht möglich. Ein hervorragender Live-Support-Chat hilft Benutzern bei Fragen und Problemen.

ESET Smart Security 3.0 bietet sowohl dem erfahrenen, als auch dem weniger technisch versierten Anwender eine hervorragende Suite an:



Je nach Anwendertyp kann die Benutzeroberfläche mit „Toggle Advanced mode“ gewechselt werden. Allerdings ist die Vielzahl an Konfigurationsmöglichkeiten auf den ersten Blick versteckt und kann erst nach kurzer Eingewöhnungszeit unter „Setup“ gefunden werden.

Sehr gut sind neben der übersichtlichen Benutzeroberfläche, die Reportdateien. In den Werkseinstellungen ist besonders hervorzuheben, daß der Anwender nur dann über Vorfälle benachrichtigt wird, sofern diese eine Gefahr darstellen. Nach der Installation ist kein Neustart erforderlich. Allerdings ist die Suite auch lediglich auf die Grundschutzmodule wie Anti-Malwarescanner (Anti-Viren, Anti-Rootkit, Personal Firewall und Anti-Spam) beschränkt. Eine Kindersicherung zum Beispiel werden Anwender vergeblich suchen. Der http-Scanner ist bereits in den Werkseinstellungen aktiviert, allerdings ist keine bootfähige Notfall-CD vorhanden und kann auch nicht erstellt werden.

F-Secure Internet Security 2008

Im Gegensatz zur Vorgängerversion 2007 ist die aktuelle Version 2008 des finnischen Herstellers F-Secure durch modernere Techniken im Bereich der Erkennung von Ad- und Spyware verbessert worden. Die Suite enthält zudem eine Kindersicherung, die optional während der Installation mit installiert werden kann. Die Benutzeroberfläche ist anwenderfreundlich und zeigt nicht nur übersichtlich den Schutzstatus, sondern auch Sicherheitsinformationen (Informationen von F-Secure über neue Schutzfunktionen, Viren im Umlauf, uvm.) seinen Anwendern an.

Im Allgemeinen zeigte sich, dass die Menüführung leichter verständlich ist, als bei den Security Suites von BitDefender, BullGuard, Eset und Symantec. Über den Klick auf „erweitert“ im Hauptmenü lässt sich zudem eine Vielzahl an individuellen Einstellungen vornehmen. Allerdings ist aufgefallen, dass der Benutzer nach der



Installation – im Gegensatz zu allen anderen getesteten Suites - nicht daran erinnert wird, seinen Computer einem vollständigen Malwarescan zu unterziehen. Dies wird jedoch empfohlen. Die Warnmeldungen und Protokolle sind verständlich und für die meisten Anwender ausreichend. Allerdings ist der http-Scanner deaktiviert und muss manuell aktiviert werden. Eine bootfähige Notfall-CD ist zwar erhalten, sie bietet jedoch keine Unterstützung für NTFS-Partitionen und kann auch nicht mit neuen Signaturdaten aktualisiert werden.

G DATA Internet Security 2008

Die aktuelle Internet Security Suite von G DATA zeigt im Vergleich zu seiner Vorgängerversion einige verbesserte Eigenschaften – nicht jedoch eine neue Benutzeroberfläche oder neue Funktionen.



Das Handbuch erklärt nicht nur das Produkt sehr ausführlich, sondern gibt auch allgemeine Tipps zur Computersicherheit. Es liegt der Retailpackung in gedruckter Form bei, befindet sich aber auch als PDF-Datei auf der beiliegenden CD-ROM. Der Installationsumfang kann durch den Benutzer selbst bestimmt werden. Alle einzelnen Optionen sind ausreichend beschrieben und erleichtern die Entscheidung. Alle Meldungen und Protokolle des Programms sind ausführlich und übersichtlich. Jedes Signaturupdate, jeder Virenfund und Suchlauf werden protokolliert. Die Protokolle selbst lassen sich nochmals „erweitert“ betrachten. (Sie zeigen dann nicht gescannte Dateien an). Die Benutzeroberfläche ist klar strukturiert. Per Registerkarte kann man sich durch die einzelnen Elemente der Suite klicken. Durch Doppelklick auf einen Begriff startet die gewählte Option. Insgesamt gefällt die Benutzerfreundlichkeit der Lösung, denn die einzelnen Schutzmodule sind klar voneinander abgegrenzt, das Programm insgesamt sehr übersichtlich gehalten.

Kaspersky Internet Security 7.0 bietet eine benutzerdefinierte Installation. Zudem lässt sich eine Notfall-Boot-CD



Firewall attackiert, so gibt es keine Warn-PopUps oder Hinweise.

Microsoft Live OneCare 2.0

Die Schutzsuite Live OneCare 2.0 von Microsoft präsentiert sich als Komplettpaket zur Sicherheit und Systemwartung des Computers.

Die Installation der Lösung dauerte überdurchschnittlich lange, da der Anwender trotz einer Installations-CD aus dem Internet weitere Daten nachladen muss. Das Hauptmenü wirkt auf den ersten Blick ungewohnt und aufgrund von viel Text und Beschriftungen unübersichtlich. Dennoch ist die Oberfläche aufgeräumt und sämtliche Informationen wie „Virus- und Spywareüberwachung“, „Letzter Virus- und Spyware-Scan“, uvm. sind für den Benutzer

aus dem Programm heraus erstellen. Dazu ist allerdings das Zusatzprogramm BartPe (kostenlos als Download erhältlich) notwendig und ist für unerfahrene Anwender insgesamt etwas kompliziert zu handhaben. Die Security Suite von Kaspersky zeichnet sich zudem über eine moderne Benutzeroberfläche, ein umfangreiches Berichtswesen und einen guten Taskplaner aus. Spam- oder verdächtige Mails lassen sich direkt auf dem Server löschen. Die Restlaufzeit der Lizenz wird übersichtlich im Programmfenster angezeigt. Upgrades auf Nachfolgeversionen sind während der Lizenzlaufzeit möglich.

McAfee Internet Security 2008

Die Installation der Security Suite von McAfee verläuft problemlos und sehr anwenderfreundlich. Nach der Installation ist kein Neustarter erforderlich. Die Oberfläche ist übersichtlich gehalten und spricht vor allem Heimanwender an, die sich nicht mit technischen Einstellungsmöglichkeiten und dem Fachjargon der IT-Sicherheit beschäftigen möchten. Allerdings wirkt die Benutzeroberfläche etwas antiquiert. Sie wurde seit den letzten Versionen von McAfee kaum erneuert. Wird die integrierte

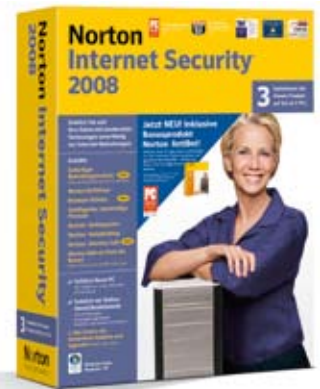


gut sichtbar. Außerdem helfen farbliche Hervorhebungen dem Anwender, welche Aktionen seinerseits erforderlich sind (bspw. Signaturupdate oder Konfiguration der Datensicherung). Außerdem bietet die Lösung einen komfortablen Zugang zu Windowsfunktionen und Systemoptimierungen.

Norton Internet Security 2008

Die Installation dauerte im Vergleich zu anderen Lösungen überdurchschnittlich lange. Es gibt keinerlei Möglichkeiten die Installation nach Anwenderwünschen zu beeinflussen, einzelne Module abzuwählen oder den Installationspfad zu ändern.

Auch die Suite von Symantec verlangt keinen Neustart des Windows



Betriebssystem, sondern ist (fast) einsatzbereit: Symantec besteht zwingend auf die Einrichtung eines Kundenaccounts. Andernfalls lässt sich die Installation nicht abschließen. Nach Fertigstellung der Installation stehen drei Module zur Verfügung: Norton Auto-Protect (der Echtzeitscanner), das Norton-Security-Center (es bietet eine Übersicht über den Status der Suite - aber auch das Windows-eigene Sicherheitscenter lässt sich einbinden) und die eigentliche Programmoberfläche, genannt „Internet Security 2008“. Aufgefallen ist, dass die Firewall weitestgehend automatisiert ist und selbständig genutzte Anwendungen und auch Online-Games erkennt und konfiguriert. Allerdings sind in Sachen Benutzerfreundlichkeit die relativ geringen Konfigurationsmöglichkeiten zu erwähnen. Es lässt sich lediglich die Heuristik („Bloodhound“) zuschalten.

Erwähnenswert ist, dass Symantec ein neues Sicherheitsmodul namens „Norton AntiBot“ als kostenlosen Download für sein Produkt „Norton Internet Security 2008“ (sowie Norton AntiVirus 2008 und Norton 360) zur Verfügung gestellt hat. Norton AntiBot arbeitet Signatur-unabhängig (Prozessbeobachter) und erkennt Schadcodes zuverlässig am jeweiligen Verhalten.

Panda Internet Security 2008

Die Installation der umfangreichen Software verläuft reibungslos und anwenderfreundlich. Bereits während





der Installation der Suite prüft ein Malwarescanner nach evtl. Schadsoftware. In den meisten Fällen fand dieser Scanner bereits während der Installation auf den Testrechnern vorhandene Spyware. Die Menüoberfläche ist seit der letzten Version nicht bzw. nur gering verändert worden. Zudem steht Anwendern kein Handbuch zur Verfügung, sondern lediglich eine Onlinehilfe.

Im Gegensatz zu früheren Versionen von Panda Security ist die aktuelle Version mit einem Backup-Tool und einem neuen Feature ausgestattet: dem Online-Scanner Totalscan Pro. Er untersucht den Rechner zusätzlich auf Schädlinge und leitet Informationen über infizierte Dateien zur Analyse an den Hersteller weiter. Dadurch verspricht der Hersteller allen Benutzern der Software schnell(er) ein Signatur-Update zur Verfügung stellen zu können.

Trend Micro Internet Security 2008

Die Security Suite von Trend Micro tritt seinem Anwender mit einer der übersichtlichsten und aufgeräumtesten Benutzeroberflächen – im Vergleich zu seinen zwölf getesteten Konkurrenten



- entgegen. Sämtliche Einstellungen und Menüführungen sind sofort und auf einen Blick erkennbar. Optimaler Einsatz von Farben und Symbolen machen die Menüführung sowohl für den Anfänger als auch fortgeschrittenen Internetuser zum Kinderspiel.

Benutzerfreundlich sind ebenfalls die Optionen, die Anwender festlegen können, wie sich das Programm zu einem bestimmten Zeitpunkt verhalten soll. Wann und wie erfolgt ein Scan oder die Aktualisierung. Ist evtl. sogar eine Eigendiagnose notwendig um das Schutzniveau aufrecht zu erhalten. Möchte man mit Pop-Ups oder/und mit akustischen Signalen bei der Erkennung von Vorfällen gewarnt werden uvm.

G.) TEST: PERFORMANCE

Wie bereits in „Allgemeine Erläuterung der Testverfahren“ genannt, ist die Performance – also die Leistungsfähigkeit und Geschwindigkeit eines Produktes - sehr entscheidend:

Moderne Security Suites - wie die vom ProtectStar™ TestLab überprüften 13 Produkte - enthalten eine Vielzahl an einzelnen Schutzmodulen die zusammen in der sog. **Internet Security Suite** vereint werden.

Zu diesen Schutzmodulen gehören in der Regel immer ein **Anti-Malwarescanner**, eine **Personal Firewall** und ein **Anti-Spam Filter**. Sie sind in allen Security Suites in der einen oder anderen Form als Mindestmaß enthalten. ESET Smart Security 3.0 hat sich ausschließlich auf diese **drei Grundschutzmodule** beschränkt. Norton Internet Security 2008 von Symantec bietet den Anti-Spam Filter beispielsweise nur in einem kostenlosen Add-On Pack mit integrierter Kindersicherung an. Alle anderen analysierten Security Suites wie die von BitDefender, BullGuard, GDATA, Kaspersky, McAfee, Microsoft, Panda Security und Trend Micro enthalten in der Auslieferung weitere Schutzmodule und Programme, die zum Teil weit über die drei

Grundschutzkomponenten hinaus gehen. In den vergangenen Jahren sind zunehmend weitere Schutzkomponenten in die Security Suite integriert worden, wie Angriffsprävention (Intrusion Prevention), Personal Wireless Network Monitor, Internet- und E-Mail-Steuerung, Suche nach Sicherheitslücken (Schwachstellenbewertung), Anti-Phishing, Anti-Pharming, Wurmschutz, uvm. Immer häufiger finden sich darüber hinaus zusätzliche Tools wie ein PC-Reinigungsassistent, Datensicherung/Backup, Datenschredder, Systemoptimierung und eine Kindersicherung wieder.

Alle in den Security Suites genannten Sicherheitsmodule und Tools bieten dem Benutzer auf der einen Seite ein **höheres Maß an Sicherheit** und **Benutzerfreundlichkeit**, auf der anderen Seite jedoch wird aufgrund der Vielzahl an Schutzkomponenten der Prozessor zum Teil stark **ausgelastet**. Dies zeigt sich durch Verzögerungen beim Seitenaufbau im Internet. Das Starten von Programmen und auch der Systemstart werden verzögert. Je nach Schutzlösung und Konfiguration können die Verzögerungen durchaus 75% und mehr betragen, als ohne Security Suite.

Eine Regel wie zum Beispiel „Je mehr Produkte in einer Suite enthalten, desto mehr wird der Computer ausgebremst“ kann generell jedoch **nicht** aufgestellt werden. Vielmehr liegen die Gründe an den unterschiedlichen Einstellungen der im Hintergrund aktiven „Schutzwächter“ wie Anti-Malwarescanner, Personal Firewall, usw. sowie deren Ressourcenverbrauch des Arbeitsspeichers. **Norton Internet Security 2008** zeigt beispielsweise auf Computersystemen mit lediglich 256 bis 512 MB Hauptspeicher unter Windows XP/Windows Vista ungewohnte Performanceeinschränkungen. Ein Arbeiten auf solch ausgestatteten Systemen mit der Suite ist daher nur in Ausnahmefällen sinnvoll. Die Computersysteme auf denen **F-Secure**



Internet Security 2008 installiert wurde, verlangsamten sich zunächst stark nach dem ersten Neustart der Computer; egal ob es sich um ein ältere oder moderne Computersystemen mit Intel QuadCore Prozessoren und 4 GB Hauptspeicher handelte. Der Grund hierfür liegt darin, dass sich die Suite nach der Installation über das Internet aktualisiert und zugleich aktive Programme und Dienste scannt. Der Anwender wird darüber nur über das Icon bei der Systemuhr unter Windows informiert. Anwendern wird empfohlen, den Computer nach der Installation der Suite von F-Secure circa zwei bis vier Minuten „ruhen“ zu lassen, damit sich die Software erfolgreich aktualisieren und die Installation vervollständigen kann.

G DATA Internet Security 2008 bildet in Sachen Performance einen Spezialfall: Aufgrund der beiden integrierten Anti-Malwarescanner wird das System beim Rechnerstart und dem Öffnen von Dateien und Programmen verzögert. Anwender sollten daher einen leistungsstarken Computer besitzen, um nicht allzu starke Verzögerungen in Kauf nehmen zu müssen. Überhaupt wird einem Betrieb der Suite auf älteren Computersystemen mit weniger als 512 MB Hauptspeicher abgeraten. Allerdings kann sich durch diverse Einstellungen die Performance verbessern. Insbesondere der Wächter

lässt sich genau den eigenen Wünschen anpassen. In der Werkseinstellung sind beide Engines aktiv (Performance optimiert) und können individuell an die Bedürfnisse des Anwenders angepasst werden, wodurch sich eine Performancesteigerung ergeben kann; allerdings auch etwas auf Kosten der Sicherheit.

Einen durchweg **positiven Eindruck** in Sachen Performance hinterließen die Security Suites von **AVIRA, BitDefender, ESET, McAfee, Microsoft, und Trend Micro**. Die **Outpost PRO Security Suite 2008** von Agnitum und **Norton Internet Security 2008** von Symantec zeigten beispielsweise in den Werkseinstellungen durchschnittlich gute Performanceeigenschaften. Allerdings werden diese stark eingeschränkt, sofern der Anwender die Standardeinstellung auf „maximale Sicherheitsstufe“ ändert. Zugleich generiert sich eine enorme Menge an Warnmeldungen.

AVIRA Premium Security 2008, McAfee Internet Security 2008, Microsoft Live OneCare 2.0 und Trend Micro Internet Security 2008 bieten **gute Performanceeigenschaften**, selbst auf älteren Computersystemen mit lediglich 512 MB Hauptspeicher. Der **Spitzenreiter** im Test im Bereich der Performance ist ungeschlagen: **ESET Smart Security**

3.0. Es wurde ebenfalls festgestellt, dass die von den Herstellern angegebenen technischen **Mindestanforderungen** i.d.R. lediglich ein absolutes **Minimum** darstellen, um die jeweilige Schutzlösung überhaupt installieren zu können. Ein reibungsloses Arbeiten ist jedoch nicht möglich gewesen und zeigte sich durch enorme Verzögerungen in den unterschiedlichen Bereichen (Starten von Programmen, Seitenaufbau im Internet, etc.).





H.) Test: PREIS-/AUSSTATTUNGSVERHÄLTNIS

Hersteller	Preis (Box)	Preis (Download)	Amazon-preis	Lizenzen	Inhalt (Software)	PUNKTE max. 20	Bewertung
Agnitum	49,95	49,95	---	1x	AV, FW, PF, AS	14	befried.
Avira	39,95	39,95	31,95	1x	AV, FW, PF, AS, KS, (BP)	16	gut
BitDefender	29,95	29,95	20,95	1x	AV, FW, PF, AS, KS, ID	19	sehr gut
BullGuard	69,95	69,95	46,99	3x	AV, FW, PF, AS, BP	15	befried.
Eset	44,95	44,95	---	1x	AV, FW, PF, AS	14	befried.
F-Secure	39,95	37,95	30,45	1x	AV, FW, PF, AS, KS	15	befried.
G Data	39,95	35,95	29,95	1x	AV, FW, PF, AS, WF, DS	18	sehr gut
Kaspersky	48,45	39,95	28,95	1x	AV, FW, PF, AS, WF, KS, ID	15	befried.
McAfee	69,95	69,95	---	3x	AV, FW, PF, AS, KS, BP	15	befried.
Microsoft	49,95	49,95	47,95	3x	AV, FW, PF, BP, ST	16	gut
Panda	69,95	69,95	49,99	1x	AV, FW, PF, AS, KS, BP, ID, ON	15	befried.
Symantec	29,99	29,99	25,95	1x	AV, FW, PF, AS, KD, ID, AB	20	exzellent
Trend Micro	49,95	49,95	48,95	3x	AV, FW, PF, AS, KS, ID, WiFi	18	sehr gut

Legende:

AV = Antiviren-Scanner
 FW = Firewall
 PF = Phishingfilter
 KS = Kindersicherung
 BP = Backup
 ID = Identitätsschutz
 WF = Webfilter
 DS = Datenschredder
 ON = Onlinescanner
 ST = Systemtuner
 WiFi = WLAN Schutz
 AB = Norton AntiBot

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 gravierende Unterschiede bestehen. Ein Preisvergleich lohnt daher immer. Viele Hersteller locken mit

vergünstigten Folge-lizenzen oder Rabatten, wenn man gleich eine mehrjährige Laufzeit von zwei oder drei Jahren bestellt.

Auch hier sollte man berechnen, ob das Angebot eines Onlineversandhauses nicht doch preiswerter ist. Eine weitere Falle droht bei Mehrfachlizenzen. Wer meint, damit günstig eine lange Laufzeit einzukaufen, kann irren.



I.) FAZIT

Bevor nun das finale Ergebnis dieses Vergleichstest bekannt wird, müssen zunächst einige wesentliche Erkenntnisse erwähnt werden: Die perfekte Security Suite gibt es nicht. Das hat dieser Vergleichstest eindeutig bewiesen. Keine der getesteten Security Suites erwies sich als schlecht, aber auch keine wiederum als wirklich ausgezeichnet.

Eine Suite, die eine starke Personal Firewall besitzt und auch sonst durchwegs gute Resultate zeigt, patzt leider an der Malwareerkennungsrate. Beispielsweise „Agnitum Outpost Security Suite 2008“ und „Microsoft Live OneCare 2.0“ sind hier zu erwähnen. Dieses Malheur sorgt insgesamt für einen Punkteabzug bei beiden Suites, die doch in allen anderen Testbereichen stets gute bis sehr gute Resultate

erzielten. Besonders zu spüren bekommt dies die Suite von **Panda Security** und von **Agnitum**.

Durch eine Malwareerkennungsrate von 75,6% bildet Agnitum nicht nur das Schlusslicht in der Erkennungsrate der getesteten Produkte, sondern belegt punktuell gesehen auch den letzten Platz in diesem Vergleichstest.

Interessenten wird daher empfohlen, die Firewall-Einzelplatzlösung von „Agnitum OutPost Pro Firewall 2008“ näherer Betrachtung zu unterziehen und als Anti-Virens Scanner ein Produkt eines anderen Herstellers wie beispielsweise Avira/G DATA/ESET / Symantec einzusetzen. **G DATA Internet Security 2008** und **Trend Micro Internet Security 2008** zei-

gen sehr gute Resultate. Allerdings erhalten beide Suites Punkteabzug aufgrund der gefundenen Mängel im Bereich der inneren Schutzwirkung der Firewall.

ESET Smart Security 3.0 erhielt einen leichten Punkteabzug in der Malwareerkennung und im Preis-/Ausstattungsverhältnis, so dass der Hersteller Eset eine Topplatzierung ganz **knapp verfehlt**.

Wertet man die Testreihen bezüglich Sicherheit, Benutzerfreundlichkeit, Performance und Preis-/Ausstattungsverhältnis gemäß den festgelegten Bewertungskriterien (Vgl. C – Bewertungskriterien) aus, so werden im Detail folgende Punkte erzielt:

HERSTELLER	SICHERHEIT (Außen/Innen./Malw./Sonst.)	BENUTZERFREUND. & PERFORMANCE	PREIS-/ AUSSTATTUNG	PUNKTE	%
Symantec	30 / 20 / 42.7 / 05	36 / 35	20	188.7	94.35%
Trend Micro	30 / 18 / 43.0 / 04	39 / 36	18	188.0	94.00%
Avira	30 / 20 / 44.6 / 03	36 / 38	16	187.6	93.80%
G DATA	30 / 18 / 44.5 / 05	38 / 33	18	186.5	93.25%
ESET	30 / 20 / 42.7 / 03	36 / 40	14	185.7	92.85%
BitDefender	30 / 20 / 41.5 / 04	35 / 35	19	184.5	92.25%
F-Secure	30 / 20 / 42.5 / 04	37 / 32	15	180.5	90.25%
BullGuard	30 / 20 / 41.5 / 04	35 / 35	15	180.5	90.25%
Microsoft	30 / 20 / 38.9 / 03	36 / 37	16	180.9	90.45%
Kaspersky	30 / 17 / 43.3 / 04	36 / 35	15	180.3	90.15%
McAfee	30 / 17 / 39.9 / 03	36 / 37	15	177.9	88.95%
Panda	30 / 20 / 30.5 / 04	36 / 35	15	170.5	85.25%
Agnitum	30 / 20 / 20.6 / 04	36 / 34	14	158.6	79.30%



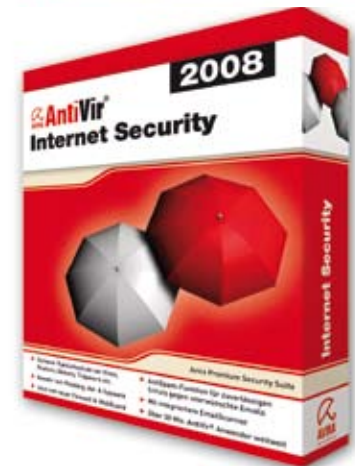
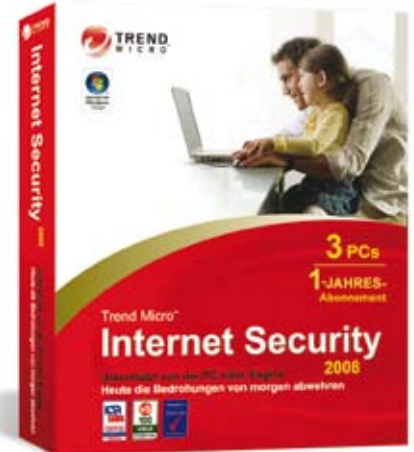
Laut dem Punktebewertungssystem (maximal erhältliche Punktzahl 200) gehen die Plätze 1 bis 3 an folgende Security Suites:

1. Platz mit 188.7 Punkten an:
Norton Internet Security 2008

2. Platz mit 188.0 Punkten an:
Trend Micro Internet Security 2008

3. Platz mit 187.6 Punkten an:
Avira Premium Security Suite 2008

Der **Testsieger** dieses großen Vergleichstests ist das Produkt **NORTON INTERNET SECURITY 2008** von **SYMANTEC**. Aufgrund der sehr knappen und äußerst nah zusammenliegenden Punkteplatzierung - mit einer Differenz von lediglich einem Punkt und weniger - hat sich das ProtectStar™ TestLab dazu entschieden, alle drei Erstplatzierten Security Suites mit dem **ProtectStar™ AWARD 2008** auszuzeichnen.



J.) FAZIT II (Empfehlungen)

Ein Punktebewertungssystem wie in I.) **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.

Erfahrene Anwender und Profis steigen zum Beispiel auf Einzellösungen verschiedener Hersteller um. Nicht zuletzt setzt diese Benutzergruppe auch mehrere Anti-Virencanner im Dualbetrieb ein, um sich so die bestmögliche Security Suite selbst zu erstellen.

Sowohl für den erfahrenen als auch weniger technisch versierten Anwender – sei es im Home- oder auch Businessbereich – kann das ProtectStar™ TestLab die beiden Schutzlösungen **G DATA Internet**

Security 2008 und **ESET Smart Security 3.0** empfehlen. Das Produkt von **G DATA** glänzt mit einer umfangreichen Ausstattung, Dual-Malwarescannern sowie hoher Benutzerfreundlichkeit und **ESET** mit einer unschlagbaren Performance sowie hervorragenden Sicherheitsmodulen.

Beide Lösungen werden 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 wohlthätige 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

Copyright by ProtectStar™, Inc. Alle Rechte vorbehalten. Alle Texte, Bilder, Grafiken, etc. unterliegen dem Urheberrecht und anderen Gesetzen zum Schutz geistigen Eigentums. Insbesondere dürfen Nachdruck, Aufnahme in Online-Dienste, Internet und Vervielfältigung auf Datenträger wie CD-ROM, DVD-ROM usw., auch auszugsweise, nur nach vorheriger schriftlicher Zustimmung durch die ProtectStar™, Inc. erfolgen.

Sie dürfen weder für Handelszwecke oder zur Weitergabe kopiert, noch verändert und auf anderen Webseiten verwendet werden. Einige Texte, Bilder, Grafiken, usw. der ProtectStar™, Inc. enthalten auch Material, die dem Urheberrecht derjenigen unterliegen, die diese zur Verfügung gestellt haben.

Die Informationen stellt die ProtectStar™, Inc. ohne jegliche Zusicherung oder Gewähr für die Richtigkeit, sei sie ausdrücklich oder stillschweigend, zur Verfügung. Es werden auch keine stillschweigenden Zusagen betreffend die Handelsfähigkeit, die Eignung für bestimmte Zwecke oder den Nichtverstoß gegen Gesetze und Patente getroffen.

Kontakt

Corporate Headquarter:

ProtectStar, Inc.
TestLab
1901 60th Place
Suite L3604
34203 Bradenton, FL
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