PROTECTSTAR™

Großer Vergleichstest

Internet Security Suiten 2010

INHALTSVERZEICHNIS:

Seite 2		Inhaltsverzeichnis
Seite 3		A) Getestete Produkte und Versionen
Seite 3		B) Allgemeine Erläuterung der Testverfahren
Seite 4		C) Bewertungskriterien
Seite 5		D) Test SICHERHEIT
		1. DIE FIREWALL – der äußere Schutz
		2. DIE FIREWALL –der innere Schutz
		3. DIE MALWAREERKENNUNG
		4. Empfehlungen von PROTECTSTAR
Seite 10		E) Test BENUTZERFREUNDLICHKEIT & PERFORMANCE
Seite 16		F) Test SCANZEITEN (Kurztest)
Seite 17		G) Test PREIS-/AUSSTATTUNGSVERHÄLTNIS
Seite 18		H) Fazit
Seite 20		Anregungen, Kritik und Spenden
Seite 20		Kontakt & Copyright

A) Getestete Produkte und Versionen

Hersteller	Produktname	Release/Version
AVG	Internet Security 9.0	9.0.663
Avira	Premium Security Suite	9.0.0.381
BitDefender	Internet Security 2010	13.0.16.313
BullGuard	Internet Security 8.7	8.7
ESET	Smart Security 4.0	4.0.467
F-Secure	Internet Security 2010	k.A.
G DATA	Internet Security 2010	20.2.0.6
Kaspersky	Internet Security 2010	9.0.0.463
McAfee	Internet Security 2010	k.A.
Norman	Security Suite	7.30
Symantec	Norton Internet Security 2010	17.0.0.136

k.A. = Keine Angabe, da im Programm selbst nicht angezeigt

B) Allgemeine Erläuterung der Testverfahren

Getestet wurde sowohl unter Labor- als auch realen Bedingungen.

Im Bereich der **SICHERHEIT** liegt der Fokus auf dem äußeren und inneren Schutz der in den Security Suiten integrierten Personal Firewall. Das Hauptaugenmerk hierbei, die werkseitigen Einstellungen, also der Auslieferungszustand der Suite.

„Äußerer Schutz“ bedeutet, dass die Sicherheitsüberprüfung mit einem direkt an das Intenet angeschlossenen Computer erfolgt. Zum Beispiel via Direktanschluß des Computers am DSL-Modem (nicht Router, Hardware-Firewall, o.ä.).

„Innerer Schutz“ bedeutet, die Durchführung von Sicherheitstests der Personal Firewall, wenn der entsprechende Computer im LAN eingebunden ist. Ein LAN (bspw. Heim- oder Firmennetzwerk) gilt als vertrauenswürdige Zone und wird daher von vielen Firewalls nur mit niedrigeren Sicherheitseinstellungen überwacht.

In diesem Bereich soll daher analysiert werden, was passieren könnte, wenn ein LAN-Rechner bereits verseucht ist, oder ein Gast-Computer als „Angreifer“ agiert.

Die umfangreichen Bestimmungen und Analysen der Malwareerkennungsraten fanden in Kooperation mit der gemeinnützigen Organisation **AV-Comparatives** e.V. (www.av-comparatives.org) statt. Der in diesem Bereich verwendete Begriff „Malware“ beinhaltet sowohl Viren, Würmer, Trojaner und andere Schädlinge. Im Bereich der **BENUTZERFREUNDLICHKEIT** primär Installation, Deinstallation, Verständlichkeit der Meldungen sowie die individuellen Einstellungs- und Konfigurationsmöglichkeiten; sowohl während der Installation als auch im aktiven Betrieb. Weitere Augenmerke liegen auf dem Handbuch (teilweise im Lieferumfang als gedruckte Version enthalten) und dessen Verständlichkeit, der Onlinehilfe und bereitgestellten FAQs.

Fragen nach der Verfügbarkeit einer bootfähigen Rettungs-CD/DVD oder der Möglichkeit selbst eine Rettungs-CD erstellen zu können runden diesen Themenblock ab.

Im Segment der **PERFORMANCE** stehen für die Security Suiten eine Vielzahl unterschiedlicher Rechnersysteme zur Verfügung:

Ausstattungsmerkmale der Testrechner (von – bis):

Betriebssystem: Windows XP mit SP 3 und/oder Windows Vista mit SP2 und/oder Windows 7

CPU: 1000MHz [Single Core] – 2.660 MHz [Quad-Core] (Durchschnitt: 1.8GHz Dual Core)

Ram: 512–8.192 MB SD-Ram und DDR-Ram (Durchschnitt: 2048 MB DDR-Ram)

Festplatte: 30–1.000 GB, IDE und S-ATA (Durchschnitt: 250 GB S-ATA Festplatte)

Außerhalb der Testreihen gab es Bewertungen bezüglich der Mindestanforderungen an die Systeme lt. Herstellervorgaben. Hier lag das Augenmerk speziell auf der benutzergerechten Anwendbarkeit des jeweiligen Produktes.

PREIS-/AUSSTATTUNGSVERHÄLTNIS: Wie stehen Preis und Ausstattung einer Security Suite zueinander? Welche zusätzliche Software wie bspw. Backup, Tuning, usw. werden dem Anwender ausgeliefert und wie viele Lizenzen sind enthalten?

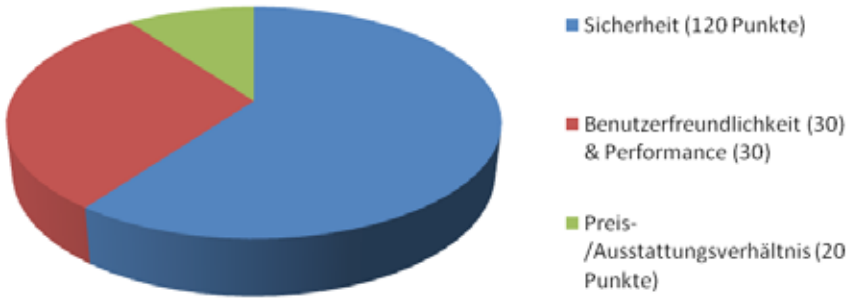
Darüber hinaus wird der Preisunterschied zwischen einer Box- und Downloadversion beim Hersteller gegenüber dem sog. „Straßenpreis“ am Beispiel des Onlineversandhauses Amazon verglichen.

C) Bewertungskriterien

Bei allen getesteten Security Suiten handelt es sich ausschließlich um Sicherheitslösungen, die dem Anwender Schutz vor modernen Gefahren wie Hackern, Trojanern, Viren, Rootkits, Keyloggern, Phishing-Angriffen, uvm. versprechen und vor allem auch gewährleisten sollen. Da es sich also um **Sicherheitsprodukte** handelt, muss das Haupt-augenmerk zwangsläufig auch auf die enthaltenen Schutzfunktionen der jeweiligen Suite gelegt werden.

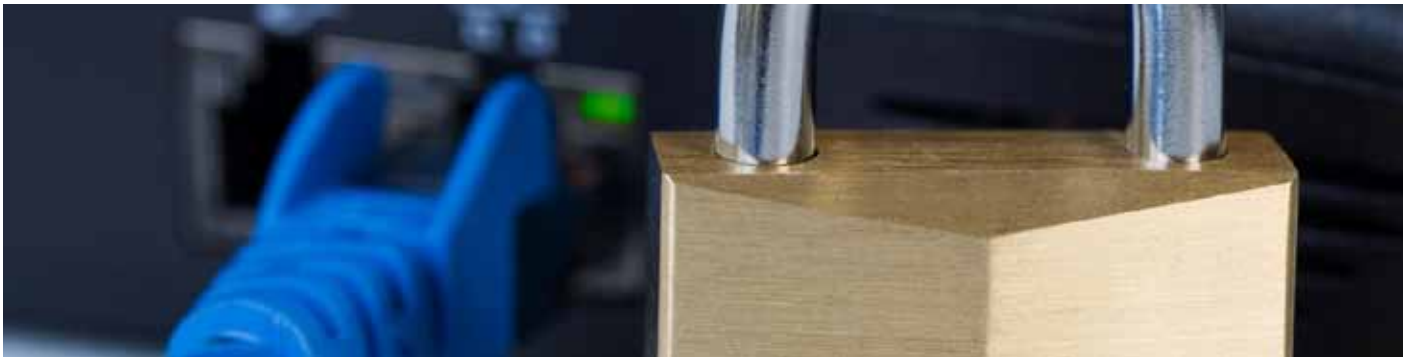
Sowohl die **Benutzerfreundlichkeit** als auch die **Performance** sind neben der Sicherheit vor allem in der Praxis essentiell. Aus diesem Grund sollen sich beide Bereiche zu jeweils gleichen Tei-len in der Bewertung widerspiegeln. Weniger essentiell für die Sicherheit eines Produktes, aber dennoch erwähnenswert ist der Testbereich des **Preis-/Ausstattungsverhältnis**. Eine moderne Security Suite sollte unabhängig von ihrem höheren oder niedrigeren Verkaufspreis einen maximalen Schutz gewährleisten. Hier soll der Anwender nicht durch zusätzliche Features wie Tuning- und Backup-Programmen oder weiteren Lizenzen zum Kauf beeinflusst werden. Auf der anderen Seite jedoch ergeben sich besondere Preisvorteile für den Anwender, wenn er durch den Kauf einer Suite kein separates Backupprogramm mehr erwerben müsste, wenn eine gleichwertige Speicherlösung bereits in dem Produkt enthalten ist.

Aus den genannten Gründen wird sich das Preis-/Ausstattungsverhältnis lediglich zu **zehn Prozent** in der Gesamtbewertung wiederfinden. Die Sicherheitsexperten von **ProtectStar™** haben sich daher – wie auch in den vergangenen Jahren - 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 Punktzahl ist so aufgeteilt, dass bis zu **40** Punkte für den äußeren Schutz der Firewall und **20 Punkte** für den inneren Schutz zu vergeben sind. Insgesamt **50 Punkte** können an den Testbereich der Malwareerkennung vergeben werden. Dabei können die Produkte bis zu **25 Punkte** für die **On-Demand** und nochmals **25 Punkte** für die **retrospektive** (heuristische) Malwareerkennung verdienen.



Bei der **On-Demand Malwareerkennung** werden pro fehlendem Prozentpunkt in der Erkennungsrate **1.0 Punkte** und bei der **retrospektive Malwareerkennung 0.1 Punkte** abgezogen.

Die retrospektive Erkennung kann generell als Ergänzung zur herkömmlichen Malwareerkennung (On-Demand Erkennung) betrachtet werden. Bis zu **10 weitere Punkte** können für sonstige Sicherheitsfunktionen wie die Qualität der Warnmeldungen, Log-Dateien, Intrusion Prevention Systeme, Hostprotection, mehrere Anti-Virenscanner, HIPS, Behaviorblocker, usw. vergeben werden. Für die beiden Testbereiche **Benutzerfreundlichkeit** und **Performance** werden insgesamt **60 Punkte** vergeben. Jeder Bereich kann dabei maximal **30 Punkte** erhalten. Zuletzt können für den Testbereich **Preis-/Ausstattungsverhältnis** bis zu **20 Punkte** an die Security Suiten vergeben werden.



D) Test: SICHERHEIT

1.) DIE FIREWALL – der äußere Schutz

Jede durch das ProtectStar™ Test Lab bewertete Security Suite enthält eine integrierte Firewall, die ein- und ausgehende Verbindungen überwacht. Analysiert wurden die Firewalls in den Werkseinstellungen, also in den jeweiligen Konfigurationen des Auslieferungszustandes.

Die Firewalls sind – wie bereits in „Allgemeine Erläuterung der Testverfahren“ erwähnt – auf zweierlei Weise analysiert worden: Zum einen der **äußere Schutz** der Schutzmauer (Angreifer -> Internet -> Testrechner) und zum anderen der **innere Schutz** (Angreifer -> LAN -> Testrechner).

Die in den Security Suiten integrierten Firewalls haben in den Durchläufen bezüglich des äußeren Schutzes, alle zum Testzeitpunkt bekannten **20.890** differenten **Angriffs- und Sicherheitstests** erfolgreich bestanden (Stand: November 2009). Getestet wurden die 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 drei Gefahrenstufen (Low, Medium, High) im Bereich der DoS-Angriffe, zum Beispiel im „Microsoft SMS Client“, „ping of death“, „RPC DCOM Interface DoS“ und „WinLogon.exe DoS“, uvm. und aus den Bereichen Microsoft Bulletins- und Windows-Angriffe gehörten zum Beispiel „Buffer Overrun in Messenger Service (828035)“, „Buffer Overflow in Windows Troubleshooter ActiveX Control (826232)“, uvm. zur Testauswahl. 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** 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 **13609** (Stand: November 2009) weitere Sicherheitstests und Angriffstaktiken auf die Firewalls ausführte, als auch durch die manuell durchgeführten Prüfungen konnten keine Schwachstellen oder Sicherheitsrisiken festgestellt werden. Den einstündigen Dauer-Penetrationstest absolvierten die Firewalls ebenfalls **erfolgreich**, ohne nennenswerte Performanceverluste. Auch in diesem Jahr zeigte glücklicherweise **keine** Firewall im Bereich des **äußeren Schutzes** irgendwelche Sicherheitsrisiken. Allerdings werden wieder die Warnhinweise, Logdateien und Warnbenachrichtigungen via Pop-Up bemängelt, welche dem Anwender während eines Angriffs angezeigt werden. Sie könnten zum Teil bei einigen Produkten verbessert oder die Angriffe entsprechend ihrer Priorität sortiert werden. Bei den Warnhinweise / Alarmmeldungen zeigten sich die Produkte von **Avira**, **BitDefender**, **BullGuard**, **F-Secure**, **Kaspersky** und **Symantec** bereits in den Werkseinstellungen **vorbildlich**. Besonders lobenswert im Bereich der Konfigurationsmöglichkeiten sind die Firewalls **AVG**, **BitDefender**, **BullGuard** und **Norman**. Bei diesen Produkten lassen sich Einstellungen bis in das kleinste Detail vornehmen. Allerdings sollte der Anwender auch ausreichend Erfahrung und Wissen bezüglich IT-Sicherheit mitbringen, bevor er manuell die Regeln modifiziert oder gar neu definiert. Nur allzu wenig hat sich bei den aktuellen Security Suiten 2010 in Sachen „Angriffserkennung und Angriffstechniken“ getan. Die Schutzsuiten erkennen auch dieses Jahr wieder kaum unterschiedliche Angriffstechniken. Die Mehrheit der analysierten Suiten beschränkt in diesem Bereich lediglich auf das Melden von entdeckten Portscans und simplen Angriffsformen. Spezielle Brute-Force Attacken und Denial of Service Attacken werden zwar geblockt, jedoch erhielt der Anwender über diese – zum Teil aggressiven Angriffsarten - keine Meldungen; selbst dann nicht, wenn diese Angriffe permanent andauerten.

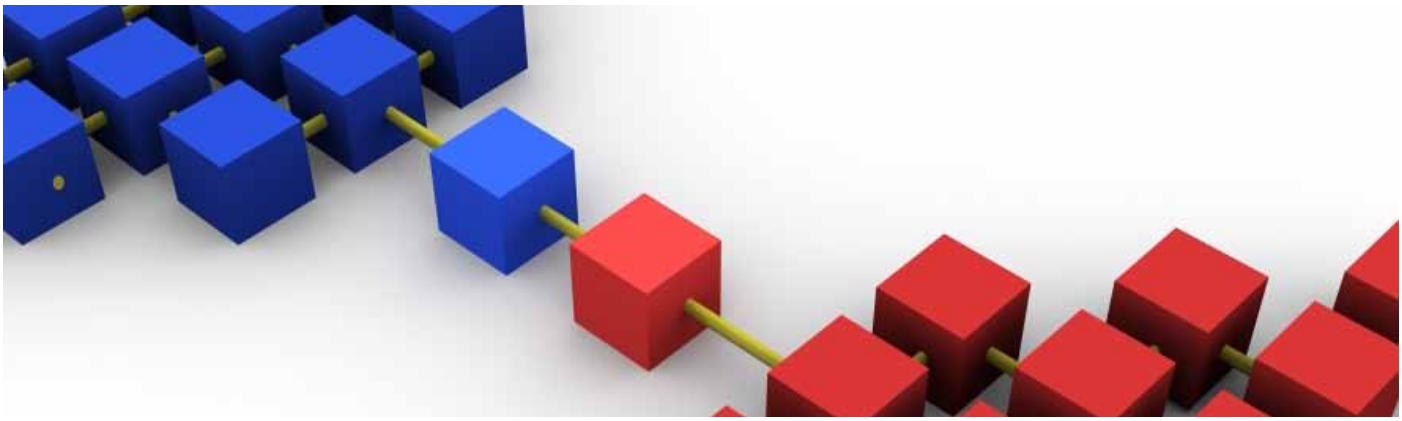
2.) DIE FIREWALL – der innere Schutz

Der vorhergehende Test zeigt, dass alle Firewalls **ausreichend Schutz** gegen Angriffe aus dem Internet bieten. Wie sieht es aber aus, wenn ein Computersystem direkt aus einer vertrauenswürdigen Zone - wie dem LAN – angegriffen wird?

Die Sicherheitsexperten des ProtectStar™ Test Lab analysierten daher auch in diesem Jahr wieder die Firewalls in den Werkeinstellungen bezüglich der Schutzwirkungen im LAN mit differenten **Angriffs- und Sicherheitstests**. Getestet worden sind die aktuell bekannten **Denial of Service** (DoS)-Angriffsarten, sowie **Schwachstelle**n in Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und andere Sicherheitschecks.

Die meisten Produkte zeigen hier wie auch schon in anderen publizierten Testreihen einige **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 Werkseinstellungen „anwenderfreundlicher“ für die vertrauenswürdige Zone.

Dadurch sind die Computer in der Lage im Netzwerk beispielsweise Dateien auszutauschen, gemeinsame Drucker zu verwenden und auf freigegebene Order



zuzugreifen, ohne dass der Anwender manuelle Konfigurationen an der Firewall vornehmen muss. Deshalb schützen die Firewalls einiger Hersteller die Ports (tcp) 135 (msrpc), 139 (netbios-ssn) und 445 (microsoft-ds) nur **unzureichend**. Dieses Manko weisen in den **Werkseinstellungen** die Lösungen von **AVG**, **F-Secure**, **GDATA**, **Kaspersky**, **McAfee**, **Norman** und **Symantec** auf. Einen Ausnahmefall bilden jedoch die Security Suiten von **ESET**, **Kaspersky**, **Norman**, **Symantec**.

Bei diesen Produkten können die Benutzer jeweils nach der Installation des Produktes auswählen, ob der eigene PC mit anderen Computern im LAN kommunizieren soll oder nicht. Dementsprechend werden die genannten tcp-Ports von der Firewall entweder geschützt oder offen gelassen.

Etwas versteckt ist diese Option in **Norton Internet Security 2010**: Hier muss der Anwender im Hauptmenü auf „Heimnetzwerk anzeigen“ klicken, dann auf „Netzwerkdetails bearbeiten“ und zuletzt die Vertrauensstufe auf „Eingeschränkt“ umstellen. Erwähnenswert ist jedoch, dass es sich bei der „Portfreigabe im LAN“ bzw. den offenen Ports in der vertrauenswürdigen Zone im klassischen Sinne nicht um Sicherheitsrisiken handelt. Lediglich erfahrene Internet-Sicherheitsspezialisten erhalten 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 (LAN) und verfügt über das notwendige Know-How. Die oben genannten Gefährdungen - TCP Sequence prediction und IP ID Field Prediction Vulnerability - weisen in den Werkseinstellungen **nicht** die Produkte von **Avira**, **BitDefender**, **BullGuard** und **Eset** auf, sofern nach der Installation die entsprechende Netzwerkoption durch den Nutzer ausgewählt wird.

Einen **Pluspunkt** erhalten im Bereich der „inneren Schutzwirkung der Firewalls“ die Produkte von BitDefender, BullGuard, Kaspersky und Symantec aufgrund guter Warnmeldungen und Logdateien.Wie bereits in den beiden vergangenen großen Vergleichstests „Security Suiten 2008“ [http://www.protectstar-testlab.org/award/protectstar-iss2008test_ger_web.pdf] und „Security Suiten 2009“ [http://www.protectstar-testlab.org/content/site/dateien/759protectstar-bigiss2009_ger.pdf] kritisiert, ist auch diesmal wieder aufgefallen, dass einige Produkte den Anwender zwar darüber benachrichtigen, wenn ein Angriff aus dem Internet gegen seinen Computer durchgeführte wird, nicht aber wenn Angriffe ihre Herkunft aus dem LAN haben.

Eine **positive Ausnahme** bilden hier die Security Suiten von BitDefender, F-Secure, GData, Kaspersky und Symantec. Einen **negativen Ausrutsche**r hat sich die neue Firewall von **AVG** auf einem aktuellen Vista 32-Bit Betriebssystem geleistet: In den Werkseinstellungen fror das Betriebssystem bei zwei unabhängigen Testreihen bei dem Penetrationstest ein.

Offenbar handelt es sich hierbei um einen **Remote Heap Bufferoverflow** welcher über den Port 5357/tcp verursacht wird. Der Hersteller ist über die Schwachstelle informiert worden und analysiert derzeit das Problem.

Nachstehende Tabelle zeigt die bei den Security Suiten gefundenen Gefährdungen (äußerer und innerer Schutz) geordnet nach Gefahrenlevel und Anzahl gefundener Risiken im Überblick:

Stand:	**November 2009**
Anzahl der Angriffe (Internet):	20.890 + 13.609 **= 34.499**
Anzahl Angriffe (LAN):	**13.609**
Produkt analysiert in:	**Werkseinstellungen**

	Angriffe direkt via Internet		**Angriffe direkt via LAN**			
Hersteller	High / Medium / Low		High	Medium	Low	Sonstiges
AVG	0 / 0 / 0		1	1	5	D
Avira	0 / 0 / 0		0	0	0	A
BitDefender	0 / 0 / 0		0	0	0	A
BullGuard	0 / 0 / 0		0	0	0	A
ESET	0 / 0 / 0		0	0	0	A, B
F-Secure	0 / 0 / 0		0	1	4	A
G DAta	0 / 0 / 0		0	2	11	A, C
Kaspersky	0 / 0 / 0		0	2	11	A, C
McAfee	0 / 0 / 0		0	2	11	C
Norman	0 / 0 / 0		0	1	2	A, C
Symantec	0 / 0 / 0		0	2	10	A, C

Legende	
A	Firewall zeigte sich widerstandsfähig gegen durchgeführte Attacken
B	Keine Sicherheitsrisiken, da Profil „Strict Protect“ ausgewählt
C	Sicherheitsrisiken können einfach durch manuelle Einstellungen an Firewall behoben werden
D	High Risk Schwachstelle Wsdapi Server Heap Overflow (5357/tcp)

3.) DIE MALWAREERKENNUNG

In Kooperation mit dem unabhängigen Testcenter **AV-Comparatives**, sind die Malwareerkennungsraten der in den Suiten integrierten Malwarescannern herangezogen worden (siehe: Link1* und Link2**).

Um eine genaue Erkennungsrate bestimmen zu können, wurden alle

Produkte an einem Tag aktualisiert und dann „eingefroren.“ Eine automatische Aktualisierung der Produkte war somit unmöglich. Zudem erfolgte eine **optimale Produktkonfiguration**, damit möglichst alle Schädlinge erkannt werden konnten. Bei F-Secure konnten lediglich die Standardeinstellungen getestet werden.

In Tabelle 1 ist ausschließlich der signaturbasierte und heuristische Schutz (on-demand/on-access) der Malwarescanner

[Stand: August 2009] überprüft worden.

Einige Produkte bieten weitere Schutzmechanismen an, die beispielsweise ein Virus an seinem Verhalten erkennen (proaktiver Schutz), nachdem es vom Anwender ausgeführt wurde.

Diese verhaltensbasierte Erkennung/ Schutzmechanismen (wie z.B. Behaviorblocker, HIPS, usw.) werden im Retrospective Test nicht erfasst, da solche Mechanismen erst dann greifen wenn die Malware ausgeführt wird. Der Retrospective Test in Tabelle 2 „Retrospective“ [Stand: November 2009] zeigt daher

Link1* = http://www.av-comparatives.org/images/stories/test/ondret/avc_report23.pdf

Link2** = http://www.av-comparatives.org/images/stories/test/ondret/avc_report24.pdf

nicht die proaktiven Schutzfunktionen sondern die retrospektiven/proaktiven Erkennungsraten anhand Heuristik und generische Erkennung. Das Malware-Testset der **On-Demand** Erkennung besteht aus knapp **1,6 Millionen** Schädlingen. Unterteilt in Windows Viren, Macro Viren, Script Viren, Würmer, Backdoors, Bots, Trojanern und anderer Malware. Das Testset der **retrospektiven Erkennung** besteht aus **23.237** Schädlingen (davon 4903 Würmer, 2839 Backdoors, 15053 Trojaner und 442 sonstiger Malware). Zu nennen ist an dieser Stelle, dass **BullGuard** auf der Malwareengine von BitDefender basiert. Im Detail ergeben sich folgende Resultate und Erkennungsraten:

Tabelle 1: „On-demand comparative“:

Pos.	Hersteller	Fehlalarm (false positives)	optimale ERkennungsrate
1.	**G DATA**	wenig	**99,8%**
2.	**Avira**	viel	**99,4%**
3.	**McAfee**	viel	**98,7%**
4.	**Symantec**	wenig	**98,4%**
5.	**F-Secure**	wenig	**97,9&**
6.	**BitDefender & BullGuard**	wenig	**97,8%**
7.	**Eset**	wenig	**97,2%**
8.	**Kaspersky**	wenig	**94,7%**
9.	**AVG**	wenig	**94,0%**
10.	**Norman**	wenig	**84,8%**
Anmerkung: Stand von Ende August 2009, daher wurden die zu diesem Zeitpunkt aktuellen Versionen der Hersteller verwendet.			

wenig	0 – 15 False Positives
viel	16 – 100 False Positives

Tabelle 2: „Retrospective Test“:

Pos.	Hersteller	Fehlalarm (false positives)	optimale ERkennungsrate
1.	**Avira**	viel	**74%**
2.	**G DATA**	wenig	**66%**
3.	**Kaspersky**	wenig	**64%**
4.	**Eset**	wenig	**60%**
5.	**F-Secure**	wenig	**56&**
6.	**BitDefender & BullGuard**	wenig	**53%**
7.	**AVG**	wenig	**49%**
8.	**McAfee**	viel	**47%**
9.	**Symantec**	wenig	**36%**
10.	**Norman**	viel	**32%**
Anmerkung: Stand November 2009			

wenig	3 – 15 False Positives
viel	über 15 False Positives

4.) EMPFEHLUNGEN VON PROTECTSTAR™

Bezüglich der durchgeführten Testreihen im Bereich der Sicherheit spricht das ProtectStar™ Test Lab folgende allgemeine Empfehlungen aus: Um die Sicherheit einer Security Suite zu erhöhen, sollte jedes Produkt mit einem **Passwortschutz** versehen werden. Nahezu 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.: http://www.protectstar.com/passwortlaenge.pdf). Dies verhindert, dass die vollständige Suite oder Teilprodukte wie Anti-Virenscanner oder Firewall deaktiviert, deinstalliert oder modifiziert werden können. 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.) durch die Firewall schützen lassen.

E) Test: BENUTZERFREUNDLICHKEIT & PERFORMANCE

Bezüglich der Benutzerfreundlichkeit und Performanceeigenschaften der analysierten Security Suiten, sind dem ProtectStar™ Test Lab folgende Merkmale aufgefallen:

1. AVG Internet Security 9.0

BENUTZERFREUNDLICHKEIT:

(+) ausgezeichnete und benutzerfreundliche Installationsoptionen. Zudem können Schutzmodule Einzeln und nach Bedarf installiert werden.
(+) gute und zuverlässige Programmsteuerung
(+) gute und praktische Angriffserkennung, aber ggf. auch Schwierigkeiten für unerfahrene Anwender
(+) gute Firewall Log- und Reportdateien
(-) Schutzmodule werden einzeln im Hauptmenü aufgelistet. Dadurch teilweise „Überfüllung“ der GUI
(-) kein Bootmedium
(-) Updates werden in default nur alle 4 Stunden heruntergeladen

PERFORMANCE:

(+) gute Gesamtperformance
(+) wirksame Fingerprinttechnologie

Was wir uns noch gewünscht hätten:

Eine übersichtlichere Benutzeroberfläche und die Möglichkeit, ein Nofallbootmedium zu erstellen.

2. Avira Premium Security Suite:

BENUTZERFREUNDLICHKEIT:

(+) anwenderfreundliche Konfigurationsmöglichkeiten bereits während der Installation
(+) übersichtliche Benutzeroberfläche
(+) gut durchdachte Werkseinstellungen sowohl für Heimanwender als auch Profis
(+) via „Expertenmodus“ lassen sich eine Vielzahl an Einstellungen vornehmen
(+) Rettungs-Bootmedium einfach erstellbar und benutzerfreundlich
(+) gutes Handbuch
(+) Game-Modus einstellbar
(-) kein HIPS

PERFORMANCE:

(+) gute Performanceeigenschaften

Was wir uns noch gewünscht hätten:

Ein Schutzmodul zur proaktiven Malwareerkennung
(wird im 1.Quartal 2010 verfügbar sein).

3. BitDefender Internet Security 2010:

BENUTZERFREUNDLICHKEIT:

(+) übersichtliche Benutzeroberfläche und Vielzahl an Einstellungs-möglichkeiten je nach Benutzertyp (Standard, Gamer, Profi, etc.) möglich
(+) sehr individuelle Benutzer- und Netzwerkeinstellungen durch Installationsassistent möglich
(+) Vielzahl an Einstellungsmöglichkeiten für erfahrene Anwender
(+) gute Integration des Spammoduls
(+) Fingerprint-Technologie
(+) gute Berichte. Allerdings nur mit dem Internet Explorer betrachtbar.
(+) gutes Notfall-Bootmedium mitgeliefert
(+) guter Spamfilter
(+) Game-Modus einstellbar
(-) http-Scan per default deaktiviert

PERFORMANCE:

(+) Im Vergleich zur Vorgängerversion gesteigerte Performance
(+) gute Allgemeinperformance

Was wir uns noch gewünscht hätten:

Ein übersichtliches Scanfenster mit Fortschrittsanzeige

4. BullGuard 8.7:

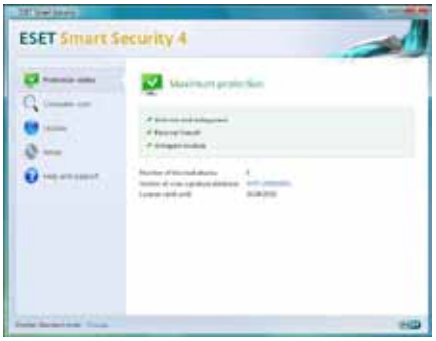
BENUTZERFREUNDLICHKEIT:

(+) gute und zuverlässige Firewall-Programmsteuerung
(+) hervorragender Live-Support-Chat
(+) gute Werkseinstellungen
(+) hilfreicher Backup-Assistent und Online-Backup Account verfügbar
(+) gute Integration des Spammoduls
(+) erweiterter Modus bei Firewall verfügbar. Dadurch umfangreiche Einstellungsmöglichkeiten
(+) Hilfeanforderung und Support praktisch in die Benutzeroberfläche integriert.
(-) relativ unübersichtliche Benutzeroberfläche und Gesamtübersicht
(-) schwache Hilfstexte
(-) kein Notfall-Bootmedium
(-) http-Scan per default deaktiviert

PERFORMANCE:

(-) im Gegensatz zu Konkurrenzprodukten immer noch langsamer Malwarescanner enthalten

5. Eset Smart Security 4.0:



BENUTZERFREUNDLICHKEIT:

(+) sehr guter Gesamteindruck
(+) sehr gutes Updateverhalten in Verbindung mit kleinen Updatepaketen
(+) übersichtliche Benutzeroberfläche und erweiterte Einstellungsmöglichkeiten je nach Anwendertyp (Standard / Advanced)
(+) sehr gute retrospektive Erkennung („Advanced Heuristik“)
(+) für Anfänger und erfahrene Anwender (über „Erweiterter Modus“) geeignet
(+) Eset SysInspector als sehr hilfreiches Zusatzmodul im Produkt integriert
(+) bootfähiges Rettungsmedium
(-) wenig Warnmeldungen bei abgewehrten Angriffen durch die Firewall

PERFORMANCE:

(+) Testsieger im Bereich der Gesamtperformance
(+) ausgezeichnet schneller Anti-Virenscanner

Was wir uns noch gewünscht hätten:

Ein Schutzmodul zur proaktiven Malwareerkennung, sowie die Möglichkeit weitere Feineinstellungen an der Heuristik vornehmen zu können.

6. F-Secure Internet Security 2010:

BENUTZERFREUNDLICHKEIT:

(+) sehr guter Gesamteindruck
(+) detaillierte und gute Logdateien und Warn-Pop-Ups bei Angriffen
(+) Übersichtliche Benutzeroberfläche
(+) gute Hilfsanzeigen
(+) hilfreiche Live-Sicherheitsinformationen
(+) durchdachte Einstellungsmöglichkeiten für Heimanwender und Profis
(+) über „erweitert“ lassen sich eine Vielzahl an Konfigurationsmöglichkeiten vornehmen
(+) gutes Notfall-Bootmedium
(+) einfache Installation
(+) sehr guter http-Scanner
(-) Updatefrequenz nicht wählbar
(-) keine Historie über die Scanberichte
(-) http-Scan per default deaktiviert
(-) Spamfilter schwer konfigurierbar

PERFORMANCE:

(+) Im Vergleich zur Vorgängerversion stark gesteigerte Performance
(-) langsamer On-Demand Malwarescan

7. G DATA Internet Security 2010:

BENUTZERFREUNDLICHKEIT:

(+) hervorragender Gesamteindruck
(+) klar strukturierte und moderne Benutzeroberfläche
(+) ausgezeichnete und sichere Standardeinstellungen im Bereich des AV-Scanners
(+) benutzerdefinierte Installation
(+) sehr gute Werkseinstellungen
(+) sehr gute Hilfetexte und Handbuch
(+) gute Reporte mit Historie
(+) Einfache Erstellung von Rettungsmedien
(+) IMAP-Konten werden überwacht
(+) Game-Modus einstellbar
(-) kein optimaler Schutz in den Werkseinstellungen bezüglich vertrauenswürdigen Zonen.
(-) kein Passwortschutz für Einstellungen möglich
(-) Integration des Anti-Spammoduls nur in Outlook

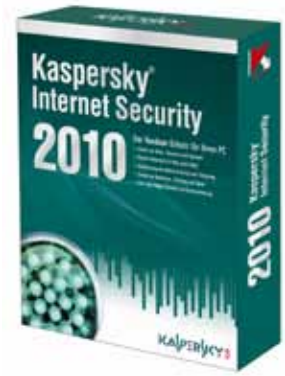
PERFORMANCE:

(+) Im Vergleich zur Vorgängerversion gesteigerte Performance
(-) leicht verzögerter Bootvorgang und Verzögerungen beim Surfen im Internet

Was wir uns noch gewünscht hätten:

Ein Schutzmodul zur proaktiven Malwareerkennung, sowie die Möglichkeit diverse Feineinstellungen an der Heuristik vorzunehmen. Darüber hinaus sollte es möglich sein, die Produkteinstellungen mit einem Passwortschutz zu versehen.

8. Kaspersky Internet Security 2010:



BENUTZERFREUNDLICHKEIT:

(+) hervorragender Gesamteindruck
(+) gute und benutzerdefinierte Installation
(+) sehr gut durchdachte Werkseinstellungen sowohl für Heimanwender als auch Profis
(+) sehr gute und ausführliche Warnmeldungen via Pop-Up in allen Sicherheitsbereichen
(+) sehr guter Anti-Spam Filter bzw. „Inhaltsfilterung“ und Integration des Spammoduls in gängige Mailclienten
(+) Sandbox und HIPS in den Werkseinstellungen aktiviert
(+) ausgezeichneter und anwenderfreundlicher Anti-Spam Filter
(+) Scan auf Systemschwachstellen
(+) IMAP-Konten werden überwacht
(+) Gamer-Modus (Vollbildmodus)
(+) gutes Mailschutzmodul mit integrierter Voransicht der Mails auf dem Server
(+) gute Erkennung des Intrusion Prevention System auf unterschiedliche Angriffsvariationen
(-) unübersichtliche Berichte

PERFORMANCE:

(+) wirksame „Fingerprint“-Technologie
(+) geringer Einfluss auf die Systemperformance und sehr gute Allgemeinperformance
(-) Updates werden schleppend heruntergeladen

9. McAfee Internet Security 2010:

BENUTZERFREUNDLICHKEIT:

(+) einfache und benutzerdefinierte Installation
(-) altmodische Benutzeroberfläche (GUI), die seit Jahren unverändert ist
(-) unzureichende Logeinträge
(-) ausreichend Schutz in vertrauenswürdigen Zonen, nur durch manuelle Modifikation der Firewall-Regeln möglich
(-) kein Rettungsmedium erstellbar

PERFORMANCE:

(+) gute Allgemeinperformance

Was wir uns noch gewünscht hätten:

Eine vollständig erneuerte und moderne Benutzeroberfläche mit der Möglichkeit verschiedene Einstellungen im Bereich der Heuristik feiner einstellen zu können.

10. Norman Security Suite:

BENUTZERFREUNDLICHKEIT:

(+) Vielzahl an Verbesserungen und Optimierungen im Vergleich zur Vorgängerversion
(+) guter und benutzerfreundlicher Anti-Spamfilter
(+) ausgezeichneter Einführungswizard inklusive ausführlicher Erklärungen
(+) übersichtliche und aufgeräumte Benutzeroberfläche
(+) gute und zuverlässige Firewall-Programmsteuerung
(+) intelligenter Sreensaver-Scanner
(+) starke Sandbox-Technologie
(+) „Deinstallationsschutz“ via Codeeingabe.
(-) 24 Stunden als Updateintervall, kleinstmögliche Einstellung 6 Stunden
(-) kein Rettungsmedium erstellbar

PERFORMANCE:

(+) gute Allgemeinperformance
(+) gute Performance des Echtzeitschutzes

Was wir uns noch gewünscht hätten:

Die Erstellung von Rettungsbootmedien und mehr Möglichkeiten der Feineinstellungen im Bereich des Malwarescanners (manueller Scanner). Eine proaktive Malwareerkennung würde das Produkt zudem perfekt abrunden.

11. Norton Internet Security 2010:

BENUTZERFREUNDLICHKEIT:

(+) hervorragender Gesamteindruck
(+) Vielzahl an Verbesserungen im Gegensatz zur Vorgängerversion
(+) ausgezeichneter und anwenderfreundlicher Anti-Spam Filter
(+) sehr gut für technisch unversierte Anwender geeignet
(+) hervorragendes Updateverhalten
(+) Game- bzw. Silent-Modus einstellbar
(+) gute Angriffsformenerkennung
(+) ausgezeichnete Onlinehilfe und Supportoptionen
(+) benutzergerechte Programmsteuerung
(+) einfache Installation und Produktaktivierung
(+) übersichtliche und moderne Benutzeroberfläche
(+) bootfähiges Notfallmedium
(+) kostenlose Kindersicherung als Add-On verfügbar
(-) zu geringe Konfigurationsmöglichkeiten im Bereich der Heuristik und Quarantäne

PERFORMANCE:

(+) schnelle Installation
(+) schneller Anti-Virenscanner (On-Demand)
(+) ausgezeichnete Performanceeigenschaften

F) Test: SCANZEITEN (Kurztest)

In diesem Kurztest erfolgt die Analyse der Scanzeiten bzw. Scangeschwindigkeiten des in der jeweiligen Security Suite integrieren Malwarescanner analysiert. Jedes Produkt ist dabei manuell mit den höchsten Sicherheitseinstellungen konfiguriert worden. Ebenfalls wurde die Heuristik aktiviert.Testkriterium war hier die Scanzeiten auf einem Computersystem (Core2Duo E 6300, 2048MB Ram, WD-Sata Festplatte) mit einer 220 GB Partition, wo von 150GB belegt sind mit typischen Nutzerdaten, Dokumenten, zip, rar, iso Archiven, mp3, jpg, gif, pdf, avi und viele weitere. Die gesamten Testdateien werden dabei von jedem Malwarescanner jeweils **drei Mal** hintereinander überprüft. Nachfolgende Tabelle zeigt die Scanzeiten des ersten bis dritten Scans an:

Pos.	Hersteller	1. Scan	2. Scan	3. Scan
1.	**AVG**	00:21:17	00:16:17	00:05:43
2.	**Avira**	00:21:30	uv	uv
3.	**BitDefender**	00:27:24	00:06:39	00:04:32
4.	**BullGuard**	00:30:40	uv	uv
5.	**ESET**	00:33:52	uv	uv
6.	**F-Secure**	01:17:44	uv	uv
7.	**G DATA**	00:54:29	00:00:16	00:00:06
8.	**Kaspersky**	00:25:12	00:03:17	00:02:51
9.	**McAfee**	00:21:12	uv	uv
10.	**Norman**	00:20:38	uv	uv
11.	**Symantec**	00:24:42	00:04:44	00:03:10
uv= Unverändert bzw. mit 1. Scan identisch				

Nicht nur die Scanzeiten müssen an diesem Ergebnis näher betrachtet werden, sondern auch die Performanceeinbußen, die während des Malwarescans aufgefallen sind.

So ist F-Secure besonders negativ aufgefallen, da der Computer während des Scanvorgangs kaum noch benutzbar war. Während des Scanvorgangs wurden am wenigsten die Test-Computer durch Avira, BitDefender, Eset und Symantec belastet. GData zeigte zwar die besten Scanergebnissen bei dem zweiten und dritten Scanvorgang, allerdings machten sich vor allem bei dem ersten Scanvorgang einige Performanceeinbußen bemerkbar.

Bei diesem Scanzeiten-Kurztest muss beachtet werden, dass die genannten Zeiten lediglich eine Momentaufnahme darstellen.

Wenn zum Beispiel manuelle Modifikationen an den Konfigurationseinstellungen eines Produktes vorgenommen werden oder viele verschiedene Dateien - und vor allem Dateiformate gescannt werden müssten - würden die Scanzeiten entsprechend besser bzw. schlechter ausfallen.

G) Test: PREIS-/AUSSTATTUNGSVERHÄLTNIS							
	Preis (Box)	**Preis (Download)**	**Amazon-preis**	**Lizenzen**	**Inhalt (Soft-ware)**	**PUNKTE max. 20**	**Bewertung**
AVG	... ...	52,95 38,95	... ...	3x 1x	AV, FW, AS, WF	**16**	**gut**
Avira	... ...	59,95 39,95	47,99 29,99	3x 1x	AV, FW, AS, KS, BP	**17**	**gut**
BitDefender	... ...	49,95 ...	34,95 26,98	3x 1x	AV, FW, AS, KS, ID, WiFi, DT, Sys	**18**	**sehr gut**
BullGuard	... ...	69,95 ...	... ...	3x 1x	AV, FW, AS, Sys	**15**	**befriedigend**
Eset	49,90 39,90	49,90 39,90	... ...	3x 1x	AV, FW, AS, Sys	**16**	**gut**
F-Secure	... ...	39,95 29,95	39,95 29,89	3x 1x	AV, FW, AS, KS	**18**	**sehr gut**
G DATA	39,95 29,95	39,95 29,95	29,95 20,95	3x 1x	AV, FW, AS, DS	**19**	**sehr gut**
Kaspersky	59,95 39,95	59,95 39,95	42,95 27,95	3x 1x	AV, FW, AS, WF, KS, ID	**17**	**gut**
McAfee	59.95 39,95	59.95 39,95	29,45 25,83	3x 1x	AV, FW, AS, KS, DP, BP	**17**	**gut**
Norman	... ...	49,00 ...	... ...	3x 1x	AV, FW, KS, AS	**16**	**gut**
Symantec	59,99 39,99	59,99 39,99	36,99 25,95	3x 1x	AV, FW, AS, KS, ID, WiFi	**17**	**gut**

Preise in Euro
AV = Antiviren-Scanner / FW = Firewall / KS = Kindersicherung / BP = Backup / DT = Datentresor / ID = Identitätsschutz / WF = Webfilter / DS = Datenshredder / ON = Onlinescanner / ST = Systemtuner / WiFi = WLAN Schutz / Sys = SysInspector

Online Einkaufstipp:

Bei der Beurteilung des Preis-/Ausstattungsverhältnisses fällt auf, dass zwischen den empfohlenen Preisen der Hersteller, den von den Herstellern eigens betriebenen Onlineshops und den Verkaufspreisen von Amazon teilweise gravierende Unterschiede bestehen. Generell noch preiswerter als bei Amazon können Interessenten eine Vielzahl der getesteten Security Suiten bei Hasa-Shop unter http://www.hasa-shop.de/?refID=777 beziehen.
Zum Beispiel sind folgende aktuelle Preisbeispiele bei Hasa-Shop heraus gesucht worden:

Produkt:	Preis:	Bestell-Link:
Avira Internet Security 2010, 3-User	EUR 44,90	www.hasa-shop.de/::4825.html?refID=777
BitDefender Internet Security 2010,1-User	EUR 23,90	www.hasa-shop.de/::4270.html?refID=777
G Data Internet Security 2010,3-User	EUR 29,95	www.hasa-shop.de/::3561.html?refID=777
Kaspersky Internet Security 2010, 1-User	EUR 24,20	www.hasa-shop.de/::3941.html?refID=777
Norton Internet Security 2010, 3-User	EUR 32,00	www.hasa-shop.de/::4153.html?refID=777

H) FAZIT

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:

Pos.	Hersteller	SICHERHEIT (Fw-A/ Fw-I / On / Ret / Sonst.)	BENUTZERFREUND. & PERFORMANCE	PREIS-/ AUSSTATTUNG	PUNKTE
1.	Avira	40 / 20 / 24.4 / 22.4 / 7	28 / 29	17	187.8
2.	G DATA	40 / 18 / 24.8 / 21.6 / 8	28 / 27	19	186.4
3.	Eset	40 / 20 / 22.2 / 21.0 / 7	27 / 30	16	183.2
4.	Symantec	40 / 18 / 23.4 / 18.6 / 9	28 / 29	17	183.0
5.	BitDefender	40 / 20 / 22.8 / 20.3 / 7	27 / 27	18	182.1
6.	Kaspersky	40 / 18 / 19.7 / 21.4 / 9	28 / 28	17	181.1
7.	F-Secure	40 / 18 / 22.9 / 20.6 / 7	28 / 25	18	179.5
8.	McAfee	40 / 17 / 23.7 / 19.7 / 5	25 / 28	17	175.4
9.	BullGuard	40 / 20 / 22.8 / 20.3 / 6	25 / 25	15	174.1
10.	AVG	40 / 13 / 19.0 / 19.9 / 5	27 / 27	16	166.9
11.	Norman	40 / 19 / 9.8 / 18.2 / 6	27 / 27	16	164.0

Legende	
Fw-A	Äußerer Schutz der Firewall (max. 40 Punkte)
Fw-I	Innerer Schutz der Firewall (max. 20 Punkte)
On	On-Demand Malwareerkennung (max. 25 Punkte)
Ret	Retrospektive Malwareerkennung (max. 25 Punkte)
Sonst.	Sonstiges: Qualität der Logdateien, Behaviorblocker, IDP, HIPS, etc. (max. 10 Punkte)

1. Platz mit **187.8** Punkten an:
Avira Premium Security Suite

1st Place

2. Platz mit **186.4** Punkten an:
G Data InternetSecurity 2010

2nd Place

3. Platz mit **183.2** Punkten an:
Eset Smart Security 4.0

3rd Place

Der Testsieger des „Großen Vergleichstest – Internet Security Suiten 2010“ ist in diesem Jahr die Schutzlösung **Avira Premium Security Suite**.

Avira zeigte in allen Testreihen durchwegs sehr gute Testergebnisse und konnte zusammen mit dem dicht gefolgten zweitplatzierten Produkt **GData Internet-Security 2010**, alle Hersteller im Bereich der Sicherheit und Malwareerkennung abhängen.

Überhaupt geben sich die beiden Hersteller **Avira** und **GData** mit ihren Security Lösungen in diesem Jahr ein Kopf an Kopf rennen: Während GData beispielsweise eine etwas bessere Malwareerkennung in den On-Demand Testreihen beweist, zeigt Avira wiederum bessere Erkennungsleistungen in den Retrospektive Testreihen.

In der Gesamtperformance kann Avira verstärkt Punkte sammeln. Im Preis-/Ausstattungsverhältnis ist GData der eindeutige Testsieger.

Ebenfalls hervorragend hat sich das drittplatzierte Produkt **Eset Smart Security 4.0** in diesem Jahr geschlagen. Die Security Suite zeichnet sich durch ein sehr gut abgerundetes Gesamtbild aus. Die Stärken von Eset liegen vor allem im Bereich der Performance, Benutzerfreundlichkeit, guter retrospektiven Malwareerkennung und wenigen Fehlalarmen (False Positives). Zudem zeigt sich, dass das Produkt von Jahr zu Jahr kontinuierlich verbessert und optimiert worden ist.

Gefehlt hat uns bei Eset, wie auch bei Avira und GData, lediglich ein Schutzmodul zur proaktiven Malwareerkennung, das hoffentlich bei allen Herstellern in Zukunft verfügbar sein wird.

Zu beachten ist, dass das Gesamtresultat lediglich eine Momentaufnahme darstellt und sich jederzeit jeder Hersteller durch das Bereitstellen von Produktpatches oder Signaturupdates verbessern könnte.

Generell ist aufgefallen, dass sich bis auf wenige Ausnahmen die meisten Produkte gegenüber den Vorgängerversionen teilweise deutlich verbessern konnten. Dies gilt vor allem für die Hersteller Avira, BitDefender, Eset und F-Secure. Allerdings ist auch zunehmend in den letzten Jahren der Testreihen erkennbar geworden, dass die klassische signaturbasierte Malwareerkennung stark an Bedeutung verloren hat. Gerade unbekannte oder speziell auf ein Produkt abgestimmte Malware, wird in der Regel nicht von der signaturbasierten oder auch heuristischen Malwareerkennung entdeckt.

Aber gerade diese signaturbasierte und heuristische Malwareerkennung ist nach wie vor das Terrain der meisten analysierten Produkte in diesem Test. Sei es Avira, GData, Eset, McAfee, Norman, usw., sie alle sollten schnellstmöglich Schutzmodule zur proaktiven Erkennung bereitstellen, um überhaupt noch den aktuellen Sicherheitsanforderungen gerecht werden zu können.

Avira hat beispielsweise angekündigt, seine Produkte ab März 2010 mit einem proaktiven Schutzmodul auszustatten. Ein Statement der anderen Hersteller bleibt zunächst noch abzuwarten.

1st Place

Anregungen, Kritik und Spenden

Das ProtectStar™ Test Lab arbeitet strikt unabhängig.

Die hier durchgeführten Testanalysen, die Aufbereitung und Ausarbeitung der Testresultate, Design des Testberichts, Übersetzungen, Publizierungen, Arbeitszeiten, Löhne, Bereitstellungen, uvm. wurden ausschließlich von der ProtectStar™, Inc. finanziert. Die im Testbericht genannten Hersteller stellten lediglich und nur zum Teil die für die Testreihen benötigten Testversionen bzw. Lizenzen bereit.

Um die Testreihen in Zukunft weiter verbessern zu können, dankt ProtectStar™ jeder Art von Anregung und Kritik seiner Leserinnen und Leser. Bitte teilen Sie uns mit, was Ihnen besonders gut gefallen hat und welcher Test für Sie hätte ausführlicher behandelt werden können.

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 danken wir Ihnen für **Ihre materielle Unterstützung** an die wohltätige **ProtectStar™ Foundation** (www.protectstar-foundation.org). Ihre Unterstützung kommt weltweit **gemeinnützigen Hilfsprojekten** zugute.

Kontakt

Corporate Headquarter:

ProtectStar, Inc.
Test Lab
444 Brickell Avenue
Suite 51103
33131 Miami, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505

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

Mail: testcenter@protectstar.com
Web: www.protectstar-testlab.org