

ProtectStar™ Test Lab

Einzeltest

Kaspersky Internet Security 2011



INHALTSVERZEICHNIS:

Seite 2	Inhaltsverzeichnis
Seite 3	Einleitung: Kaspersky Internet Security 2011
Seite 3	A.) Getestetes Produkt und Version
Seite 3	B.) Allgemeine Erläuterung der Testverfahren
Seite 4	C.) Bewertungskriterien
Seite 5	D.) Test: SICHERHEIT
Seite 5	1.) DIE FIREWALL – DER ÄUSSERE SCHUTZ
Seite 6	2.) DIE FIREWALL – DER INNERE SCHUTZ
Seite 7	3.) DIE MALWAREERKENNUNG
Seite 8	4.) EINSTELLUNGSEMPFEHLUNGEN VON PROTECTSTAR™
Seite 9	E.) Test: BENUTZERFREUNDLICHKEIT & PERFORMANCE
Seite 10	F.) Test: SCANZEIT (Kurztest)
Seite 11	G.) Test: PREIS-/AUSSTATTUNGSVERHÄLTNIS
Seite 11	H.) FAZIT
Seite 13	Anregungen, Kritik und Spenden
Seite 13	Kontakt & Copyright

Einleitung: Kaspersky Internet Security 2011

Der Hersteller bewirbt seine neue Schutzlösung beispielsweise mit nachfolgendem Werbesatz:

„Kaspersky Internet Security 2011 hat alles, was Sie fürs sichere Surfen im Netz brauchen. Es schützt Sie und Ihre Familie jederzeit zuverlässig vor allen Cyber-Bedrohungen – ob beim Arbeiten, im Internet, beim Online-Banking, Online-Shopping oder bei Online-Spielen. Seien Sie den Bedrohungen immer um eine Nasenlänge voraus – mit Kaspersky Internet Security 2011!“

Quelle: www.kaspersky.de

Ob die Schutzsoftware diesen Versprechen gerecht werden kann wird dieser Einzeltest zeigen.

A.) Getestetes Produkt und Version

Die in den hier durchgeführten Testreihen analysierte Version von Kaspersky Internet Security 2011 ist **11.0.0.232 (a)**



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 der Security Suite

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 Internet 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 der Malwareerkennungsraten wurden aus den öffentlich verfügbaren Ergebnissen der gemeinnützigen Organisation AV-Comparatives e.V. (www.av-comparatives.org) entnommen.

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 Augenmerkmale liegen auf dem Handbuch 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 Suite 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 (32- und 64-Bit)

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), sowie 128GB SSD (S-ATA).



Außerhalb der Testreihen gibt es Bewertungen bezüglich der Mindestanforderungen an das System laut Herstellervorgabe. Hier liegt das Augenmerk speziell auf der benutzergerechten Anwendbarkeit des Produktes.

PREIS-/AUSSTATTUNGSVERHÄLTNIS: Wie stehen Preis und Ausstattung der Kaspersky Internet Security 2011 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 und ggf. weiteren verglichen.

C.) Bewertungskriterien

Bei dem analysierten Produkt Kaspersky Internet Security 2011 handelt es sich ausschließlich um eine Sicherheitslösung, die dem Anwender Schutz vor modernen Gefahren wie Hackern, Trojanern, Viren, Rootkits, Keyloggern, Phishing-Angriffen, uvm. versprechen und vor allem auch gewährleisten sollte. Da es sich also um **Sicherheitsprodukte** handelt, muss das Hauptaugenmerk zwangsläufig auch auf die enthaltenen Schutzfunktionen der Internet Security 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 Teilen in der Bewertung widerspiegeln.

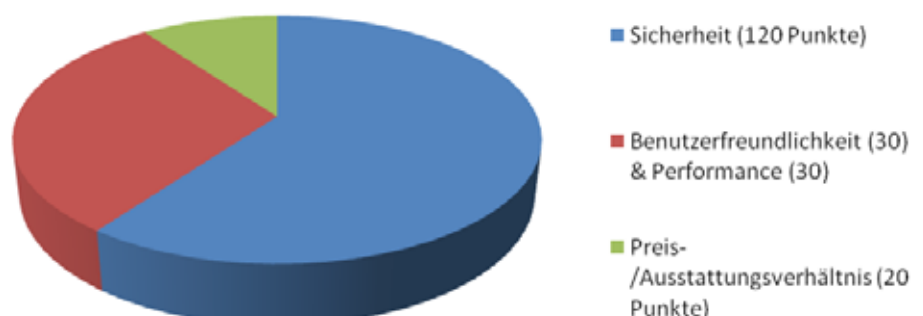
Weniger essentiell für die Sicherheit eines Produktes, aber dennoch erwähnenswert ist der Testbereich des **Preis-/Ausstattungsverhältnisses**. Eine moderne Security Suite sollte unabhängig von ihrem höheren oder niedrigeren Verkaufspreis einen maximalen Schutz gewährleisten. Hier soll der Anwender nicht 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 **proaktive/retrospektive** (heuristische) Malwareerkennung verdienen. Bei der **On-Demand Malwareerkennung** werden pro fehlendem Prozentpunkt in der Erkennungsrate **1.0 Punkte** und bei der **proaktiven/retrospektiven 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-Virencscanner, 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 Suite vergeben werden.

D.) Test: SICHERHEIT

1.) DIE FIREWALL – der äußere Schutz

Die durch das ProtectStar™ Test Lab bewertete Kaspersky Internet Security 2011 Suite enthält eine integrierte Firewall, die ein- und ausgehende Verbindungen kontrolliert. Analysiert wurde die Firewall in den Werkseinstellungen, also in den jeweiligen Konfigurationen des Auslieferungszustandes.



Die Firewall ist – 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 Personal Firewall hat in den Durchläufen bezüglich des äußeren Schutzes, alle zum Testzeitpunkt bekannten **24.570** differenten **Angriffs- und Sicherheitstests** erfolgreich bestanden (Stand: Juni 2010). 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.

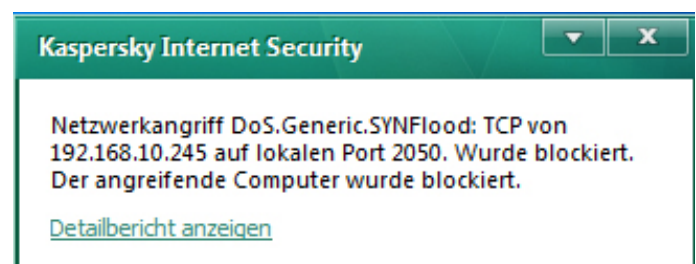
In der Grundeinstellung prüften standardisierte Portscans nach geöffneten TCP- und UDP- Ports. Die Scanrange umfasste alle Ports (0 – 65535). Im zweiten Schritt wurde die Firewall einem SYN-Portscan (half-open) - dem so genannten Stealth-Scan - unterzogen.

Darüber hinaus wehrte die Kaspersky Personal Firewall **erfolgreich** 33 speziellen Angriffsvariationen für Firewalls 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 könnten.

Sowohl durch die automatisch ablaufenden Testreihen des hardwarebasierenden und hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **43208** (Stand: Juni 2010) weitere Sicherheitstests und Angriffstaktiken auf die Firewalls ausführte, als auch durch die manuell durchgeführten Prüfungen konnten **keine Sicherheitsrisiken** festgestellt werden.

Den mehrstündigen **Dauer-Penetrationstest** absolvierte die Firewall ebenfalls **erfolgreich**, ohne nennenswerte Performan- ceverluste.



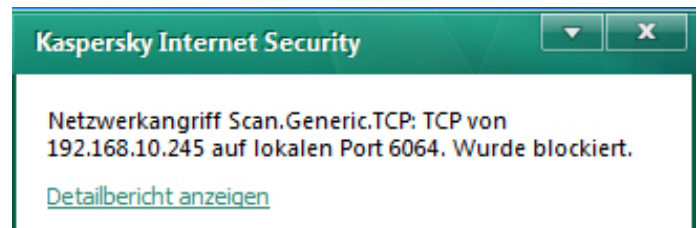
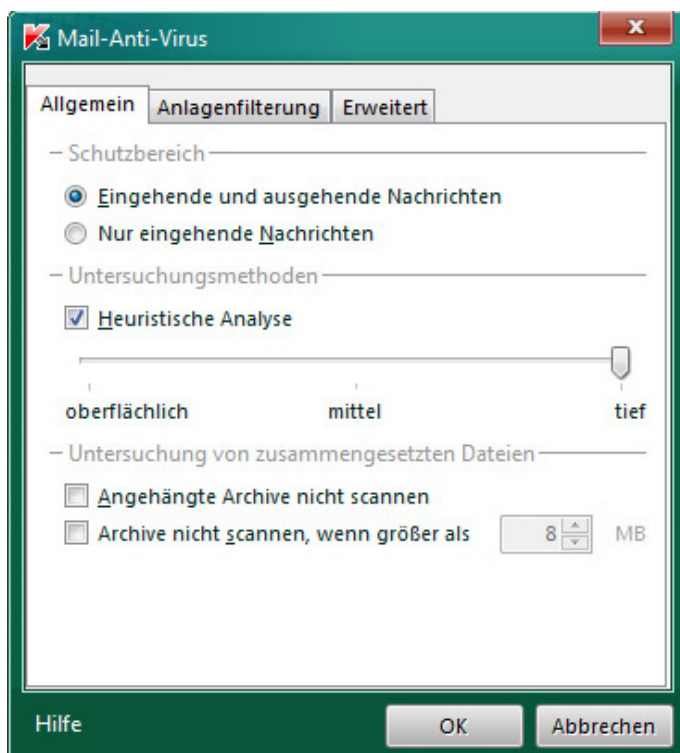
Bei den Warnhinweisen und Alarmmeldungen zeigte sich die neue Schutzlösung von Kaspersky bereits in den Werkseinstellungen **vorbildlich**.

2.) DIE FIREWALL – der innere Schutz

Der vorhergehende Test zeigt, dass die Kaspersky Firewall **ausreichend Schutz** gegen Angriffe aus dem Internet bietet. Wie sieht es aber aus, wenn ein Computersystem mit installierter Kaspersky Internet Security 2011 Suite direkt aus einer vertrauenswürdigen Zone - wie dem LAN – angegriffen wird?

Die Sicherheitsexperten des ProtectStar™ Test Lab analysierten daher die in dem Produkt integrierte Kaspersky Firewall in den Werkeinstellungen bezüglich der Schutzwirkungen im LAN mit unterschiedlichen **Angriffs- und Sicherheitstests**. Getestet worden sind die aktuell bekannten **Denial of Service (DoS)**-Angriffsarten, sowie **Schwachstellen** in Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und andere Sicherheitschecks.

Die meisten auf dem Markt erhältlichen Personal Firewall Produkte zeigen hier in der Regel, wie bereits in anderen publizierten Testberichten von ProtectStar™ genannt, eine Reihe



von Schwächen. Um den zunehmenden Forderungen nach mehr Benutzerfreundlichkeit gerecht zu werden, konfigurieren einige Hersteller ihre Firewalls bereits in den Werkseinstellungen „anwenderfreundlich“ 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.

Äußerst positiv zu nennen ist, dass die neue **Kaspersky Internet Security 2011** dieses Manko nicht mehr aufweist. Bei der Vorgängerversion 2010 ist dies beispielsweise noch von den Sicherheitsexperten von ProtectStar™ bemängelt worden. Kaspersky Internet Security 2011 gehört damit aktuell gerade zu einer Handvoll an Schutzlösungen auf dem weltweiten Markt, die sowohl bei der äußeren als auch inneren Schutzwirkung der Firewall, ein umfassendes Schutzniveau gewährleistet.

Einen weiteren Pluspunkt im Bereich der „inneren Schutzwirkung der Firewall“ kann aufgrund guter Warnmeldungen und Logdateien an die Kaspersky Suite 2011 vergeben werden. Überhaupt zeigen sich die Berichte ordentlich sortiert und detailliert. Die Angriffssignaturen bezüglich der Netzwerkangriffserkennung könnten weiter verbessert werden, so dass Anwender künftig auch von anderen Netzwerk-Angriffsvariationen gewarnt werden können.

Das hervorragende Schutzniveau der in der Kaspersky Internet Security 2011 Suite integrierten Personal Firewall (100% Schutzwirkung bezüglich der Testreihen im äußeren und inneren Schutz) erfüllen anstandslos die Kriterien zum **ProtectStar™ Firewall Award 2010**.

Nachstehende Tabelle zeigt die bei der Kaspersky Internet Security 2011 Suite 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			
High / Medium / Low		High	Medium	Low	Sonstiges
0 / 0 / 0		0	0	0	A

Legende	
A	Personal Firewall zeigte sich widerstandsfähig gegen die durchgeführten Attacken

Das hervorragende Schutzniveau der in der Kaspersky Internet Security 2011 Suite integrierten Personal Firewall (100% Schutzwirkung bezüglich der Testreihen im äußeren und inneren Schutz) erfüllen anstandslos die Kriterien zum **ProtectStar™ Firewall Award 2010**.

3.) DIE MALWAREERKENNUNG

In Zusammenarbeit mit dem unabhängigen Testcenter **AV-Comparatives**, ist die Malwareerkennungsrates der in der Kaspersky Suite integrierte Malwarescanner herangezogen worden.

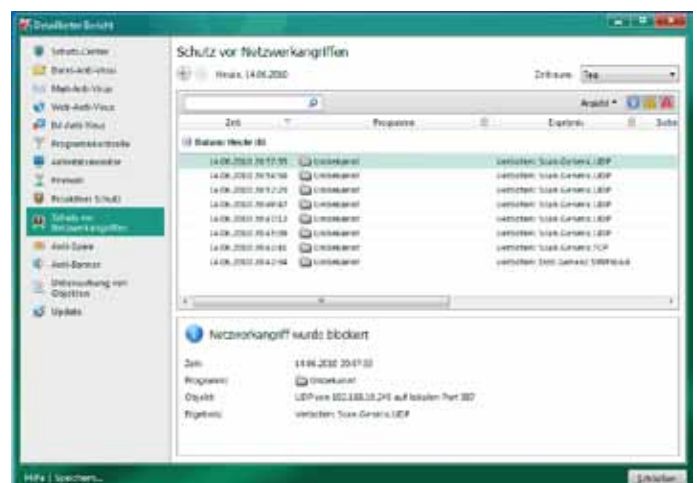
Um eine genaue Erkennungsrate bestimmen zu können, ist das Produkt an einem Tag aktualisiert und dann „eingefroren“ worden. Eine automatische Aktualisierung ist dadurch nicht mehr möglich gewesen. Zudem erfolgte eine **optimale Produktkonfiguration**, damit möglichst alle Schädlinge erkannt werden konnten.

In Tabelle 1 „On-demand detection“ ist ausschließlich der signaturbasierte und heuristische Schutz (on-demand/on-access) des Malwarescanners [Stand: März 2010] überprüft worden.

Der Retrospective Test in Tabelle 2 „proactive/retrospective Test“ [Stand: Mai 2010] zeigt die retrospektiven/proaktiven Erkennungsrates anhand Heuristik und generische Erkennung.

Das Malware-Testset der **On-Demand** Erkennung besteht aus über **1,2 Millionen** Schädlingen. Unterteilt in Windows Viren, Macro Viren, Script Viren, Würmer, Backdoors, Bots, Trojanern und anderer Malware.

Das Testset der **proactive/retrospektiven** Erkennung besteht aus **27.271** Schädlingen.





Im Detail ergeben sich folgende Resultate und Erkennungsraten:

Tabelle 1: „On-demand detection“:	
Fehlalarm (false positives)	optimale Erkennungsrate
wenig	97,1%

Anmerkung: Stand März 2010, daher wurde die zu diesem Zeitpunkt aktuelle Produktversion der Kaspersky Internet Security Suite verwendet

Legende	
wenig	0 - 15 False Positives

Der Malwarescanner von Kaspersky konnte in den Testreihen bezüglich der signaturbasierten Erkennung von insgesamt 1.224.732 Schädlingen 1.188.872 Dateien als Malware erkennen, was einer optimalen Erkennungsrate von 97,1% entspricht.

Tabelle 2: „proactive / retrospective Test“:	
Fehlalarm (false positives)	optimale Erkennungsrate
wenig	59%

Anmerkung: Stand März 2010, daher wurde die zu diesem Zeitpunkt aktuelle Produktversion der Kaspersky Internet Security Suite verwendet

Legende	
wenig	3 - 15 False Positives

Die optimale Erkennungsrate im „proactive / retrospective Test“ beträgt 59%. Im Detail hat der integrierte Kaspersky Malwarescanner von insgesamt 6.541 Würmern 5.336 (82%), von 3.342 Backdoors 1.748 (52%), von 17.046 Trojanern 8.898 (52%) und von 342 sonstiger Malware 105 (31%) proaktive bzw. retrospektiv erkannt. Auch wenn 59% in diesem Test eher gering klingen mag, ist diese optimale Erkennungsrate - im Vergleich zu Konkurrenzprodukten [beispielsweise avast! (29%), BitDefender (50%), McAfee (38%) und Symantec (43%)] - hoch.

4.) EINSTELLUNGSEMPFEHLUNGEN VON PROTECTSTAR™

Bezüglich der durchgeführten Testreihen zum Produkt Kaspersky Internet Security 2011 können die Sicherheitsexperten des ProtectStar™ Test Lab folgende allgemeine Empfehlungen nennen: Um die Sicherheit der Kaspersky Internet Security 2011 Suite zu erhöhen, sollte die Schutzsuite mit einem **Passwortschutz** versehen werden. In den Werkseinstellungen ist diese Option deaktiviert. 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-Virens Scanner oder Firewall deaktiviert oder modifiziert werden können. Unter den Einstellungen von Kaspersky Internet Security 2011 sollte im Bereich „Einstellungen für Proxyserver und Kontrolle des Netzwerkverkehrs“ die Option „Alle Netzwerkports kontrollieren“ ausgewählt werden. Hier ist in den Werkseinstellungen „nur ausgewählte Ports überwachen“ gesetzt.

Optional sollte zudem die „Heuristische Analyse“ des „Mail-Anti-Virus“ auf „tief“ gesetzt werden. Außerdem genügt es, wenn „nur eingehende Nachrichten“ auf Malware hin untersucht werden.

Den Testern und Sicherheitsexperten ist lediglich das Updateverhalten der Kaspersky Internet Security 2011 **negativ** aufgefallen.

Aus Sicht der Benutzerfreundlichkeit ist das Updateverhalten des Produktes nicht immer nachvollziehbar. Manchmal werden verfügbare Updates erst nach einer Zeitdauer von Stunden automatisch heruntergeladen. Bei anderen Testreihen wiederum nach 25 Minuten.

Ähnliches Verhalten war ebenso bei manueller Modifikation der Updateeinstellungen zu beobachten. Hier ist der Wert auf 15 Minuten gesetzt worden, so dass die Schutzlösung automatisch alle 15 Minuten nach verfügbaren Updates auf dem Kaspersky-Servern sucht.

Hier zeigte sich, dass nach dem Neustart eines Testrechners unter Windows 7 (64-Bit) erstmalig nach über 30 Minuten ein Aktualisierung stattgefunden hat.

Aus Sicht der Performance sind die verfügbaren Signaturupdates - im Vergleich zu Konkurrenzprodukten - relativ groß. In den durchgeführten Testreihen sind die Downloads der

Signaturupdates durchschnittlich zwischen 0.5 - 3.5 Megabyte groß gewesen. Außerdem werden die Updates, trotz schneller Internetverbindungen, schleppend heruntergeladen. Im Bereich des Updateverhaltens sollte der Hersteller Kaspersky mittelfristig nachbessern.

F.) Test: SCANZEIT (Kurztest)

In diesem Kurztest erfolgt die Analyse der Scanzeiten bzw. Scangeschwindigkeiten des in dem Produkt Kaspersky Internet Security 2011 integrierten Malwarescanners. Das Produkt ist dabei manuell mit den höchsten Sicherheitseinstellungen konfiguriert worden. Ebenfalls wurden die maximal möglichen Heuristikeinstellungen ausgewählt.

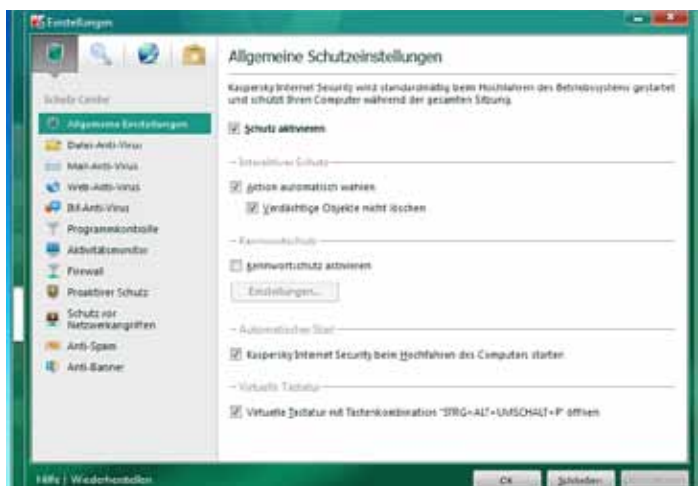
Testkriterium war hier die Scanzeit auf einem Computersystem (Core2Duo E 6300, 2048MB Ram, WD-Sata Festplatte) mit einer 220 GB Partition, wovon 150GB belegt sind mit typischen Nutzerdaten, Dokumenten, zip, rar, iso Archiven, mp3, jpg, gif, pdf, avi und viele weitere.

Die gesamten Testdateien werden dabei von dem Malwarescanner jeweils drei Mal hintereinander überprüft.

Nachfolgende Tabelle zeigt die Scanzeiten des ersten bis dritten Scans an:

Tabelle 3: Scanzeiten:		
1. Scan	2. Scan	3. Scan
41:53 min.	01:05 min.	00:53 min.

Nicht nur die Scanzeiten müssen an diesem Ergebnis näher betrachtet werden, sondern auch die Performanceeinbußen die Teilweise während des Malwarescans aufgefallen sind. Diese waren jedoch nur beim ersten Scandurchlauf erkenntlich. Bei diesem Scanzeit-Kurztest muss beachtet werden, dass die genannten Zeiten lediglich eine Momentaufnahme darstellen. Wenn zum Beispiel manuelle Modifikationen an den Konfigurationseinstellungen des Produktes vorgenommen werden oder viele verschiedene Dateien - und vor allem Dateiformate gesannt werden müssten - würden die Scanzeiten entsprechend besser bzw. schlechter ausfallen.





G.) Test: PREIS-/AUSSTATTUNGSVERHÄLTNIS

Preis (Retailbox)	Preis (Download)	Amazonpreis	Lizenzen	Inhalt (Software)	Punkte (max. 20)	Bewertung
59,95	59,95	52,59	3x	AV, FW, AS, WF, KS, ID	17	gut
39,95	39,95	29,90 (DVD)	1x			

Preise in Euro

Legende: AV = Malware-Scanner / FW = Firewall / AS = Anti-Spam / KS = Kindersicherung / ID = Identitätsschutz / WF = Webfilter

Bei der Beurteilung des Preis-/Ausstattungsverhältnisses fällt auf, dass aktuell (Stand: Juni 2010) kaum nennenswerte Preisunterschiede zwischen dem des Herstellers Kaspersky betriebenen Onlineshop und den Verkaufspreisen von Amazon bestehen.

wird empfohlen die **preiswertere DVD-Box** der herkömmlichen Retailbox vorzuziehen. Diese kann beispielsweise bei Amazon Deutschland unter nachfolgendem Direktlink portofrei bestellt werden:

http://www.amazon.de/Kaspersky-Internet-Security-2011-DVD-Box/dp/B003KTNY5G/ref=sr_1_1?ie=UTF8&s=software&qid=1276728415&sr=8-1

Künftigen Benutzern von Kaspersky Internet Security 2011, die an einer Einzelplatz-Lizenz der Schutzlösung interessiert sind,

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:

SICHERHEIT (Fw-A/ Fw-I / On / Ret / Sonst.)	BENUTZERFREUND. & PERFORMANCE	PREIS-/ AUSSTATTUNG	PUNKTE
40 / 20 / 22.1 / 20.9 / 10	30 / 28	17	188

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)



Das seit wenigen Wochen auf dem Markt erhältliche neue Softwareprodukt Kaspersky Internet Security 2011, geht als ausgezeichnetes Produkt mit nahezu hervorragenden Testergebnissen aus diesem Einzeltest hervor.

Von insgesamt 200 zu vergebenen Punkten erreicht die Schutzlösung 188 Punkte.

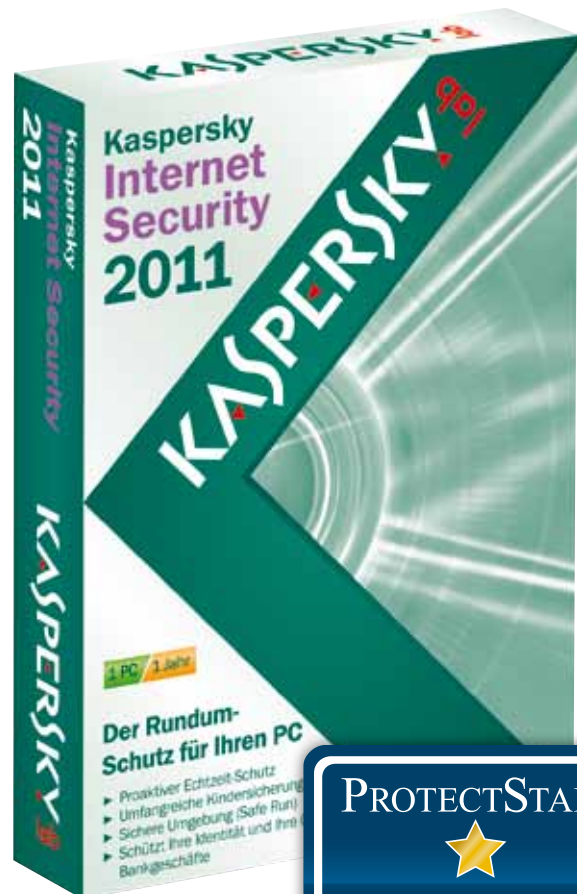
Die Security Suite ist sowohl für Heimanwender, als auch für Profis gleichermaßen geeignet und zeichnet sich durch ein sehr gut abgerundetes Gesamtbild aus. In allen Testbereichen, sei es im Bereich der Sicherheit, Benutzerfreundlichkeit oder der Performance zeigt Kaspersky Internet Security 2011 durchwegs sehr gute Resultate. Vor allem in den Bereichen Malwareerkennung sowie der äußeren und inneren Schutzwirkung der integrierten Firewall kann das Produkt nicht zuletzt auch im Vergleich zu auf dem Markt erhältliche Konkurrenzprodukte ganz eindeutig punkten. Außerdem zeigt sich, dass sich die Version 2011 zur Vorgängerversion 2010 in einigen Bereichen weiter verbessert werden konnte.

Zu nennen an dieser Stelle auch die hilfreichen Zusatzfeatures wie Kindersicherung, Schwachstellensuche, virtuelle Tastatur und das ausführliche Benutzerhandbuch. Die Werkseinstellungen sind nahezu perfekt.

Lediglich im Bereich der Aktualisierungen bzw. des Updateverhaltens sollte der Hersteller mittelfristig Optimierungen vornehmen und nachbessern.

Anwendern von Kaspersky Internet Security 2010 und auch Kaspersky Anti-Virus 2010 wird ein Upgrade auf die neue **Kaspersky Internet Security 2011** empfohlen.

Aufgrund der hervorragenden Gesamtergebnisse und der äußerst positiv aufgefallenen Testergebnisse im Bereich der äußeren und inneren Schutzwirkung der integrierten Personal Firewall, wird **Kaspersky Internet Security 2011** mit den beiden Auszeichnungen „**ProtectStar™ Award 2010**“ und „**ProtectStar™ Firewall Award 2010**“ ausgezeichnet.





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.

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.
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