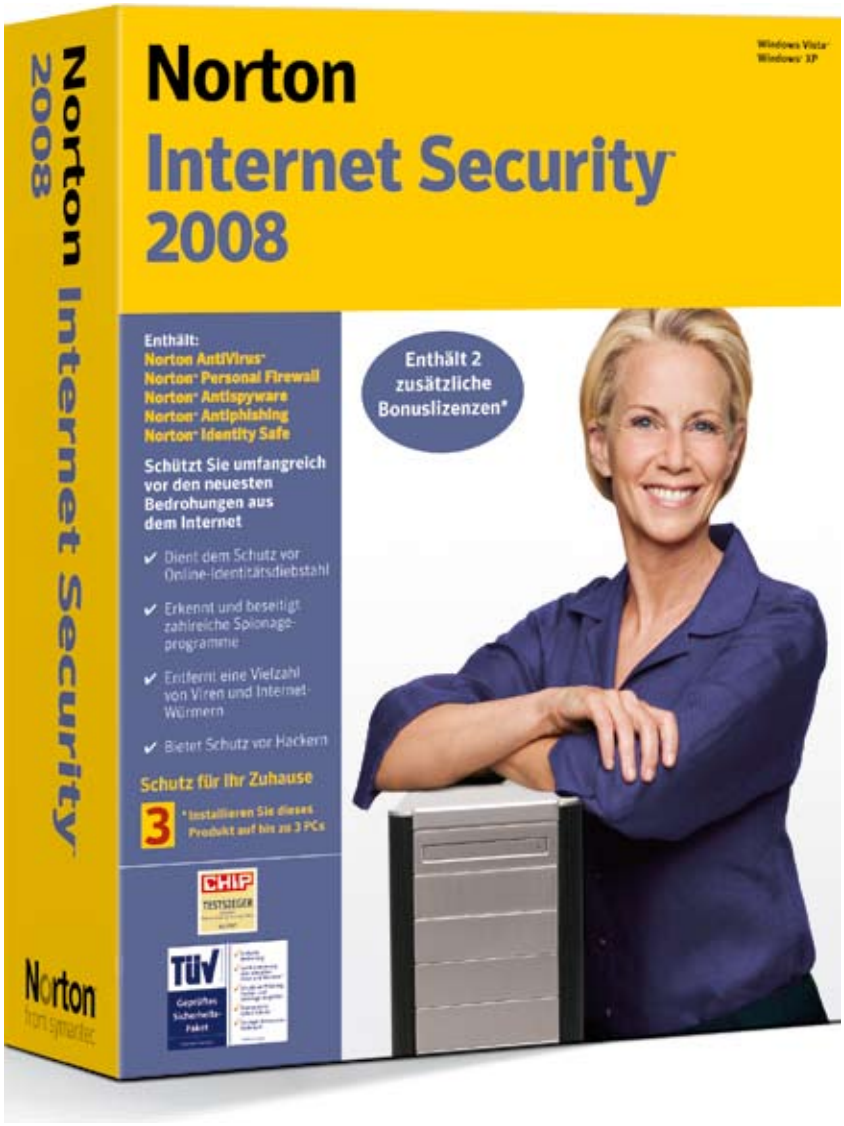
PROTECTSTAR AWARD 2007

PROTECTSTAR™



Norton

Internet Security 2008

SICHERHEIT

Die aktuelle Sicherheitslösung **Norton Internet Security 2008** von **Symantec** zeichnet sich durch eine Mehrzahl an integrierten Schutzmodulen aus. Zu diesen Modulen gehören Virenschutz, Antispyware, Wurmschutz, Rootkit-Erkennung, Angriffsprävention (Intrusion Prevention), Prüfen von Websites auf Echtheit, Schutz vor „Lauschangriffen" und die Verwaltung vertraulicher Informationen.

Das optional erhältliche und **kostenlose Add-On Pack** macht aus **Norton Internet Security 2008** eine Rundum-Sicherheitslösung für die ganze **Familie** mit integriertem Spam-Schutz und Kindersicherung. Das **Add-on Pack** kann auf den Webseiten von **Symantec** heruntergeladen werden; ist jedoch nicht vom **ProtectStar™-Testcenter** analysiert worden.

Norton Internet Security 2008 (zur Verfügung stand die aktuelle Version; Stand: November 2007) wurde sowohl unter **Laborbedingungen** als auch unter **realen Bedingungen** getestet. Die integrierte Personal Firewall, die **ein- und ausgehende** Verbindungen überwacht, hat in den Durchläufen alle zum Testzeitpunkt bekannten **12.564** differenten **Angriffs- und Sicherheitstests** erfolgreich bestanden (Stand: November 2007). 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".

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".

Darüber hinaus wurde die integrierte Norton Personal Firewall 33 **speziellen Angriffsvariationen** für **Firewalls** ausgesetzt. Die Firewall wehrte alle Angriffe **erfolgreich** ab.

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.

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 hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **9634** weitere Sicherheitstests und Angriffstaktiken auf die Norton Firewall ausführte, als auch durch die **manuell** durchgeführten Prüfungen wurden **keine** Schwachstellen oder Sicherheitsrisiken festgestellt. Den **mehrstündigen** Dauer-**Penetrationstest** absolvierte die Firewall **erfolgreich** ohne nennenswerte Performanceverluste.

Ein zusätzlicher Pluspunkt der **Norton Internet Security 2008** ist der umfassende Schutz des vertrauenswürdigen Netzwerkes, falls sich ein Angreifer bereits Zugang verschafft hat. Gerade in diesem Bereich zeigen andere vergleichbare Produkte erhebliche Schwächen. Sie bieten zwar Schutz vor Angriffen aus dem Internet, nicht jedoch vor gezielten Attacken aus dem eigenen (vertrauenswürdigen) Netzwerk/ LAN.

So zeigen vergleichbare Produkte Schwachstellen, wie z. B. **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.

Interessant ist, dass **Norton Internet Security 2008** auch **andere Geräte** im Netzwerk **überwacht**; so moniert das Programm beispielsweise ungesicherte WLan-Verbindungen. Eine gute und sinnvolle Funktion, da bei den meisten Routern die Verschlüsselungsfunktionen ab Werk nicht aktiviert ist. Viele Anwender kommunizieren deshalb oft unbewußt über ungeschützte WLan-Verbindungen.

Der enthaltene **Norton Identity Safe** speichert und verschlüsselt Kennwörter und andere vertrauliche Daten. Nach Aufforderung werden die Angaben sogar selbständig ergänzt. Das spart Zeit und verhindert, dass Fremdprogramme zum Aufzeichnen von Tastatureingaben (Keylogger) Daten auslesen. Zusätzliche Schutzfunktionen übernehmen auch der **Browser Defender.** Dieser erkennt Schadcode die über Drive-by-Download versuchen Sicherheitslücken im Browser auszunützen. Um die Schutzfunktionen des **Anti-Virenscanners** testen zu können, wurden mehrere umfangreiche Viren- und Malwarearchive erstellt. Diese Archive umfassten insgesamt über **zwanzigtausend** verschiedene Schädlinge. Von neuen und aktuellen Viren, Würmern, Trojanern, Dialern und Spyware, bis hin zu alten MS-DOS Bootviren und selbstentwickelten unbekannten Schädlingen. Zusammenfassend konnte die **Malware-Erkennungsrate** auf **98,83%** bestimmt werden. Dieses **sehr gute** Resultat im Bereich der Virenerkennung deckt sich ebenfalls mit den Ergebnissen von anderen bekannten und renommierten Virentest-Laboren wie beispielsweise AV-Comparatives.

BENUTZERFREUNDLICHKEIT

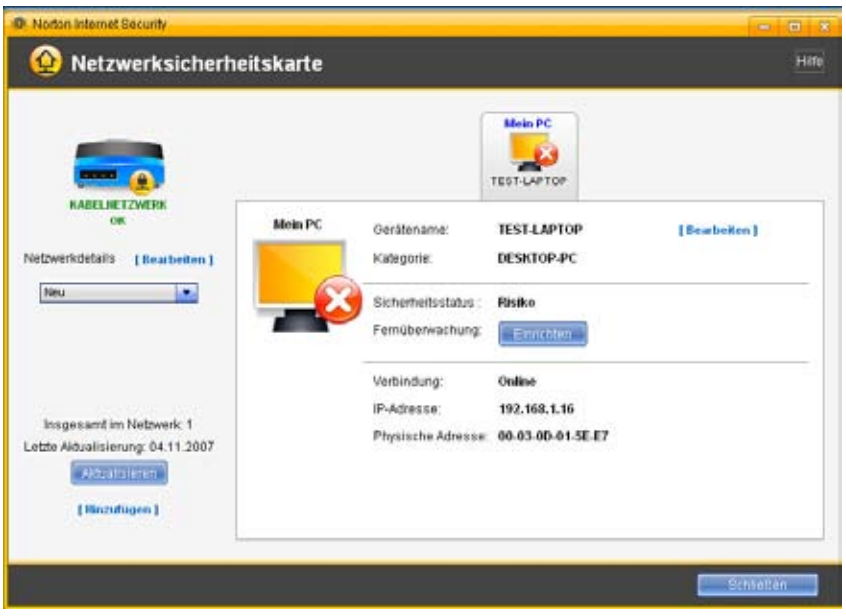
Norton Internet Security 2008 richtet sich an alle Anwender, die eine moderne Internet Security Suite wünschen und zugleich auf eine integrierte BackUp-Funktion verzichten möchten. Für Benutzer, die alles aus einer Hand wünschen, bietet Symantec daher die Lösung „Norton 360" an. Gleichzeitig richtet sich **Norton Internet Security 2008** aber auch an den normalen Heimanwender, der einen Schutz „Out-Of-The-Box" haben möchte. Dieser Eindruck entsteht zumindest durch den großen Werbeaufwand und wird durch das Programm selbst bestärkt.

Einige der in der Suite integrierten Produkte sind auch als **Einzellösungen** erhältlich, wie beispielsweise Norton Anti-Virus 2008 und Norton Confidential. Die Installation des knapp 70 MB großen Software-Paketes verläuft **unproblematisch**, wenn auch etwas ungewohnt. Bevor die eigentliche Installation beginnt, prüft Symantec, ob auf den Servern eine aktuellere Version bereit steht. Ist dies nicht der Fall,

beginnt die Malware-Überprüfung des Computers. Was hier genau passiert erfährt der interessierte Nutzer leider **nicht**. Es folgt die obligatorische Bestätigung der „EULA." Danach beginnt sofort die Installation. Es gibt keinerlei Möglichkeiten die Installation nach Anwenderwünschen zu beeinflussen. Einzelne Module abzuwählen oder den Installationspfad zu ändern. Seitens Symantec ist das nicht vorgesehen.
Auf der anderen Seite, kauft der Kunde eine Suite, weil er alle Lösungen wie Anti-Virus, Firewall, Anti-Spam, etc. verwenden möchte.

Während der Installation zeigt Symantec einen farbig animierten Balken, der jedoch keinerlei Rückschlüsse auf den Fortschritt des Installationsverlaufes zulässt. Überraschenderweise verlangt **Norton Internet Security 2008** keinen Neustart des Windows Betriebssystems, 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**".

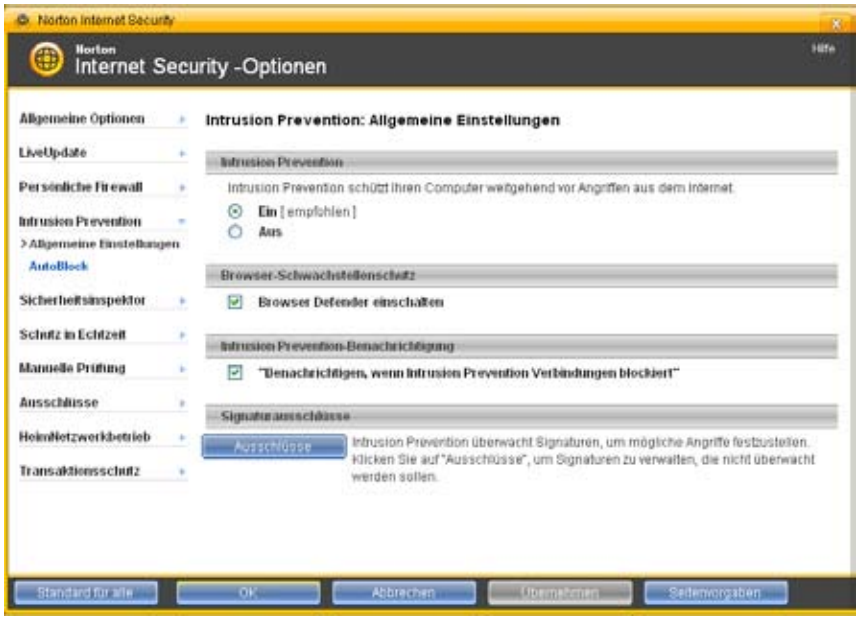


Nach der Installation beginnt **Norton Internet Security 2008** nicht mit dem automatischen herunterladen aktueller Virendefinitionen und Patches. Die Updates werden über das Modul **Live-Update** gesteuert. Nur erfährt der Anwender im Programm selber nichts Detaillierteres über dieses Modul.
Es gibt keinerlei Einstellmöglichkeiten oder eine Protokollfunktion an dieser Stelle. Das Live-Update bindet sich in die Systemsteuerung von Windows ein. Hier kann das Updateintervall eingestellt werden.

Voreingestellt ist ein **Update-Intervall** von **240 Minuten**. Protokolliert wird die korrekte Funktion des Live-Updates über das **Ereignissprotokoll** von Windows. Aus diesem Protokoll kann man ein großes **Manko** erkennen: Symantec schaut erst 15 Minuten nach dem Rechnerstart nach Updates. Ist ein Anwender also nur kurz an seinem Computer, um beispielsweise seine E-Mails abzurufen, wird u.U. **kein Update** durchgeführt. Das kann dazu führen, dass der Benutzer nach einiger Zeit mit veralteten Signaturen seine Mails abruft und ein ausreichender Schutz nicht gewährleistet wird. Den Hersteller Symantec haben wir diesbezüglich kontaktiert. Dort teilte man den Sicherheitsexperten des ProtectStar™ Testlab mit, dass das LiveUpdate vollständig zeitunabhängig arbeitet. Der Anwender kann zwar auch zeitgesteuerte Updates fahren, doch das LiveUpdate holt sich immer alle aktuellen Updates von den Symantec-Servern, sobald diese dort bereitstehen.

Die in **Norton Internet Security 2008** integrierte Firewall funktionierte in allen Testreihen gut. In der Grundkonfiguration erstellt Norton Regeln für die Anwendungen nach eigenen definierten Regelsätzen.
Eine Abfrage, ob ein Programm Verbindungen ins Internet aufnehmen soll, erfolgt in den Voreinstellungen nicht; der Anwender muss dies explizit aktivieren.
Aufgefallen ist, dass die Firewall weitestgehend automatisiert ist und selbständig genutzte Anwendungen und auch Online-Games erkennt und konfiguriert.

Nortons Virenwächter - **Auto Protect** genannt - überzeugt durch seine Schnelligkeit. Auch der HTTP-Scan funktioniert mit allen getesteten Internet-Browsern wie Opera, Firefox und InternetExplorer, reibungslos. Auch umfangreiche Webseiten oder Streams wie Youtube.com oder clickfish.com werden ohne erwähnenswerte Verzögerungen angezeigt - unabhängig vom verwendeten Browser.



Allerdings sind in Sachen der Benutzerfreundlichkeit die relativ geringen Konfigurationsmöglichkeiten von **Norton Internet Security 2007** zu erwähnen:
Es lässt sich lediglich die Heuristik („Bloodhound") zuschalten.
Allerdings werden die Aktivitäten des Wächters **umfangreich protokolliert** - auch wenn diese Funktion nicht einfach zu finden ist.

Weiterhin integriert Symantec die **SONAR-Technologie**. Hierbei handelt es sich um eine verhaltensbedingte Analyse von Anwendungen, die eine Verbindung ins Internet aufbauen wollen. Zu verstehen ist dieses Feature als ein Zusatz zur klassischen **heuristischen Erkennung,** welche auch neue **Rootkits** erkennen soll. Insgesamt gefällt die Benutzerfreundlichkeit von **Norton Internet Security 2008**. Die einzelnen Schutzmodule sind klar voneinander abgegrenzt, das Programm insgesamt sehr übersichtlich gehalten.

PERFORMANCE
Verglichen mit früheren Versionen ist die Performance der aktuellen **Norton Internet Security 2008** verbessert worden. Man sollte dennoch einen leistungsfähigen Rechner besitzen, der dem heutigen Industriestandard entspricht Der Rechnerstart wird auf aktuellen Systemen kaum verzögert. Programme (auch komplexe wie Nero) öffnen sich schnell. Ebenso der OnDemand-Scan und Wächter arbeiten schnell. Anwendern, denen die Performance von **Norton Internet Security 2008** nicht ausreicht, können per Telefon den Support von Symantec kontaktieren. Der Support richtet dann die Suite so kostenlos ein, dass die maximale Performance erreicht wird. Dieses geschieht über ein Remote-Tool. Allerdings war für die Testingenieure des ProtectStar-Testcenters nicht ersichtlich und transparent was von einem Symantec-Techniker konfiguriert wurde.

Die Installation erfolgte auf Systemen mit Prozessoren von 1,8 bis 3,2 GHz Taktfrequenz. Zur Verfügung stand unterschiedliche Hardware mit 512 – 4096 MB Hauptspeicher unter Windows XP und Windows Vista. Der Scanner arbeitet relativ zügig. Für den Scan eines kompletten Testsystems –bestehend aus drei Partitionen, Gesamtbelegung ~ **200 GB** - benötigte der integrierte Anti-Virenscanner **1 Stunde 6 Minuten**.

Betrachtet man aktuelle Vergleichstests, liegt die Scanleistung des Norton Anti-Virenscanners im vorderen Drittel. Allerdings **übersieht** Norton einen SDBot im Thunderbird-Mailarchiv. Nero-Backuparchive werden von dem Norton Scanner nicht durchsucht; hier arbeiten G Data, F-Secure und Kaspersky genauer und prüfen auch diese Archive auf Malware. Der Scan wird wieder durch einen animierten Balken geleitet, der jedoch nicht als Fortschrittsbalken arbeitet. Die Konfigurationsmöglichkeiten des Scanners sind gering. Ein ausführliches Protokoll wird leider nicht erstellt. Scans lassen sich planen; die Funktion ist jedoch versteckt. Interessant

ist die Möglichkeit des **Quickscans**, bei dem laut Symantec „häufig betroffene Verzeichnisse" und der Arbeitsspeicher gescannt werden. Der Seitenaufbau beim surfen im Internet wird wenig, aber dennoch spürbar verzögert. Die gelobte Performance des OnDemand-Scanners wird durch die Voreinstellungen des Programms **begünstigt**: Der Scanner läuft mit hoher Priorität und es wird die automatische Dateierkennung angewendet.

SUPPORT

Mit dem Erwerb von **Norton Internet Security 2008** erhalten Anwender wie gewohnt **ein Jahr** lang Software- und Patternupdates sowie den Support von Symantec **inklusive**. Alle verfügbaren Serviceleistungen können Benutzer nach **Aktivierung** bzw. **Registrierung** der Sicherheitslösung nutzen. Sie ermöglichen zum Beispiel das Programm automatisch zu aktualisieren, technische Anfragen per E-Mail zu stellen sowie Feedback und Erfahrungen über das Produkt an den Hersteller zu versenden.

PREIS- und LEISTUNG

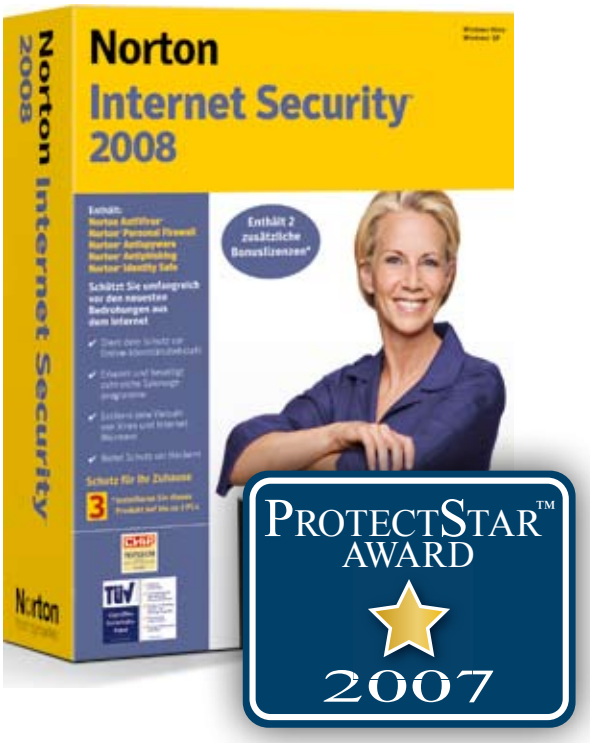
Die aktuelle **Norton Internet Security 2008** wird als Box- oder Downloadversion mit einem empfohlenen Verkaufspreis von **Euro 59,99** (inkl. Lizenz für bis zu 3 Computer) angeboten. Alternativ existiert auch eine 1-User Box zum Preis von **Euro 39,99**

FAZIT

Die Testreihen haben gezeigt, dass **Symantec** mit seiner neuen Sicherheitslösung **Norton Internet Security 2008** – nicht zuletzt im Vergleich zur Vorgängerversion - eine Vielzahl an **positiven Verbesserungen** hervorgebracht hat. Für knapp 60 Euro erhält der Anwender die Komplettlösung mit insgesamt **drei Lizenzen**. Es lässt sich somit ein kleines Heimnetzwerk günstig absichern. Für den gebotenen Preis erhält der Anwender eine solide und zuverlässig arbeitende Internet Security Suite die zudem **sehr guten Grundschutz** mit **angenehmer Benutzerfreundlichkeit** kombiniert. Hervorzuheben sind die hohe Virenerkennungsrate von **98,83%** und die **sehr guten** Schutzfunktionen des Anti-Viren- und Anti-Spyware-Scanners sowie der integrierten Firewall

Einzig die Verzögerung des Updates nach dem Rechnerstart und etwas lange Reaktionszeit auf neue Viren stören das sehr gute Gesamtbild. Allerdings wirbt Symantec mit den proaktiven Technologien wie SONAR, das selbst unbekannte Schädlinge erkennen soll und dadurch auch eine „Verzögerung" der Updates vom Anwender in Kauf genommen werden kann. Wer sich intensiver mit dem Thema Sicherheit am PC beschäftigen will, der wird von den eher geringeren Konfigurationsmöglichkeiten enttäuscht sein.

Norton Internet Security 2008 von **Symantec** wird aufgrund der durchwegs sehr guten Testergebnisse mit dem „**ProtectStar™ AWARD 2007**" ausgezeichnet.



PROTECTSTAR™
Inc.
1901 60th Place
Suite L 3604
Bradenton, FL
34203 USA
http://www.protectstar.com
testcenter@protectstar.com