# SICHERHEIT

Die aktuelle Sicherheitslösung für Microsoft Windows, Internet Security 2007 des finnischen Herstellers F-Secure zeichnet sich durch eine Reihe an integrierten Schutzmodulen aus. Zu diesen Modulen gehören Anti-Virus, Anti-Spyware, Personal Firewall, Kindersicherung, Anti-Spam, Anti-Pharming und ein Schutz gegen Rootkits und Zero-Day-Angriffe.


In den Testreihen wurde F-Secure Internet Security 2007 sowohl unter Laborbedingungen, als auch unter realen Bedingungen gleichermaßen getestet.

Im Testlabor von ProtectStar™ konnte die Security Suite in der aktuellen Softwareversion getestet werden. Turnusmäßig musste die Sicherheitslösung umfassende Testreihen durchlaufen.

Die integierte Stateful Packet Inspection Firewall mit zusätzlichem Intrusion Prevention System hat an den Tagen der Testverfahren alle zum Zeitpunkt bekannten 11.759 verschiedenen Angriffs- und Sicherheitstests erfolgreich bestanden.

Die Sicherheitstests enthielten alle bekannten Denial of Service (DoS) – Angriffsarten, sowie die Ausnutzung aller zum Zeitpunkt der Testverfahren bekannten Schwachstellen von Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors, Sicherheitschecks, uvm.

In einer weiteren Testphase wurde die Personal Firewall in den verfügbaren Sicherheitsprofilen von F-Secure Normal, Büro, Streng und „Alles Blockieren“ betrieben und mit standardisierten Portscans nach eventuell geöffneten TCP- und UDP- Ports gescannt. Dabei wurden alle Ports (0 – 65535) gescannt.
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 können.

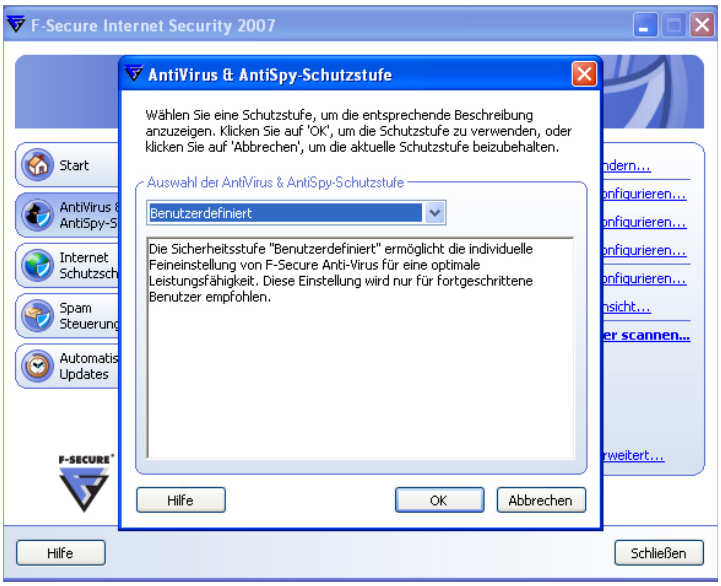
Sowohl durch die automatisch ablaufenden Testreihen des hauseigenen ProtectStar™ Security-Scanners (zusätzlich 7348 weitere Sicherheitstests und Angriffstaktiken) als auch durch die manuell durchgeführten Prüfungen konnten – zumindest unter den Firewall-Profilen „Büro“, „Streng“ und „Alles blockieren“ keine Schwachstellen festgestellt werden.

Allerdings zeigte sich, dass zumindest theoretisch und durch entsprechende Kenntnis ein erfahrener Angreifer die in F-Secure Internet Security 2007 integrierte Firewall unter dem Sicherheitsprofil „Normal“ (Werkseinstellung) manipulieren könnte. Im Rahmen der durchgeführten und erweiterten Sicherheitstests fand sich im Bezug auf die TCP Sequence prediction, dass der TCP/IP Stack nicht vollständig geschützt ist. Dies hätte zur Folge, dass ein Angreifer die Sequenz-Nummer vorhersagen bzw. erraten, und somit bestehende Verbindungen manipulieren könnte.

Ferner ließen sich unter den Werkseinstellungen (Profil der Firewall: Normal) die NetBIOS name tables erlangen, so dass ein Angreifer Informationen über den Rechnername, Netzwerk, Arbeitsgruppe, usw. erhalten könnte.
Ebenso ließ sich die MAC Adresse, Uhrzeit und Zeitzone des Testssystems eindeutig bestimmen.

Die genannten Informationen sind allerdings nur über das Firewall-Profil „Normal“ zugänglich. Alle anderen Profile wie „Büro“ und „Streng“ zeigten keine Sicherheitsrisiken.
Es wird Anwendern daher empfohlen, nach der Installation von F-Secure Internet Security 2007, manuell auf das Firewall-Profil „Büro“ oder „Streng“ umzuschalten, sofern der Computer/Notebook direkt am Internet – ohne vorgeschaltetem Firewall-Router – angeschlossen ist.

Den zweistündigen Dauer-Penetrationstest konnte die Personal Firewall uneingeschränkt und erfolgreich absolvieren.




Mit Hilfe der so genannten „Leaktests“ wurde weiterhin überprüft, ob die Firewall verschiedene Techniken erkennt, um Informationen (Passwörter, persönliche Daten, usw.) von einem Computer aus - in das Internet vorbei an der Firewall zu schleusen:

Hier zeigte die in F-Secure Internet Security 2007 integrierte Firewall ihre Schwächen, denn von insgesamt 25 verschiedenen Leaktests konnte die Firewall lediglich 2 (mit deaktiviertem Anti-Virenscanner) und 4 (mit aktiviertem Anti-Virenscanner) Leaktests erkennen und blockieren.

Hier sollte der Hersteller dringend nachbessern, denn vergleicht man die Resultate anderer durchgeführter Tests an aktuellen Internet Security Suite oder Personal Firewalls, so schneiden Fremdprodukte in diesem Bereich besser ab (bspw. Vergleich zu PC-cillin Internet Security 2007 von Trend Micro: 23 von 25 Leaktests konnten erfolgreich blockiert werden).

Die Erkennungsrate bei den Leaktests könnte lediglich durch die Einbindung und Konfiguration der integrierten Kindersicherung höher ausfallen. Zudem ist es nötig zu erwähnen, dass bei F-Secure Internet Security 2007 der ausgehende Datenverkehr in der Werkseinstellung grundsätzlich zugelassen wird, um einen höheren Grad an Benutzerfreundlichkeit gewährleisten zu können. Einen wesentlich höheren Schutz erreicht man durch Aktivieren des Firewall-Profils "Streng", das ausgehenden Datenverkehr stark reglementiert. Dies erfordert aber fundiertes PC-Wissen.

die Virenerkennungsrate aufgrund der weniger sicherheitsspezifischen Einstellungen mit 98,20% etwas niedriger.

Besonders erwähnenswert ist auch, dass der Anti-Virenscanner von F-Secure zu den wenigen Anti-Virenscanner auf dem IT-Sicherheitsmarkt gehört, der keine Schwierigkeiten mit getesteten „Zip of Death" – Archiven hat.

Positiv aufgefallen ist ebenfalls, das F-Secure Internet Security 2007 sehr schnell den während der Testreihen kursierten „GEZ-Trojaner" („Nurech AC") erkannte, während beispielsweise andere Konkurrenzprodukte selbst nach über 12 Stunden keine Signaturen zur Verfügung gestellt hatten.

Nimmt man aktuelle Virenerkennungstests einer asiatischen Computerfachzeitschrift zu Rate, so besitzt F-Secure sogar eine 100% Virenerkennungsrate aufgrund folgender Resultate:

1. Neue Trojaner (52) -> 52 erkannt
2. Alte Trojaner (130) -> 130 erkannt
3. Backdoors (130) -> 130 erkannt
4. Runtime packed (125) -> 125 erkannt
5. Hijacker (25) -> 25 erkannt
6. Rootkits (11) -> 11 erkannt
7. Macro Viren (46) -> 46 erkannt
8. Win32 Viren (28) -> 28 erkannt
9. Würmer (326) -> 326 erkannt

F-Secure Internet Security 2007 sucht in den Werkseinstellungen automatisch alle zwei Stunden nach neuen Updates und lädt diese automatisch herunter. Bei globalen oder lokalen Virenausbrüchen (Outbreaks), gibt es zudem Eilupdates, die in der Regel sofort für den Anwender bereit stehen.
Das Update selbst in mehrere Downloads unterteilt in denen alle einzelnen Programmteile wie zum Beispiel Anti-Spam und Anti-Virenscanner aktualisiert werden. Der Updateserver zeigte sich während der Testreihen als gut erreichbar und eine Aktualisierung fand durchschnittlich in 1-3 Minuten statt.

Außerdem sind die Schutzfunktionen des Anti-Virenscanners im Vergleich zur Vorgängerversion soweit optimiert worden, dass nicht nur beim Öffnen/Starten einer Datei nach verdächtigen Viren in der Datei gesucht werden, sondern auch beim Kopieren, Verschieben und Speichern einer Datei.

Positiv erwähnenswert ist auch, dass F-Secure Internet Security 2007 nach einem Systemneustart automatisch nach verfügbaren Updates sucht.

Dem immer größer werdenden Ansturm von betrügerischen E-Mail Nachrichten und Webseiten (Phishing) wirkt F-Secure mit dem integrierten Phishing-Modul entgegen. Es ist vor allem für Heimanwender oder unerfahrene Anwender nützlich. Sobald diese Option aktiviert wurde, erkennt und neutralisiert dieses Schutzmodul E-Mails, die darauf abzielen, falsche Webseiten zu verwenden und vertrauliche Daten zu stehlen.

Wird eine solche Phishing-E-Mail erkannt, wird der Anwender umfassend über den Vorfall informiert.

Pharming basiert auf einem ähnlichen Prinzip wie Phishing, nutzt jedoch keine E-Mails um den Nutzer auf gefälschte Webseiten zu lenken, sondern verändert die Host Datei und sorgt so dafür, dass Anwender permanent auf falsche Webseiten weitergeleitet werden.

Optisch ansprechend und vor allem informativ sind die in F-Secure Internet Security 2007 integrierten Benachrichtigungsfunktionen bzw. das Pop-Up Informationssystem, welches den Anwender kontinuierlich über aktuelle Gefahren informiert.

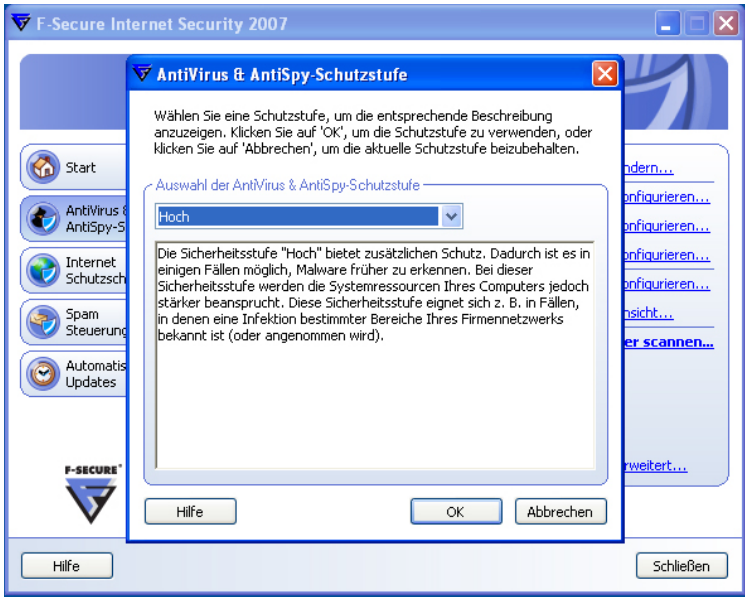
Es informiert Benutzer beispielsweise in Echtzeit über die neuesten Virenausbrüche.

Mit Hilfe einer integrierten Schutzfunktion vor sog. Zero-Day-Attacken, möchte der Hersteller den Anwender von F-Secure Internet Security 2007 selbst vor noch unbekannten Angriffen und unvorhersehbare Bedrohungen schützen.

Ermöglicht wird dies durch die neue DeepGuard™ Technologie von F-Secure, die beispielsweise auch Rootkits entdecken soll. So werden Programme beim Eintreten in das System nicht nur analysiert, sondern überwacht. F-Secure DeepGuard™ beobachtet das Verhalten der Software im Echtzeitmodus, scannt das System nach verdächtigem Programmverhalten und bricht potenziell risikoreiche Aktivitäten einfach ab. Das Produkt vereint mehrere proaktive Technologien und bietet so einen Schutz gegen zuvor unbekannte Bedrohungen. Praktisch für Familien ist die integrierte Kindersicherung mit Zeitsperre und Anwenderprofilen. F-Secure Internet Security 2007 verfügt nun über drei verschiedene Kindersicherungsprofile:

| | |
|---|---|
| Kinder | (nur zugelassene Sites können aufgerufen werden) |
| Teenager | (inhaltsbasierte Filterung) |
| Erwachsene | (uneingeschränkter Zugriff). |

Der Zugriff auf Sites, die außerhalb der durch diese Profile festgelegten Parameter liegen, wird automatisch blockiert. Wie gewohnt können Elterndie Surfzeit ihrer Kinder aber auch über die Zeitsperrfunktion beschränken.




# BENUTZERFREUNDLICHKEIT

Die Installation von F-Secure Internet Security 2007 verläuft wie gewohnt problemlos und anwenderfreundlich. Während der Installation wird der Benutzer durch einen Wizard über bereits auf dem Computersystem installierte Sicherheitsprogramme, wie Anti-Virenscanner und Personal Firewall informiert.

Leider kann man während der Installation nur die integrierte Kindersicherung aus- bzw. abwählen. Hier wäre es anwenderfreundlicher, wenn der Anwender die einzelnen Schutzmodule individuell auswählen könnte.

Bereits während der Installation fragt F-Secure den Anwender nach einem Aktivierungsschlüssel. Gibt man dort keinen Aktivierungscode ein, kann man das Programm lediglich 30-Tage nutzen. Nach der Installation beginnt ein 120 Sekunden-Countdown bis zum Neustart. Diesen kann man selbstverständlich abkürzen oder auch ganz abbrechen.

Nach dem ersten Neustart merkt der Benutzer, dass das Computersystem länger als gewohnt benötigt. Dann beginn F-Secure Internet Security 2007 unverzüglich mit der Aktualisierung der neuesten Patches, Virensignaturen, Spam-Regeln, etc. Der Fortschritt der Updates wird durch einen kleinen Fortschrittsbalken unter dem Trayicon symbolisiert.

Diskussionswürdig sind teilweise die Werks- bzw. Voreinstellungen von F-Secure Internet Security 2007:
Der Http-Scan ist in den Voreinstellungen deaktiviert, ebenso die Anwendungssteuerung der Firewall. Laut des Herstellers F-Secure hat wurde der http-Scanner deshalb standardmäßig deaktiviert, um eine bessere Performance gewährleisten zu können.

Wenn der Anwender höhere Sicherheit gegenüber Performance präferiert, empfehlen wir natürlich, trotzdem den http-Scanner einzuschalten, um vor Malware geschützt zu sein, die direkt im Browser geöffnet wird (Bspw.: jpg-Exploit).

Der http-Scan funktionierte während der Testreihen zuverlässig mit den aktuellen Versionen von Opera, Firefox und Internet Explorer.

Die Sicherheitslösung prüft alle zwei Stunden ob neue Updates vorliegen. Dieses Intervall lässt sich manuell nicht verändern, was auf ein Unverständnis des Benutzers stoßen könnte. Allerdings ist eine Updateprüfung jederzeit manuell aus dem Programm heraus möglich.

Leider kann ein Virenscan nicht pausiert, sondern nur komplett gestoppt oder abgebrochen werden. Scanberichte werden nicht aufbewahrt; es ist immer nur der jeweils letzte verfügbar. Der Scanbericht selbst ist jedoch sehr ausführlich, so werden beispielsweise auch alle nicht gescannten Dateien genannt.

Eine Fortschritts- oder Zeitanzeige während des Virenscans wäre eventuell ein zukünftiges Feature für kommende Releases, welches die Benutzerfreundlichkeit von F-Secure Internet Security 2007 noch steigern könnte.

Der Effekt ist, dass der Benutzer nicht weiß, ob der Browser komplett abgestürzt ist oder nicht.

Die Original CD-Rom kann in Notfällen als bootfähiges Rettungsmedium eingesetzt werden. Allerdings lässt sich diese nicht automatisch mit neuen Virensignaturen aktualisieren.

Sollten Anwender Probleme oder Fragen haben, helfen neben dem Support von F-Secure das Handbuch und die Online-Programmhilfe, in der die Benutzer eine Vielzahl von Hilfestellungen, Tipps und eine FAQ erhalten.

Positiv ist hier vor allem das ausführliche Handbuch mit einem sehr gutem Glossar zu erwähnen.

Anwender, die die Vorgängerversion 2006 von F-Secure Internet Security verwenden und auf die aktuelle Version upgraden möchten, brauchen sich um bereits erstellte Personal-Firewall-Profile keine Gedanken zu machen. Sie werden automatisch in die aktuelle Version importiert.

Während der Testreihen ist aufgefallen, dass das integrierte Anti-Spammodul aggressiv zu Werke geht. So werden Adressen wie „Amazon.de“ oder „Discountfan.de“ als Spam klassifiziert. Leider fügt das Anti-Spam-Modul keinen Hinweis in den Betreff der entsprechenden E-Mail ein, so dass man nicht erkennen kann, ob eine E-Mail von dem verwendeten E-Mail Programm wie beispielsweise Microsoft Outlook oder von dem Anti-Spam-Modul selbst in den Spamordner verschoben wurde.

Nutzt der Anwender beispielsweise Opera oder Firefox als Internetbrowser und besucht Webseiten wir clipfish oder youtoube, so fällt auf, dass F-Secure Internet Security 2007 den Aufruf von Flash-Filmen verzögert.
Überhaupt beeinflusst die Sicherheitslösung ab und zu störend einen Download: Beim Start eines Downloads vergeht daher oftmals eine längere Zeitspanne bis der Downloaddialog erscheint. Dann scheint der Browser wie „eingefroren“ zu sein. Es ist dann auch nicht möglich auszuwählen, wie mit der Datei zu verfahren ist.

# PERFORMANCE

Bereits die Vorgängerversion F-Secure Internet Security 2006 ist in Sachen Performance ein großer Kritikpunkt gewesen. Die aktuelle Version der Schutzlösung zeigt hier zwar leicht bessere Resultate, kann jedoch noch nicht gut glänzen:

Nach dem ersten Neustart benötigten die Test-Computer je nach dessen Systemperformance bezüglich CPU und Hauptspeicher, zwischen 15 – 40 Sekunden länger für das Hochfahren von Windows XP, als ohne die aktuelle Sicherheitslösung von F-Secure. Auch arbeiten insgesamt 14 Prozesse im Hintergrund, die Durchschnittlich circa 80MB, und bei Belastungstests sogar 140MB Arbeitsspeicher belegen.

Im Allgemeinen zeigt sich, dass sich aufgrund der Installation von F-Secure Internet Security 2007 der Bootprozess verzögert, Kopieaktionen im Windows-Explorer länger dauern und das Starten von Programmen wie Nero, PhotoShop, Outlook, etc. verzögert wird.


Befriedigende Ergebnisse zeigte die Scangeschwindigkeit des Anti-Virenscanners:

So benötigte eine komplette Systemüberprüfung auf einem Intel Core 2 Duo 6300 mit 1.86 GHz Taktfrequenz, rund 82 Minuten für eine Systempartition mit 17GB, eine Datenpartition mit insgesamt 55GB (davon 33GB Musikdateien, 2.5GB Bilder, 9.5GB Videodateien, 0.2 GB Dokumente, sowie Treibern, Programme, Iconpacks, etc.). -> Systeminformationen

Ein weiterer Test mit einem 3.2 GHz Intel-Prozessor benötigte für eine 65GB belegte Festplatte knapp 90 Minuten.

Während der Testverfahren wurde F-Secure Internet Security 2007 bezüglich der Performance einwandfrei auf unterschiedlichen Testsystemen zwischen 1200-3200 MHz und 512-2000 MB Hauptspeicher erfolgreich getestet.

Ein reibungsloses Arbeiten mit F-Secure Internet Security 2007 ist beispielsweise auf einem Computersystem unter Windows XP mit 500MHz Taktfrequenz und 256MB Hauptspeicher nicht mehr möglich gewesen. Hier wurden Reihen von Performanceeinschränkungen analysiert, die sich vor allem durch ein zu langes Laden/Starten von Programmen bemerkbar machte, was den Arbeitsablauf stark beeinträchtigte.

Nichts desto trotz arbeitet F-Secure Internet Security 2007 auf allen aktuellen Computersystem und welche, die nicht älter als circa zwei Jahre alt sind, sehr zuverlässig und nahezu ohne spürbaren Performance-Einschränkungen zu versenden.

## SUPPORT

Mit dem Erwerb von F-Secure Internet Security 2007 erhalten Anwender wie gewohnt ein Jahr lang Software- und Patternupdates sowie den Support von F-Secure inklusive.

Alle verfügbaren Serviceleistungen können Benutzer nach Aktivierung durch die Eingabe des persönlichen Aktivierungscodes der Security Suite nutzen. Sie ermöglichen, das Programm automatisch zu aktualisieren, verdächtige Dateien via Onlineformular zur Analyse einzusenden, technische Anfragen per E-Mail zu stellen sowie Feedback und Erfahrungen über das Produkt


## PREIS UND LEISTUNG

Die aktuelle F-Secure Internet Security 2007 wird mit einem empfohlenen Verkaufspreis von Euro 39,95 angeboten. Eine zweite zusätzliche Lizenz kann für nur Euro 10,00 erworben werden.

Im Preis enthalten sind tägliche Virensignatur-Updates für 12 Monate sowie kostenloser, deutschsprachiger E-Mail- und Telefonsupport.

Zusätzlich bietet der Hersteller ein kostenloses Online-Tutorial unter folgender Webadresse:

http://support.f-secure.de/enu/home/elearning/is2007el_deu/index.html

Kunden mit einem gültigen Abonnement von F-Secure Internet Security 2006 erhalten ein kostenfreies Upgrade auf die 2007er Version.

Anwender des neuen Betriebssystems Microsoft Windows Vista erhalten ebenfalls ein kostenfreies Upgrade.

Darüber hinaus gehen bei einer Lizenzverlängerung oder Upgrade die Lizenzzeiten nicht verloren, sondern werden zusätzlich an die neue Lizenz hinzugefügt.

## FAZIT

Die Testreihen zeigen, dass F-Secure mit seiner aktuellen Sicherheitslösung Internet Security 2007 mehrere Verbesserungen hervorzubringen hat.

Hervorzuheben sind vor allem die Vielzahl an integrierten Schutzmodulen, die hohe Virenerkennungsrate von 98,92%, die guten Schutzfunktionen des Anti-Viren- und Anti-Spyware-Scanners sowie die sehr guten Schutzfunktionen der Stateful Packet Inspection Firewall gegen externe Angriffe.

Die integrierte Firewall zeigte jedoch unzureichende Resultate im Bereich der Leaktests, denn in den durchgeführten Testreihen konnte die Firewall in Verbindung mit dem Anti-Virenscanner lediglich 4 von 25 durchgeführten Leaktests abwehren.

Dennoch hängt die Sicherheitslösungen aufgrund ihrer großen Ressourcenbelastung hinter anderen auf dem IT-Sicherheitsmarkt erhältlichen Security Suiten zurück.

Aus diesem Grund verfehlt F-Secure Internet Security 2007 den „ProtectStar™ AWARD 2007“.

Die Internet Security Suite von F-Secure wird jedoch aufgrund der guten Resultate im Bereich der Virenerkennung und der sehr guten Schutzwirkungen der Firewall gegen externe Angriffe mit der Empfehlung „ProtectStar™ Excellent Security 2007“ ausgezeichnet.


PROTECTSTAR™ INC.

1901 60TH PLACE
SUITE L 3604
BRADENTON, FL
34203 USA

HTTP://WWW.PROTECTSTAR.COM
TESTCENTER @ PROTECTSTAR.COM