Andreas Marx, Vera Günther

Einsatz der Virenkiller

Seit es Krankheiten gibt, arbeitet die Menschheit an deren Ausrottung. Ebenso forschen die Hersteller von Virenscannern ständig nach Algorithmen gegen Computerviren. Zehn Programme beweisen im WIN-Test ihre Qualitäten als Virenjäger.

Kurzgefaßt

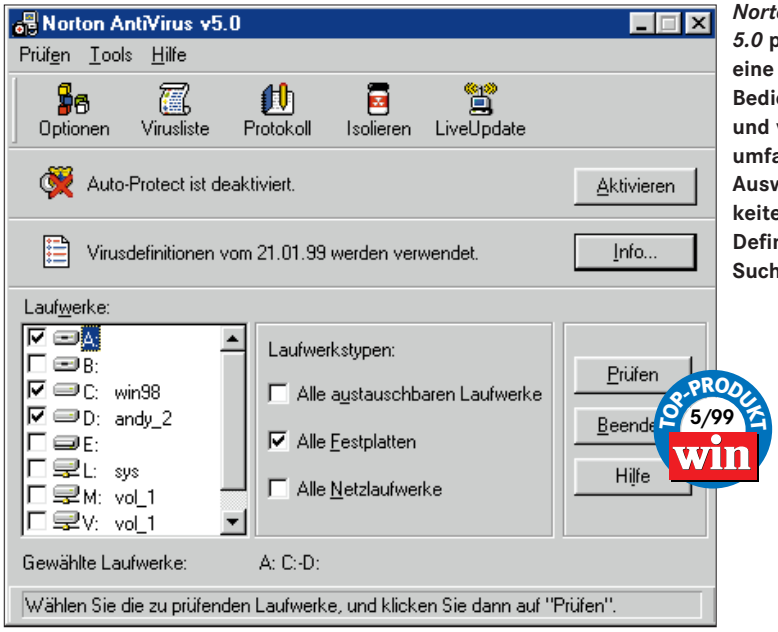
- Zehn Virenscanner im Praxistest
- So arbeiten Virenprogramme
- Tips für den Notfall

Michelangelo war ein Waisenknabe gegen den CIH-Virus, der seit Sommer letzten Jahres die Festplatten unsicher macht. Jeden Monat zur selben Zeit, am 26. nämlich, frißt sich dieser bösartige Parasit durch Teile des Flash-BIOS und setzt den Computer damit erst einmal außer Gefecht. Doch ein Virus ist immer nur so gefährlich, wie Antiviren-Software veraltet ist. So scheinen Antivirenprogramme zu jener seltenen Software-Spezies zu gehören, deren Update-Berechtigung keiner anzweifelt – denn Aktualität ist dabei das A und O.

Über andere Kriterien, mit denen die Hersteller werben, kann man dagegen geteilter Meinung sein. Denn was nützt etwa eine große Anzahl Signaturen, wenn die neuesten Viren dabei nicht vertreten sind? Ebenso stellt sich die Sinnfrage bei den heuristischen Verfahren, die unbekannten Viren auf die Spur kommen sollen, wenn sie eine Vielzahl von Fehlalarmen auslösen?

Zehn Virenscanner nehmen im WIN-Test den Kampf gegen 26.000 Viren auf. Dabei müssen sie diese nicht nur identifizieren, sondern möglichst auch zerstören. Wie sich die Programme dabei bewähren, lesen Sie auf den nächsten Seiten.

Norton Antivirus



TOP-PRODUKT 5/99 win

***Norton Antivirus 5.0* präsentiert eine vorbildliche Bedienerführung und verfügt über umfangreiche Auswahlmöglichkeiten bei der Definition von Suchjobs.**

Bedienung/Funktionen: Die Installation ist problemlos, jedoch ist an ihrem Ende bereits das erste *Live-Update* fällig, da die in der Verpackung enthaltene Version älter als ein halbes Jahr ist. Auf der CD befinden sich die Handbücher als PDF-Datei, daneben *Videos* zum Thema Viren und eine Einführung in *Norton Antivirus* (NAV). Das Handbuch ist verschwenderisch bebildert, und alle Sachverhalte sind gut verständlich erklärt.

Die Konfiguration ist ausführlich und übersichtlich über Registerkarten möglich, einzelne Funktionen lassen sich mit *Kennwortschutz* versehen. Das Virenlexikon beschreibt in Tabellenform wesentliche Merkmale der Erreger, die in einigen Fällen mit englischen Anmerkungen versehen sind.

Unter Windows 98 verwendet NAV den von dem Betriebssystem bereitgestellten Scheduler. Nützlich ist die *Quarantäne*-Funktion, um infizierte Dateien zu isolieren und ans Symantec-Virenforschungszentrum zu schicken. Die Fortschrittsanzeige beim Scanvorgang ist verwirrend, da sie bereits bei den ersten durchsuchten Dateien 99 Prozent anzeigt und dort während der restlichen Suche verbleibt.

Virenerkennung: NAV läßt nur das Durchsuchen von kompletten Laufwerken zu, einzelne Ordner sind manuell zu checken. Boot- und polymorphe Viren erkennt die Software mit über 97prozentiger Zuverlässigkeit. Die Erkennung von Skriptviren ist dagegen nicht berauschend, nur knapp die Hälfte der versteckten Viren wird erkannt.

Die vom Hersteller stark angepriesene Heuristik entpuppt sich als Mogelpackung, findet sie doch weniger Viren als alle anderen Programme im Test, obwohl sie auf höchste Empfindlichkeit eingestellt ist. Dafür halten sich aber mit nur fünf Blindgängern die Fehlalarme in Grenzen.

Virenentfernung: NAV zerstört zwei Dateien, sonst schlägt es sich mit einer 95prozentigen Reinigung von DOS-Schädlingen sowie einer Rettungsquote von 50 Prozent bei Windows-Erregern wacker. Insbesondere die vollständige Entfernung von Makroviren hinterläßt einen guten Eindruck.

Virenwächter: Der speicherresidente Scanner verbraucht einiges an Prozessorleistung, dafür zeigt er mehr als respektable Ergebnisse, wehrt er doch alle Zugriffe auf infizierte Dateien, E-Mail-Attachments, Downloads und Bootviren mühelos ab. Bereits das Kopieren von infizierten Dateien quittiert Norton mit einer Viruswarnung auf einem blauen Bildschirm.

Beim Abfangen infizierter Dateien in Office sammelt Antivirus jedoch Minuspunkte. Die Warnmeldungen kommen zudem zwei- bis fünfmal direkt hintereinander. Das ist unsinnig und verunsichert nur.

Norton Antivirus

Preis: um 100 Mark
Info: Symantec, 40880 Ratingen, Tel. (069) 66 41 03 00, *www.symantec.de*

Fazit: Noch mit einigen kleinen Tücken beim Umgang mit Office- und Skriptviren behaftet, ist *Norton Antivirus* einfach zu bedienen und zeigt sehr gute Suchleistungen insbesondere bei Boot- und polymorphen Viren. In Sachen Bedienerfreundlichkeit ist die Software führend.

win TEST	
Bedienung	●●●●●○
Virenerkennung	●●●●●○
Virenentfernung	●●●●●○
Virenwächter	●●●●●○
Preis/Leistung	●●●●●●

win Tips zum Virenschutz

Backups. Eine regelmäßige Datensicherung hilft nicht nur bei Virenbefall, sondern schützt auch vor unvorhersehbaren Schäden durch Hard- oder Software-Fehler.

Bootreihenfolge ändern. Bootviren haben keine Chance, wenn Sie die Bootreihenfolge (Boot Sequence) im BIOS-Setup von *A:, C:* auf *C:, A:* umstellen. So startet der Rechner standardmäßig von der Festplatte und nicht mehr von einer möglicherweise im Laufwerk vergessenen Diskette.

Unbekannte Dateien prüfen. Grundsätzlich ist Mißtrauen gegenüber fremden Programmen und Dokumenten angebracht. Die sollten Sie daher grundsätzlich vor Gebrauch mit einem oder mehreren Virenscannern durchsuchen. Auch der Einsatz eines Virenwächters ist empfehlenswert.

Viren unter Windows NT. Entgegen allen Gerüchten ist auch Windows NT nicht gegen Viren gefeit. Bereits ein einfacher Bootvirus kann NT-Partitionen zerstören, da die meisten aus einer Zeit vor Windows stammen oder absichtlich so programmiert wurden. Auch wer ganz unnötig als Administrator angemeldet ist, gibt Dateiviren eine große Verbreitungschance. Und gegen Makroviren ist auch unter NT kein Kraut gewachsen. Die meisten der hier getesteten Virenprogramme laufen jedoch auch unter Windows NT.

Im Notfall...

...lassen Sie keine Panik aufkommen. Übereilte Reaktionen verursachen oft genug mehr Schaden, als es der Virus jemals geschafft hätte.

...sichern Sie wichtige Daten – auch wenn sie virenverseucht sind –, bevor Sie einen Reinigungsversuch starten.

...schalten Sie den Rechner aus und starten ihn von einer sauberen Bootdiskette; bei den meisten Antivirenprogrammen gehört sie mittlerweile zum Lieferumfang.

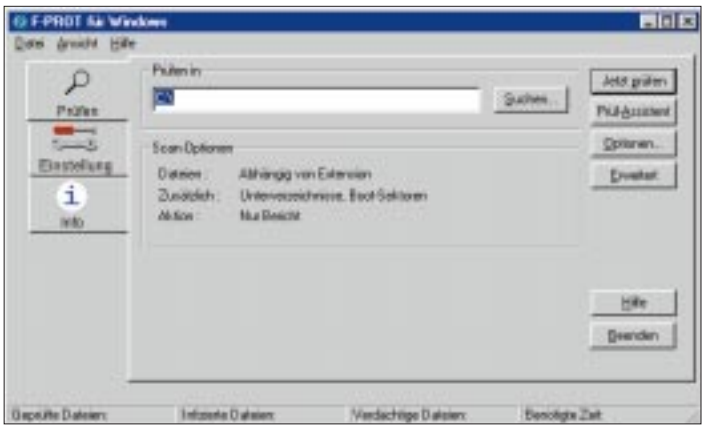
...konsultieren Sie die Hersteller-Hotline, falls die manuelle Reinigung der Daten sich als zu schwierig erweist oder Ihre Kenntnisse unter DOS nicht ausreichen.

...informieren Sie umgehend Ihre Software-Tauschpartner. Wahrscheinlich sind deren Dateien auch infiziert, oder man kann sie noch rechtzeitig davor bewahren.

Links zum Thema Viren

Eine FAQ zum Thema Viren finden Sie unter *http://www.vhm.haitec.de*. Aktuelle Infos zur Virenproblematik gibt es unter *http://members.aol.com/rlink/*. Die gerade verbreiteten Viren veröffentlicht monatlich die Wildlist unter *http://www.wildlist.org*. Im Virus Bulletin *http://www.virusbtn.com* finden sich ebenfalls einige Tips.

F-Prot für Windows Privat



Solange der Erweitert-Button in Ruhe gelassen wird, präsentiert sich *F-Prot* noch übersichtlich. Durch die erweiterten Funktionen entsteht dann ein unübersichtliches Menü-Chaos.

Bedienung/Funktionen: *F-Prot* gibt es in zwei Versionen: In der Privat-Version ist es – im Gegensatz zur Vollversion – nicht möglich, Netzlaufwerke zu durchsuchen oder Reportdateien per E-Mail zu verschicken. Die Installation des Programms, das als einziges noch auf Disketten ausgeliefert wird, ist problemlos. Über sie installiert man den Scanner und den Virenwächter *F-Stop W*, der ohne Windows-Neustart sofortigen Schutz bietet. Ein Handbuch gibt es weder gedruckt noch auf CD. Auf eine Bootdiskette muß man ebenfalls verzichten.

Die Konfiguration des Scanners und des Virenwächters ist umständlich durchzuführen und unnötig kompliziert. Dies liegt unter anderem an den überladenen Fenstern und der unübersichtlichen Anordnung der Elemente. Eine Not, die der *Suchassistent* allerdings etwas entschärft. Ein Virenlexikon ist nicht vorhanden, auch ein Hinweis auf ein gutes Online-Virenlexikon fehlt. Einen Scheduler gibt es gleichfalls nicht.

Wer in den F-Prot-Standardeinstellung nicht genug Optionen findet, kann die *er-*

win Testkriterien

Zehn Virenscanner stellen sich einem vierstufigen Testverfahren.

1. Virenerkennung (On-Demand-Scanner)

Grundlage sind die Erkennungsraten, die der Virenscanner bei der Verbreitung von etwa 26.500 Viren in 210.000 Dateien erzielt. Die Probanden müssen dazu möglichst viele Erreger in den Kategorien Datei-, Makro-, Boot- und Skriptviren finden.

Eine harte Nuß für Virenscanner sind die vielgestaltigen (polymorphen) Datei- und Makroviren, die ihr Aussehen bei jeder Infektion ändern. Trojanischen Pferde wie zum Beispiel Back Orifice oder Netbus und sonstiger Malware (mehr zu Viren und Malicious Code lesen Sie am Schluß des Beitrags) sollten die Scanner gleichfalls auf die Spur kommen.

Viele Hersteller versprechen Traumquoten beim Erkennen von neuen Viren. Ein Test der heuristischen Verfahren soll beweisen, wie viele neue Schädlinge die Programme tatsächlich einfangen.

Aus diesen Ergebnissen wird eine Zwischennote *Nicht-ITW-Viren* gebildet, die mit 40 Prozent in die Wertung für die Virenerkennung eingeht. Da aber weniger als ein Prozent der großen Anzahl schädlicher Programme jemals bei Privatanwendern aufgetreten ist, überprüfen die Scanner eine zweite Virensammlung mit allen verbreiteten Erregern, die Computerbesitzer treffen können. Die Quote bei dieser *ITW*-Virensammlung bringt 60 Prozent der Wertung für den On-Demand-Scanner.

Wenn ein Programm zu häufig falschen Alarm schlägt, also Viren findet, wo keine sind, wird jeweils ein halbes Prozent der Gesamtwertung – maximal aber zwölf Prozent – abgezogen.

2. Virenentfernung

ITW-Viren sollte ein gutes Produkt in jedem Fall entfernen können. Hierzu müssen die Antivirenprogramme knapp 180 verbreitete Datei- und Makroviren finden und entfernen. Wenn die Dateien nach der Reinigung noch zu gebrauchen sind, gibt es einen Punkt, können die Scanner sie nicht reinigen, gibt es keinen Punkt. Falls die Dokumente oder Programme jedoch nur noch Datenmüll sind, gibt es Punktabzug, und zwar ein Prozent je Datei, maximal 25 Prozent.

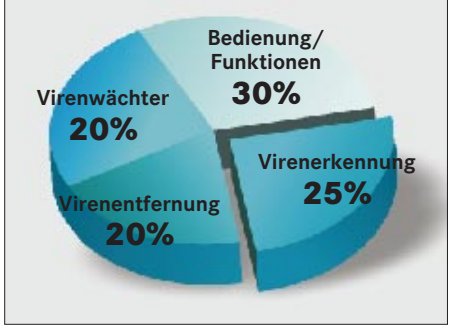
3. Virenwächter (On-Access-Scanner)

Kaum jemand wird Internet-Seiten mit einem Virenscanner durchsuchen. Ebensowenig ist es zumutbar, jede E-Mail und jede neue Diskette einzeln zu prüfen. Für diesen Zweck enthalten Virenscanner stets aktive Wächterprogramme, die jede Datei auf gefährliche Inhalte hin checken. Im Test sind die Viren beim Dateizugriff abzufangen und die Ausführung infizierter Programme zu verhindern.

Makroviren sollten beim Öffnen eines verseuchten Dokuments keine Chance bekommen, aktiv zu werden. Die Virenscanner müssen den Zugriff auf mit Bootviren infizierten Disketten melden und das Speichern von infizierten E-Mail-Anhängen oder gefährlichen Downloads unterbinden.

Wenn ein Wächter zuviel Prozessorleistung oder Speicherkapazität für sich abzwackt, gibt es Punktabzüge.

So gewichtet WIN



4. Bedienung, Funktionen

Ein Antivirenprogramm muß nicht nur gute Ergebnisse bei der Virenvorbeugung, Erkennung und Beseitigung zeigen, sondern auch einfach bedienbar und funktional sein. Die Installation soll die freie Wahl über zusätzliche Komponenten lassen, und mit der Deinstallation muß das Programm rückstandsfrei wieder entfernbar sein. Handbücher und Online-Hilfe stehen im Idealfall immer helfend zur Seite. Eine selbsterklärende Oberfläche gilt als selbstverständlich.

Zudem geht in die Bewertung ein, ob die Programme einen Scheduler, ein Prüfsummenprogramm (siehe Kasten „So arbeiten Antivirenprogramme“), ein brauchbares Virenlexikon und eine Bootdiskette enthalten. Das Entpacken von Archivdateien wird durch zusätzliche Punkte belohnt. Trotz aller Anforderungen soll das Programm aber auch nicht zu verschwenderisch mit dem Festplattenplatz umspringen und schnell sein.

Erfüllen die Programme mehr als 75 Prozent der hier beschriebenen Kriterien, gibt es die volle Punktzahl.

weiterten Funktionen aktivieren. Dann drängen unzählige Elemente gleichzeitig ins schier überquellende Fenster. Dafür kann man anschließend aber auch mehrere Suchziele auswählen, statt eines einzelnen.

Für die Deinstallation muß zunächst der Virenwächter manuell deaktiviert werden. Erst danach läßt sich F-Prot ohne Spuren aus dem System entfernen.

Virenerkennung: Der Hersteller macht die Anpassung an spezielle Bedürfnisse leicht: F-Prot erlaubt die Anlage zahlreicher unterschiedlicher Jobs und Suchprofile.

Tadellose Suchergebnisse zeigt F-Prot bei Boot- und Dateiviren mit rund 98 Prozent. Bei den Dateiviren rutscht die Erkennung lediglich bei Access-, Powerpoint- und BAT-Viren in den Keller. Hier übersieht der Scanner fast alle Infektionen. Bei den ITW-Viren gibt sich F-Prot keine Blöße, das Programm findet sie zuverlässig. Auch Malware geht dem Scanner zu 96 Prozent ins Netz.

Die Heuristik ist von durchschnittlicher Qualität und kommt nur etwas mehr als einem Drittel der neuen Viren auf die Schliche. Die Zahl der Fehlalarme hält sich in Grenzen, bemerkenswert ist jedoch, daß F-Prot andere Antivirenprogramme als infiziert bemängelt.

Virenentfernung: Ganze zwei DOS-Programme kann F-Prot nicht reinigen, sonst sieht die Bilanz mit einer hundertprozentigen Erfolgsquote bei Datei- und Makroviren sehr positiv aus.

Virenwächter: Das Wächter-Modul *F-Stop W* zeigt sich sämtlichen Aufgaben im Test gewachsen und wehrt alle Zugriffe auf gefährliche Programme, E-Mail-Anhänge und Downloads ab. Die beanspruchte Prozessorleistung liegt dabei auf unterstem Niveau. Infizierte Dateien blockiert der Wächter sofort. Per Voreinstellung oder auf Anfrage reinigt er die Dateien oder löscht sie.

Gelegentliche Abstürze des Rechners – wenn man zum Beispiel in der DOS-Box Dateien auf das Netzwerk kopiert – trüben das Bild ein wenig.

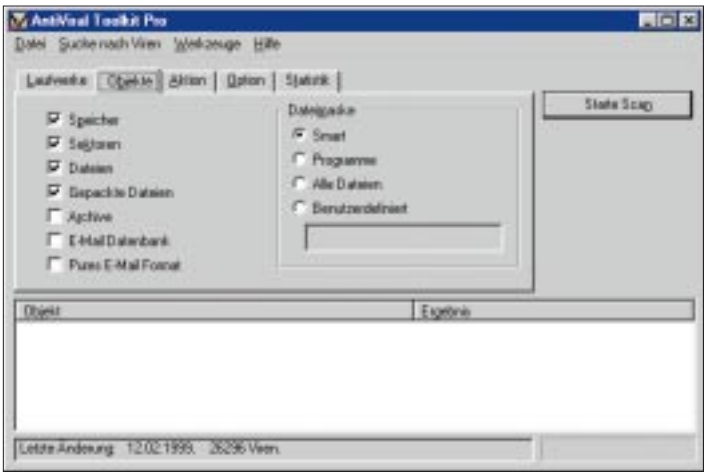
F-Prot für Windows Privat

Preis: um 170 Mark
Info: Frisk/Percomp, 22041 Hamburg, Tel. (040) 6 93 20 33, *www.percomp.de*

Fazit: Besonders die schlechte Bedienung und die fehlenden Zusätze wie Bootdiskette und Scheduler kosten *F-Prot* den Testsieg. Die hohen Update-Kosten sind gleichfalls negativ anzumerken. In Sachen Virenerkennung präsentiert sich der Klassiker jedoch vorbildlich.

Bedienung ●●○○○○
Virenerkennung ●●●●●●
Virenentfernung ●●●●●●
Virenwächter ●●●●●●
win TEST ●●●●●○
Preis/Leistung ●●○○○○

Antiviral Toolkit Professional



Die Laufwerke, Ordner und Dateien lassen sich beliebig in die Suchliste aufnehmen. Löschen kann man den Eintrag dann allerdings nicht mehr.

Bedienung/Funktionen: Die Installation von *Antiviral Toolkit Professional* (AVP) verläuft reibungslos und bietet mehrere Auswahlmöglichkeiten zwischen den Zusatzmodulen. Dazu gehören das *Control Center* (Scheduler), der Scanner, der Virenwächter, der *Monitor* (Prüfsummenprogramm) und eine nützliche, jedoch teilweise zu technische und englischsprachige Virendatenbank im HTML-Format. Eine Bootdiskette steht nicht zur Verfügung.

Das gedruckte Handbuch ist kurz geraten, aber hilfreich für die Einarbeitung. Konfiguration und Bedienung der einzelnen Teile sind leider zu unübersichtlich, da jedes Modul unterschiedlich zu bedienen ist. Eine einheitliche Oberfläche wäre dem schnelleren Programmverständnis dienlich.

Die Deinstallation sollte in zwei Schritten ablaufen: erst die Virendatenbank, danach die restlichen Programmteile. Erstere denkt aber gar nicht daran, sich löschen zu lassen, und bricht mit einer Fehlermeldung ab. Das Löschen der anderen Teile klappt dann auch nicht. Eine selektive Deinstallation ist nicht vorgesehen, es gibt nur alles oder nichts.

Virenerkennung: Die Anlage von Jobs ist nicht möglich, dafür lassen sich Laufwerke, Ordner oder Dateien beliebig zusammen in die Suchliste aufnehmen. Merkwürdigerweise gibt es jedoch nur eine Funktion zum Auswählen von Zielen – einmal in die Suchliste aufgenommen, kann man das Ziel nicht mehr löschen, allenfalls deaktivieren.

AVP beweist in nahezu allen Bereichen professionelle Erkennungsleistung, so findet es Boot-, Datei, Makro- und polymorphe Viren mit mindestens 98prozentiger Wahrscheinlichkeit. Lediglich bei Skriptviren (VB-Script und HTML) bricht die Erkennungsrate ein, hier bemerkt es nur noch 76 Prozent der infizierten Datenbestände.

Im Heuristik-Test identifiziert der Scanner fast 50 Prozent aller neuen Viren und ist damit das beste Programm in diesem Bereich. AVP lokalisiert auch alle ITW-Viren mühelos. Dies kann jedoch über elf Fehlalarme, unter anderem bei der FASTFIND.EXE von Office 97, nicht hinwegtrösten

Virenentfernung: Eine sichere Beseitigung von Office-95-Viren ist mit AVP kein Problem, auch bei Office-97-Dokumenten zeigt sich die Software relativ zielsicher (80 Prozent). Die Säuberung von DOS-Viren ist mit 96 Prozent hoch, und von Windows-Viren kann AVP nur eine Datei nicht befreien. Negativ fallen aber zwei nicht mehr benutzbare, zerstörte Dateien auf.

Virenwächter: Wenn AVP einen Virus findet, meldet es sich sofort mit einem Hinweisfenster und blockiert den Zugriff auf die Datei. Aber manchmal etwas zu übereifrig: Beim Office-Test bemängelt AVP mehrmals dasselbe infizierte Dokument. Mit Skriptviren kommt AVP überhaupt nicht klar, so beanstandet es in einer Endlosschleife immer wieder die gleichen Infektionen von VBS- und HTML-Viren. Nur mit einem Neustart ist dem Fehler noch beizukommen.

Verdächtigen Downloads aus dem Internet und infizierten E-Mail-Anhängen gibt der Virenwächter jedoch keine Chance, unentdeckt zu bleiben.

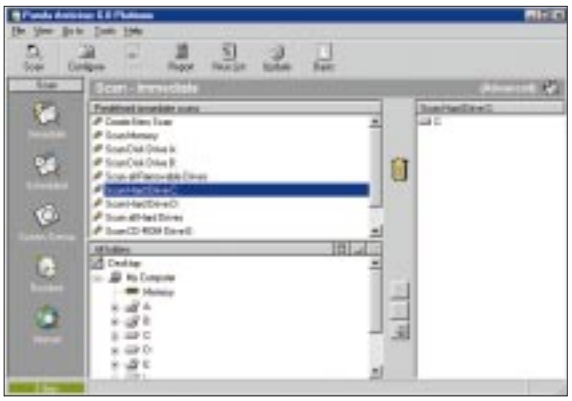
Antiviral Toolkit Professional

Preis: um 80 Mark
Info: Kaspersky Lab/Fuhs Security, 65203 Wiesbaden, Tel. (0611) 6 77 13, *www.fuhs.de*

Fazit: *AVP* zeigt ordentliche Leistungen bei Boot-, Datei- und Makroviren. Mit Skriptviren steht der Virenscanner etwas auf dem Kriegsfuß. Die uneinheitliche Bedienung und Konfiguration der Programmodule sowie die vielen Fehlalarme stören den Gesamteindruck.

Bedienung ●●●●●○
Virenerkennung ●●●●●○
Virenentfernung ●●●●○○
Virenwächter ●●●○○○
win TEST ●●●○○○
Preis/Leistung ●●●●●○

Panda Antivirus Platinum



***Panda Antivirus* hat seine Oberfläche an Windows 98 angepaßt und verfügt auch über einen Web-Browser.**

Bedienung/Funktionen: Bereits bei der Installation kann sich der Anwender *Online registrieren* lassen und gleich die neuesten *Updates* abholen. Neben dem eigentlichen Virenscanner findet sich auf der CD unter anderem eine *Multimedia-Show*, in der Viren und der Umgang mit fremden Daten kurz erläutert werden.

Das Handbuch ist kurz, und der Hersteller verschwendet den Platz mehr zur Selbstbeweihräucherung als für nützliche Hinweisen und Tips. Die durch Hologramme aufwendige Gestaltung des Handbuchs und der Verpackung täuschen über die inhaltlichen Mängel kaum hinweg.

Für jedes Programmsegment – Scanner, Wächter und *Internet-Scanner* gibt es ein eigenes Konfigurationsprogramm. Die Parameter sind für alle Suchziele getrennt einstellbar, zudem lassen sich im Internet-Scanner einzelne *Ports* und *IP-Adressen sperren*. Zwar ist *Panda Antivirus* in Bedienerführung und Aussehen völlig an Windows 98 angelehnt, dennoch benutzt es einen eigenen Scheduler statt des in Windows 98 enthaltenen.

Das Virenlexikon besteht lediglich aus einer Datenbank mit Charakteristika, allerdings ohne weiterführende Beschreibungstexte.

Virenerkennung: Suchjobs mit individuell einstellbaren Zielen und Optionen, etwa *Protokoll*- oder *Reinigungs*-Optionen, lassen sich problemlos anlegen und speichern.

Die Erkennung von Boot- und Dateiviren ist mit jeweils 89 Prozent lediglich durchschnittlich. Makro- und Skriptviren erkennt der Scanner dagegen mit 95prozentiger beziehungsweise 97prozentiger Sicherheit. Größere Mängel zeigt die Software bei polymorphen Viren aller Art (nicht einmal 70 Prozent), mit DOS-Viren kommt die Software immerhin noch zu 88 Prozent zurecht. Der Scanner spürt jedoch nur die Hälfte der Makroviren auf. Zwei Drittel der Malware ertappt er auf frischer Tat.

Pandas Heuristik findet über ein Drittel aller neuen Viren. Punktabzüge gibt es für sieben überflüssige Fehlalarme und zwei übersehene ITW-Bootviren.

Virenentfernung: Panda Antivirus beseitigt so gut wie alle Makroviren zuverlässig, läßt aber bei DOS-Dateiviren – mit 93prozentiger Erkennung – gering nach. Bei Windows-Viren entfernt das Programm nur ein Viertel und hinterläßt dabei zudem zwei nicht mehr lauffähige Programme.

Virenwächter: Sobald der speicherresidente Schutz von Panda Antivirus installiert ist, wird der Computer zusehends langsamer, Aktionen laufen dann fast schon in Zeitlupe ab. Findet der Wächter einen Virus, zeigt er dies mit einem grünen Bildschirm und einem Hinweis auf die infizierte Datei und den enthaltenen Erreger an. Fehlermeldungen bringt das Programm dagegen auf Spanisch.

Beim Office-Test meldet die Software Dateien gleich mehrmals hintereinander als infiziert, öffnet aber virenverseuchte Dateien in keinem Fall. Auch E-Mails und Downloads fängt Antivirus sicher ab.

Panda Antivirus Platinum

Preis: um 100 Mark
Info: Omega See, 85764 Oberschleißheim, Tel. (089) 37 50 73 00, *www.omega-see.com*

Fazit: *Panda Antivirus* trumpft zwar mit einem scharfen Virenwächter auf, der den Rechner jedoch sichtlich verlangsamt. Einige Funktionen kommen dem Anwender nicht nur spanisch vor, sie sind tatsächlich nur in spanischer Sprache implementiert.

win TEST
Bedienung ●●●○○○
Virenerkennung ●●●●○○
Virenentfernung ●●●●●○
Virenwächter ●●●●●○
Preis/Leistung ●●●●○○

So arbeiten Antivirenprogramme

Ein Virenscanner soll Viren finden, bevor sie ausgeführt werden und Schäden verursachen können. Eingeteilt werden die Programme in **On-Demand-** und **On-Access-Scanner.** Erstere müssen manuell gestartet werden, bevor sie mit der Suche loslegen, oder ihr Start wird durch einen zeitgesteuerten **Scheduler** ausgelöst. **On-Access-Virenwächter** oder **VXD-Scanner** bleiben dagegen permanent, aber unsichtbar im Hintergrund aktiv und schlagen bei verdächtigen Dateien Alarm.

Beide Scanner verwenden mehrere Methoden, um Viren zu entdecken. Die Eindringlinge werden mittels einer **Signatur** (Fingerabdruck) gesucht, was aber nur bei bereits bekannten oder leicht abgewandelten Schädlingen funktioniert.

Gegen verschlüsselte und polymorphe Viren verspricht eine **Code-Emulation** Abhilfe. Dabei führen die Scanner verdächtige Programme Schritt für Schritt auf einem im Scanner enthaltenen virtuellen Rechner mit simuliertem Speicher- und Prozessor aus. Die Virenscanner lösen eine vorhandene Codierung auf und identifizieren den Virus anhand einer Signatur.

Allerdings braucht eine Emulation mitunter sehr viel Zeit, was die Suche verlangsamt. Deshalb sind noch immer schnelle **algorithmische Erkennungsroutinen** beliebt, die nach typischen Verschlüsselungen genau bestimmter Viren forschen. Sie zerlegen die Programme über mathematische Vergleichsverfahren und bestimmen, ob die Datei durch den Virus infiziert ist.

Unbekannte Erreger sind mit **heuristischen** Mitteln (Faustregeln) aufzuspüren. Auf der Grundlage bekannter Viren versucht eine Heuristik zu erkennen, ob eine Datei möglicherweise durch einen unbekannten Virus infiziert ist oder nicht. Der **Behaviour Blocker** eines Virenwächters sucht nach typischen Aktionen von Viren, Trojanischen Pferden und anderen Schadprogrammen und versucht, sie zu unterbinden.

Wenn Scanner sich irren und beispielsweise Signaturen von Viren in harmlosen Dateien finden und dann zu Unrecht Alarm geschlagen wird, spricht man von einem **Fehlalarm.**

Um legitime oder willkürliche Veränderungen von Daten zu erkennen, leisten **Prüfsummen-** oder **CRC-Programme** ihren Dienst. Sie legen für jede Datei eine Signatur ab. Bei einer Abweichung wird der Anwender informiert.

Beim **Impfen** hängen die Scanner Prüfsummen und ein kleines Programm an die Daten, um eine Infektion selbständig festzustellen. Jedoch vertragen die meisten Anwendungen eine solche Manipulation nicht, sie hat Ähnlichkeit mit einer Vireninfektion.

McAfee Virusscan Deluxe

***McAfees* Ratschläge zur Virenbekämpfung sind nicht immer informativ und hilfreich.**

Bedienung/Funktionen: Die Installation ist mit wenigen Klicks ausgeführt, so daß man nicht zu dem ohnehin schlecht übersetzten und wenig informativen Handbuch greifen muß. Die Oberfläche präsentiert sich unverändert altmodisch. Die Konfigurationsmöglichkeiten sind ausführlich. So gibt es beispielsweise die Option, alle Dateien oder nur einzelne Dokumente zu durchsuchen. Auch ein *Paßwortschutz* ist vorgesehen. Das Virenlexikon gibt es nur online und in Englisch auf der Homepage des Anbieters.
Virenerkennung: Unter der erweiterten Oberfläche lassen sich mehrere Suchziele zusammenfassen, unter der einfachen Oberfläche ist nur ein Laufwerk beziehungsweise Pfad einstellbar. Die Zusammenstellung von Jobs ist nur umständlich möglich.

McAfee Virusscan sinkt bei Boot-, Datei-, und Makroviren nie unter 98 Prozent Erfolgsquote. Ausreißer sind dabei lediglich die Powerpoint-Viren, die den Virenjäger vollständig außer Gefecht setzen, auch Access-Viren bereiten noch etwas Schwierigkeiten. Leistungseinbrüche gibt es ebenso bei HTML- und VB-Script-Viren, hier liegt die Quote nur bei 82 Prozent.

Malware erkennt Virusscan zu 87 Prozent noch gut genug. Die ITW-Viren erfaßt es lückenlos, verdächtigt aber viel zu viele gesunde Dateien einer Infektion. Die Heuristik verspricht zwar laut Hersteller einen Fahndungserfolg von mehr als 80 Prozent, im Test sind es aber nur 43 Prozent.
Virenentfernung: Virusscan kann nahezu allen Virenarten den Garaus machen, nur bei drei Dateien ist sich das Programm unsicher und will sie vorsichtshalber löschen. Bei einer Datei entfernt Virusscan voreilig nicht nur den Virus, sondern auch Teile des ursprünglichen Programms.
Virenwächter: Der Wächter blockierte alle Gefahrenquellen sofort. So läßt sich kein E-Mail-Anhang beziehungsweise Download ohne eine vorherige Inspektion durch Virusscan speichern. Bei jeder Infektion bietet die Software eine ausführliche Liste mit Auswahlmöglichkeiten. So kann man die Datei löschen, verschieben oder entfernen, auch der Zugriff ist möglich, was bei Fehlalarmen interessant ist.

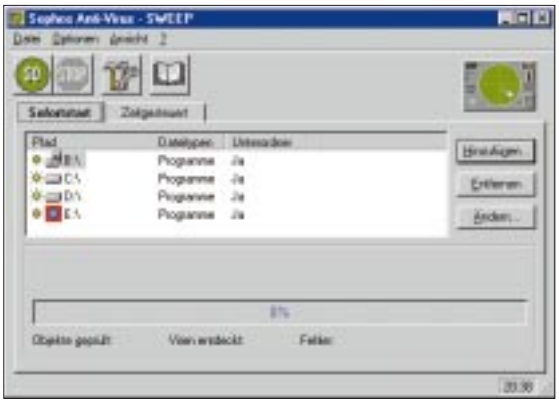
McAfee Virusscan Deluxe

Preis: um 100 Mark
Info: Network Associates, 85716 Unterschleißheim, Tel. (089) 3 70 70, *www.mcafee.de*

Fazit: 17 Fehlalarme und Schwächen bei der Identifikation von Skriptviren sind die Mankos von *Virusscan,* das dank der implementierten Suchmaschine des früheren Konkurrenten Dr. Solomon's sonst hervorragende Werte bei der Virenerkennung erzielt.

Bedienung ●●●○○○
Virenerkennung ●●●●○○
Virenentfernung ●●●●●○
Virenwächter ●●●●●●
win TEST ●●●○○○
Preis/Leistung ●●●●●○

Sophos Sweep



Einfacher geht's nicht: Über Go- und Stop-Buttons steuert *Sophos Sweep* den gesamten Scanvorgang.

Bedienung/Funktionen: Die Programm-CD enthält zusätzlich ein hervorragendes *Expert-System*, das die Installation bei einer großen Anzahl von Netzwerk-Clients vereinfacht, zudem erzeugt es Diskettenversionen der Software. Die mehrere Kilo schweren Handbücher sind ausführlich und bieten ein Glossar zum Thema Viren, allerdings sind sie etwas merkwürdig übersetzt.

Die Möglichkeiten zur Konfiguration von *Sophos Sweep* sind auf das Nötigste beschränkt, der Wächter läßt sich nur unter Windows NT einrichten. Ein wenig informatives Virenlexikon liegt bei. Die Bedienung des Scanners gestaltet sich über die Go- und Stop-Buttons denkbar einfach. Ein Scheduler ist integriert, er bietet aber nur die nötigsten Funktionen wie Tageszeiten oder Suchbereiche.
Virenscanner: Mehrere Laufwerke oder Verzeichnisse lassen sich gleichzeitig durchsuchen, dabei kann man für jedes Objekt individuelle Einstellungen vornehmen. Die Ergebnisse sind nur bei Boot- und Dateiviren ausgezeichnet. Makroviren machen noch Probleme, hier sinkt die Leistung auf 92 Prozent ab, Access- und Powerpoint-Viren findet der Scanner dabei überhaupt nicht.

Auf Skriptviren reagiert Sweep nicht immer. Mit heuristischen Mitteln erkennt es gerade mal ein Viertel der neuen Viren, und Malware identifiziert es nur etwa zur Hälfte. Zwölf Fehlalarme trüben zusätzlich den Gesamteindruck.
Virenentfernung: Für Dateiviren muß man spezielle Reinigungsprogramme von Sophos anfordern. Für den zur Zeit stark verbreiteten *W95/CIH*-Virus liegt ein spezielles Killerprogramm bei. Dafür befreit Sweep alle Office-95-Dateien und 90 Prozent der 97-Dokumente verlustfrei von Makroviren.
Virenwächter: Der speicherresidente Sucher findet leider keine Skriptviren, was Sweep für die Internet-Surfer ungeeignet macht. Der Wächter besticht jedoch durch seinen geringen Bedarf an Prozessorleistung. Infizierte E-Mail-Anhänge und potentiell gefährliche Downloads fängt die Software ab. Da sich der Wächter nicht konfigurieren läßt, gibt es dennoch Punktabzüge.

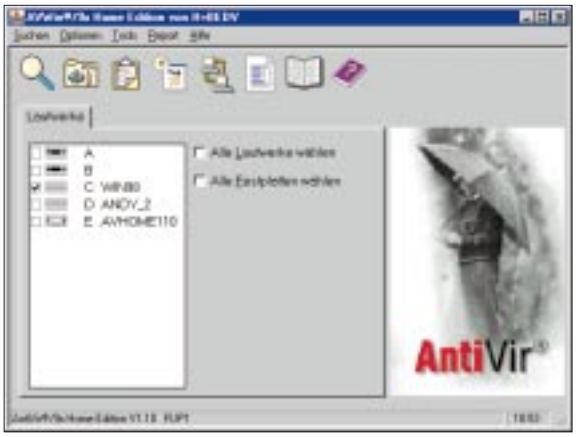
Sophos Sweep

Preis: um 400 Mark
Info: Sophos, 55268 Nieder-Olm, Tel. (06136) 9 11 93, *www.sophos.com*

Fazit: Seine volle Funktionalität und optimale Schutzwirkung entfaltet *Sweep* erst in einem NT-Netzwerk, für den Heimgebrauch ist es allein schon wegen des hohen Preises nicht zu empfehlen. Auch die Mängel bei der Erkennung von Skriptviren fallen negativ ins Gewicht.

Bedienung ●●●●●○
Virenerkennung ●●●●○○
Virenentfernung ●●○○○○
Virenwächter ●●●○○○
win TEST ●●●○○○
Preis/Leistung ●●○○○○

Antivir Home Edition



Der Schutz gegen Viren ist zwar durchlässig, dennoch läßt *Antivir* den Anwender nicht im Regen stehen.

Bedienung/Funktionen: Die Installation von *Antivir* läuft reibungslos. Schade nur, daß man danach keinen Zugang mehr zum Netzwerk hat. Die Konfiguration ist etwas zu technisch gehalten. Der Virenwächter bietet nur die notwendigsten Einstellungen, der Scanner hingegen präsentiert sich mit einer großen Fülle an Karteikarten.

Im Virenlexikon findet man einiges Wissenswerte über die digitalen Schädlinge, allerdings sollte man dafür besser Informatik studiert haben. Als einziges Programm im Test wartet Antivir mit einer bootfähigen CD-ROM auf, von der man im Notfall starten kann.

Virenerkennung: Antivir läßt keine Suchjobs zu und untersucht nur komplette Laufwerke oder einzelne Ordner gleichzeitig. Der *Luke Filewalker* getaufte Scanner findet Bootviren und Malware zuverlässig mit über 95 Prozent Erkennungsrate. Bei Makroviren liegt die Quote nur noch im mittleren Bereich: Vor allem mit Access-, Powerpoint- und Excel-Formel-Viren hat der Scanner einige Probleme. Skriptviren findet er – von BAT-Dateien abgesehen – nur unzuverlässig, für Mirc-Würmer interessiert er sich überhaupt nicht.

Bei ITW-Viren übersieht Antivir zwei Dateien. Zudem erkennt die Heuristik gerade mal 20 Prozent der neuen Viren. Wer sich viel im Internet aufhält, sollte daher nicht auf Antivir setzen. In Sachen Fehlalarm ist es der negative Spitzenreiter im Test.

Virenentfernung: Die Desinfektionsroutine beseitigt Makroviren für Office 95 vollständig. Bei Office 97 zeigen sich mit zehn Prozent Fehlerquote nur leichte Schwächen. Dafür entfernt das Programm nur 86 Prozent aller DOS- und nur die Hälfte der Windows-Viren und zerstört zwei Dateien.

Virenwächter: Zugriffe auf infizierte Dateien blockiert der *AV-Guard* – manchmal aber auch mehrfach hintereinander. Ebensowenig ist es möglich, E-Mail-Anhänge zu öffnen und Downloads vor einer eingehenden Kontrolle zu speichern. Zudem verlangsamt der AV-Guard den Rechner nur minimal.

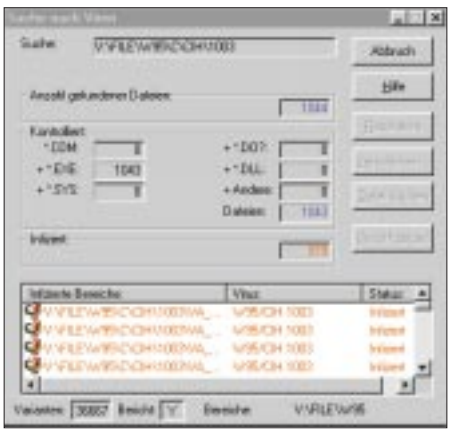
Antivir Home Edition

Preis: um 50 Mark
Info: H+B EDV, 88069 Tettnang, Tel. (07542) 9 30 40, *www.antivir.de*

Fazit: Auch ein günstiger Preis täuscht über die unterdurchschnittliche Erkennungsleistung von *Antivir* nicht hinweg. Vor allem Skriptviren sind dem Scanner suspekt. Die häufigen Fehlalarme und die mangelhafte Virenentfernung verhindern zudem eine bessere Plazierung.

Bedienung ●●●●●○
Virenerkennung ●●●○○○
Virenentfernung ●●●○○○
Virenwächter ●●●○○○
win TEST ●●●○○○
Preis/Leistung ●●●●○○

Norman Virus Control



Die Oberfläche von *NVC* ist zu klein geraten, und das Fenster läßt sich nicht vergrößern.

Bedienung/Funktionen: Bei der Installation von *Norman Virus Control* (NVC) gibt es bereits die Option, eine Diskettenversion für Notfälle anzufertigen. Das Handbuch geizt mit Bildern, nicht jedoch mit Informationen. Ein Viren-Handbuch liegt ebenfalls bei, das fast schon einer wissenschaftlichen Abhandlung gleicht. NVC besteht aus drei Teilen: dem Scanner, dem Virenwächter *Cat's Claw* und dem *Smart Behavior Blocker*, der virenähnliche Aktivitäten – etwa von Malware – verhindern soll. Alle drei Module sind einzeln zu konfigurieren und ganz unterschiedlich zu bedienen. Zudem ist in einigen Teilen die Übersetzung der Funktionen mißglückt. Der Scheduler bietet nur wenige Auswahlmöglichkeiten, etwa den Startzeitpunkt und die zu durchsuchenden Laufwerke. Ab und zu meldet er sich aber auch mit leeren Hinweisfenstern.

Virenerkennung: Suchjobs sind nur schwer definierbar und auf komplette Laufwerke beschränkt. Der Scanner zeigt durchschnittliche Leistungen bei Datei- (90 Prozent) und Makroviren (88 Prozent), Skriptviren erkennt die Software nur zu 82 Prozent. Excel-Formel-, Access- und Powerpoint-Viren entgehen dem Virensucher völlig.

Von den polymorphen Viren identifiziert er knapp zwei Drittel. Die Wahrnehmung von Malware liegt mit 79 Prozent dagegen weit über dem üblichen Durchschnitt, die Heuristik findet immerhin 30 Prozent der neuen Viren. Außerdem entdeckt die Suchmaschine elf Viren, die gar keine sind.

Virenentfernung: NVC selbst kann nur Makroviren reinigen, im Test klappt das mit 100 Prozent der Office-95- und 80 Prozent der Office-97-Dateien. Der extra beiliegende Kommandozeilen-Virenkiller NVCLEAN.EXE beseitigt 95 Prozent der DOS-Viren, greift aber keinen Windows-Virus an. Zu beanstanden gibt es eine kaputte Datei.

Virenwächter: Bei Bootviren tritt der Smart Behaviour Blocker in Aktion, der per Blue Screen auf das Virenproblem aufmerksam macht, es aber nicht beheben kann. Meldet sich Cat's Claw bei Datei- oder Makroviren, bietet das Modul auch eine Reinigungsfunktion an. Den Zugriff auf eine fremde Datei verhindert es in jedem Fall. Der Wächter zwackt nicht allzuviel von der Prozessorleistung ab, nur zeigt er – wie auch der Scanner – Mängel bei Excel-Formel-Viren.

Norman Virus Control

Preis: um 70 Mark
Info: Norman, 42697 Solingen, Tel. (0212) 26 71 80, *www.norman.de*

Fazit: *Norman Virus Control* leidet unter der uneinheitlichen Benutzerführung der Programmteile. Auch die Suchleistung des Scanners läßt noch etwas zu wünschen übrig. Insbesondere fallen elf Fehlalarme negativ auf. Der Virenwächter arbeitet dagegen ordentlich.

Bedienung ●●○○○○
Virenerkennung ●●●●○○
Virenentfernung ●●●○○○
Virenwächter ●●●●●○
win TEST ●●●○○○
Preis/Leistung ●●●○○○

Cheyenne Inoculan Antivirus

Noch spricht *Inoculan* Deutsch, nach dem ersten Update wird es das Programm verlernt haben.

Bedienung/Funktionen: Umständlich über mehrere Auswahlmenüs führt der Weg zur *Inoculan*-Installation. Das Handbuch ist etwas älter und nicht sonderlich gut übersetzt, immerhin geht es gut auf Bedienung und Virenbeseitigung ein. Die Konfiguration des Scanners und des Wächters bietet umfangreiche Funktionen, etwa auszuschließende Dateien, Suchtiefe und Reinigung.

Das Virenlexikon beschränkt sich auf eine Virenliste mit Eigenschaften. Recht mysteriös: Nach einem *Internet-Update* spricht das Programm nur noch Englisch. Der Scheduler läßt sich nur über einen Assistenten einrichten, Änderungen an den Einstellungen sind dadurch umständlich.

Virenerkennung: Zwar sind keine Jobs definierbar, dafür bietet das Programm mit die besten Auswahlmöglichkeiten für die zu untersuchenden Objekte im Test. Dateien oder komplette Ordner und Laufwerke lassen sich einzeln auswählen.

Leider erreichen die Erfolgsquoten von Inoculan nur bei Boot- und Makroviren über 97 Prozent. Rund 86 Prozent erreicht der Scanner bei Dateiviren, bei Skriptviren 79 Prozent. Im Heuristik-Test schlägt sich die Software mit immerhin 45 Prozent gut. Dafür produziert sie viel zu viele Fehlalarme. Die ITW-Viren findet Inoculan immerhin zuverlässig.

Virenentfernung: Makroviren entfernt Inoculan verläßlich. Bei DOS-Viren arbeitet der Scanner unvorsichtiger und zerstört zwei Dateien, den Rest reinigt er korrekt. Von den mit Windows-Viren befallenen Dateien kann die Software ein Viertel retten.

Virenwächter: Völlig unzureichend ist der Wächter des Programms. Den Makroviren schenkt er keine Beachtung, und beim Start von Office läßt er alle infizierten Dokumente ohne Widerspruch passieren. Mit Bootviren verseuchte Disketten würdigt er keines Alarms. Mit VBS- und HTML-Viren kann er ebenso wenig anfangen.

Cheyenne Inoculan Antivirus

Preis: um 90 Mark
Info: Microbasic 85622 Weißenfeld, Tel. (089) 90 49 90 49, *www.microbasic.de*

Fazit: Durch gute Selektionsmöglichkeiten wirkt *Inoculan* vielversprechend, jedoch ist der Virenwächter nur eine Farce. Die sehr zahlreichen Fehlalarme des Scanners haben einen großen Punktabzug bei der Virenscanner-Note zur Folge. Die Virenentfernung funktioniert zuverlässig.

Bedienung ●●●●○○
Virenerkennung ●●●○○○
Virenentfernung ●●●●●○
Virenwächter ●○○○○○
winTEST ●●●○○○
Preis/Leistung ●●○○○○

AVG

***Virus Detected!* ist nicht wörtlich zu nehmen: *AVG* läßt noch so manchen Virus durch seine Fänge schlüpfen.**

Bedienung/Funktionen: *AVG* bietet bei der Installation gleich ein *Internet-Update* an. Die Handbücher sind ausführlich, wenn auch etwas phantasielos übersetzt. Ein Virenschutz-Handbuch mit ausführlichen Erklärungen ist zusätzlich enthalten.

Die Konfiguration ist auf das Nötigste beschränkt. Das Wächtermodul läßt sich nicht im Scanner, sondern nur separat im *Control Center* konfigurieren, hier findet man auch die Einstellungen für den *E-Mail-Scanner*. Auch ein Scheduler steht zur Verfügung, nur beschränkt sich dieser bei den Einstellungen auf eine mögliche Uhrzeit. Das Virenlexikon ist eine Volltext-Datenbank, die jedoch nicht nicht immer funktioniert. Für die verseuchten Dateien gibt es das *Quarantäne*-Verzeichnis: Hier hält die Software die Erreger zurück, bis sie entfernt werden.

Virenerkennung: Für Suchläufe wählt man einen vorgegeben Job oder stellt einen neuen zusammen, alle Optionen und Laufwerke sind individuell einstellbar. AVG zeigt nur unterdurchschnittliche Suchergebnisse in allen Bereichen: Es findet nur 82 Prozent aller Datei- und 91 Prozent der Makroviren. Zudem erspäht es überhaupt keine Skriptviren.

Besonders viele neue Schädlinge findet die Heuristik nicht gerade. Bei der Malware kann AVG ebenfalls nicht mit guten Ergebnissen glänzen. Zudem übersieht es vier ITW-Viren und erzeugt elf Fehlalarme.

Virenentfernung: Makroviren vernichtet AVG zuverlässig. Auch bei DOS-Viren ist das Programm nützlich (98 Prozent), aber bei Windows-Viren versagt es mit nur 25 Prozent. Zwei zerstörte Dateien trüben außerdem das Bild.

Virenwächter: Falls AVG auffällige Dateien entdeckt, schlägt der Wächter mit einem Blue Screen Alarm. Die Reaktionsmöglichkeiten sind auf *Zugriff erlauben* oder *löschen* beschränkt. Bei Bootviren erscheint nur ein Hinweis auf das Problem, beheben kann man den Schaden nicht. Skriptviren läßt AVG grundsätzlich passieren. Mit Office arbeitet es zusammen. Der Wächter beansprucht nur minimale Prozessorleistung.

AVG

Preis: um 80 Mark
Info: Grisoft/Jakob, 37081 Göttingen, Tel. (0551) 6 69 50, *www.jakobsoftware.de/Avg*

Fazit: Die etwas unübersichtliche Programmaufteilung, die fehlende Erkennung von Skriptviren und das mangelhafte Wächtermodul sind die Gründe für eine eher mittelmäßige Plazierung. Die Virenentfernung klappt bei den verbreiteten Viren jedoch meist tadellos.

Bedienung ●●●○○○
Virenerkennung ●●●○○○
Virenentfernung ●●●●●○
Virenwächter ●●○○○○
winTEST ●●●○○○
Preis/Leistung ●●●○○○

Test: Virenscanner

Alle getesteten Virenscanner in der Übersicht

Produkt	Norton Antivirus 5.00.02	F-Prot für Windows Privat 3.04a	Antiviral Toolkit Professional 3.0.129	Panda Antivirus Platinum 6.03.00	McAfee Virusscan Deluxe 4.0.02.4012
Info	Symantec, 40880 Ratingen, Tel. (069) 66 41 03 00, *www.symantec.de*	Frisk/Percomp, 22041 Hamburg, Tel. (040) 6 93 20 33, *www.percomp.de*	Kaspersky Lab, Fuhs Security, 65203 Wiesbaden, Tel. (0611) 6 77 13, *www.fuhs.de*	Omega See, 85764 Oberschleißheim, Tel. (089) 37 50 73 00 *www.omega-see.com*	Network Associates, 85716 Unterschleißheim, Tel. (089) 3 70 70, *www.mcafee.de*
Preis	um 100 Mark	um 170 Mark	um 80 Mark pro Jahr	um 100 Mark	um 100 Mark
Enthaltene Updates	1 Jahr via Internet	4mal CD und via Internet	1 Jahr via Internet	1 Jahr via Internet	unbegrenzt via Internet
Update-Kosten	10 Mark pro Jahr	ab 140 Mark	20 Mark/Update-Disk	Neukauf	keine
Betriebssysteme	DOS, Windows 3.1x, 95/98, NT	DOS, Windows 3.1x, 95/98, NT	DOS, Windows 95/98, NT	DOS, Windows 3.1x, 95/98, NT	Windows 95/98, NT
Bedienung/Funktionen					
Handbuch/Online-Hilfe	✓/✓	–/✓	✓/✓	✓/✓	✓/✓
Scheduler	✓	–	✓	✓	✓
CRC-Summer	–	–	✓	–	–
Virenlexikon	✓	✓	✓	✓	✓
Bootdiskette	✓	geplant	–	✓	✓
Unterstütze Packformate	ARJ, LHA, Zip	ARJ, Zip	ARJ, LHA, RAR, Zip	ARJ, Zip	ARJ, LHA, Zip
Anzahl Signaturen	21.180	24.408	26.296	21.086	40.574
Virenerkennung					
Bootviren	99,58 %	99,72 %	100,00 %	89,76 %	99,93 %
Dateiviren	93,44 %	97,75 %	99,30 %	89,52 %	98,88 %
Makroviren	93,89 %	98,29 %	98,80 %	95,10 %	98,34 %
Skriptviren	43,68 %	86,40 %	75,60 %	97,12 %	81,80 %
Polymorphe Viren	96,88 %	97,11 %	98,91 %	69,20 %	97,47 %
Sonstige Malware	88,17 %	95,70 %	90,05 %	65,86 %	87,37 %
Heuristik-Test	13,25 %	34,94 %	49,40 %	36,05 %	43,37 %
ITW-Viren	99,54 %	100,00 %	100,00 %	99,07 %	100,00 %
Anzahl Fehlalarme /Abzug	3/1,50 %	5/2,50 %	11/5,50 %	7/3,50 %	17/8,50 %
On-Demand-Note	91,07 %	95,01 %	91,42%	89,88 %	88,58 %
Virenentfernung					
Entfernung Dateiviren	83,75 %	98,13 %	90,94 %	75,63 %	99,06 %
Entfernung Makroviren	100,00 %	100,00 %	90,00 %	99,36 %	94,36 %
Anzahl zerstörte Dateien/Abzug	2/2,00 %	0/0,00 %	2/2,00 %	2/2,00 %	1/1,00 %
Note Virenentfernung	93,13 %	99,44 %	88,28 %	90,24 %	94,77 %
Virenwächter					
Dateizugriff abfangen	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
Office-97-Start	75,00 %	100,00 %	75,00 %	75,00 %	100,00 %
Skriptviren abfangen	100,00 %	100,00 %	30,00 %	100,00 %	100,00 %
Bootviren-Test	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
Internet-Infektionen	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
Abzug Ressourcenbelastung	3,30 %	1,30 %	2,40 %	3,90 %	4,70 %
On-Access-Note	91,70 %	98,70 %	78,60 %	91,10 %	95,30 %
Bewertung					
Bedienung, Funktionen	●●●●●○	●●○○○○	●●●●●○	●●●○○○	●●●○○○
Virenerkennung	●●●●●○	●●●●●●	●●●●●○	●●●●○○	●●●●○○
Virenentfernung	●●●●●○	●●●●●●	●●●●○○	●●●●●○	●●●●●○
Virenwächter	●●●●●○	●●●●●●	●●●○○○	●●●●●○	●●●●●●
WIN-TEST	●●●●●○	●●●●●○	●●●●○○	●●●●○○	●●●●○○
Preis/Leistung	●●●●●●	●●●○○○	●●●●●○	●●●●○○	●●●●●○

TOP-PRODUKT 5/99 win

WIN-Autor Andreas Marx will die Viren das Fürchten lehren.

Fazit: Den perfekten Virenscanner gibt es nicht, dennoch ist Vorsorge zu empfehlen

Für Geld kann man heute vieles kaufen – nur keinen perfekten Schutz vor Viren. Die Virenscanner sind ja schon per Definition veraltet, wenn sie auf den Markt kommen. Denn sie können nur Viren bekämpfen, die bereits Schaden angerichtet haben.

Einige der Programme wollen über 57.000 Viren finden und beseitigen, andere nur 19.000. Letztere schneiden im Test trotzdem besser ab. Die Anzahl der Signaturen ist eben nicht alles. Dennoch versucht jeder Anbieter, den anderen mit solchen Versprechen zu übertreffen. Wenn die Heuristik jedoch tatsächlich so gut funktionieren würde, wie die Werbung behauptet, wären teure Updates überflüssig. Oft versprechen Hersteller Erkennungsraten von mehr als 80 Prozent bei neuen Viren, in Wirklichkeit schafft kein Programm über 50 Prozent – und die meisten produzieren dabei reichlich Fehlalarme.

Nur wenige Scanner hinterlassen einen durchweg guten Eindruck, dazu gehören *Norton Antivirus, F-Prot* und *Antiviral Toolkit*. Diese Programme haben nur wenige Schwachstellen, die sie wiederum durch exzellente Ergebnisse in anderen Disziplinen ausgleichen.

Die drei Schlußlichter sind *Norman Virus Control*, *AVG* und *Cheyenne Inoculan* Sie sind den Mitbewerbern in Bezug auf Leistung, Funktionsumfang und Bedienbarkeit deutlich unterlegen.

Internet-Surfer und Chatter sollten vor allem auf einen guten Virenwächter achten, hier sind *F-Prot* und *McAfee Virusscan* eine ausgezeichnete Wahl. Wer wenig Daten tauscht und kaum online geht, ist durch *Norton Antivirus, F-Prot,* oder *Antiviral Toolkit* gut geschützt.

	Sophos Sweep 3.18	Antivir Home Edition 1.10	Norman Virus Control 4.62	AVG 6.018	Cheyenne Inoculan Antivirus 5.0.67
	Sophos, 55268 Nieder-Olm, Tel. (06136) 9 11 93, *www.sophos.com*	H+B EDV, 88069 Tettnang, Tel. (07542) 9 30 40, *www.antivir.de*	Norman, 42697 Solingen, Tel. (0212) 26 71 80, *www.norman.de*	Grisoft/Jakob 37081 Göttingen, Tel. (0551) 6 69 50, *www.jakobsoftware.de/Avg*	Microbasic 85622 Weißenfeld, Tel. (089) 90 49 90 49, *www.microbasic.de*
	um 400 Mark	um 50 Mark	um 70 Mark	um 80 Mark	um 90 Mark
	1 Jahr via CD (12mal) und Internet	1 Jahr via Internet	1mal Disk und 3 Monate via Internet	unbegrenzt via Internet	12mal via Internet
	Neukauf	Neukauf	60 Mark	keine	Neukauf
	DOS, Windows 3.1x, 95/98, NT	DOS, Windows 3.1x, 95/98, NT,	DOS, Windows 3.1x, 95/98, NT, OS/2	DOS, Windows 3.1, 95/98, NT	Windows 95/98
	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
	✓	✓	–	–	✓
	–	–	✓	–	–
	✓	✓	–	✓	✓
	✓	Boot-CD	–	–	–
	–	Zip, ARJ	ARJ, Zip	ARJ, RAR, Zip	ARJ, LHA, Zip
	17.896	57.604	36.667	keine Angabe	keine Angabe
	99,79 %	99,16 %	97,35 %	96,93 %	99,09 %
	97,40 %	90,03 %	90,15 %	81,86 %	85,91 %
	92,42 %	86,66 %	88,27 %	91,26 %	97,01 %
	75,36 %	47,84 %	81,97 %	0,00 %	78,89 %
	98,85 %	90,85 %	66,23 %	88,25 %	94,98 %
	51,34 %	95,70 %	79,00 %	12,05 %	73,12 %
	22,89 %	20,48 %	30,12 %	18,39 %	44,58 %
	99,54 %	99,52 %	99,54 %	98,60 %	100,00 %
	12/6,00 %	38/12,00 %	11/5,50 %	11/5,50 %	31/12,00 %
	88,55 %	79,84 %	86,82 %	79,01 %	83,09 %
	6,25 %	77,19 %	71,25 %	79,06 %	79,38 %
	95,00 %	90,00 %	90,00 %	100,00 %	100,00 %
	0/0,00 %	2/2,00 %	1/1,00 %	0/0,00 %	2/2,00 %
	68,38 %	84,16 %	83,38 %	93,72 %	91,81 %
	87,50 %	100,00 %	100,00 %	50,00 %	75,00 %
	100,00 %	60,00 %	80,00 %	100,00 %	0,00 %
	0,00 %	60,00 %	100,00 %	0,00 %	40,00 %
	100,00 %	100,00 %	100,00 %	100,00 %	0,00 %
	100,00 %	100,00 %	100,00 %	100,00 %	100,00 %
	1,70 %	1,70 %	2,20 %	1,10 %	2,10 %
	75,80 %	82,30 %	93,80 %	68,90 %	40,90 %
	●●●●●○	●●●●●○	●●○○○○	●●●○○○	●●●●○○
	●●●●○○	●●●○○○	●●●●○○	●●●○○○	●●●○○○
	●●○○○○	●●●○○○	●●●○○○	●●●●●○	●●●●●○
	●●●○○○	●●●○○○	●●●●●○	●●○○○○	●○○○○○
	●●●○○○	●●●○○○	●●●○○○	●●●○○○	●●●○○○
	●●○○○○	●●●●○○	●●●○○○	●●●○○○	●●○○○○

Viren und Malicious Code im Überblick

Bootviren infizieren die Systembereiche von Disketten und Festplatten (Bootsektoren oder den Master-Boot-Record). Sie werden bereits beim Booten aktiv und vor dem Betriebssystem geladen. **Dateiviren** befallen ausführbare Programme und verändern sie so, daß vor ihrem Start der Virus ausgeführt wird.

Makroviren verstecken sich in Dokumenten und Tabellen. Sie basieren auf den Makrosprachen von Word und Excel und verrichten mit der Ausführung der Funktionen ihr schädliches Werk. **HTML-Viren** sind in Visual Basic Script geschrieben und infizieren HTML-Dateien. **Hybridviren** bestehen aus mehreren Teilen, etwa einem Bootvirus-Teil, der die Systembereiche infiziert, und einem Dateiviren-Teil, der Programme verseucht. **ITW-Viren** (In The Wild) sind alle bei Anwendern verbreiteten Erreger. Ein Virenscanner sollte sie – im Gegensatz zu den **Laborviren,** die noch nie bei Benutzern gesichtet wurden – problemlos erkennen. **Polymorphe Viren** verändern bei jeder Infektion ihr Aussehen, was eine Erkennung erschweren soll.

Als weitere Störenfriede auf dem PC betätigen sich allerlei Programme, die unter dem Namen **Malicious Code** zusammengefaßt werden. **Backdoors** zum Beispiel sind Programme, mit denen man Daten anderer Rechner ausspionieren und manipulieren kann, ohne daß der Geschädigte etwas davon merkt. **Computerwürmer** benötigen kein Wirtsprogramm und kopieren sich auf Rechner, die mit einem befallenen PC vernetzt sind. Und **Trojanische Pferde** sind Programme, die etwas ganz anderes tun, als sie vorgeben, zum Beispiel Daten ausspähen, löschen oder verändern. So spioniert beispielsweise *Back Orifice* sämtliche Paßwörter aus.