

Die besten Virenkiller für Ihren PC

PC-Virenkiller

Die Computerviren sterben nicht aus – im Gegenteil. Mit den Makroviren ist eine völlig neue Klasse von Viren entstanden.

Wie Sie Ihren Rechner am besten vor alten und neuen Erregern schützen, zeigt unser Test von zehn Virenkillern



ILLUSTRATION: JIM LUDTKE

Die Lage hat sich geändert: Seit etwa zwei Jahren gibt es außerhalb der Virenlabors keine wirklich neuen Dateiviren mehr. Experten

führen das darauf zurück, daß die technischen Möglichkeiten, DOS-basierte Viren zu schreiben, ausgeschöpft sind und zwischen 1994 und 1996 viele der

bisher bekannten Virenautoren in der Versenkung verschwunden sind. Die wenigen wirklich neuen und raffinierten Viren wie Zhengxi oder Neuro-

ANTIVIREN-PROGRAMME IM TEST

Antiviral Toolkit Pro

Shareware

Anbieter: Howard Fuhs Elektronik,
Wiesbaden, Tel. 0611/67713

<http://www.avp.ch>

Preis: 73 Mark

(siehe Test Power-Antivirus, Seite 194)

Dr. Solomon's Antivirus Toolkit 7.72

Anbieter: Guntram Stoll, Weißensberg
Tel. 08389/92020

<http://www.drsolomon.com/de/>

Preis: ab 69 Mark

Seite 182

F-Prot Professional 95 2.26a

Anbieter: Percomp Verlag, Hamburg
Tel. 040/6932033

<http://www.datafellows.fi/f-prot/>

Preis: 284 Mark (inklusive 4 Updates)
Seite 184

H+BEDV Antivir 1.01.01

Anbieter: H+BEDV, Tett nang
Tel. 07542/93040

<http://www.antivir.de>

Preis: 448,50 Mark

Seite 187

McAfee Virusscan 3.0.2

Anbieter: McAfee, Germering
Tel. 089/8943560

<http://www.mcafee.com/german/>

Preis: 119 Mark

(inklusive 4 Updates)

Seite 188

Norman Virus Control 95 4.10

Anbieter: Norman Data Defense
Systems, Solingen, Tel. 0212/267180

<http://www.norman.de>

Preis: 195,50 Mark

(inklusive 1 Update)

Seite 190

Norton Antivirus 2.0

Anbieter: Guntram Stoll, Weißensberg
Tel. 08389/92020

<http://www.symantec.com/nav/>

Preis: 129 Mark

Seite 192

Power-Antivirus 3.0

Anbieter: G-Data, Bochum, Tel. 0234/97620

<http://www.gdata.de/Produkte/pav.htm>

Preis: 49,95 Mark

Seite 194

Thunderbyte Antivirus 8.01

Anbieter: Androtec, Hamm
Tel. 02381/996000

<http://members.aol.com/androtec/>

Preis: ab 124 Mark

Seite 195

Trend Desktop Viruswall 2.0

Anbieter: GSP, Petershausen
Tel. 08137/1318

<http://www.trendmicro.de>

Preis: 149 Mark

Seite 196

Turbo Antivirus 97/IV

Anbieter: Hilchner Daten und Medien,
Neuss, Tel. 02131/34940

<http://www.hilchner.de/>

Preis: 349 Mark

Seite 198

quila sind mit Tarn- und Mutationsmechanismen so hochgezüchtet, daß sie nur noch auf ganz wenigen Rechnern wirklich laufen und sich daher kaum verbreiten. Virenforscher sind oft froh, wenn sie von irgendwoher lauffähige Mutationen solcher Viren bekommen.

Nach wie vor weit verbreitet sind allerdings viele alte Bekannte wie die Bootsekturviren Parity.Boot.B oder Form.A, aber auch einfachste Dateiviren wie Honecker oder Taipan tauchen immer wieder auf. Bei uns in der Redaktion landen immer wieder infizierte Disketten von Lesern, die nicht im geringsten ahnen, daß sie einen Virus auf ihrem Rechner haben.

MAKROVIREN

Alte Gefahren in neuer Verkleidung

Einfacher ist der Kampf gegen die elektronischen Erreger nicht geworden. Die Makrofähigkeiten von Programmen wie Word oder Excel haben die Voraussetzungen für eine völlig neue Virenart geschaffen: die Makroviren. Diese vermehren sich mit atemberaubender Geschwindigkeit: Anfang 1996 gab es gerade mal vier Makroviren, im Juli 1997 zählten die Hersteller von Antiviren-Software bereits den tausendsten Makrovirus. Hauptproblem bei den Makroviren sind die vielen Varianten. Ändert man nur einen Befehl oder einen Variablennamen im Makro, entsteht bereits eine neue Virusvariante, die unter Umständen nicht mehr kor-

rekt erkannt wird. Von verbreiteten Makroviren wie Concept oder Wazzu gibt es bereits mehr als einhundert Varianten. Für die meisten Varianten sind übrigens nicht bössartige Programmierer verantwortlich, sondern Winword selbst: Die Makroreproduktion unter Winword 6.0 und 95 arbeitet extrem unzuverlässig und erzeugt bei der Weitergabe von Makros in neue Dokumente oft selbständig neue Virenvarianten. Waren die ersten Makroviren noch sehr einfache Konstruktionen, die oft aus nur einem einzigem Makro bestanden oder nur mit einer bestimmten Sprachversion von Winword liefen, zeigen neuere Makroviren, daß sich die Hersteller von Antiviren-Software warm anziehen sollten: Der weitverbreitete Makrovirus Cap.A stellt selbständig fest, welche Sprachversion von Winword läuft, und paßt sich automatisch an; andere Makroviren verstecken sich unter Winword komplett oder sind hochgradig polymorph, so daß die korrekte Erkennung und Beseitigung der Virenmakros zum Glücksspiel wird.

ANTIVIREN-PROGRAMME

Es gibt keine Alleskönner

Die Programme hatten in unserem Test daher keine leichte Aufgabe. Eines vorweg: Hundertprozentig überzeugt hat uns kein Programm, vor allem nicht bei den Makroviren. Einige der Testkandidaten können auch Monate nach dem

PC WELT KURZGEFASST

Antiviren-Programme für Windows 95

Wer kein Antiviren-Programm benutzt, setzt seine Daten aufs Spiel. Auf Nummer Sicher gehen Sie mit einem Antiviren-Programm, das speziell auf Ihr Betriebssystem zugeschnitten ist und hohe Erkennungsraten aufweist.

+ Fast alle Antiviren-Programme sind inzwischen für DOS und alle Windows-Versionen von 3.1 bis NT erhältlich. Residente Virenwächter erkennen Viren bereits, bevor die infizierte Datei geöffnet wird.

- Viele Antiviren-Programme haben noch immer Probleme mit Makroviren. Einige Scanner kommen mit den Dateiformaten von Office 97 nicht zurecht. Manche Programme erkennen nicht einmal weitverbreitete Viren, die schon älter als zwei Jahre sind.

Empfehlung: Der Hersteller eines Antiviren-Programms sollte schnell auf aktuelle Entwicklungen bei Viren und Dateiformaten reagieren. Programme, die noch immer keine Office-97-Dokumente prüfen, sind technisch im Rückstand. Außerdem sollten Sie mit der Benutzerführung zurechtkommen – ein Programm, dessen Optionen man nicht nutzt und nicht versteht, das hilft nur wenig. Im Internet gibt es von fast allen Produkten Demoversionen zum Download.

ENTSCHEIDUNGSHILFE: ANTIVIREN-PROGRAMME

WENN...

...DANN

Sie oft Dateien aus dem Internet laden oder E-Mails mit Anhängen (Attachments) bekommen,

► ... sollten Sie unbedingt einen residenten Scanner für Ihr Betriebssystem einsetzen.

Sie oft Winword-Dokumente oder Excel-Tabellen mit anderen Anwendungen austauschen,

► ... ist eine gute Makroheuristik äußerst wichtig für Sie.

Sie nicht mit Microsoft Office oder Word arbeiten,

► ... sind Makroviren für Sie kaum ein Problem.

Sie Ihren privaten Rechner ohne großen finanziellen Aufwand sichern wollen,

► ... reicht auch eine kostenlos erhältliche Demoversion oder Freeware aus. Dr. Solomon's und AVP sind hier die erste Wahl.

Erscheinen von Office 97 noch keine Word- und Excel-97-Dokumente prüfen, andere können mit Excel-Tabellen jeder Version nichts anfangen. Die Erkennungsrate bei den polymorphen Makroviren ist bei fast allen Programmen erschreckend niedrig. Einige Hersteller haben zudem noch nicht verstanden, daß ein polymorpher Makrovirus sich bei jeder Neu-Infektion verändert: Ihre Software erkennt nur das sogenannte Generation-1-Sample, also den Virus im Urzustand. Alle weiteren Mutationen, die ein solcher Virus erzeugt, werden von manchen Programmen einfach ignoriert.

Keines der getesteten Programme schaffte es, alle Makroviren erfolgreich zu erkennen.

STEFAN KURTZHALS / RS ►

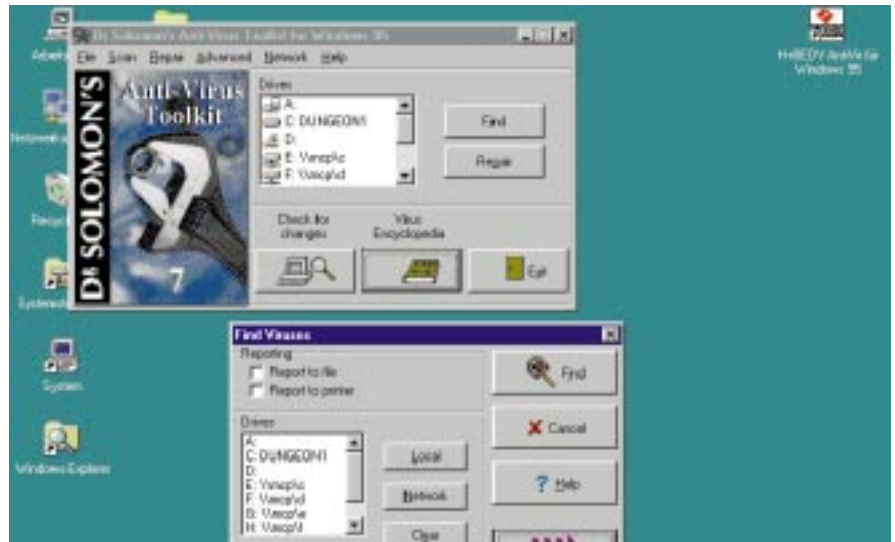
Die besten Virenkiller für Ihren PC

VERALTETE OBERFLÄCHE

Dr. Solomon's Antivirus Toolkit 7.72

Ausstattung: Das Solomon-Paket enthält eine Notfalldiskette, mit der die Viren-beseitigung ohne eigene Bootdiskette, dafür aber auch quälend langsam abläuft. Die Ausstattung des Programms läßt kaum etwas zu wünschen übrig. Besonders für DOS-Freaks sind viele kleine Utilities und Programme dabei, mit denen sich die Virensuche gut automatisieren läßt. Weniger gefallen haben uns das ziemlich nutzlose, aus Standardtexten zusammengesetzte Virenlexikon und die Handbücher der Vollversion, die planlos zusammengestellt wirken und deren Überarbeitung schon seit langem überfällig ist.

Bedienung: So gut die Technik unter der Haube ist, so rostig ist die Oberfläche: Anfänger haben wegen der unfreundlich gestalteten Benutzerführung Probleme, die optimale Leistung aus dem technisch hervorragenden Scanner herauszukitzeln. Viele Optionen sind nur über schlecht oder überhaupt nicht dokumentierte Aufrufparameter zugänglich. Die Schwächen der Oberfläche ver-



Dr. Solomon's Antivirus Toolkit: Nur ein Teil der mächtigen Programmfunktionen ist über die veraltete Bedienungsführung zugänglich

decken damit die technischen Glanzlichter des Scanners fast völlig. Einzig der residente Virenwächter ist gut integriert und läßt sich sinnvoll konfigurieren.

Erkennung und Beseitigung: Für das Erkennen und Entfernen von DOS-Viren, ist dieses Produkt neben Power-Antivirus und AVP die beste Wahl. Ein wenig an-

ders sieht es allerdings bei den Makroviren aus: Hier hat der Scanner einige Schwächen. Die Makroheuristik lieferte einen Fehlalarm, und bei der Erkennung von Makroviren liegt Dr. Solomon immer nur im oberen Mittelfeld. Einen Makrovirus konnte das Programm außerdem nicht korrekt entfernen. ▶

ANTIVIREN-PROGRAMME: UNSERE FAVORITEN

PC WELT
EMPFEHLUNG
11/97

Vorweg gesagt: Keines der zehn getesteten Programme läßt sich uneingeschränkt empfehlen. Schwächen gibt es sowohl bei der Virenerkennung und -beseitigung als auch bei der Programmoberfläche, die bei einigen Programmen ziemlich undurchsichtig und unfreundlich ausgefallen ist. Am besten gefallen haben uns Dr. Solomon's Antivirus Toolkit, Norton Antivirus von Symantec und der Desktop Viruswall von Trend.

Dr. SOLOMON'S
Anti-Virus

Dr. Solomon glänzt mit einer sehr guten Such-Engine und ist das einzige Pro-

gramm ohne gravierende Schwächen bei der Virensuche. Für die Entfernung von Computerviren ist Dr. Solomon's Antivirus Toolkit auf alle Fälle die erste Wahl. Die schlechte Benutzerführung spricht allerdings gegen das Toolkit. Es erfordert einiges Hantieren mit kryptischen Aufrufparametern oder Batchdateien, um die Stärken und die Vielseitigkeit des Virenkillers wirklich auszunutzen.

Wer sich das zutraut und sich mit dem Programm ein wenig länger beschäftigen will, erhält mit Dr. Solomon's Antivirus Toolkit ein echtes Profi-Werkzeug zur Virensuche. Die einzige Möglichkeit, Dr. Solomon aktuell zu halten, ist ein Update-Vertrag – es gibt derzeit keine kostenlosen Updates im Internet.

NORTON
AntiVirus

Symantecs Norton Antivirus und Trends Desktop Viruswall zeigen weniger gute

Erkennungsraten bei der Virensuche, glänzen aber mit einer hervorragenden Oberfläche und sehr guter Integration in Windows 95.

Wer Wert auf einfache Bedienung und sinnvolle Benutzerführung legt, ist mit Norton Antivirus und Desktop Viruswall gut beraten. Beide Programme sind technisch gut und besitzen einen empfehlenswerten residenten Virenwächter.



Ein echtes Highlight ist der Säuberungs-Assistent des **Desktop Viruswall**: Kein anderes Programm hilft dem Anwender im Falle einer Vireninfection so durchdacht und sorgfältig weiter. Sowohl Symantec als auch Trend bieten für ihre Virenscanner kostenlose Updates im Internet an, mit denen sich die Programme auch ohne großen finanziellen Aufwand über längere Zeit auf dem neuesten Stand halten lassen.

Die besten Virenkiller für Ihren PC

Fazit: Dr. Solomon liefert einen technisch hervorragenden Virenscanner mit ausgezeichneter DOS-Viren-erkennung, der die gefundenen Viren auch zuverlässig entfernt. Bei Makroviren allerdings zeigte das Produkt einige Schwächen. Die seit fünf Jahren kaum überarbeitete Oberfläche macht es Anfängern schwer, den Scanner wirklich sinnvoll einzusetzen. Wer sich aber davon nicht abschrecken lässt, bekommt mit Dr. Solomon einen zuverlässigen Scanner. Die deutsche Solomon-Zentrale scheint Probleme mit Updates zu haben: Einige Leser haben die nach der Registrierung versprochenen Updates erst nach einem Anruf beim Vertrieb in Hamburg bekommen.

BEWERTUNG

Ausstattung	2,0
Bedienung	4,0
Erkennung und Beseitigung	1,5

Schulnoten (1–5)

NEUE VERSION KOMMT

F-Prot Professional 95 2.26a

Ausstattung: Die Windows-Version von F-Prot Professional ist ziemlich spartanisch ausgestattet – anders als die DOS-Version, die als Freeware zu haben ist, besitzt sie weder eine CRC-Prüfung noch eine Heuristik für Dateiviren und ist damit das einzige Programm im Test, bei dem die kostenlose DOS-Version mehr kann als die teure Windows-Version. Die Makroviren-Erkennung des Windows-Programms selbst ist nur rudimentär, dafür liegt zusätzlich der Makroscanner F-Macrow bei. Das Handbuch wirkt ein wenig zusammengefasst, ist aber gut und informativ.

Bedienung: Die Bedienung von F-Prot ist gewöhnungsbedürftig, denn die Oberfläche hält sich an keinen Standard. In Windows 95 ist das Programm eher schlecht integriert. Die Virensuche wird über „Aufgabenpläne“ definiert,

was zwar zur regelmäßigen Festplattenprüfung gut ist, aber am Anfang für einige Verwirrung sorgt.

Erkennung und Beseitigung: In der Viren-erkennung schlug sich das Produkt dank gut gepflegter und aktueller Signaturdatenbanken gut bis sehr gut – lediglich polymorphe Makroviren brachten F-Prot aus dem Konzept: Von drei dieser Viren erkannte der Makroscanner nur die Generation-1-Samples. Die Mutationen dieser Viren gingen F-Prot durch die Lappen. Excel- und Word-97-Viren erkannte es dagegen. Als Schwachpunkt erwies sich die Reinigungsfunktion: F-Prot scheiterte an der technisch komplizierten Entfernung von polymorphen Viren und landet deshalb im Punkt Dateireinigung auf einem der hinteren Plätze. Offenbar war es den Programmierern zu aufwendig, diese komplizierte Funktion noch in die alte Programmversion einzubauen. In der neuen Version 3.0 sollen diese Probleme

FACHCHINESISCH: ANTIVIREN-SOFTWARE (I)

Behaviour Blocker

Ein Virenwächter, der als Behaviour Blocker arbeitet, überprüft sämtliche Systemaktivitäten und filtert alle verdächtigen Aktionen heraus, die auf einen Virenbefall hindeuten könnten. Wird beispielsweise versucht, ein existierendes Programm zu manipulieren, zeigt der Behaviour Blocker eine Warnung an, daß Programm A gerade versucht, das Programm B zu verändern. Der Anwender hat dann die Möglichkeit, dies zu blockieren oder zuzulassen. Behaviour Blocker können dadurch nicht nur bekannte Viren erkennen, sondern auch auf „Trojanische Pferde“ aufmerksam machen.

Bootsektorvirus

Bootsektorviren infizieren Boot- und/oder Partitionssektoren von Festplatten und Disketten. Dabei wird der Viruscode in den vorhandenen Startsektor eingefügt oder der Sektorinhalt komplett durch den Viruscode ersetzt. Der ursprüngliche Sektor wird zuvor an einer Stelle abgelegt, die bei den meisten DOS-Systemen ungenutzt ist. Aktiviert werden diese Viren durch Bootversuche von infizierten Datenträgern. Ist ein Bootsektorvirus aktiv, infiziert er jede nicht schreibgeschützte Diskette. Bei Betriebssystemen wie Win-

dows NT, OS/2 und Linux kann es geschehen, daß sie nach einer Infektion nicht mehr bootfähig sind.

CRC

Die Abkürzung steht für „Cyclical Redundancy Check“. Es handelt sich dabei um ein sehr sicheres → Prüfsummenverfahren, mit dem sich feststellen läßt, ob eine Datei unverändert geblieben ist.

Fehlalarm

Ein Fehlalarm liegt vor, wenn ein Antiviren-Programm eine nicht virenbefallene Datei fälschlicherweise als infiziert meldet. Ursache dafür ist entweder eine schlecht gewählte Signatur zur Viren-erkennung oder, weit häufiger, eine schlechte Heuristik. Fehlalarme verursachen oft mehr Schäden als eigentliche Viren: Den vermeintlichen „Virus“ kann das Antiviren-Programm logischerweise nicht entfernen. Viele Anwender geraten deshalb in Panik und formatieren vielleicht sogar die Festplatte neu – nur um nachher festzustellen, daß das Programm noch immer Alarm schlägt. Ein gutes Antiviren-Programm sollte neue Viren heuristisch erkennen, aber trotzdem keine oder zumindest möglichst wenige Fehlalarme liefern.

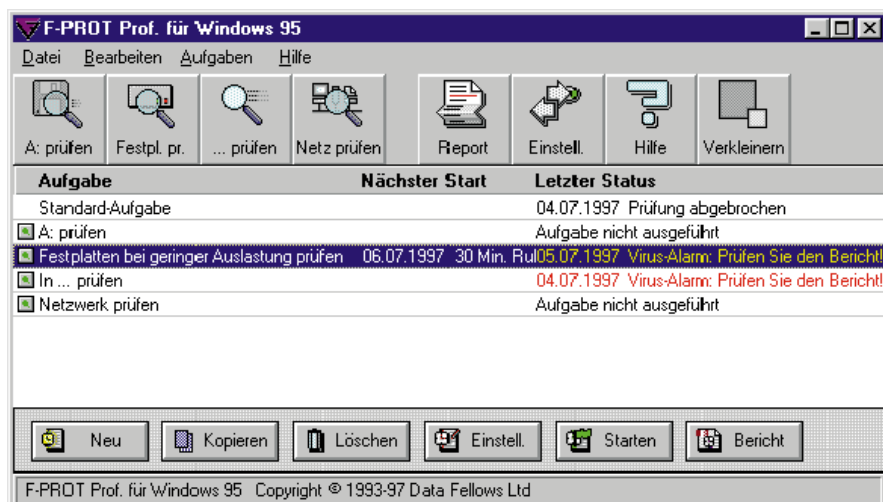
Heuristik

Dieser Begriff steht für einen regelbasierten Suchansatz, mit dem Antiviren-Programme auch unbekannte Viren identifizieren können. Anders als beim normalen Scannen sucht die Heuristik nach typischen Virenmerkmalen. Weist ein Programm oder Dokument eine gewisse Anzahl solcher Merkmale auf, ist es höchstwahrscheinlich infiziert. Mit einer gut programmierten Heuristik erkennen Programme immerhin etwa 80 Prozent aller neuen Viren. Nachteil der heuristischen Erkennung ist jedoch, daß dabei → Fehlalarme auftreten können, also ungefährliche Programme und Dokumente unter Umständen als „wahrscheinlich infiziert“ gemeldet werden.

ITW

ITW steht für „In The Wild“ und bezeichnet Viren, die wirklich in der freien Wildbahn, also auf Rechnern, die nicht in Virenlabors stehen, verbreitet sind. Von den knapp 10.000 bekannten Viren sind weltweit etwa 300 ITW, davon etwa 200 in Deutschland. Alle anderen Viren existieren zur Zeit nur in Labors und Sammlungen von Spezialisten. Ein gutes Antiviren-Programm sollte alle ITW-Viren erkennen und entfernen können. ►

Die besten Virenkiller für Ihren PC



F-Prot Professional für Win 95: Die Virensuche läßt sich über „Aufgabenpläne“ definieren, was am Anfang etwas ungewohnt ist

behoben sein. Bei Experten gilt der mit F-Prot gelieferte Makrovirens Scanner als Referenzscanner – in erster Linie deshalb, weil die Signaturen des Makro-

scanners auf dem FTP-Server des Herstellers im Internet mehrmals täglich aktualisiert werden und somit immer auf dem neuesten Stand sind.

Fazit: F-Prot ist seit Jahren ein weitverbreiteter Klassiker, vor allem, weil die DOS-Version für Privatanwender Freeware ist. Die Entwickler haben die Arbeit an der alten Version vor etwa einem Jahr eingestellt und fügen seitdem nur noch neue Virensignaturen hinzu. Das brachte den bewährten Scanner F-Prot in letzter Zeit technisch ein wenig ins Hintertreffen. Die neue Version 3.0, an der die Programmierer seit mehr als einem Jahr arbeiten, soll dieser Tage fertig werden – zu spät also für unseren Test. Einige Leser haben ihre Lizenz übrigens beim amerikanischen Vertrieb erworben, der F-Prot auch mit einer völlig anderen Windows-Oberfläche anbietet.

BEWERTUNG

Ausstattung	4,0
Bedienung	4,0
Erkennung und Beseitigung	2,5
Schulnoten (1–5)	

FACHCHINESISCH: ANTIVIREN-SOFTWARE (II)

Makrovirus

Ein Makrovirus ist ein Virus, der sich in Dokumentdateien von Office-Anwendungen versteckt. Der Virus wird aktiv, wenn ein infiziertes Dokument geladen wird. Verbreitet sind Makroviren in erster Linie für Winword. Excel-Viren tauchen derzeit nur sehr selten in freier Wildbahn auf. Viren für andere Anwendungen sind theoretisch denkbar. Mit Ausnahme eines Forschungsvirus für die Textverarbeitung Ami Pro sind sie bisher nicht in Erscheinung getreten.

Polymorphe Viren

Polymorphe Viren ändern bei jeder Infektion ihre Gestalt, sie scheinen also zu mutieren. Dazu verschlüsselt sich der Virus in jeder infizierten Datei anders. Diese variable Verschlüsselung bildet quasi eine Hülle um den eigentlichen Virus, die sich ständig verändert. Dadurch ist der Virus gegen die üblichen Signaturscanner gefeit. Gut programmierte polymorphe Viren können mehrere Millionen von Mutationen erzeugen – da bleibt kein Byte auf dem anderen. In Deutschland verbreitet sind Tremor, Nightfall, Neuroquila, One.Half und Hare. Seit kurzem gibt es auch polymorphe Makroviren, die den meisten Antiviren-Programmen noch Probleme bereiten.

Prüfsummen (Check-Summen)

Mit Prüfsummen läßt sich feststellen, ob eine Datei in ihrer ursprünglichen Form vorliegt. Für jedes Programm auf der Festplatte wird eine solche Prüfsumme berechnet. Dringt ein Virus in das System ein und ändert dabei den Code einer Datei, stellt das Antiviren-Programm eine Veränderung der Prüfsumme fest. Mit Hilfe von Prüfsummen können Antiviren-Programme auch Infektionen durch unbekannte Viren erkennen und manchmal sogar die befallenen Dateien reinigen. Auch die residenten Virenwächter mancher Programme arbeiten mit Prüfsummen. Gegen gewiefte Tarnkappenviren sind Prüfsummen-Checks nutzlos: Ein solcher Virus gaukelt dem System eine korrekte Prüfsumme vor.

UU-Encoded

Damit Sie Programme oder Word-Dokumente per E-Mail verschicken können, müssen die Daten zuvor in Ascii-Text ohne Sonderzeichen umgewandelt sein. Dazu gibt es Formate wie UU-Encode oder Mime. Die derart konvertierten Programme lassen sich dann problemlos als elektronische Briefe verschicken und vom Empfänger wieder zu einem ausführbaren Programm decodieren. Wollen Sie

verhindern, daß Ihr Rechner sich etwa durch Attachments von E-Mails einen Virus einfängt, sollte Ihr Virens Scanner mit diesen Formaten arbeiten können.

Virusvarianten

Nur ein geringer Teil der etwa 10.000 bekannten Viren wurde vollständig neu programmiert. Die meisten sind lediglich Modifikationen bereits bekannter Viren. Meist reicht es schon aus, ein paar Assembler-Befehle im Virenquellcode zu vertauschen, damit viele Antiviren-Programme einen eigentlich bekannten Virus nicht mehr erkennen.

VxD (Virtual Device)

Als VxD oder Virtual Device wird eine spezielle Programmart bezeichnet. Die meisten Gerätetreiber und speicherresidenten Programme für Windows 95 sind als VxD programmiert. So gibt es unter anderem VxD-Treiber für den Zugriff auf Grafikkarte, Festplatte und Drucker. Über VxDs wird auch das Multitasking von Windows 95 gesteuert. Anders als ein residentes DOS-Programm kann ein VxD das gesamte System überwachen. Es bietet deshalb die beste Möglichkeit, das System im Hintergrund gegen Viren zu schützen. ■

PROFESSIONELLER PREIS

H+BEDV Antivir 1.01.01

Ausstattung: Antivir kommt mit einer ausreichenden Standardausstattung. Auf der CD sind Versionen für DOS und Windows 95 enthalten, zusätzlich gibt es ein Scanprogramm, das sich per Batchdatei steuern läßt. Erwähnenswert ist das mit viel Engagement geschriebene Handbuch, das sich nicht nur auf die Bedienung von Antivir beschränkt, sondern jede Menge Informationen über Viren im allgemeinen liefert – und über große Strecken sehr amüsant zu lesen ist.

Bedienung: Antivir ist gut in Windows 95 integriert. Die Oberfläche wirkt manchmal ein wenig verspielt, ist aber alles in allem einfach zu bedienen und erlaubt es, Antivir gut zu konfigurieren. Der residente Virenwächter von Antivir ist derzeit noch im Betastadium, liefert aber auch in unserem Härtetest, der andere Virenwächter gelegentlich durcheinanderbrachte, völlig ohne Probleme.

Erkennung und Beseitigung: Antivir hat alle DOS-Viren in unserem Test einwandfrei erkannt. Bei den Makroviren gab es dagegen noch einige Probleme: Mit Excel- und Word-97-Dateien konnte Antivir überhaupt nichts anfangen –



Antivir für Windows 95: Der „Luke Filewalker“ genannte Virens Scanner durchsucht Festplatten und Netzlaufwerke nach infizierten Dateien

Viren in diesen Dokumentformaten blieben unerkannt. Die Makroheuristik sorgt für eine sehr hohe Erkennungsrate bei normalen Makroviren, bedarf aber noch einiger Nachbesserungen: In unserem Test lieferte sie satte 27 Fehllarmen

und brachte bei polymorphen Makroviren nur durchschnittliche Erkennungsraten. Die Virenentfernung ist insgesamt gut, nur zwei DOS-Viren konnte Antivir nicht entfernen, und ein Makrovirus wurde nicht korrekt beseitigt.

DIESE VIREN SOLLTEN SIE KENNEN (I)

Delwin

Delwin ist ein Multipartite-Virus, das heißt: Er infiziert sowohl Dateien als auch Bootsektoren. Zur Selbsterkennung ändert Delwin den unter DOS nicht sichtbaren Sekundenwert des Dateidatums von infizierten Dateien auf „62“. Der Virus setzt die DOS-Versionsnummer auf „2.10“ und den Hersteller auf „IBM“, ein Wert, der normalerweise von OS/2 zurückgegeben wird. Versucht man anschließend, Windows zu starten, bricht es wegen der vermeintlich falschen DOS-Version den Start ab.

Form.A

Form.A ist einer der ältesten Bootsektorenviren, mit dem schon Millionen Disketten infiziert sind und der deshalb wohl nie mehr ganz auszurotten sein wird. Form.A hat keine eigene Schadenswirkung. Allerdings gibt es Kompatibilitätsprobleme mit einigen Programmen und Betriebssy-

stem. Das Ergebnis: Einige Programme laufen nicht mehr korrekt. Form.A läßt sich nach dem Booten von einer sauberen, bootfähigen Diskette mit dem Befehl „sys a: c:“ beseitigen.

Honecker

Bei „Honecker“ handelt es sich strenggenommen nicht um einen Virus. Er besteht aus dem Programm DOSINFO.EXE, das sich in alle erreichbaren Batchdateien auf der Festplatte als erste Zeile hineinschreibt und damit unauffällig immer wieder ausgeführt wird. An den Nationalfeiertagen der DDR und am 25.12. zeigt der Virus den Text „Hiermit wurde Ihre Autoexec auf Anordnung des Ministerrates der DDR gelöscht. Erichs letzte Rache. P.S. Ich komme wieder!“ Dazu dudelt aus dem Lautsprecher die Nationalhymne der DDR, auf modernen Rechnern meistens so schnell, daß sie nicht mehr als solche erkennbar ist. Die AUTOEXEC.BAT wird

währenddessen wirklich gelöscht, sonst entsteht aber kein Schaden. Honeky läßt sich ganz einfach beseitigen, indem Sie die Zeile „@DOSINFO.EXE“ aus der ersten Zeile aller Batchdateien löschen und alle DOSINFO.EXE-Dateien auf der Festplatte entfernen.

Parity.Boot.B

Parity.Boot.B ist einer der am weitesten verbreiteten Bootsektorenviren. Er verbreitet sich ausschließlich über infizierte Disketten und hat nur eine geringe Schadenswirkung: Der Rechner stürzt gelegentlich ab, nachdem der Virus die Fehlermeldung „Parity Check“ ausgegeben hat. Parity.Boot.B verbreitet sich wie alle Bootsektorenviren über infizierte Disketten. Versucht man, von einer infizierten Diskette zu booten, greift der Virus auf die Festplatte über. Er läßt sich nach dem Booten von einer virenfreien Diskette mit dem DOS-Befehl „fdisk /mbr“ beseitigen.

Die besten Virenkiller für Ihren PC

Fazit: H+BEDV Antivir war eines der letzten Programme, das als Windows-95-Version auf den Markt gekommen ist. Die Programmierer haben die erste Version kurz vor der Freigabe verworfen und von vorn angefangen. Die Arbeit hat sich gelohnt: Antivir ist ein solides Programm mit guter Erkennungsrate, allerdings nicht für Word-97- und Excel-Dateien geeignet. Der hohe Preis der Software ist nur gerechtfertigt, wenn man im Rahmen eines Update-Vertrags professionell mit Antivir arbeitet. Antivir ist das einzige Programm im Test, das komplett in Deutschland programmiert wird.

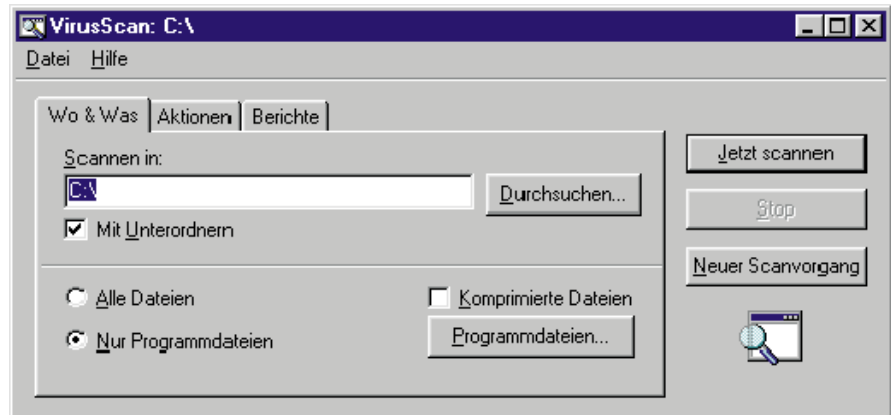
BEWERTUNG

Ausstattung	3,0
Bedienung	3,0
Erkennung und Beseitigung	3,5
Schulnoten (1-5)	

SCHLECHTE REPARATUR

McAfee Virusscan 3.0.2

Ausstattung: McAfee Virusscan ist spartanisch ausgestattet, es sind aber die nötigsten Funktionen implementiert. Unschön: Ein Teil der Handbücher findet sich nur im Adobe-Acrobat-Format auf der CD-ROM. Ebenfalls nur



McAfee Virusscan: Die Programmoberfläche wirkt sehr aufgeräumt und läßt sich auch von einem Laien ohne lange Einarbeitungszeit bedienen

auf der CD-ROM: das Virenlexikon. Ein Scheduler zum automatischen Starten des Programms fehlt ganz. Eine heuristische Virensuche sucht man bei Virusscan vergeblich, dafür bietet es die Möglichkeit eines einfachen Direkt-Updates per Internet.

Bedienung: Die Oberfläche ist hervorragend in Windows 95 integriert. Das Programm wirkt zwar auf den ersten Blick etwas trist, ist aber einfach und auch für Laien schnell und unkompliziert zu bedienen. Allerdings stürzte Virusscan regelmäßig ab, wenn wir Optionen geändert hatten und danach

einen Scanvorgang starteten. Erst nach einem Windows-Neustart arbeitete das Programm ohne weitere Abstürze.

Gut gefiel uns der residente Virenwächter: Er blockiert das Öffnen von infizierten Dateien auf Systemebene und verhindert damit sehr zuverlässig, daß sich ein Virus im System aktivieren kann.

Erkennung und Beseitigung: Bei der Virenerkennung zeigte Virusscan durchwegs annehmbare Resultate, die Ergebnisse bei der Erkennung polymorpher Makroviren waren sogar herausragend: Nur zwei unserer 80 infizierten Dateien

DIESE VIREN SOLLTEN SIE KENNEN (II)

Ripper

(Jack the) Ripper ist ebenso bösartig wie weitverbreitet: Der Virus gehört zu den Top 10 der am häufigsten gemeldeten Viren. Ripper ist extrem heimtückisch: Bei jedem Schreibvorgang auf die Festplatte gibt es eine Chance von 1:1024, daß er 2 Bytes im geschriebenen Sektor vertauscht. Da davon hauptsächlich Datendateien betroffen sind, wird der Schaden oft erst nach Wochen oder Monaten entdeckt, wenn Programme beim Öffnen von Dateien immer häufiger einen Datenfehler melden. Ausführbare Dateien werden meist nur einmal beim Installieren geschrieben und bleiben daher von Ripper verschont.

Taipan

Taipan ist ein ganz simpler unverschlüsselter Dateivirus, von dem es drei Varianten gibt. Taipan verursacht keine Schäden, abgesehen davon, daß eini-

ge EXE-Programme einen Selbst-Check besitzen, der verhindert, daß das von Taipan veränderte Programm weiterhin läuft.

Tequila

Tequila ist ein Multipartite-Virus, befällt also sowohl EXE-Dateien wie auch Bootsektoren. Er tarnt sich zwar vor DOS, fängt aber nicht wie andere Viren die Zugriffe des DOS-Programms Chkdsk ab. Das Resultat: Chkdsk meldet eine Menge Fehler. Wollen Sie dann mit Hilfe von „chkdsk /f“ diese Fehler korrigieren, gehen die „korrigierten“ Programme dabei kaputt, da der Virus dem Betriebssystem falsche Dateidaten vorgaukelt und Chkdsk die befallenen Dateien entsprechend kürzt. Drei Monate nach der Erstinfektion zeigt Tequila beim Beenden infizierter Programme einen von mehreren Texten an – etwa „Beer and TEQUILA forever“ oder „Loving thoughts to LINDA“.

Tremor

Tremor war einer der ersten wirklich verbreiteten polymorph verschlüsselten Tarnkappenviren. Er tritt nach wie vor häufig auf. Tremor verlängert Programme um genau 4000 Bytes und addiert bei allen infizierten Programmen zum Dateidatum 100 Jahre dazu, aus 1995 wird also 2095. Unter DOS fällt diese Änderung nicht auf, da es die Jahreszahl zweistellig anzeigt. Drei Monate nach der ersten Infektion bringt Tremor nach einer gewissen Anzahl von Dateizugriffen den Bildschirminhalt durch direkten Zugriff auf die Grafikkarte zum „Zittern“ und erzeugt gleichzeitig Geräusche über den PC-Lautsprecher. Drückt man dann <Strg>-<Alt>-<Entf>, zeigt Tremor den Text an: „* T.R.E.M.O.R was done by NEUROBASHER / May-June'92, Germany *“, „-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE-“. Nach ein paar Sekunden führt er den Reset durch. ►

Die besten Virenkiller für Ihren PC

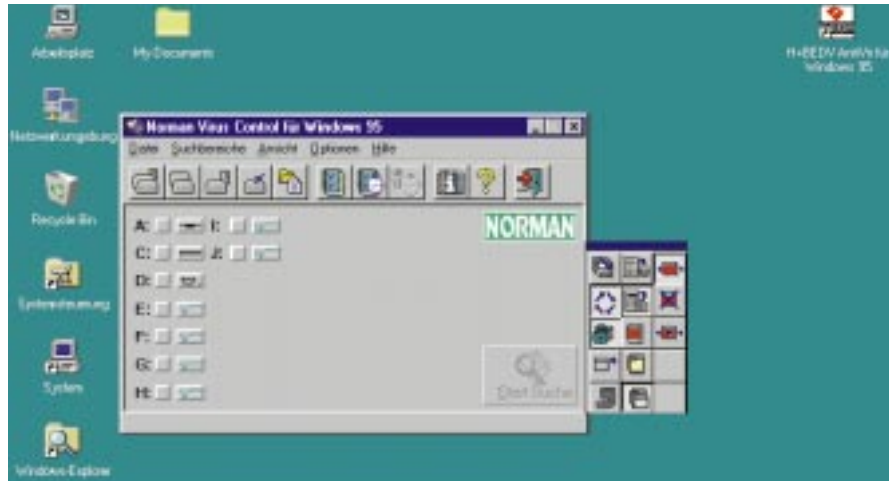
fielen Virusscan nicht auf. Traurig sah es dagegen aus, als Virusscan die erkannten Viren aus den infizierten Dateien entfernen sollte. 45 von 140 als infiziert erkannten Programme zerstörte es bei dem Versuch, sie zu reinigen. Das bestätigt ähnliche Ergebnisse aus unseren früheren Tests und rechtfertigt eine ausdrückliche Warnung vor dem Versuch, infizierte Dateien mit Virusscan säubern zu wollen.

Fazit: Virusscan ist ein Klassiker unter den Antiviren-Programmen, der im Markt nach wie vor ein gutes Ansehen genießt. Doch das Programm wird dem nur teilweise gerecht, wie unser Test zeigt. Virusscan ist einfach zu bedienen und liefert gute bis sehr gute Erkennungsraten.

Solange die Software allerdings ein Drittel aller als „wiederherstellbar“ bezeichneten Programme kaputtrepariert, sollten Sie sie auf keinen Fall zum Säubern infizierter Dateien einsetzen – sonst richtet das Antiviren-Programm mehr Schaden an als jeder Virus.

BEWERTUNG

Ausstattung	2,0
Bedienung	2,0
Erkennung und Beseitigung	3,0
Schulnoten (1–5)	



Norman Virus Control: Die Benutzerführung wirkt schnell zusammengeschustert und eher häßlich, sie ist aber durchaus funktional

NUR MIT UPDATE-VERTRAG

Norman Virus Control 95 4.10

Ausstattung: Die Ausstattung von Norman Virus Control (NVC) kann sich sehen lassen: Der residente Virenwächter glänzt mit Behaviour Blockern für DOS- und Makroviren und macht damit die im Scanner fehlende Heuristik durchaus entbehrlich. Vermissen haben wir lediglich eine Möglichkeit, Dateien auch mit Hilfe von Check-Summen zu überprüfen.

Bedienung: Die Oberfläche von Norman Virus Control wirkt wie eine Beta-Baustelle. Bei Norman legt man offenbar wenig Wert auf Äußerlichkeiten. Die Hilfedatei hat tote Links und ist kaum benutzbar, die Benutzerschnittstelle wirkt hingeschludert und entspricht keinem Standard. Die Optionen und Einstellungen des Programms sind allerdings gut zu finden. Wir haben im Test kein besonderes Gewicht auf die Scangeschwindigkeit gelegt, da bei dem Tempo heutiger Rechner und dank

DIESE VIREN SOLLTEN SIE KENNEN (III)

WM.Cap

Der Makrovirus Cap kommt aus Venezuela und verbreitet sich in Windeseile in alle Welt. Bei der ersten Infektion löscht Cap alle Makros aus der Datei NORMAL.DOT und kopiert seine eigenen Makros hinein. Dann überprüft Cap die Menüstruktur (abhängig von der Sprache) und paßt seine Makros entsprechend an. Durch diesen Trick arbeitet der Virus mit jeder Sprachversion von Winword. Die Zahl und die Namen der Makros unterscheiden sich ebenfalls bei den verschiedenen Sprachversionen. Cap infiziert auch RTF-Dateien, die der Virus dann im Word-Dateiformat speichert – die Dateiendung bleibt aber weiterhin RTF. Ansonsten arbeitet Cap wie alle Makroviren und enthält keine Schadensfunktionen.

WM.Concept

Concept war der erste Makrovirus für Microsoft Word, der in freier Wildbahn

auftauchte. Erste Infektionen wurden im August 1995 gemeldet, heute hat dieser Virus in puncto Verbreitung selbst Bootviren-Klassiker wie Form überholt. Concept hat keine Schadensfunktion und ist für die englische Word-Version programmiert. Im deutschen Word infiziert der Virus zwar die NORMAL.DOT. Danach geschieht nichts mehr. Obwohl sich der Virus mit dem deutschen Winword nicht verbreitet, ist Concept auch in Deutschland ziemlich häufig, was in erster Linie auf den Austausch von Word-Dokumenten mit amerikanischen und englischen Anwendern zurückzuführen ist.

WM.Nop

Der Makrovirus Nop ist einer der einfachsten Makroviren überhaupt: Er besteht lediglich aus zwei Makros, und sein Auftritt hat keine Schadenswirkung. Nop ist ausschließlich mit deutschsprachigen Word-Versionen lauffähig, und er gehört

im deutschsprachigen Raum zu den am weitesten verbreiteten Makroviren.

WM.Wazzu

Wazzu ist einer der wenigen wirklich weltweit verbreiteten Makroviren. Er besteht aus einem einzigen, nur 632 Bytes großen, unverschlüsselten Makro namens „AutoOpen“. Wazzu richtet Schaden an. Das Virenmakro wird beim Öffnen von Dateien je dreimal hintereinander aufgerufen. Mit einer Wahrscheinlichkeit von etwa 20 Prozent löscht Wazzu ein Wort im aktuellen Text und fügt es an anderer Position wieder ein. Mit einer Wahrscheinlichkeit von etwa 25 Prozent wird irgendwo im Text das Wort „wazzu“ eingefügt, der Spitzname der Washingtoner Universität. Wazzu funktioniert mit jeder Word-Version. Mittlerweile existieren weit über 100 Varianten von Wazzu, die sich meist nur durch geringe Veränderungen vom Original unterscheiden. ■

Die besten Virenkiller für Ihren PC

Multitasking die Geschwindigkeit eines Antiviren-Programms kaum mehr ins Gewicht fällt. NVC erwies sich jedoch im Vergleich zu den anderen Programmen als geradezu unglaublich langsam, die Virensuche verlief selbst auf einem schnellen Pentium-Rechner zäh und träge. Gründlichkeit in allen Ehren – aber andere Programme beweisen, daß man gute Erkennungsraten auch schneller haben kann.

Erkennung und Beseitigung: Die Erkennungsraten von NVC waren durchweg gut, lediglich bei polymorphen Makroviren gab es Probleme. Viren in Word-97-Dateien erkannte NVC überhaupt nicht. Das mitgelieferte Reinigungsprogramm läuft nur unter DOS und konnte im Test nur wenige Viren entfernen. Der Hersteller Norman Data Defense hat allerdings eine ganze Reihe von zusätzlichen Reinigungsprogrammen erstellt, die der Support bei Bedarf kostenlos verschickt, so daß sich mit dem Programm in der Praxis doch mehr Viren entfernen lassen. Im Ernstfall steht der Rechner allerdings so lange still, bis die Diskette mit dem entsprechenden Programm per Post angekommen ist. Die Bootsektorviren erkannte NVC durchweg mit Hilfe der Heuristik. NVC besitzt nicht nur einen residenten Virenwächter, sondern auch einen „Smartblocker“, der den Rechner auf virentypische Aktionen überwacht. Dieser Behaviour Blocker ist der beste, den wir bisher im Test hatten. Für Makroviren gibt es einen eigenen Behaviour Blocker namens „Cat's Claw“, der ebenfalls mit guten Erkennungsraten aufwarten konnte. Als wir allerdings den „Auto-Clean“-Modus des Blockers deaktivierten, zeigten sich bei Virenbefall teilweise seltsame Verhaltensweisen wie blockierte DOS-Boxen oder Anwendungen.

Fazit: Norman Virus Control gehört zu den teuren Antiviren-Programmen. Die Support- und Update-Strategie des Herstellers zielt in erster Linie auf Firmenkunden, die Norman Virus Control im Rahmen eines Update-Vertrags kaufen. NVC glänzt mit hohen Erkennungsraten und einem hervorragendem Behaviour Blocker. Dem stehen allerdings eine wenig attraktive Benutzerführung, miserable Reinigungsfunktion, träge Weiterentwicklung und ein hoher Preis gegenüber. Dennoch: Wer einen guten

Behaviour Blocker und hohe Erkennungsraten zu schätzen weiß und im Zweifelsfall auf ein anderes Programm zur Virenbeseitigung zurückgreifen kann, sollte Norman Virus Control in die engere Wahl ziehen.

BEWERTUNG

Ausstattung	2,0
Bedienung	3,0
Erkennung und Beseitigung	3,0
Schulnoten (1–5)	

EMPFEHLENSWERT

Norton Antivirus 2.0

Ausstattung: Symantec gehört zu den wenigen Herstellern, die ihrem Paket eine fertige, bootfähige Notfalldiskette beilegen. Das finden wir sehr gut – denn meistens steht im Fall einer Virusinfektion keine garantiert virenfreie Bootdiskette zur Verfügung. Norton Antivirus (NAV) besitzt keine Heuristik, dafür aber einen einfachen Behaviour Blocker, der die meisten neuen Viren erkennt, bevor sie den Rechner infizieren. Updates für Norton Antivirus sind weit verbreitet und in vielen Online-Diensten und im Internet zu haben. Auf Wunsch kann NAV die Updates auch selbständig aus dem Internet holen.

Bedienung: Norton Antivirus ist hervorragend in Windows 95 integriert

und lehnt sich in der Bedienung an die anderen Norton-Produkte an. Wer beispielsweise die Norton Utilities kennt, wird sich auch in Norton Antivirus schnell zurechtfinden. Warum die CRC-Überwachung der Dateien und der Behaviour Blocker standardmäßig ausgeschaltet waren, konnten wir uns nicht erklären: Schließlich sind beide Funktionen wesentliche und empfehlenswerte Bestandteile des Symantec-Antivirenpakets.

Erkennung und Beseitigung: Bei der Virenerkennung liegt Norton Antivirus durchweg im oberen Mittelfeld, lediglich bei der Erkennung polymorpher Makroviren sollten die Norton-Programmierer noch ein paar Hausaufgaben machen: Norton Antivirus erkannte kein einziges unserer 80 Dokumente als infiziert. Dafür fand NAV Viren in Word-97-Dokumenten ebenso wie Excel-Viren, auch wenn bei beiden die Erkennungsfunktion besser arbeiten könnte.

Die Ergebnisse bei der Reinigung infizierter Dokumente und Dateien waren durchweg ordentlich. Warum NAV den simplen Checkbox-Virus nicht entfernen konnte, ist uns allerdings schleierhaft. Beim Entfernen des hochpolymorphen Virus Nightfall gab es ebenfalls einen Ausrutscher: Eine der zehn infizierten Dateien wollte Symantecs Virenkiller nicht reinigen. ►

ANTIVIREN-PROGRAMME: DER TEST

Datei- und Bootsektorviren

Die Programme mußten ein Standard-Set von 15 der am weitesten verbreiteten Bootsektor- und Dateiviren erkennen. Pro Virus waren zehn infizierte Dateien oder ein infizierter Bootsektor zu erkennen und zu reparieren. Fast alle diese Viren sind älter als zwei Jahre und treten in ganz Deutschland auf. Die Programme sollten sie deshalb durchweg ohne Fehler erkennen und entfernen. Kann ein Programm das nicht, liegt ein klarer Mangel vor, der nicht mit alten Signaturen oder mit einem rein lokalen Auftreten eines Virus entschuldigt werden kann.

Makroviren

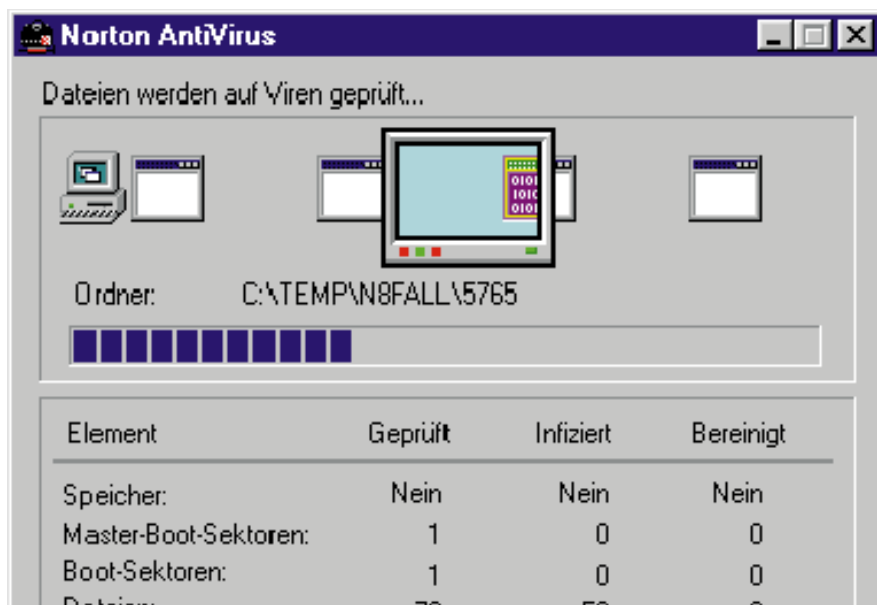
Ein Schwerpunkt des Tests lag bei den Makroviren: Zu finden und zu entfernen waren 20 ITW-Makroviren in Word-7.0-

Texten, 15 Makroviren in Word-97-Dokumenten, zehn Excel-Viren und acht polymorphe Makroviren. Anschließend ließen wir die Programme noch auf unsere Virensammlung mit 672 Makroviren los. Um herauszufinden, ob sie zu Fehlalarmen neigen, haben wir die Virens Scanner schließlich noch auf 94 Winword-Dokumentvorlagen mit vielen Makros angesetzt.

Wertung

Für den Einsatz in der Praxis ist entscheidend, wie gut die Programme mit Viren umgehen können, die tatsächlich in freier Wildbahn auftreten. Darüber hinaus ist vor allem für Makroviren eine gute Heuristik wichtig, weil sie das Programm in die Lage versetzt, auch bisher unbekannte Viren zu erkennen und den Benutzer davor zu warnen. ■

Die besten Virenkiller für Ihren PC



Norton Antivirus: Während das Programm die Festplatte nach infizierten Dateien durchsucht, blickt man auf eine animierte Lupe, die Dateisymbole vergrößert

Fazit: Norton Antivirus war das erste für Windows 95 erhältliche Antiviren-Programm. Der moderate Preis und die einfache Bedienung machen Norton Antivirus in erster Linie für Endanwender interessant, die Wert auf einfache Installation und leichte Handhabung des Programms legen.

BEWERTUNG

Ausstattung	1,0
Bedienung	2,0
Erkennung und Beseitigung	2,5

Schulnoten (1–5)

und Staubsaugern, die allerdings eher unterhaltsam als sinnvoll ist.

Bedienung: Die Oberfläche von Power-Antivirus ist mit der von AVP identisch und ein wenig gewöhnungsbedürftig. Fehlende Funktionen, die aber in AVP enthalten sind, beispielsweise die Heuristik, sind in Power-Antivirus einfach abgebildet. Ganz verzichten müssen PAV-Anwender auf die Heuristik allerdings nicht: In der DOS-Version ist sie aktiv.

Erkennung und Beseitigung: Trotz der fehlenden Heuristik zeigte Power-Anti-

virus hervorragende Ergebnisse bei der Virenerkennung und -beseitigung. Lediglich bei der Erkennung von Makroviren lieferte Power-Antivirus eher schwache Ergebnisse. AVP bringt hier dank der Makroheuristik deutlich bessere Erkennungsraten bei den Word-Viren.

Bei der Entfernung von DOS-Viren schlugen sich beide Programme gleichermaßen hervorragend: Alle infizierten Programme und Bootsektoren wurden korrekt wiederhergestellt. Die Funktionen zur Erkennung und zur Reinigung infizierter Word-Dokumente könnten dagegen durchaus noch verbessert werden.

Fazit: Power-Antivirus ist eine registrierte Version des russischen Shareware-Antiviren-Programms AVP (Antiviral Toolkit Pro). Der Funktionsumfang von Power-Antivirus ist gegenüber dem Original stark eingeschränkt. Anwender von PAV können jedoch die im Internet erhältlichen AVP-Updates uneingeschränkt nutzen. Wer Wert auf einen residenten Virenwächter legt, sollte lieber zum einige Mark teureren AVP greifen. Abgesehen davon bietet PAV für wenig Geld einen soliden Scanner mit guten Erkennungsraten und Reinigungsfähigkeiten.

BEWERTUNG

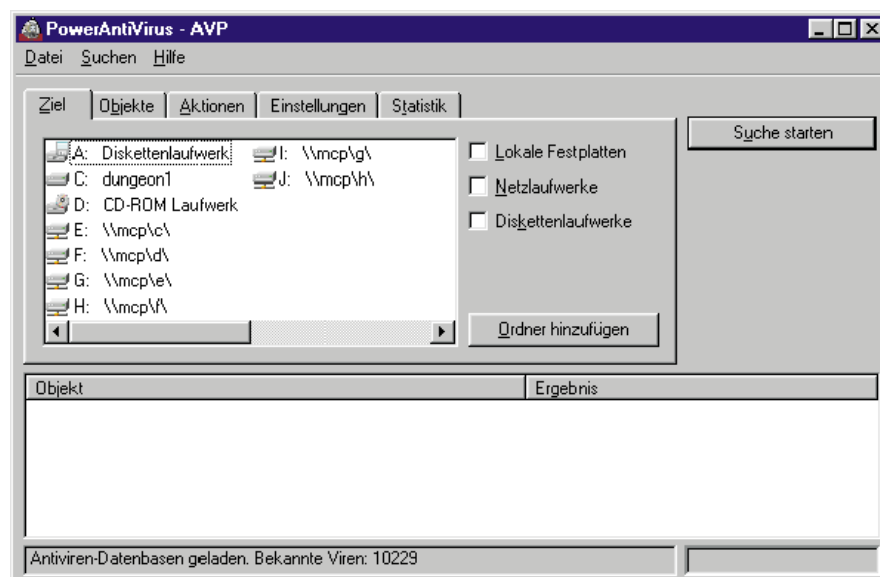
Ausstattung	4,0
Bedienung	3,0
Erkennung und Beseitigung	2,5

Schulnoten (1–5)

UNGLEICHE BRÜDER

Power-Antivirus 3.0 und AVP

Ausstattung: Power-Antivirus (PAV) ist eine stark eingeschränkte Version des Antiviren-Programms AVP (Antiviral Toolkit Pro). Es fehlen die DOS- und Makrovirenheuristik und die CRC-Prüfung von Dateien. Außerdem besitzt Power-Antivirus im Unterschied zu AVP und allen anderen Programmen im Test keinen residenten Virenwächter. Auf der Power-Antivirus-CD finden sich neben einer DOS- und einer Windows-Version des Programms ein ebenfalls von AVP bekanntes, beispielhaftes Virenlexikon, das viele Vireneffekte sogar vorführt und sehr kompetente Infos über die am meisten verbreiteten Exemplare bietet. Zusätzlich gibt es noch eine Viren-Multimediashow mit Schafen

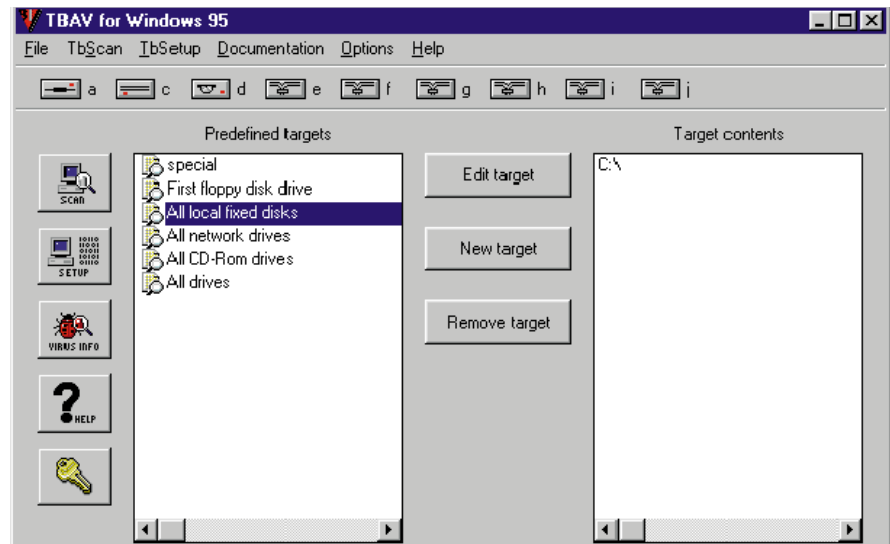


Baugleich: Power-Antivirus ist eine funktionsreduzierte Version des als Shareware vertriebenen russischen Antiviren-Programms Antiviral Toolkit Pro

FÜR TÜFTLER

Thunderbyte Antivirus 8.01

Ausstattung: Thunderbyte Antivirus (TBAV) kommt mit einer DOS- und einer Windows-95-Version. Die Installation erfordert einiges an Eigeninitiative, wenn Sie eine Notfalldiskette und einen DOS-Viren-Check vor dem Booten von Windows 95 einrichten wollen. Thunderbyte besitzt eine gute, aber empfindliche Heuristik für DOS-Programme, aber keine Makroheuristik. Das mitgelieferte Virenlexikon besteht aus wenigen Textbausteinen und ist deshalb ziemlich unbrauchbar. Zur Virenentfernung gibt es drei Möglichkeiten: Zum einen wird das Norman-Reinigungsprogramm NVC mitgeliefert, das allerdings nicht viele Viren entfernen konnte. Als Alternative gibt es die TBAV-eigenen Reinigungsfunktionen, die entweder mit Hilfe von vorher erstellten Checksummen oder komplett heuristisch arbeiten. Updates lassen sich direkt übers Internet ziehen.



Thunderbyte Antivirus: Die Oberfläche wurde komplett der Windows-3.1-Version entnommen und entspricht nicht den Windows-95-Standards

Bedienung: Thunderbyte Antivirus ist ein Programm mit langer Geschichte – was man seiner Benutzerführung auch deutlich ansieht. Die Bedienung ist gewöhnungsbedürftig, und viele nützliche Funktionen sind tief in schwer zu

durchschauenden Menüs versteckt. Ein residenter Virenwächter ist vorhanden, aber nur eingeschränkt brauchbar: Er erkannte Viren nur beim Kopieren. Das Öffnen einer infizierten Datei ließ ihn dagegen völlig kalt. ►

TEST: MAKROVIREN

Erkennung: Makroviren-Sammlung

Produkt	Viren erkannt
Dr. Solomon's Antivirus Toolkit 7.72	646
F-Prot Professional 95 2.26a	662
H+BEDV Antivir 1.01.01	668
McAfee Virusscan 3.0.2	602
Norman Virus Control 95 4.10	654
Norton Antivirus 2.0	634
Power-Antivirus 3.0	577
Thunderbyte Antivirus 8.01	621
Trend Desktop Viruswall 2.0	621
Turbo Antivirus 97/IV	536

Zu erkennen waren 672 Makroviren für Word 6.0/7.0

Erkennung: Excel-95-Makroviren

Produkt	Viren erkannt
Dr. Solomon's Antivirus Toolkit 7.72	5
F-Prot Professional 95 2.26a	1
H+BEDV Antivir 1.01.01	0
McAfee Virusscan 3.0.2	8
Norman Virus Control 95 4.10	5
Norton Antivirus 2.0	4
Power-Antivirus 3.0	9
Thunderbyte Antivirus 8.01	2
Trend Desktop Viruswall 2.0	8
Turbo Antivirus 97/IV	0

Zu erkennen waren zehn Makroviren für Excel 95

Erkennung: Word-97-Makroviren

Produkt	Viren erkannt
Dr. Solomon's Antivirus Toolkit 7.72	4
F-Prot Professional 95 2.26a	11
H+BEDV Antivir 1.01.01	0
McAfee Virusscan 3.0.2	9
Norman Virus Control 95 4.10	0
Norton Antivirus 2.0	7
Power-Antivirus 3.0	12
Thunderbyte Antivirus 8.01	0
Trend Desktop Viruswall 2.0	14
Turbo Antivirus 97/IV	0

Zu erkennen waren 15 Makroviren für Word 97

Erkennung: polymorphe Makroviren

Produkt	Viren erkannt
Dr. Solomon's Antivirus Toolkit 7.72	51
F-Prot Professional 95 2.26a	13
H+BEDV Antivir 1.01.01	42
McAfee Virusscan 3.0.2	78
Norman Virus Control 95 4.10	23
Norton Antivirus 2.0	0
Power-Antivirus 3.0	45
Thunderbyte Antivirus 8.01	23
Trend Desktop Viruswall 2.0	54
Turbo Antivirus 97/IV	30

Zu erkennen waren acht polymorphe Makroviren für Word 6.0/7.0 in je zehn verschiedenen Generationsstufen

Die besten Virenkiller für Ihren PC

Erkennung und Beseitigung: Die Stärke von TBAV ist seine DOS-Virenheuristik, die auch bei komplexen DOS-Viren für hohe Erkennungsraten sorgt – allerdings auch für viele Fehlalarme. Wer die Heuristik einsetzt, sollte in der Lage sein, einen Fehlalarm von einer echten Vireninfektion zu unterscheiden.

Bei der Virenerkennung schlug sich Thunderbyte im Test durchweg gut. Negativ aufgefallen ist uns, daß TBAV noch keine Word-97-Dokumente durchsuchen kann und die Erkennung polymorpher Makroviren schlampig programmiert ist: Bei drei Viren erkannte das Produkt nur Generation-1-Samples. Die Ergebnisse des mitgelieferten NVC-Reinigungsmoduls waren nicht zufriedenstellend. Es empfiehlt sich daher, CRC-Check-Summen zu erstellen – dann lassen sich die meisten Infektionen auch mit dem Thunderbyte-Reinigungsmodul beseitigen.



Fazit: Thunderbyte Antivirus ist eine Shareware, wird unlimitiert über CD-ROMs, Internet und Mailboxen vertrieben und kann in Deutschland registriert werden. Thunderbyte ist für fortgeschrittene Anwender durchaus zu empfehlen. Wer sich in die Programmfunktionen einarbeitet und gerne tüfelt, hat mit dem Programm ein brauchbares Antiviren-Tool, das allerdings bei eingeschalteter DOS-Heuristik viele Fehlalarme liefert und Infektionen kaum automatisch beseitigen kann.

BEWERTUNG

Ausstattung	4,0
Bedienung	4,0
Erkennung und Beseitigung	4,0

Schulnoten (1–5)



Desktop Viruswall: Der „Säuberungs-Assistent“ führt den Anwender im Ernstfall Schritt für Schritt mit klaren Anweisungen durch die Virenentfernung

SÄUBERUNGS-ASSISTENT

Trend Desktop Viruswall 2.0

Ausstattung: Desktop Viruswall gehört zu den wenigen Programmen, die mit einer fertigen Rettungsdiskette ausgeliefert werden – das ist im Fall einer Vireninfektion eine unschätzbare Hilfe, da meistens gerade in diesem Moment keine bootfähige und garantiert virenfreie Diskette zur Hand ist. Eine CRC-Prüfung und DOS-Heuristik haben wir vergeblich gesucht, dafür bietet Trend aber eine Makroheuristik und ein Live-Update übers Internet.

Bedienung: Die Oberfläche von Viruswall ist nicht schlecht, aber ein wenig bunt und verspielt. Im Fall einer Vireninfektion erweist sich die Benutzer-

führung dagegen als nahezu genial: Zunächst bietet Viruswall Informationen über den gefundenen Virus, danach tritt ein „Säuberungs-Assistent“ in Aktion, der Schritt für Schritt hilft, den Virus zu beseitigen und alle Aktionen genau erklärt. Tritt ein unbekannter Virus auf, bietet das Programm an, ihn übers Internet an das Trend-Virenlabor zu senden. Wenn Sie infizierte Dateien oder Dokumente versandt oder von anderen bekommen haben, schlägt Viruswall gleich einen Text vor, den Sie per E-Mail als Warnung verschicken können. Mit dieser hervorragenden Benutzerführung verhindert Desktop Viruswall im Ernstfall eine Panikreaktion, die erfahrungsgemäß oft mehr Schaden anrichtet als der Virus selbst. ►

Die besten Virenkiller für Ihren PC

Erkennung und Beseitigung: Bei der Virenerkennung schlug sich das Programm recht passabel – bei den Dateiviren verpaßte es lediglich drei der hochpolymorphen Nightfall-Viren. Einen Fauxpas leistete sich der Viruswall bei den Bootsekturviren, wo er als einziges Programm im Test einen Virus übersah. Die Makroviren-Erkennung war durchweg gut bis sehr gut. Allerdings erkannte das Programm alle Makroviren nur mit Hilfe der Heuristik und konnte sie daher nicht genau identifizieren. Im Ernstfall wissen Sie mit dieser Version also nie, mit welchem Virus Sie es eigentlich zu tun haben. Die Makroheuristik sorgte außerdem im Test für haufenweise Fehlalarme. Die Virenentfernung lief eher durchschnittlich: Ein Dokument wurde nicht von einem Makrovirus gereinigt, und auf die technisch schwierige Entfernung polymorpher Viren wie Tremor oder Neuroquila verzichtete Viruswall von vornherein. Gut gefallen hat uns der residente Virenwächter, der wirklich alles überprüft: sogar UU-codierte Viren in E-Mail-Attachments erkannte Viruswall bereits vor dem Decodieren. Weniger überzeugt hat uns der residente Makroscanner, der als Word-Add-on im WLL-Format realisiert ist. Ein solches Programm kann für Kompatibilitätsprobleme sorgen. Außerdem war der Makrowächter nicht mehr lauffähig, nachdem wir die neuesten Updates installiert hatten.



Fazit: Der Desktop Viruswall wurde vor kurzem noch unter dem Namen PC-Cillin verkauft. In der Szene der Virenbekämpfer hat der taiwanische Hersteller Trend einen schlechten Ruf: Im Internet kursieren viele Exemplare, die offensichtlich aus der Trend-Virensammlung stammen. Das Produkt halten wir trotz einiger technischer Schwächen vor allem für Laien für durchaus empfehlenswert: Der Säuberungs-Assistent für infizierte Programme ist vorbildlich, während andere Programme den Anwender bei einem Virenfund oft im Regen stehen lassen.

BEWERTUNG

Ausstattung	2,0
Bedienung	1,0
Erkennung und Beseitigung	3,0
Schulnoten (1–5)	

VERBESSERUNGSBEDÜRFTIG

Turbo Antivirus 97/IV

Ausstattung: Das Handbuch zu Turbo Antivirus (TNT) ist verständlich und ausreichend. Auf der CD befinden sich zusätzlich Multimedia-Demonstrationen zum Thema Viren, die aber mehr Unterhaltungs- als wirklichen Nutzwert haben. Der Scanner ist als DOS- und Windows-Version auf der CD, dazu kommt ein VxD-basierter residenter Virenwächter. Eine Makroheuristik ist vorhanden, Excel- und Word-97-Viren dagegen suchten wir mit Turbo Antivirus vergeblich. Sehr gut finden wir die mitgelieferte fertige Notfalldiskette, die im Fall einer Infektion die Suche nach einer virenfreien Bootdiskette erspart.

Bedienung: Turbo Antivirus ist nicht besonders gut in Windows 95 eingebunden. Trotzdem läßt es sich auch ohne Vorkenntnisse leicht bedienen. Die Billigvariante Turbo Antivirus Energy (69 Mark) besitzt dagegen eine futuristisch anmutende Oberfläche, die keinem Standard entspricht und gewöhnungsbedürftig ist. Im Test erwies sich Turbo Antivirus als recht stabil, allerdings brachten beschädigte Word- und Excel-Dateien das Programm oft zum Absturz. Einen massiven Fehler fanden wir im Virenwächter: Beim Öffnen einer mit Concept infizierten Word-Datei wurde der Virus aktiv, bevor der Wächter Alarm schlug. Die NORMAL.DOT war trotz aktivem Virenwächter bereits infiziert! Der Hersteller sollte schleunigst für Abhilfe sorgen.

Erkennung und Beseitigung: Sowohl bei der Erkennung als auch bei der Entfernung von Dateiviren belegt Turbo Antivirus mit Abstand den letzten Platz. Die Reinigungsfunktion scheiterte an einfachsten Dateiviren wie Major oder Checkbox. Viele Dateien wurden gar nicht gereinigt, mit Tequila infizierte Dateien sogar beim Versuch zerstört. Bei der Erkennung hochpolymorpher Viren wie Nightfall erwies sich TAV als unzuverlässig: Es erkannte nur sechs von zehn infizierten Dateien. Die Makroheuristik ist einfach gestrickt. Sie identifizierte nur simple Viren, lieferte dabei aber ebenso wie die DOS-Virenheuristik viel zu viele Fehlalarme. Da TNT viele Makroviren nur mit Hilfe der Heuristik findet und somit nicht genau identifiziert, konnte das Programm

Die besten Virenkiller für Ihren PC



Turbo Antivirus: Die Oberfläche hält sich nicht an bekannte Standards, ist aber auch für Laien einfach und unkompliziert zu bedienen

auch nur einen kleinen Teil der infizierten Dokumente reinigen. Drei der von Turbo Antivirus gereinigten Dokumente wurden nicht korrekt repariert.

Fazit: Turbo Antivirus fiel bei früheren Tests immer wieder durch schlechte Erkennungsraten und viele Programmabstürze negativ auf. Der deutsche Anbieter hat schon vor einiger Zeit die Programmierung, die vorher nur in Israel stattfand, zumindest teilweise selbst in die Hand genommen und sicher nicht zuletzt dadurch die Qualität des Programms gegenüber älteren Versionen erheblich verbessert.

Trotz der Leistungsverbesserung gegenüber früheren Versionen gehört Turbo-Antivirus noch immer zu den Produkten am untersten Ende der Leistungsskala. Der hohe Preis für das Vollprodukt ist kaum zu rechtfertigen.

BEWERTUNG

Ausstattung	2,0
Bedienung	3,0
Erkennung und Beseitigung	5,0

Schulnoten (1–5)

VIREN-QUIZ: SIND SIE GEGEN VIREN GEFEIT?

Sie starten Ihren PC nicht von Diskette. Sie holen sich Software nur aus verlässlichen Quellen. Bisher sind Sie von Viren verschont geblieben. Es droht also keine Gefahr. Oder doch? Testen Sie Ihren Gefährdungsquotienten.

- Antiviren-Software läuft bei Ihnen ...
 - regelmäßig, wenn der PC läuft
 - nur, wenn Sie Dateien downloaden
 - nur, wenn man Sie erinnert
 - nach einem Virenbefall
- Wann haben Sie die Virensignatur-Datenbank Ihrer Antiviren-Software zuletzt aktualisiert?
 - vor einem Monat
 - vor einem Jahr
 - in den 90er Jahren
 - in den 80er Jahren
- Ihre Arbeitskollegen und Freunde dürfen ...
 - auf Ihren paßwortgeschützten Screensaver blicken
 - Daten von ihren PCs auf Ihren PC kopieren
 - Daten übers Netzwerk von ihren PCs auf Ihren PC überspielen
 - Ihren PC benutzen, wenn Sie nicht da sind
- Sie lassen Programme auf Ihrem PC laufen, die ...
 - von einem Datenträger stammen, den Sie auf Viren geprüft haben
 - Sie aus kommerziellen Online-Diensten wie CompuServe und AOL überspielt haben
 - im Internet oder in privaten Mailboxen fanden
 - auf einer Diskette waren, die Ihnen Ihr Schwager mitbrachte
- Sie haben neulich ...
 - Bilder aus dem XY-Forum einer entlegenen Ecke des Internets angeschaut
 - eine Excel-Datei geladen, die Sie per E-Mail erhalten hatten
 - die Langeweile damit vertrieben, daß Sie den Inhalt alter Disketten inspiziert haben
 - sich geärgert, daß Ihr Sohn den Familien-PC von Laufwerk A: per Diskette gestartet hat

Punktwertung

Für jede **A**-Antwort gibt es **0** Punkte.

Für jede **B**-Antwort gibt es **1** Punkt.

Für jede **C**-Antwort gibt es **2** Punkte.

Für jede **D**-Antwort gibt es **3** Punkte.

12 bis 15

Ihr PC ist extrem gefährdet. Schalten Sie ihn aus, und lesen Sie den Artikel erneut.

8 bis 11

Sie und Ihr PC leben gefährlich!

4 bis 7

Bisher könnten Sie Glück gehabt haben.

0 bis 3

Entwarnung.



Die besten Virenkiller für Ihren PC

ANTIVIREN-PROGRAMME: FUNKTIONSUMFANG										
	Dr. Solomon's Antivirus Toolkit 7.72	F-Prot Pro- fessional 95 2.26a	H+BEDV Antivir 1.01.01	McAfee Virus- scan 3.0.2	Norman Virus Control 95 4.10	Norton Antivirus 2.0	Power- Antivirus 3.0	Thunder- byte Antivirus 8.01	Trend Desktop Viruswall 2.0	Turbo Antivirus 97/IV
DOS-Viren- schutz beim Starten des Systems (Win 95)	Ja ¹⁾	Nein ¹⁾	Nein ¹⁾	Ja ¹⁾	Ja	Ja	Nein ¹⁾	Nein ¹⁾	Ja	Ja
Viren-Check vor der Installation	Ja	Nein	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Notfall- diskette	Ja, mit- geliefert	Nein	Nein	Ja, wird angelegt	Ja, wird angelegt	Ja, mit- geliefert	Ja, wird angelegt	Nein	Ja, mit- geliefert	Ja, wird angelegt
Heuristik	Ja	Nein ³⁾	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja
Heuristik (Makroviren)	Ja	Nein	Ja	Nein	Nein	Nein	Nein	Nein	Ja	Ja
CRC-Prüfung	Ja	Nein ³⁾	Ja	Nein ³⁾	Nein	Ja	Nein	Ja	Nein	Ja
CRC- Reinigung	Ja	Nein ³⁾	Ja	Nein ³⁾	Nein	Ja	Nein	Ja	Nein	Ja
Durchsuchen von Archiven (ZIP/ARJ/ RAR)	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja
Internet- Update- Funktion	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja	Ja	Nein
Kostenlose Updates Online	Nein	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Nein
Residentes Wächter- programm	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Wächter- programm: Scanner	Ja	Ja	Ja	Ja	Ja ⁴⁾	Ja	Nein	Ja	Ja	Ja
Wächterpro- gramm mit CRC-Check	Nein	Nein	Nein	Nein	Nein	Ja	Nein	Ja	Nein	Ja
Wächterpro- gramm mit Behaviour Blocker	Nein	Nein	Nein	Nein	Ja	Ja	Nein	Ja	Ja	Nein
Wächterpro- gramm erkennt Makroviren	Ja	Ja	Ja	Ja	Ja	Ja	Nein	Ja	Ja	Ja
Scheduler (Zeitge- steuerter Start der Virensuche)	Ja	Ja	Ja	Nein	Ja	Ja	Nein	Ja	Ja	Ja
Virenlexikon	Ja ²⁾	Nein ³⁾	Ja	Nein	Ja	Ja	Ja	Ja ²⁾	Ja	Ja ²⁾

1) DOS-Version im Paket enthalten

2) Lexikon nur tabellarisch, keine wesentlichen Informationen

3) nur in DOS-Version vorhanden

4) nur für Makroviren

Die besten Virenkiller für Ihren PC

VERBREITETE VIREN: ERKENNUNG UND BESEITIGUNG

	Dr. Solomon's Antivirus Toolkit 7.72	F-Prot Pro- fessional 95 2.26a	H+BEDV Antivir 1.01.01	McAfee Virus- scan 3.0.2	Norman Virus Control 95 4.10	Norton Antivirus 2.0	Power- Antivirus 3.0	Thunder- byte Antivirus 8.01	Trend Desktop Viruswall 2.0	Turbo Antivirus 97/IV
Boom.A:De	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
Büro.A:De	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
CAPA	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2 ¹⁾
Clock.A:De	2/2 ¹⁾	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2 ¹⁾
Colors.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
Concept.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2 ¹⁾
CountTen.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/0
Divina.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/0
Friday.A:De	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/0
Macaroni.A:De	2/0	2/2	2/2	2/2	2/2	2/2	0/0	2/2	2/2	2/0
MDMA.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
NFA	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
Nomvir.A:De	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/0
NOPA:De	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	1/1
NPAD.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
Schumann.A	2/0	0/0	2/2	0/0	0/0	0/0	0/0	0/0	2/2 ¹⁾	2/0
Smiley.A:De	2/2	2/2	2/2 ¹⁾	2/2	2/2	2/2	2/0	2/2	2/2	2/0
Toten.A:De	2/2	2/2	2/2	2/2	2/2	2/2	0/0	1/1	2/2	2/0
Vicinity.A:De	2/0	0/0	2/2	0/0	0/0	2/2	0/0	0/0	2/2	1/0
Wazzu.A	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2	2/2
Gesamt										
Makroviren:	40/32	36/36	40/38	36/36	36/36	38/38	32/30	35/35	40/38	38/15
Burglar.1150	10/10	10/10	10/10	10/0 ¹⁾	10/10	10/10	10/10	10/10	10/10	10/10
Checkbox.936	10/10	10/10	10/0	10/0 ¹⁾	10/0	10/0	10/10	10/0	10/0	0/0
Delwin.1759	(10/10)	10/10	10/10	10/10	10/0	10/10	10/10	10/0	10/0	10/10
HLL. Honecker ⁵⁾	10/-	10/-	10/-	0/-	10/-	0/-	10/-	0/-	10/-	10/-
Junkie.A	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10
Major.1644	10/10	10/10	10/10	10/10	10/0	10/10	10/10	10/0	10/10	10/10
Manzon.A	10/10	10/0	10/10	10/7 ²⁾	10/0	10/10	10/10	10/0	10/10	10/0
Neuroquila.A	10/10	10/0	10/10	10/0	10/0	10/10	10/10	10/0	10/0	10/0
Nightfall.5764	10/10	10/0	10/10	10/0	10/0	10/9	10/10	10/0	7/0	6/0
Quickly.1376	10/10	10/10	10/10	10/0 ¹⁾	10/0	10/10	10/10	10/0	10/10	10/10
Tai-Pan.438.A	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/0
Tentacle.A	10/10	10/0	10/0	10/0 ¹⁾	10/0	10/10	10/10	10/0	10/10	0/0
Tequila.A	10/10	10/10	10/10	10/8 ²⁾	10/10	10/10	10/10	10/10	10/10	10/8 ¹⁾
Tremor.A	10/10	10/0	10/10	10/0	10/0	10/10	10/10	10/0	10/0	10/0
Yankee Doodle	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10	10/10
Gesamt										
Dateiviren:	150/140	150/90	150/120	140/65	150/50⁴⁾	140/129	150/140	140/50³⁾	147/100	126/58

Die Zahlen beziehen sich auf das Erkennen/Reinigen infizierter Dokumente und Programme. Bei den Makroviren waren je Virus zwei Dokumente zu erkennen und zu reinigen, bei Dateiviren mußten die Programme den Virus in jeweils zehn infizierten Dokumenten finden und korrekt entfernen.

Lesebeispiele:

Antivir hat zwei von zwei mit Boom.A:De infizierte Dokumente korrekt erkannt und aus beiden den Virus korrekt entfernt. Zwei mit Smiley.A:De infizierte Dokumente wurden zwar als infiziert erkannt, konnten aber nicht korrekt gereinigt werden.

Von zehn mit Burglar.1150 infizierten Programmen hat Antivir alle zehn korrekt erkannt. Es konnte den Virus aus allen zehn Dateien korrekt entfernen.

Von zehn mit Tentacle.A infizierten Programmen hat Antivir alle zehn korrekt erkannt, konnte den Virus aber aus keiner Datei entfernen.

1) Dateien wurden nicht korrekt gereinigt oder durch die Reinigung beschädigt oder zerstört.

2) Einige Dateien wurden durch die Reinigung beschädigt oder zerstört.

3) Thunderbyte Antivirus setzt NVCLEAN von NVC95 ein, hat aber zusätzlich noch die Möglichkeit der CRC-Reinigung.

4) Der technische Support von Norman hat für viele Dateiviren einzelne Reinigungsprogramme parat, die bei Bedarf an Kunden mit Support-Vertrag oder innerhalb der Support-Frist verschickt werden. Diese Einzelprogramme sind in der Tabelle nicht berücksichtigt.

5) HLL.Honecker kann aus technischen Gründen nicht entfernt werden.