Einführung

Panda Antivirus

Panda Antivirus ist eine komplette und wirksame Lösung, um Ihren Computer gegen jegliche Art von Computerviren geschützt zu halten. Es enthält Versionen für Windows 95, Windows NT Workstation, Windows 3.1x, DOS und OS/2, damit Sie unabhängig von dem benutzten Betriebssystem geschützt bleiben. Diese Hilfe ist die für **Panda Antivirus** für Windows NT Workstation.

Schutzstrategien

Panda Antivirus enthält mehrere Schutzstrategien gegen Viren:

- **Permanenter Schutz:** Der permanente Schutz schützt den Computer jederzeit gegen Viren, ohne Notwendigkeit eines Benutzereingriffs. Der große Vorteil dieser Schutzstrategie ist, daß damit der Computer vollautomatisch gegen Viren geschützt ist.
- **Von Benutzer eingeleitete Analyse:** Die vom Benutzer eingeleitete Analyse ermöglicht die Analyse beliebiger Bereiche des Computers wann immer erwünscht. Erst wird der zu analysierende Bereich des Computers ausgewählt und dann beginnt die Analyse auf der Suche nach Viren im angegebenen Bereich.
- **Desinfizierung:** Nach dem Finden eines Virus kann auf mehrere Arten vorgegangen werden. Eine davon ist die Desinfizierung, die darin besteht, den Virus von der Datei zu löschen und diese so zu belassen, wie sie vor de Infektion war.
- **Heuristische Analyse:** Die heuristische Analyse ist eine alternative Analysetechnik zu den vorher erwähnten. Die heuristische Analyse wird auch vom Benutzer eingeleitet, d.h. der Benutzer muß den mit dieser Methode zu analysierenden Bereich des Computers seiner Wahl angeben. Diese Analysetechnik kann unbekannte Viren finden.
- **Suche von Zeichenketten:** Genauso wie die heuristische Analyse, ist diese eine alternative Analysetechnik und wird auch vom Benutzer eingeleitet. Ihre Aufgabe ist die Suche von neuen Virus aufgrund von Daten, die vom Panda Software technischem Kundendienst geliefert werden.
- **Andere Optionen:** Dies sind bestimmte Möglichkeiten des Antivirus, die Ihnen Information liefern, oder die die Administration desselben erleichtern. Zum Beispiel, gibt es einen Ergebnisbericht, in dem die verschiedenen Operationen, die mit dem Antivirus ausgeführt wurden, und deren Zwischenfälle eingesehen werden können.

Panda Software Antivirus Lösungen

Panda Software bietet Ihnen folgenden Antivirus Lösungen:

- **24h-365d® Antivirus Insurance® für einzel PCs**. *Lizenzen.*
- **24h-365d® Antivirus Insurance ® für vernetzte PCs** (automatische Verteilung von Netzwerkservern aus).
- **24h-365d® Antivirus Insurance ® für Netzwerkserver** (Novell NetWare und Windows NT Server).
- **24h-365d® Antivirus Insurance ® für lokale Netzwerke**.
- **24h-365d® Antivirus Insurance ® für Email und Groupware Clients**.
- **24h-365d® Antivirus Insurance ® für Email und Groupware Server**.
- **24h-365d® Antivirus Insurance ® für SMTP Email Server**.
- **24h-365d® Antivirus Insurance ® für an das Internet angeschlossene PCs**.

- **24h-365d® Antivirus Insurance ® für Internet Server (SMTP, FTP und HTTP)**.
- **24h-365d® Antivirus Insurance ® für Proxys**.

Was ist die 24h-365d® Panda Software Antivirus Insurance®?

Die 24h-365d® Panda Software Antivirus Insurance®, ist ein neues und revolutionäres Konzept im Antivirusschutz, das noch mehr zur Sicherheit beiträgt. Die **24h-365d® Panda Software Antivirus Insurance®** ist eine außergewöhnliche Kombination von Produkten und Dienstleistungen, die einen sehr hohen Schutz gegen Computerviren bietet. Die **24h-365d® Panda Software Antivirus Insurance®** kann mit verschiedenen Laufzeiten des Rechtes auf Aktualisierungen und mit verschiedenen Häufigkeiten der Aktualisierung erworben werden.

Das Produkt ist **Panda Antivirus**, eine Antivirus-Software, welche die höchsten Auszeichnungen zur Entdeckung von Viren erhalten hat:

- **ICSA Bescheinigung:** Wird von der hochangesehenen Organisation ICSA in den USA an Antivirus Produkte vergeben, die periodisch 100% der Viren *In the Wild* (die zur Zeit meist verbreiteten Viren) und über 90% der *Zoo Collection* (Sammlung tausender, weniger verbreiteter Viren) entdecken.
- **CheckMark Bescheinigung:** Wird von der englischen technischen Zeitschrift für Computersicherheit *Secure Computing* vergeben.

Wenn Sie nicht über die **24h-365d® Panda Software Antivirus Insurance®** verfügen, können Sie sie mit dem der Registrierkarte beigelegtem Bestellformular bestellen. Die von der **24h-365d® Panda Software Antivirus Insurance®** angebotenen Dienstleistungen werden im Folgenden beschrieben.

- **Hotline**: Während EINES Jahres werden wir Ihre technischen Probleme per Telefon, Fax, dem Internet oder Email lösen. Ganz gleich wann Sie anrufen, stehen Ihnen jederzeit, Tag und Nacht, hochqualifizierte Techniker, 24 Stunden am Tag, 365 Tage im Jahr zur Verfügung. Dies ist ein exklusiver Service von **Panda Software**.
- **Viren SOS**: Wenn Sie einen Virus finden, den **Panda Antivirus** nicht entdeckt oder nicht entfernt, werden wir die betreffende Datei mit einem Eildienst bei Ihnen abholen lassen (oder wir werden die verdächtige Datei auf andere Art und Weise abholen), und in weniger als 24 Stunden werden wir eine neue Version entwickeln, die imstande ist den neuen Virus zu entdecken und zu entfernen. Wir werden Ihnen die neue Version kostenlos zukommen lassen.
- **Aktualisierungsservice mit Zustellung an Ihre Adresse:** Ihr Antivirus wird vollkommen aktualisiert sein. Sie werden an Ihrer Adresse monatlich oder dreimonatlich Aktualisierungen auf CD oder Diskette erhalten, wenn Sie unsere **24h-365d® Panda Software Antivirus Insurance®** erworben haben. Sie können das Produkt auch durch unser WEB ein Jahr lang so oft wie Sie möchten aktualisieren, was Ihnen mindestens eine tägliche Aktualisierung garantiert.
- **WEB Service:** Antworten auf häufige Fragen und Information über Viren.

Installation

Anforderungen

Um **Panda Antivirus** für Windows NT Workstation zu installieren benötigen Sie folgendes:

- IBM kompatibler Computer mit 486 oder hochwertigerem Prozessor.
- 16 MB Hauptspeicher (RAM).
- 4 MB freien Speicherplatz auf der Festplatte.
- Windows NT 3.51 Betriebssystem oder höher.
- CD-ROM Laufwerk.
- Maus.

Installationsprozedur

Es gibt zwei Versionen von **Panda Antivirus** für Windows NT Workstation. Die eine ist für Windows NT Workstation 3.51 und die andere für Windows NT Workstation 4.0. Sie dürfen nur die Programmversion für Ihre Version des Betriebssystems installieren.

Beide Versionen können nur vom CD-ROM installiert werden, das mit dem Produkt geliefert wird. Um irgendeine der zwei Programmversionen zu installieren, führen Sie bitte das Programm CDMENU.COM aus. Dieses Programm bietet Ihnen ein einfaches Menü mit Optionen an. Wählen Sie zuerst die gewünschte Sprache und dann die zu installierende Version. In diesem Fall müssen Sie eine der zwei Versionen von **Panda Antivirus** für Windows NT (für NT 3.51 oder NT 4.0), gemäß der auf Ihrem Computer installierten Version des Betriebssystems, wählen.

Um die Version von **Panda Antivirus** für Windows NT Workstation installieren zu können, müssen Sie Rechte als Administrator auf dem betreffenden Computer haben. Der Grund dafür sind die notwendigen Rechte, um den Treiber installieren zu können, der sich um den permanenten Schutz kümmert.

Die Installationsprozedur besteht aus folgenden Schritte:

1. Zuerst wird ein Vorstellungsbildschirm angezeigt.
2. Dann wird um die Benutzerdaten gebeten.
3. Dann wird um das Verzeichnis gebeten, in das die Anwendung installiert werden soll.
4. Danach geben Sie die Programmgruppe an, in der die Symbole für den Zugriff auf den Antivirus erstellt werden sollen.
5. Sie können dann auswählen, ob der permanente Schutz (**Sentinel** Treiber) installiert werden soll oder nicht.
6. Danach beginnt die Kopie der Dateien auf die Festplatte.
7. Nach dem Beenden der Kopie sollten Sie den Computer neu starten, damit der permanente Schutz aktiviert wird.

Aktualisierung des Antivirus

Um eine Version des Antivirus mit einer neu erhaltenen Aktualisierung desselben zu aktualisieren, brauchen Sie nur die neue Version über die alte zu installieren.

Entfernung

Bei der Version für Windows NT 3.51, erfolgt die Entfernung von **Panda Antivirus** mit dem Programm UNINST, das sich in der Programmgruppe der Anwendung befindet.

Bei der Version für Windows NT 4.0, erfolgt die Entfernung von **Panda Antivirus** mit der Option *Software* der *Systemsteuerung*. Sie brauchen dort nur **Panda Antivirus Windows NT W/S 4.0** in der Liste entfernbarer Programme auswählen, und dann auf die Schaltfläche *Hinzufügen/Entfernen* zu klicken. Um die Entfernung zu beenden, muß der Computer neu gestartet werden.

Versuchen Sie nicht, diese Version zu entfernen, indem Sie das Verzeichnis löschen, in dem die Software installiert wurde. Entfernen Sie das Programm immer mit der angegebenen Prozedur.

Was ist der permanente Schutz

Der permanente Schutz ist ein Programm, das von dem Augenblick an, wo der Computer gestartet wird, alle Operationen überprüft, die ein Ansteckungsrisiko innehaben, um sicherzustellen, daß kein Virus in das System kommt.

Der permanente Schutz funktioniert vollautomatisch, ohne jeglichen Benutzereingriff. Der dauernde Schutze beeinträchtigt nicht die Leistungsfähigkeit des Computers, und sollte deshalb immer installiert werden, da er das Schutzniveau des Systems erheblich erhöht.

Benutzung des permanenten Schutzes

Der permanente Schutz ist eine der Optionen bei der Installation. Wenn dieser Schutz installiert wurde, wird nach dem Neustart des Computers der permanente Schutz (**Sentinel**) aktiv sein.

Wenn Ihr Betriebssystem Windows NT Workstation 3.51 ist, erscheint **Sentinel** als ein minimisiertes Symbol in der Windows Benutzeroberfläche. Wenn Ihr Betriebssystem Windows NT Workstation 4.0 ist, erscheint **Sentinel** als ein Symbol neben der Uhr in der Task-Leiste.

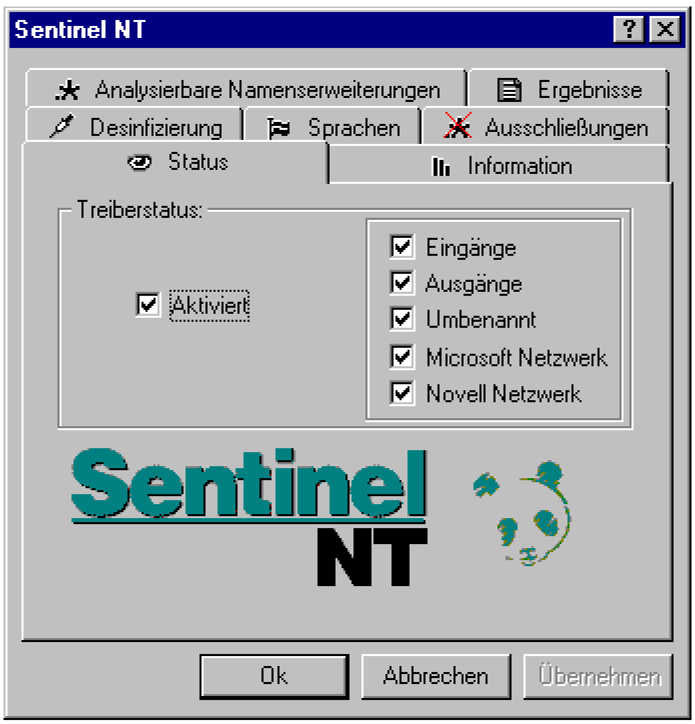
Der permanente Schutz funktioniert vollautomatisch. Wenn **Sentinel** bei irgendeiner Operation des Computers die Anwesenheit eines Virus entdeckt, gibt es eine Warnung darüber aus und führt die entsprechende Handlung aus.

Konfiguration des permanenten Schutzes

Der permanente Schutz kann an die Wünsche und Notwendigkeiten jedes Benutzers angepaßt werden. Wenn Sie auf das **Sentinel** Symbol doppelklicken, erscheint ein Fenster mit mehrere Registerkarten. In jeder dieser Registerkarten können Sie bestimmte Aspekte von Sentinel konfigurieren. Die zur Verfügung stehenden Konfigurationsoptionen sind folgende:

Status

In dieser Registerkarte wird der Zustand des permanenten Schutzes eingestellt.

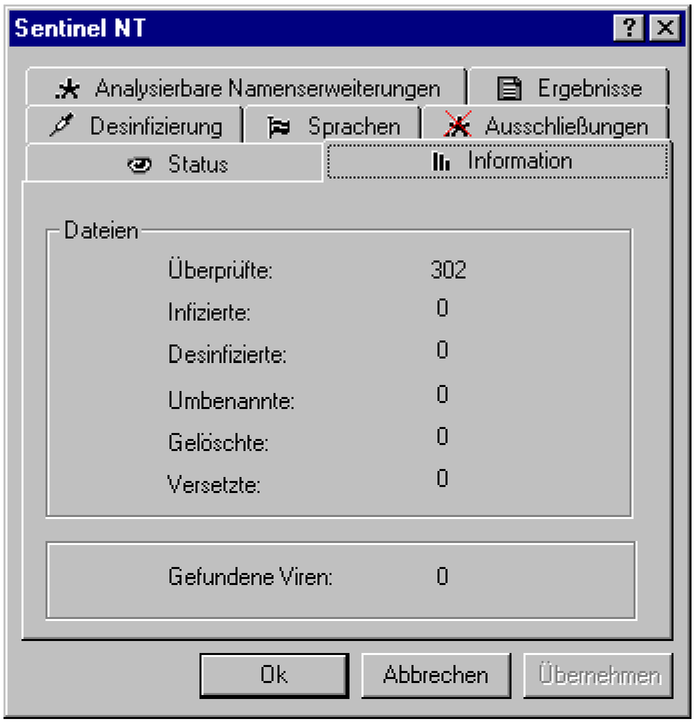


- **Aktiviert:** Mit dieser Option können Sie den permanenten Schutz aktivieren oder deaktivieren. Beachten Sie, daß bei der Deaktivierung des permanenten Schutzes der Computer nicht mehr gegen Viren geschützt ist.
- **Eingänge:** Wenn der permanente Schutz aktiviert ist, bestimmt diese Option, daß alle Dateien analysiert werden sollen, die in den Computer hineingebracht werden. Es werden auch Dateien analysiert, die neu erstellt oder verändert werden.
- **Ausgänge:** Wenn der permanente Schutz aktiviert ist, bestimmt diese Option, daß alle Dateien analysiert werden sollen, die aus dem Computer hinausgebracht werden. Es werden auch Dateien analysiert, die geöffnet oder ausgeführt werden
- **Umbenennung:** Wenn der permanente Schutz aktiviert ist, bestimmt diese Option, daß alle Dateien, die umbenannt werden, nach Viren analysiert werden sollen.
- **Microsoft Netzwerk:** Wenn der permanente Schutz aktiviert ist, bestimmt diese Option, daß alle Dateien in Operationen auf einem Microsoft Netzwerklaufwerk eines anderen Computers analysiert werden sollen.
- **Novell Netzwerk:** Wenn der permanente Schutz aktiviert ist, bestimmt diese Option, daß alle

Dateien in Operationen auf einem Novell Netzwerklaufwerk eines anderen Computers analysiert werden sollen.

Information

In dieser Registerkarte sehen Sie verschiedene Information über die Aktivität des permanenten Schutzes.



- **Überprüfte:** Gibt die Anzahl Dateien an, die der permanente Schutz auf der Suche nach Viren seit dem Systemstart überprüft hat.
- **Infizierte:** Zeigt die Anzahl gefundener, infizierter Dateien an.
- **Desinfizierte:** Zeigt die Anzahl Dateien an, die vom permanenten Schutz desinfiziert wurden.
- **Umbenannte:** Zeigt die Anzahl Dateien an, die vom permanenten Schutz umbenannt wurden.
- **Gelöschte:** Zeigt die Anzahl virenverseuchter Dateien an, die vom permanenten Schutz gelöscht wurden.
- **Versetzte:** Zeigt die Anzahl virenverseuchter Dateien an, die vom permanenten Schutz versetzt wurden.
- **Gefundene Viren:** Gibt an, wie viele Viren gefunden wurden.

Analysierbare Namenserweiterungen

Hier werden die Namenserweiterungen ausgewählt, die der permanente Schutz analysieren soll.

- **Liste der Namenserweiterungen:** In der Liste der Namenserweiterungen können all die Namenserweiterungen ausgewählt werden, die analysiert werden sollen. Der permanente Schutz greift immer bei allen Operationen mit Dateien ein, analysiert aber nur die Dateien, die eine der ausgewählten Namenserweiterungen haben. Unabhängig von der Auswahl der Namenserweiterungen, werden EXE und COM Dateien immer analysiert.
- **Erweiterungen in der Liste:** Gibt die Anzahl Namenserweiterungen in der Liste an.
- **Aktive Erweiterungen:** Gibt an, wie viele Namenserweiterungen für die Analyse ausgewählt wurden.
- **Erweiterung Hinzufügen:** Um der Liste eine Namenserweiterung hinzuzufügen, schreiben Sie die Namenserweiterung einfach in das Eingabefeld links der Schaltfläche, *Hinzufügen* und klicken Sie dann auf diese Schaltfläche.
- **Erweiterung Löschen:** Um eine Namenserweiterung von der Liste zu löschen, wählen Sie sie erst in der Liste der Namenserweiterung, und klicken Sie dann auf die Schaltfläche *Löschen*.
- **Alle Dateien:** Wenn Sie diese Option einschalten, werden alle Dateien, unabhängig von den ausgewählten Namenserweiterungen, analysiert.
- **Komprimierte Dateien Analysieren:** Wenn Sie diese Option einschalten, werden komprimierte Dateien, auf die zugegriffen wird, auch intern analysiert.

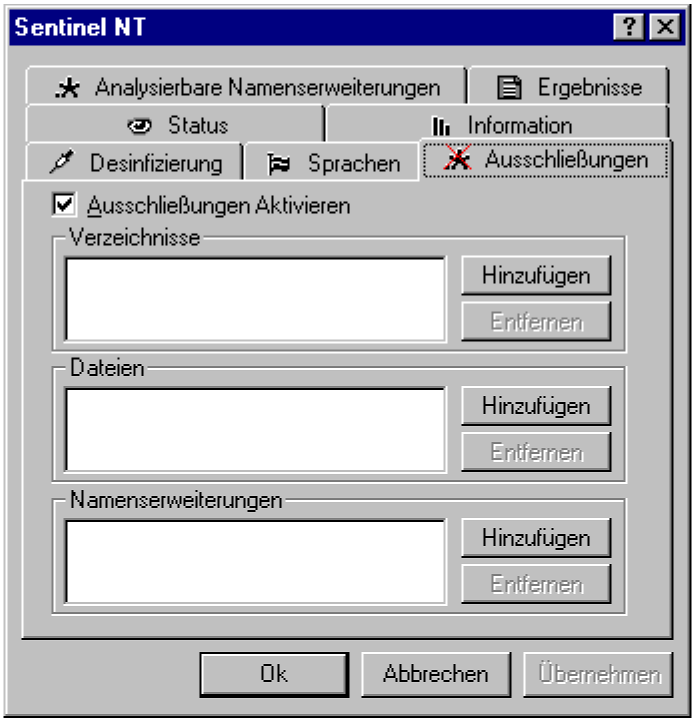
Sprachen

Diese Registerkarte zeigt Ihnen die Sprache an, die der permanente Schutz zur Zeit benutzt, und ermöglicht Ihnen auch die Auswahl einer anderen Sprache in der Liste der zur Verfügung stehenden Sprachen.

- **Zur Verfügung stehende Sprachen:** es wird eine Liste der verschiedenen, für den permanenten Schutz zur Verfügung stehenden Sprachen, angezeigt. Um die benutzte Sprache zu verändern, wählen Sie einfach die gewünschte Sprache in der Liste, und klicken Sie auf die Schaltfläche *OK* oder auf *Anwenden*.
- **Aktuelle Sprache:** Hier wird die Sprache anzeigt, die der permanente Schutz zur Zeit benutzt.

Ausnahmen

In dieser Registerkarte können Sie alle Bereiche, Dateien und Namenserweiterungen bestimmen, die nicht analysiert werden sollen. Unabhängig von den Einstellungen in der Registerkarte *Namenserweiterungen*, werden all die hier angegebenen Bereiche, Dateien und Namenserweiterungen **nicht analysiert werden**.



- **Ausnahmen Aktivieren:** Wenn Sie diese Option einschalten, werden die darunterliegenden Ausnahmen aktiviert.
- **Verzeichnisse:** Hier wird eine Liste aller Verzeichnisse anzeigt, die nicht analysiert werden sollen.
- **Verzeichnis Hinzufügen:** Hiermit können Sie der Liste der Verzeichnisse, die nicht analysiert werden sollen, Verzeichnisse hinzufügen.
- **Verzeichnis Löschen:** Hiermit können Sie von der Liste der Verzeichnisse, die nicht analysiert werden sollen, Verzeichnisse löschen.
- **Dateien:** Hier wird eine Liste aller Dateien anzeigt, die nicht analysiert werden sollen.
- **Datei Hinzufügen:** Hiermit können Sie der Liste der Dateien, die nicht analysiert werden sollen, Dateien hinzufügen.
- **Datei Löschen:** Hiermit können Sie von der Liste der Dateien, die nicht analysiert werden sollen, Dateien löschen.
- **Namenserweiterungen:** Hier wird eine Liste der Namenserweiterungen anzeigt, die nicht analysiert werden sollen. Selbst wenn die betreffende Namenserweiterungen sich schon in der Liste zu analysierender Namenserweiterungen befindet, wird sie nicht analysiert werden.
- **Namenserweiterung Hinzufügen:** Hiermit können Sie der Liste der Namenserweiterung, die nicht analysiert werden sollen, Namenserweiterungen hinzufügen.
- **Namenserweiterung Löschen:** Hiermit können Sie von der Liste der Namenserweiterung, die nicht analysiert werden sollen, Namenserweiterungen löschen.

Ergebnisse

In dieser Registerkarte stellen Sie die Berichte ein, die der permanente Schutz ausgeben soll, wenn Zwischenfälle auftreten.

- **Lokalen Bericht Erstellen:** Wenn Sie diese Option aktivieren, wird ein Bericht mit den verschiedenen Zwischenfällen erstellt, die vom permanenten Schutz gefunden werden.
- **Benutzer:** Hier wird der Name des Computerbenutzers angezeigt.
- **Bericht Ansehen:** Mit dieser Schaltfläche können Sie Sich den Bericht der bis jetzt aufgetretenen Zwischenfälle ansehen.
- **Bericht Drucken:** Mit dieser Schaltfläche können Sie den Ergebnisbericht ausdrucken.
- **Bericht Löschen:** Mit dieser Schaltfläche können Sie den Ergebnisbericht löschen.

Desinfizierung

In dieser Registerkarte wird das Verhalten des Programms eingestellt, wenn virenverseuchte Dateien vom permanenten Schutz entdeckt werden.

- **Annullieren:** Wenn Sie diese Option wählen, wird die Operation, bei der der Virus entdeckt wurde, abgebrochen. Wenn der Virus z.B. in einer Datei entdeckt wurde, die ausgeführt werden sollte, wird die Ausführung dieser Datei annulliert.
- **Ignorieren:** Wenn Sie diese Option wählen und ein Virus gefunden wird, wird dies trotzdem einfach ignoriert.
- **Desinfizieren:** Wenn Sie diese Option wählen, und der permanente Schutz einen Virus entdeckt, wird zu dessen Desinfizierung übergegangen, um die verseuchte Datei in denselben Zustand zurückzuversetzen, den sie vor der Infektion hatte.
- **Datei Umbenennen:** Wenn Sie diese Option wählen und ein Virus entdeckt wird, wird **Sentinel** die Datei auf die Namenserweiterung VIR umbenennen.
- **Datei Löschen:** Wenn Sie diese Option wählen und **Sentinel** einen Virus in einer Datei entdeckt, wird diese Datei gelöscht werden.
- **Wenn nicht desinfiziert werden kann, Datei umbenennen:** Wenn diese Option aktiviert ist und **Sentinel** einen Virus entdeckt, die Desinfizierung desselben versucht, diese aber nicht mit Erfolg ausführen kann, wird die Datei umbenannt werden.
- **Wenn nicht desinfiziert werden kann, Datei löschen:** Wenn diese Option aktiviert ist und **Sentinel** einen Virus entdeckt, die Desinfizierung desselben versucht, diese aber nicht mit Erfolg ausführen kann, wird die Datei gelöscht werden.

Was ist die vom Benutzer eingeleitete Analyse

Mit der vom Benutzer eingeleiteten Analyse können Sie jederzeit, wann immer Sie es möchten, jeglichen gewünschten Bereich Ihres Computer analysieren. Die auszuführende Analyse kann mit Hilfe einiger einfach einzustellender Optionen konfiguriert werden.

Wie man die vom Benutzer eingeleitete Analyse benutzt

Um eine vom Benutzer eingeleitete Analyse auszuführen, gehen Sie wie folgt vor:

1. **Ausführen des Antivirus:** Um den Antivirus auszuführen, gehen Sie zur Programmgruppe, in der die Symbole des Antivirus erstellt wurden. Doppelklicken Sie auf das Symbol *Panda Antivirus*.
2. **2. Gehen Sie zur Analyse:** Klicken Sie dazu auf die Schaltfläche *Analysieren* in der Schaltflächenleiste der Anwendung. Darauf erscheint ein Fenster, in dem Sie angeben, was und wie analysiert werden soll.
3. **Wählen Sie den zu analysierenden Bereich:** Sie wählen hier den Bereich des Computers, der analysiert werden soll. In einer Liste werden die verschiedenen Laufwerke des Systems angezeigt. Sie können auch ein konkretes Verzeichnis oder eine konkrete Datei mit den zugehörigen Schaltflächen auswählen.
4. **Konfigurieren Sie die Namenserweiterungen:** Dieser Schritt ist optional. Das Programm speichert immer die Konfiguration der zu analysierenden Namenserweiterungen ab. Daher brauchen Sie diese, nachdem Sie sie schon einmal konfiguriert haben, nicht bei jeder Analyse erneut zu konfigurieren
5. **Konfigurieren Sie die Analyseoptionen:** Dieser Schritt ist auch optional. Das Programm speichert immer die Konfiguration der Analyseoptionen ab. Daher brauchen Sie, nachdem Sie schon mal die Analyse konfiguriert haben, diese nicht jedesmal, bei jeder neuen Analyse, erneut zu konfigurieren. Sie brauchen diese Konfiguration nur zu ändern, wenn Sie andere Optionen für die Analyse benutzen möchten. In der Sektion über Konfiguration in dieser Hilfe finden Sie eine detailliertere Erklärung über die verschiedenen Konfigurationsoptionen, die für die Analyse zur Verfügung stehen.
6. **Angeben, ob nur das Boot analysiert werden soll:** Dieser Schritt ist optional. Wenn diese Option aktiviert ist, werden nur die Bootsysteme der ausgewählten Laufwerke, und nicht deren Dateien analysiert. Wenn diese Option nicht eingeschaltet ist, werden sowohl die Bootsysteme als auch alle Dateien auf den ausgewählten Laufwerken analysiert.

7. **Starten der Analyse:** Klicken Sie auf die Schaltfläche *Analysieren*, um die Analyse auf der Suche nach Viren in den ausgewählten Bereichen und mit den gewünschten Optionen zu starten.

Konfiguration der vom Benutzer eingeleiteten Analyse

Wie vorher erwähnt muß man bei einer Analyse folgendes angeben:

- Welcher Bereich analysiert werden soll.
- Welche Namenserweiterungen analysiert werden sollen.
- Wie die Analyse ausgeführt werden soll.

Die Konfiguration einer Analyse besteht aus der Angabe der Namenserweiterungen, die in Betracht gezogen werden sollen, und der Analyseoptionen.

Namenserweiterungen

Wenn Sie auf die Schaltfläche *Namenserweiterungen* klicken, erscheint ein Fenster, in dem Sie die Namenserweiterungen angeben, die Sie analysieren möchten.

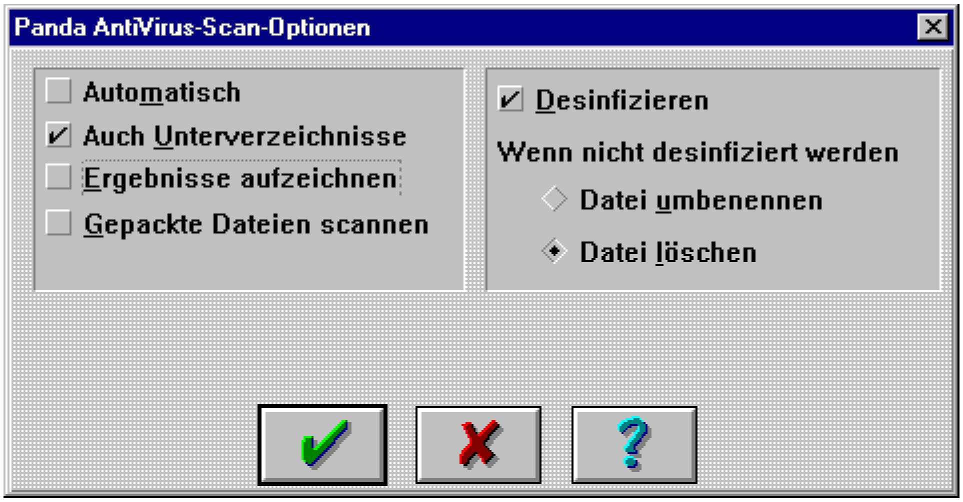
Die Option *Alle,* über der Liste der Namenserweiterungen, bestimmt, daß alle Dateien, unabhängig von deren Namenserweiterungen, analysiert werden sollen. Ist diese Option nicht aktiviert, so werden nur die Dateien analysiert, deren Namenserweiterung mit einer der in der Liste aktivierten Namenserweiterungen übereinstimmt.

Es gibt zwei Schaltflächen, mit denen Sie neue Namenserweiterungen der Liste hinzufügen und Namenserweiterungen von der Liste entfernen können. Es wird standardmäßig eine Liste der am häufigsten benutzen Namenserweiterungen geliefert, und es sind dort die Namenserweiterungen ausgewählt, die mit größter Wahrscheinlichkeit einen Virus enthalten könnten.

Unabhängig von den ausgewählten Namenserweiterungen, werden EXE und COM Dateien immer analysiert.

Analyseoptionen

Wenn Sie auf die Schaltfläche *Optionen* klicken erscheint ein Fenster, in dem Sie die möglichen Analyseoptionen, wie folgt, auswählen können:



- **Automatisch:** Wenn Sie diese Option aktivieren, wird der Analyseprozeß vollautomatisch ausgeführt. Wenn ein Virus gefunden wird, wird Sie der Prozeß darüber informieren. Die Analyse wird aber nicht unterbrochen werden. Dies ist vor allem dann nützlich, wenn Sie einen Computer desinfizieren möchten, der viele infizierte Dateien enthält.
- **Unterverzeichnisse:** Wenn Sie diese Option aktivieren, werden auch die Unterverzeichnisse der zu analysierenden Bereiche analysiert. Wenn diese Option nicht aktiviert ist, werden die Unterverzeichnisse nicht analysiert, d.h. wenn Sie z.B. ein Laufwerk zur Analyse auswählen, diese Option aber nicht aktivieren, wird nur das Grundverzeichnis des Laufwerks analysiert.
- **Ergebnisse speichern:** Wenn Sie diese Option aktivieren, werden die Daten dieser Analyse in der Ergebnisdatei gespeichert.
- **Komprimierte Analysieren:** Wenn Sie diese Option aktivieren, werden gefundene komprimierte Dateien intern analysiert.
- **Desinfizieren:** Wenn Sie diese Option aktivieren und ein Virus gefunden wird, wird der Antivirus versuchen, ihn zu desinfizieren.
- **Wenn nicht desinfiziert werden kann, Umbenennen:** Wenn Sie diese Option aktivieren und ein Virus gefunden wird, den der Antivirus **nicht desinfizieren** kann, wird die betreffende Datei **umbenannt** werden.
- **Wenn nicht desinfiziert werden kann, Löschen:** Wenn Sie diese Option aktivieren und ein Virus gefunden wird, den der Antivirus **nicht desinfizieren** kann, wird die betreffende Datei **gelöscht** werden.

Was ist die heuristische Analyse

Die heuristische Analyse ist eine zusätzliche Analysetechnik, die speziell zur Entdeckung unbekannter Viren dient.

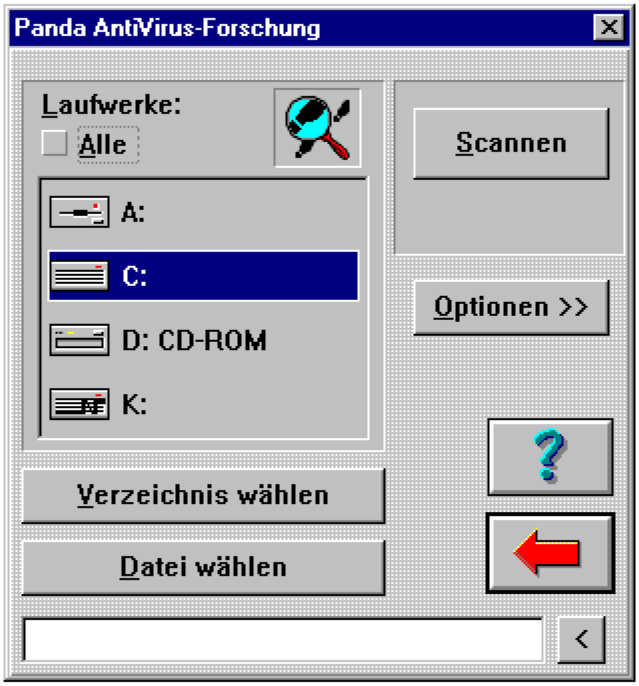
Genauso wie die vom Benutzer eingeleitete Analyse, wird die heuristische Analyse sofort, auf Befehl des Benutzers hin ausgeführt. Die Analysemethode, auf der die heuristische Analyse basiert, ist vollkommen verschieden von der Methode, die bei der vom Benutzer eingeleiteten Analyse benutzt wird. Dieser letzte basiert auf der Suche nach Viren, die dem Antivirus schon bekannt sind, während die heuristische Analyse aufgrund allgemeiner Eigenschaften, die den Viren gemeinsam sind, zu bestimmen versucht, ob ein Virus vorliegt.

Da die heuristische Analyse nur feststellen kann, daß bei einer bestimmten Datei der Verdacht besteht, daß Sie von einem Virus infiziert sein könnte, sie aber nicht über genügend Information über den angeblichen Virus verfügt, können von der heuristischen Methode gefundene, mutmaßliche Viren nicht desinfiziert werden.

Es ist wichtig zu beachten, daß die heuristische Analyse nur ein Zusatz zur vom Benutzer eingeleiteten Analyse ist.

Die Funktionsweise der heuristische Analyse ist ähnlich zu der vom Benutzer eingeleiteten Analyse.

Wie man die heuristische Analyse benutzt



Um eine heuristische Analyse auszuführen, gehen Sie wie folgt vor:

1. **Ausführen des Antivirus:** Um den Antivirus auszuführen, gehen Sie zur Programmgruppe, in der die Symbole des Antivirus erstellt wurden. Doppelklicken Sie auf das Symbol *Panda Antivirus*.
2. **Gehen Sie zur heuristische Analyse:** Klicken Sie dazu auf die Schaltfläche *Forschen* in der Schaltflächenleiste der Anwendung. Darauf erscheint ein Fenster, in dem Sie angeben, was und wie mit der heuristische Methode analysiert werden soll.
3. **Wählen Sie den zu analysierenden Bereich:** Sie wählen hier den Bereich des Computers, der analysiert werden soll. In einer Liste werden die verschiedenen Laufwerke des Systems angezeigt. Sie können auch ein konkretes Verzeichnis oder eine konkrete Datei mit den zugehörigen Schaltflächen auswählen.
4. **Konfigurieren Sie die Optionen der heuristische Analyse:** Dieser Schritt ist optional. Das Programm speichert die Konfigurationsoptionen der heuristischen Analyse immer ab. Daher brauchen Sie, nachdem die heuristische Analyse erst einmal konfiguriert ist, diese nicht jedesmal, bei jeder Benutzung der heuristischen Analyse, neu zu konfigurieren. Sie brauchen dies nur dann zu tun, wenn Sie die Optionen für die heuristische Analyse ändern möchten. In der Sektion über Konfiguration dieser Hilfe finden Sie eine detailliertere Erklärung über die verschiedenen Konfigurationsoptionen, die für die heuristische Analyse zur Verfügung stehen.
5. **Starten der Analyse:** Klicken Sie auf die Schaltfläche *Analysieren*, um die heuristische Analyse auf der Suche nach Viren in den ausgewählten Bereichen und mit den gewünschten Optionen zu starten.

Konfiguration der heuristischen Analyse

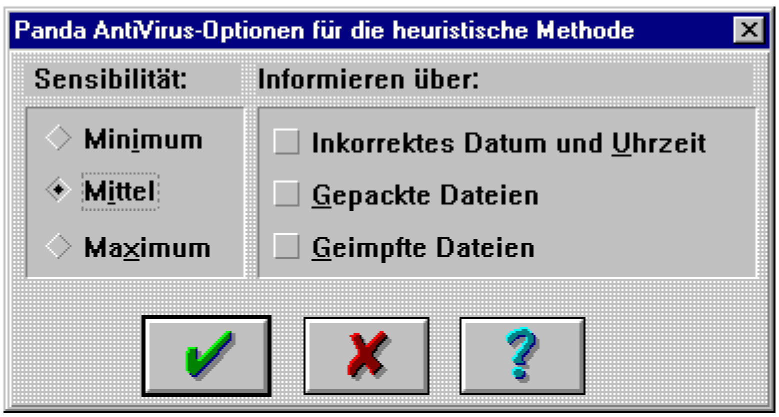
Wie vorher erwähnt muß man bei der heuristischen Analyse folgendes angeben:

- Welcher Bereich mit dieser Methode analysiert werden soll.
- Wie die angegebene Analyse ausgeführt werden soll.

Die Konfiguration einer heuristische Analyse besteht aus der Einstellung der Optionen für diese Art der Analyse.

Analyseoptionen

Wenn Sie auf die Schaltfläche *Optionen* klicken erscheint ein Fenster, in dem Sie die Optionen für die heuristische Analyse wie folgt einstellen können:



- **Minimale Empfindlichkeit:** Wenn Sie diese Option wählen, wird die heuristische Analyse die minimale Empfindlichkeit aufweisen, womit nur solche Dateien als möglicherweise virenverseucht angezeigt werden, bei denen ein sehr großer Verdacht besteht, daß sie einen Virus enthalten könnten.
- **Mittlere Empfindlichkeit:** Wenn Sie diese Option wählen, wird die heuristische Analyse eine mittlere Empfindlichkeit aufweisen, womit solche Dateien als möglicherweise virenverseucht angezeigt werden, bei denen ein großer Verdacht besteht, daß sie einen Virus enthalten könnten.
- **Maximale Empfindlichkeit:** Wenn Sie diese Option wählen, wird die heuristische Analyse die maximale Empfindlichkeit aufweisen, womit alle Dateien als möglicherweise virenverseucht angezeigt werden, bei denen eine Möglichkeit besteht, daß sie von Viren infiziert sein könnte. Selbst bei dieser Einstellung ist die Wahrscheinlichkeit minimal, daß eine Datei, die nicht virenverseucht ist, als verdächtig angezeigt würde.
- **Über inkorrektes Datum und Uhrzeit informieren:** Wenn Sie diese Option wählen, wird Sie das Programm jedesmal warnen, wenn eine Datei mit inkorrektem Datum oder Uhrzeit gefunden wird.
- **Über komprimierte Dateien informieren:** Wenn Sie diese Option wählen, wird Sie das Programm jedesmal warnen, wenn eine komprimierte Datei gefunden wird.
- **Über geimpfte Dateien informieren:** Wenn Sie diese Option wählen, wird Sie das Programm über alle **geimpften Dateien** warnen, die es findet.

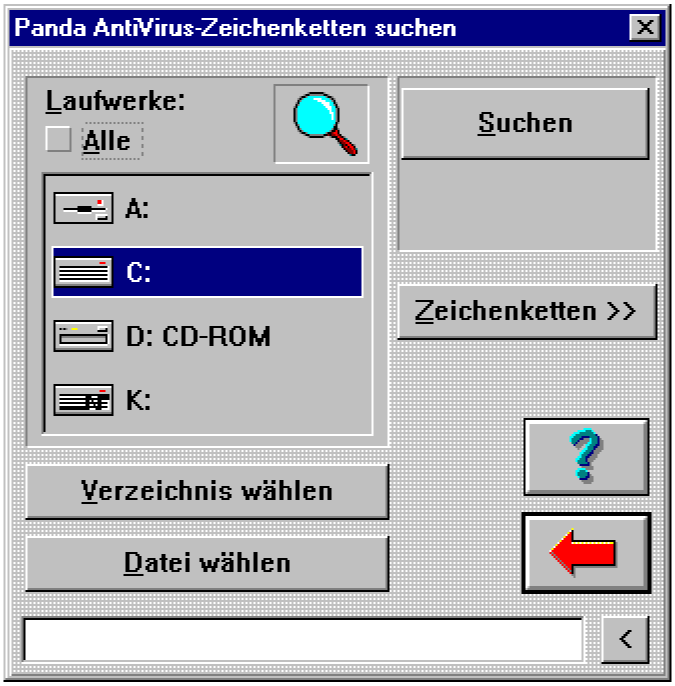
Was ist die Suche von Zeichenketten

Die vom Benutzer eingeleitete Analyse basiert auf der Suche in Dateien von Virusstücken, die dem Antivirus bekannt sind. Da täglich neue Viren erscheinen, veraltet diese Art der Analyse langsam mit der Zeit.

Die Suche von Zeichenketten benutzt dieselbe Methode wie die vom Benutzer eingeleitete Analyse, es kann hier aber eine Zeichenkette (ein Teil eines Virus) angegeben werden, nach der gesucht werden soll. Hiermit kann Ihnen der technische Kundendienst von **Panda Software** eine Zeichenkette angeben, die einem neuen Virus entspricht, damit der Antivirus danach sucht, obwohl die Information über diesen neuen Virus dem Programm noch nicht bekannt ist.

Genauso wie die vom Benutzer eingeleitete Analyse, wird die Suche nach Zeichenketten auch sofort auf Befehl des Benutzers ausgeführt.

Wie man die Suche von Zeichenketten benutzt



Um eine Suche nach Zeichenketten auszuführen, gehen Sie wie folgt vor:

1. **Ausführen des Antivirus:** Um den Antivirus auszuführen, gehen Sie zur Programmgruppe wo die Symbole des Antivirus erstellt wurden. Doppelklicken Sie auf das Symbol *Panda Antivirus*.
2. **Gehen Sie zur Suche von Zeichenketten:** Klicken Sie dazu auf die Schaltfläche *Suchen* in der Schaltflächenleiste der Anwendung. Darauf erscheint ein Fenster, in dem Sie angeben, was und wie mit der Suche von Zeichenketten analysiert werden soll.
3. **Wählen Sie den Bereich, in dem gesucht werden soll:** Sie wählen hier den Bereich des Computers, in dem Sie suchen möchten. In einer Liste werden die verschiedenen Laufwerke des Systems angezeigt. Sie können auch ein konkretes Verzeichnis oder eine konkrete Datei mit den zugehörigen Schaltflächen auswählen.
4. **Die zu suchenden Zeichenketten angeben:** Sie müssen die Zeichenketten eingeben, nach denen der Antivirus suchen soll, oder aber bereits eingegebene Zeichenketten aus einer Liste auswählen. Da das Programm die eingegebenen Zeichenketten immer speichert, brauchen Sie keine neue Zeichenketten anzugeben, wenn Sie keine neuen Zeichenketten hinzufügen möchten.
5. **Die Suche starten:** Klicken Sie auf die Schaltfläche *Suchen,* um die Suche nach den angegebenen Zeichenketten in den angegebenen Bereichen zu starten.

Konfiguration der Suche von Zeichenketten

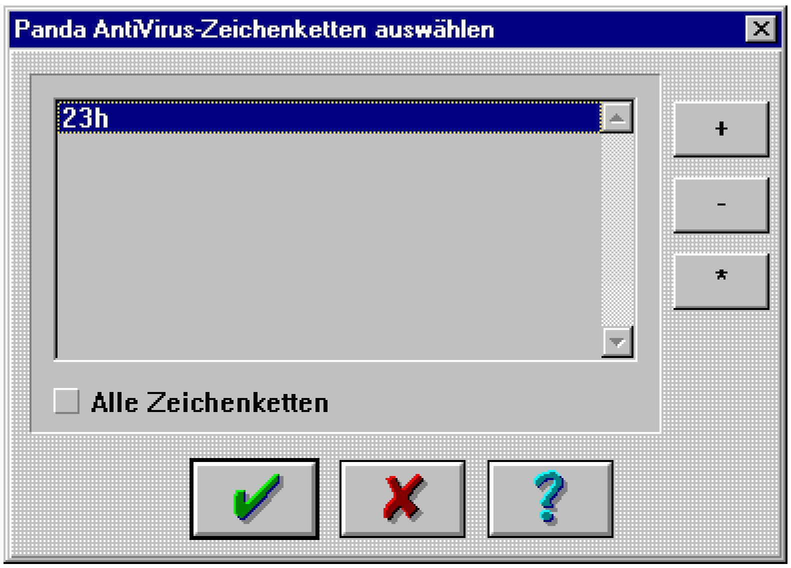
Wie schon erwähnt, müssen bei der Suche von Zeichenketten folgende Daten angegeben werden:

- Welcher Bereich mit dieser Methode analysiert werden soll.
- Nach welchen Zeichenketten gesucht werden soll.

Die Konfiguration einer Suche von Zeichenketten besteht aus den Zeichenketten, nach denen gesucht werden soll.

Zeichenketten

Wenn Sie auf die Schaltfläche *Zeichenketten* klicken, erscheint ein Fenster, in dem Sie die zu suchenden Zeichenketten auswählen können.



In diesem Fenster sehen Sie eine Liste eingegebener Zeichenketten. Mit den zugehörigen Schaltflächen können Sie dieser Liste eine Zeichenkette hinzufügen, eine der bereits eingegebenen Zeichenketten ändern oder eine Zeichenkette aus der Liste entfernen.

Es wird nicht nach allen Zeichenketten in der Liste gesucht, außer wenn die Option *Alle Zeichenketten* aktiviert ist. Wenn diese Option nicht aktiviert ist, wird nur nach den in der Liste ausgewählten Zeichenketten gesucht.

Wie man mit Panda Antivirus Computerviren desinfiziert

Es gibt in **Panda Antivirus** keine spezifische Menüauswahl zur Desinfizierung. Die Desinfizierung arbeitet immer mit der vom Benutzer ausgelösten Analyse oder mit dem permanenten Schutz zusammen. Wenn eine dieser zwei Analysearten einen Virus findet, versucht sie ihn zu desinfizieren (falls diese Option für beide Analysearten aktiviert wurde).

In der Konfiguration der Desinfizierung können Sie angeben, ob virenverseuchte Dateien, die nicht desinfiziert werden können, gelöscht oder umbenannt werden sollen.

Ein Virus kann im Boot einer Festplatte oder Diskette oder in einer Datei gefunden werden. In jedem dieser Fälle muß etwas anders vorgegangen werden. Siehe den zugehörigen Teil der Hilfe für eine detaillierte Vorgehensweise im konkreten Fall.

Desinfizierung eines Bootvirus

FAT Partition

Um einen Bootvirus vom Laufwerk C zu desinfizieren, gehen Sie wie folgt vor:

1. Schalten Sie Ihren Computer aus. Legen Sie eine virusfreie Startdiskette ein und starten Sie dann den Computer (wenn Sie vom CD-ROM desinfizieren möchten, müssen die Treiber für das CD-ROM geladen werden).
2. Nach dem Computerstart führen Sie den Befehlszeilen-Antivirus (PAVCL) folgendermaßen aus:

   - Wenn Sie **Pavcl** von einer Diskette aus ausführen möchten, legen Sie die Diskette 1 von **Panda Antivirus** für DOS/Windows 3.1x ein und schreiben Sie:

     ```
     PAVCL C: /CLV
     ```

   - Wenn Sie **Pavcl** vom Panda CD-ROM aus ausführen möchten, legen Sie es in das Laufwerk ein, gehen Sie zum Verzeichnis DOSWIN3X und dann in das Unterverzeichnis der gewünschten Sprache und schreiben Sie:

     ```
     PAVCL C: /CLV
     ```

   Wenn bei irgendeinem der zwei oben beschriebenen Vorgehensweisen eine Meldung ausgegeben wird, die besagt, daß das ausgewählt Laufwerk ungültig ist, geben Sie folgenden Befehl ein:

   ```
   PAVCL /HD0 /CLV
   ```

NTFS Partition

Um einen Bootvirus zu desinfizieren, wenn Sie eine NTFS Partition haben, ist es wichtig zu wissen, ob der Virus das Master-Boot, das Boot oder beide befallen hat. Falls der Virus nur das Master-Boot befallen hat, ist die oben beschriebene Prozedur für FAT Partitionen zu benutzen.

Wenn der Virus das Bootsystem befallen hat, muß, um den Virus zu löschen, das Bootsystem durch ein allgemeines Bootsystem ersetzt werden. Dazu können Sie irgendeines der Werkzeuge benutzen, die Ihnen Windows NT zu diesem Zweck zur Verfügung stellt.

Desinfizierung von Viren aus Dateien

Wenn ein Virus in Dateien gefunden wurde, säubern Sie Ihr System, indem Sie die Konfiguration des Antivirus wie folgt einstellen:

- Unter *Analyseoptionen* aktivieren Sie *Alle Namenserweiterungen*, *Desinfizieren* und A*utomatische Analyse*.
- Gehen Sie zur Analyse und wählen Sie die Option für das Analysieren des gesamten Systems (alle Laufwerke). Beim Ausführen der Analyse werden dann die infizierten Dateien gesäubert.

Desinfizierung mit dem permanenten Schutz

Sentinel kann von ihm gefundene Viren desinfizieren. Wenn **Sentinel** einen Virus entdeckt und die Desinfizierung per Konfiguration aktiviert ist, desinfiziert Sentinel den Virus, bevor die sich im Gang befindliche Operation ausgeführt wird. Nach der Desinfizierung fährt **Sentinel** mit der Operation fort, bei der ein Virus entdeckt wurde. **Sentinel** zeigt immer ein Fenster an, das über die Entdeckung des Virus warnt.

Befehlszeilen-Analyse

Panda Antivirus enthält das Programm **Pavcl**, das von der MS-DOS Befehlszeile aus ausgeführt wird. Der Panda Befehlszeilen-Antivirus entdeckt und desinfiziert dieselben Viren wie alle anderen Versionen von **Panda Antivirus**.

Pavcl ist ein schnelles Programm, das wenig Hauptspeicher benötigt. Um es zu benutzen müssen Sie aber die Parameter kennen, die Sie in der **Pavcl** Befehlszeile benutzen können. Pavcl finden Sie auf der Diskette 1 der DOS/Windows 3.1x Version von Panda Antivirus oder im Unterverzeichnis der betreffenden Sprache, unter dem Verzeichnis DOSWIN3X des CD-ROMs.

Parameter von Pavcl

Arbeiten

`/NOM` Den Hauptspeicher nicht analysieren.

`/NOB` Das Bootsystem nicht analysieren

`/NOF` Keine Dateien analysieren.

`/ALL` Alle Laufwerke des Systems analysieren.

`/INVx` Das Laufwerk "x" auf der Suche nach unbekannten Viren erforschen.
z.B. forscht man mit `/INVA` auf dem Laufwerk A:

`/CLV` Entdeckte Viren entfernen.

`/LIS` Eine Liste der in dieser Version erkannten Viren ausgeben.

`/HEU` Die heuristische Methode zur Entdeckung von Viren aktivieren.

`/CMP` Komprimierte Dateien analysieren.

`/CDR` Zeigt eine Liste der Ergebniscode (ERRORLEVEL) an, die Pavcl einstellen kann.

`/SAV` Die gewählten Parameter in einer Datei speichern. Beim späteren Ausführen des Programms werden dann diese Parameter den in der Arbeitssitzung angegebenen Parametern hinzugefügt.

`/IB+` Interne Impfung zum BOOT hinzufügen.
`/IB-` Interne Impfung vom BOOT entfernen.
`/IB*` Interne Impfung des BOOT überprüfen.

`/EB+` Externe Impfung zum BOOT hinzufügen.

`/EB-` Externe Impfung vom BOOT entfernen.
`/EB*` Externe Impfung des BOOT überprüfen.

`/IF+` Interne Impfung einer Datei hinzufügen.
`/IF-` Interne Impfung von einer Datei entfernen.
`/IF*` Interne Impfung einer Datei überprüfen.

`/EF+` Externe Impfung einer Datei hinzufügen.
`/EF-` Externe Impfung von einer Datei entfernen.
`/EF*` Externe Impfung einer Datei überprüfen.

`/B+` Interne und externe Impfung zum BOOT hinzufügen.
`/B-` Interne und externe Impfung vom BOOT entfernen.
`/B*` Interne und externe Impfung des BOOT überprüfen.

`/F+` Interne und externe Impfung einer Datei hinzufügen.
`/F-` Interne und externe Impfung von einer Datei entfernen.
`/F*` Interne und externe Impfung einer Datei überprüfen.

MODI:

`/NSB` Unterverzeichnisse nicht analysieren.

`/PTH` Die in der PATH Variable des DOS-Systems angegebenen Verzeichnisse analysieren.

`/ISO` Die Isolationsmethode aktivieren.

`/NOS` Akustische Meldungen abschalten.

`/AEX` Alle Dateien, unabhängig von ihren Namenserweiterungen analysieren.

`/AUT` Analyse ohne Benutzereingriff.

`/OVR` Vor dem Löschen überschreiben.

`/NOR` Keine Ergebnisdatei erstellen.

`/DEL` Infizierte Dateien löschen, selbst wenn sie desinfiziert werden könnten.

`/LOC` Alle lokalen Laufwerke analysieren.

`/NBR` Den Abbruch des Analyseprozesses nicht erlauben.

`/ITW` **Pavcl** analysiert nur auf der Suche nach *In The Wild* Viren. Dieser Parameter sollte nur unter speziellen Umständen benutzt werden.

Außerdem gibt es noch den DOS Standardumschalter "/?", der die Liste zur Verfügung stehender Umschalter ausgibt. Dies schließt auch die bei dieser **Pavcl**-Version zur Verfügung stehenden Sprachen ein.

Standardmäßig sind folgende Arbeiten aktiviert:

- Hauptspeicher analysieren.
- Boot analysieren.
- Dateien analysieren.

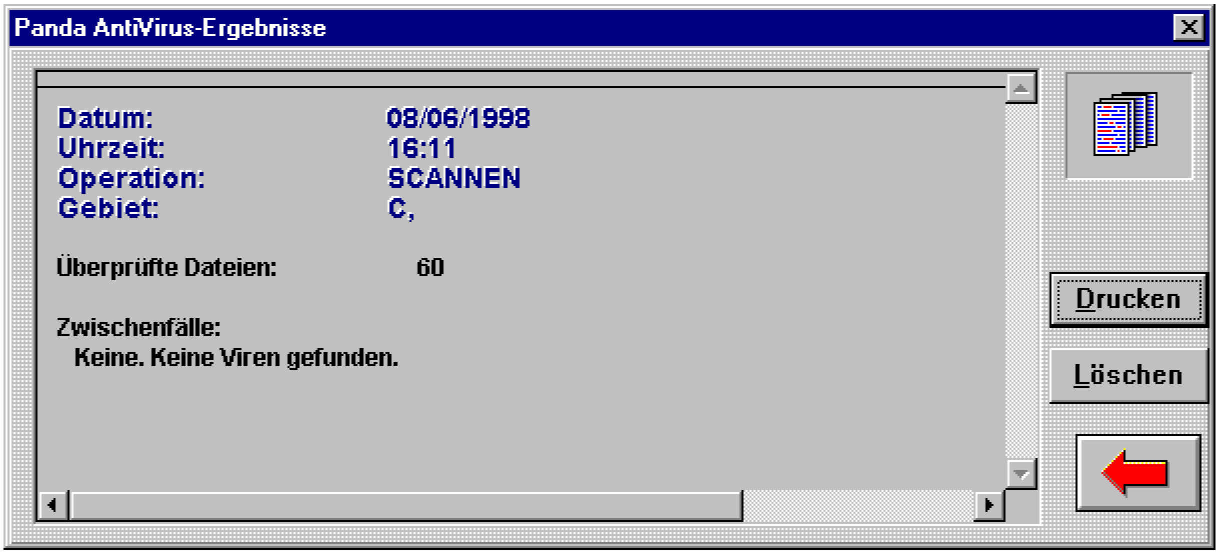
Standardmäßig sind folgende Modi aktiviert:

- Unterverzeichnisse analysieren.
- Nicht desinfizieren.
- Geräuscheffekte eingeschaltet.
- Nur ausführbare Namenserweiterungen analysieren.
- Eine Ergebnisdatei erstellen.

Die Arbeiten /?, /LIS, /INVx sind exklusiv, d.h. wenn diese angegeben werden, wird keine andere Arbeit ausgeführt. Nach dem Ende der angegebenen Arbeit kehrt das Programm zum DOS zurück. Der oder die zu analysierenden Pfade werden in der im DOS üblichen Art angegeben:

[Laufwerk:][Pfad][Dateiname]

Ergebnisbericht



Im Ergebnisbericht werden die verschiedene Operationen, die mit dem Antivirus ausgeführt werden, wies auch die möglicherweise aufgetretenen Zwischenfälle eingetragen.

Die im Ergebnisbericht enthaltene Information bleibt von einer Arbeitssitzung zur nächsten erhalten. Daher können damit jederzeit die Operationen, die mit dem Antivirus ausgeführt wurden, und deren Zwischenfälle eingesehen werden.

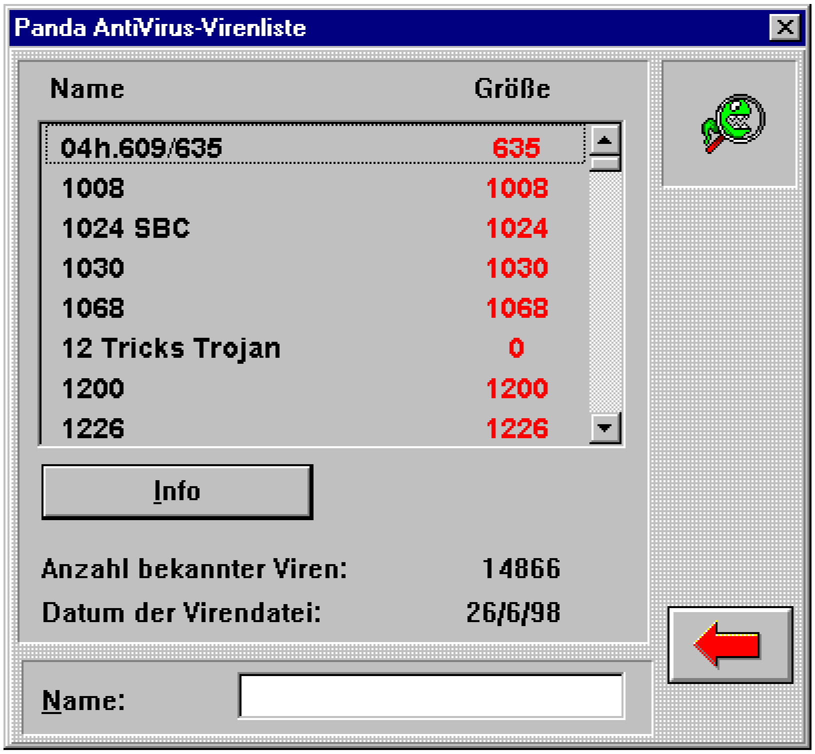
Für jede ausgeführte Operation, werden folgende Daten festgehalten:

- Datum und Uhrzeit.
- Art der Operation.
- Bereich auf dem die Operation ausgeführt wurde.
- Anzahl überprüfter Dateien.
- Alle mit Viren zusammenhängende Zwischenfälle, die aufgetreten sind.

Damit die Daten im Ergebnisbericht festgehalten werden, ist es notwendig die Option *Ergebnisse speichern* im Fenster der *Analyseoptionen* zu aktivieren.

Sie können den Inhalt des Ergebnisberichts auch ausdrucken, um Ihn leichter auswerten zu können. Sie können ihn auch jederzeit löschen, um zu verhindern, daß der Ergebnisbericht zu groß wird.

Virenliste



Die Virenliste ist die Liste der Viren, die **Panda Antivirus** zu entdecken imstande ist. In der Virenliste wird der Name und die Größe jedes einzelnen Virus angezeigt.

Neben der Liste wird auch die Gesamtzahl Viren angegeben, die von dieser Version von **Panda Antivirus** erkannt werden. Es wird auch das Datum der Virendatei angegeben, um so zu wissen, in wie weit das Antivirusprogramm aktualisiert ist oder nicht.

Im unteren Eingabefeld können Sie den Namen eines Virus eingeben, um diesen schneller in der Liste zu finden. Die Liste ist alphabetisch geordnet.

Nach der Auswahl des Virus können Sie auf die Schaltfläche *Info* klicken. Dann erscheint ein Fenster mit einer Reihe interessanter Daten über den Virus:

- Name.
- Ursprung.
- Größe.
- Alias.
- Wann er zum ersten Mal gefunden wurde.
- Ob man ihn desinfizieren kann oder nicht.
- Bereiche des Computers, die von dem Virus betroffen werden können.
- Verhaltens des Virus.

Danach erscheint eine Erklärung der verschiedenen Eigenschaften, die ein Virus aufweisen kann:

- **Speicherresident:** Wenn solch ein Virus ausgeführt wird, reserviert er einen kleinen Teil des Hauptspeichers für sich, installiert sich dort, und steckt von da aus an.
- **Stealth:** Dies ist eine Technik, die einige der speicherresidente Viren benutzen. Sie besteht darin, die Änderungen, die der Virus an Dateien bei deren Infektion ausführt, zu verstecken. Wenn sich jemand eine der Eigenschaften einer Datei ansieht, die der Virus verändert hat, und sich der Virus resident im Hauptspeicher befindet, so fängt der Virus diesen Auftrag auf und gibt die Daten zurück, die vor der Infektion vorlagen.
- **Verschlüsselt:** Diese Art von Viren können sich jedesmal, wenn Sie eine Datei infizieren, auf verschiedene Art und Weise verschlüsseln. Dadurch ist die Suche nach dem Virus mit einer Zeichenkettensuche erfolglos.
- **Überschreibt:** Diese Art von Viren, speicherresident oder nicht, überschreiben den Inhalt der Datei bei deren Infektion. Die Datei ist danach deshalb unbrauchbar. Die Größe der Datei wird in diesem Fall nicht verändert, außer wenn der Virus größer als die Datei ist. Die einzige Möglichkeit diese Art von Virus zu löschen ist es die infizierte Datei zu entfernen und Sie durch eine nicht infizierte Kopie derselben zu ersetzen.
- **Polymorph:** Polymorphe Viren sind fortgeschrittene Versionen verschlüsselter Viren. Polymorphe Viren können Ihre Verschlüsselungsmethode von Generation zu Generation verändern. So gibt es keinen Teil des Virus, der unverändert bleibt.

Allgemeine Funktionsweise

Panda Antivirus für Windows NT bietet Ihnen eine bequeme Benutzeroberfläche. Im Hauptfenster des Programms stehen die am häufigsten benutzten Optionen direkt in großen Schaltflächen zur Verfügung.

Klicken Sie auf diese Schaltflächen, um auf die verschiedenen Funktionen des Programms zuzugreifen. In dem entsprechenden Teil der Hilfe wird die betreffende Funktion im Detail erläutert.