ALWIL SOFTWARE

avast32

Komplettes Antivirus-Programm für
Windows 95
Windows NT

ALWIL Software, Lipí 1244,
193 00 Praha 9 - Horní Počernice, Tschechische Republik,
Tel. (+ 420 2) 819 216 61, 819 216 62

Inhaltsverzeichnis

1.Einleitung

Sehr geehrter Kunde, wir gratulieren Ihnen zum Kauf des AVAST32 Antivirus-Packets, das zu den besten in seiner Klasse gehört. Wir hoffen, daß Sie mit unserem Produkt zufrieden sein werden und eine angenehme Arbeit mit seiner Hilfe haben werden.

Das AVAST32-Programm ist ein System von Applikationen, deren Aufgabe darin besteht, den Rechner vor dem Virenbefall zu schützen. Bei einer richtigen und regelmäßigen Anwendung und in der Wechselvirkung mit anderen Programmen, z.B. für die die Datenaufbewahrung, können Sie das Risiko des Virenbefalls bei Ihrem Rechner in einem wesentlichen Maße reduzieren und den Datenverlust vermeiden.

Das Ziel dieser Dokumentation besteht darin, auch einen weniger erfahrenen Benutzer der Rechnertechnik mit der Beherrschung des AVAST32-Programms bekanntzumachen und ihm auf diese Art und Weise eine völlige Ausnutzung der Funktionen und Eigenschaften dieses Systems zu ermöglichen. Dabei werden auch die erfahrenen Personalrechnerbenutzer nicht vergessen, die in dieser Dokumentation auch eine Beschreibung der grundlegenden Prinzipien der Tätigkeit einzelner Applikationen oder eine Beschreibung der Wirkung der bei uns am meisten verbreiteten Computerviren finden können.

Diese Dokumentation wurde so erfaßt, daß der Leser schrittweise die Eigenschaften und vor allem die Funktionen des Programms in seiner Gesamtheit und seinen Einzelbestandteilen kennenlernt. Es wird die Kenntnis der Grundbegriffe a - fähigkeiten auf dem Gebiet der Operationssysteme Windows 95 oder Windows NT vorausgesetzt, weil ohne sie einige Passagen unverständlich bleiben könnten. Wenn Ihnen also Begriffe wie File (Mappe), Fenster, Datei nichts heißen oder wenn Sie nicht wissen, wie man ein Fenster aktivieren oder eine Taste betätigen soll, ist es empfehlenswert, das Handbuch oder die Hilfe des Operationssystems durchzulesen.

Sollten irgendwelche Probleme oder Unklarheiten über das Programm auftreten, wenden Sie Sich mit der Anfrage an Ihren Verkäufer oder an die Firma ALWIL Trade. Ihre Mitarbeiter werden Ihnen gern behilflich sein.

Eine angenehme und durch Viren nicht gestörte Arbeit mit Ihrem Computer wünschen Ihnen die Mitarbeiter der Firma ALWIL Software.

1.1 Kontakt an den Verkäufer

Sollten Lieferungsprobleme, wie z.B. Unvollständigkeit Ihrer Lieferung oder Unlesbarkeit des Installationsmediums, auftreten, bitten wir Sie, Sich an Ihren Lieferanten zu wenden. Sollten Sie hier ohne Erfolg bleiben oder sollten Sie den Lieferanten nicht kennen, wenden Sie Sich direkt an die Firma ALWIL Trade GmbH.

ALWIL Trade s.r.o. (GmbH)
Průběžná 76
100 00 Praha 10
Tschechische Republik
Tel.: +420 2 782 25 47 - 48
Fax : +420 2 781 05 48
http://www.alwil.com
http://www.vol.cz/ALWIL

Die Firma ALWIL kann auch mittels elektronischer Post und zwar unter den folgenden Adressen kontaktiert werden:

Handelsdirektor rtrnka@alwil.cz
Bestellungen und Bestellungsverarbeitung objednavky@alwil.cz
Verkauf von Programmen, AVS jberankova@alwil.cz
Fakturierung pourednikova@alwil.cz

1.2 Anforderungen an die Rechneraustattung

Damit das AVAST32-Programm in Ihrem Rechner erfogreich installiert werden und folglich fehlerfrei arbeiten kann, muß Ihr Rechnersysrem einige Grundanforderungen erfüllen.Hinsichtlich der heutigen Standarts sind diese Anforderungen wirklich minimal:

- Prozessor minimal 80386 oder voll kompatibel,
- MB installierter und genutzter RAM-Speicher für die Funktion unter dem Operationssystem Windows 95 und 16 MB für Windows NT,
- 10 MB freien Raum auf der Platte für das eigene Programm + 2 MB freien Speicherraumauf der Platte für die Installierung,
- laufendes Operationssystem Windows 95 oder Windows NT 3.51 oder ein neuereres,
- obwohl das ganze System durch die Tastatur gesteuert werden kann, empfehlen wir, zu seiner Steuerung die Maus oder eine andere Anzeigervorrichtung zu benutzen.

Generell gilt, daß je besser Ihre Rechneraus-stattung ist, desto schneller die Reaktionen einzelner Applikationen sein werden.

Der AVAST32-Programmablauf im Rechner mit weniger als 8 MB-Speicher wurde nicht geprüft! Die Reaktion des Operationssystems selbst ist bei

diesem Rechner so langsam, daß eine weitere Tätigkeit bei weiterer Belastung nicht mehr möglich ist. Es ist aber immerhin möglich, daß auch bei diesen Rechnern das AVAST32-Programm arbeiten wird. Dies wird aber nur dem wirklich geduldigen Nutzer empfohlen.

1.3 Installierung

Das AVAST32-Programm wird auf CD-ROM (bzw.auf einigen Disketten) in einem komprimierten Zustand geliefert und folglich kann nicht direkt angewendet werden. Für seine leichte Installierung wurde ein Installierungsprogramm entwickelt, das alle zum Betrieb des Systems notwendigen Funktionen durchführen wird.

Die Installierung des AVAST32 Programms besteht nicht nur im Kopieren der eigenen Programmdateien auf die Festplatte von Ihrem Computer. Die Installierung wird unter anderem alle notwendige Systemeinstellungen durchführen und sicherstellen, so daß nach dem nächsten Systemanlauf der residente Schutz ihres Systems automatisch anläuft (automatisch läuft die Aufgabe "Resident: voller Schutz" an, siehe Kapitel 2.6).

1.3.1 Vor der Installierung ...

Die Installierungsplatte CD-ROM sollte man mit größter Aufmerksamkeit betätigen und nach der Installierung auf einer sicheren Stelle aufbewahren. Wird das Instalierungsmedium beschädigt, wird es nicht möglich sein, das Programm zu installieren!

Wenn eine Diskettenversion vorhanden ist, wird als die erste Operation vor dem Installierungsbeginn das Kopieren der Originaldisketten empfohlen. Dazu wird die gleiche Anzahl von Disketten mit einer hohen Aufzeichnungsdichte empfohlen (diese Disketten werden mit den Buchstaben HD bezeichnet). Für das Kopieren des Diskenteninhaltes wird das Befehl DISKCOPY des Operationssystems empfohlen. Bei der weiteren Arbeit die neu gespeicherten Disketten anwenden und die Originaldisketten auf einer sicheren Stelle aufbewahren.

Vor dem Installierungsbeginn überzeugt man sich, daß man wirklich unter den Operationssystemen Windows 95 oder Microsoft Windows NT arbeitet. Im Falle, daß man unter keinem von diesen Systemen arbeitet (es wird zum Beispiel Microsoft Windows 3.x mit dem Ausbau Win 32s angewendet), wird man weder das AVAST32-Programm noch das Installierungsprogramm für seine Installierung benutzen können. Das wahrscheinlichste Ergebnis dieses Versuchs wird der "Rechnerzusammenbruch" sein. In diesem Fall sollte man versuchen das AVAST-Programm zu installieren!

Weiter sollte man sich überzeugen, daß keine vorausgehende Version des AVAST32-Programms installiert worden ist. Wenn dem so ist, sollte man versuchen, sie zu deinstallieren. Die Deinstallierungsbeschreibung findet man in ihrem Handbuch, bzw. in der Rechnerhilfe. Sollte man nicht so vorgehen, wird das Installierungsprogramm versuchen, die ältere Version selbst zu installieren. Dieses Vorgehen wird aber nicht empfohlen.

Um das AVAST32-Programm in die Umgebung des Operationssystems Windows NT installieren zu können, braucht man Administratorenrechte. Werden diese nicht vorhanden, wird das Installierungsprogramm darauf hinweisen und wird die Programminstallierung ablehnen! In diesem Fall wenden Sie Sich an den Administrator Ihres Netzes.

Wenn Sie die Hilfe des Programms AVAST32 ausnutzen wollen, müssen Sie vor seinem Anlauf auch das Programm **Acrobat Reader** installieren (wir empfehlen Ihnen diesen Schritt noch vor der eigentlichen Installierung des AVAST32 Programms vorzunehmen- im Gegenfall kann das Installierungsprogramm Sie auf die Abwesenheit von Acrobat Reader aufmerksam machen). Das Installierungssprogramm heißt "Ar32e30.EXE" und ist auf der gelieferten CD-ROM in der Mappe "Acrowin" zu finden. Die Installierung des Programms Acrobat Reader läuft in einer ähnlichen Umgebung wie die Installierung des Programms AVAST32 ab und ist automatisch, nach der Anfrage nach der Zielmappe.

Es ist nicht geeignet, wenn die Zielmappe, in die das Programm Acrobat Reader installiert wird, mit der Mappe des Programms AVAST32 gleich ist. Eine solche Installierung würde offensichtlich zu Konflikten zwischen den Programmen führen und auch ihre Deinstallierung würde nicht richtig arbeiten. Daher empfehlen wir, die Programme in die vorher eingestellte Mappen zu installieren. Das AVAST32 Programm findet das Programm Acrobat Reader, unabhängig von der Stelle der Installierung im Computer.

Solange alle angeführten Bedingungen erfüllt sind, kann die Produktinstallierung vorgenommen werden.

1.3.2 Installierungsanlauf

Nach dem Anlauf der Installierung des Programms AVAST32 dürfen Sie mehrere Wege ausnützen. Der einfachste Weg ist die Ausnutzung eines dazu entwickelten Mittels des Operationssystems. Allerdings müssen zunächst alle Disketten und CD-ROM aus den Laufwerken Ihres Computers entfernt und die Installierungs-CD-ROM des Programms AVAST32 (oder bei der Diskettenversion, die erste Installationsdiskette) eingelegt werden. Dann klopft man mit der linken Maustaste

auf die Taste "Start" in der Systemsteuerung und im erscheinenden Menü auf das Element “Systemsteuerung“ in der Mappe “Einstellung“ klopfen (Abb. 1).

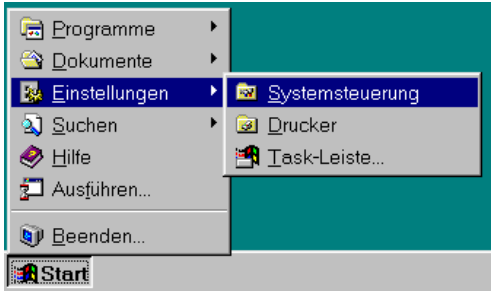

Abb. 1

Nach der Durchführung dieses Vorgangs erscheint ein Fenster, das einige Elemente enthält. Drücken Sie zweimal kurz nacheinander die linke Maustaste (dieser Vorgang nennen wir Doppelklicken oder Anklopfen) auf das Element "Software" (Abb. 2).

Abb. 2

Im Fenster, das sich auf dem Bildschirm öffnet, auf die Taste “Installieren” klopfen. Danach die Installierungs-CD-ROM (sollten Sie eine Diskettenversion haben, die erste Installierungsdiskette) in die Mechanik einlegen und auf der Taste "Weiter >" klopfen. Der Rechner wird automatisch das Installierungsprogramm finden und es bleibt nur, es anlaufen zu lassen - die Taste "Beenden" betätigen. Der eigene Installierungsprozeß wird im nächsten Kapitel beschrieben.

Erfahrene Benutzer können auch das Programm "**Setup.exe**" auf der Installierungs-CD-ROM oder auf der ersten Diskette (falls aus Disketten installiert wird) starten. Die Anlaufmethode wird detailliert im Handbuch oder in der Hilfe des Operationssystems beschrieben. Anderen Nutzern empfehlen wird die erste, oben angeführte Installierungsmethode, anzuwenden.

Alle Methoden des Installierungsanlaufs sind völlig identisch und auch ihr Ergebnis wird völlig identisch sein.

1.3.3 Wir installieren

Die Installierung des AVAST32-Programms erfolgt in der Form eines Dialogs zwischen dem Benutzer und dem Installierungsprogramm. In dem folgenden Text werden einzelne Fenster beschrieben, die im Verlauf der Installierung angezeigt werden.

Die Installierung kann jederzeit unterbrochen werden - bei den einzelnen Installierungsfenstern werden die Art und Weise der Durchführung beschrieben. Vor der eigentlichen Beendigung wird der Benutzer gefragt, ob er wirklich die Installierung beenden will. Bei der Bestätigung der Installierungsbeendigung wird alles bis dahin installierte beseitigt und der Rechner wird in den ursprünglichen Zustand gebracht.

Nach dem Anlauf des Installierungsprogramms werden Sie aufgefordert, die Sprache zu wählen, in der Sie mit dem Programm kommunizieren wollen (Abb. 3). Diese Wahl wird durch die Auswahl der entsprechenden Sprache aus einer Liste durchgeführt, die nach dem klopfen auf den Pfeil links von der aktuellen Sprache erscheint.

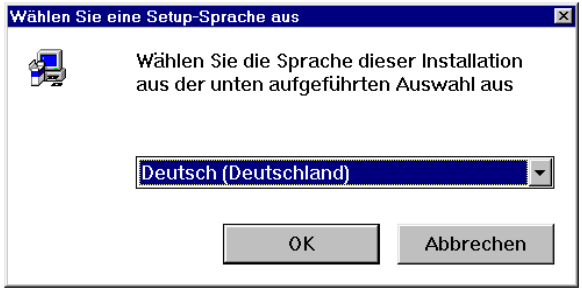

Abb. 3

Nach der Sprachenauswahl werden Sie um eine Weile Geduld aufgefordert werden, während das Programm auf der Installierungsvorbereitung arbeiten wird.

Nachdem die Installierungsvorbereitung beendet ist, wird der Bildschirm des eigenen Installierungs programms angezeigt (Abb. 4). In der Mitte ist ein sg.Begleiterfenster, das bei dem ganzen Installierungsprozeß zu Hilfe sein wird. In

seinem unteren Teil befinden sich drei Tasten, die der Befehlsmitteilung an den Begleiter dienen.

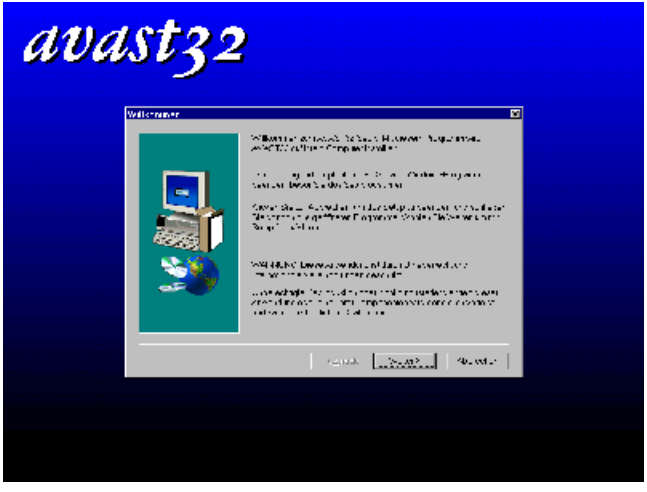

Abb. 4

Die Taste "< Zurück" dient der Rückkehr zu dem vorhergehenden Fenster des Fensterführers. Sollte es nicht möglich sein, diese Taste zu benutzen (z.B. wenn man bei dem Installierungsschritt ist, wie in der Abb. 4), ist ihre Farbe grau. Die Taste "Weiter >" dient im Gegenteil dem Übergang zum weiteren Begleiterschritt.Vor seiner Benutzung empfehlen wir, den Inhalt des Begleiterfensters gründlich durchzulesen. Durch die Betätigung der Taste "Abbrechen" kann der Installierungsprozeß jederzeit unterbrochen werden.

Das erste Fenster des Begleiters informiert den Benutzer über den Besitzer der Authorenrechte und warnt vor einer unberechtigten Manipullierung mit dem Programm oder mit seinen Bestandteilen. Nach dem Durchlesen durch das Klopfen auf der Taste "Weiter >" zum folgenden Fenster des Begleiters übergehen.

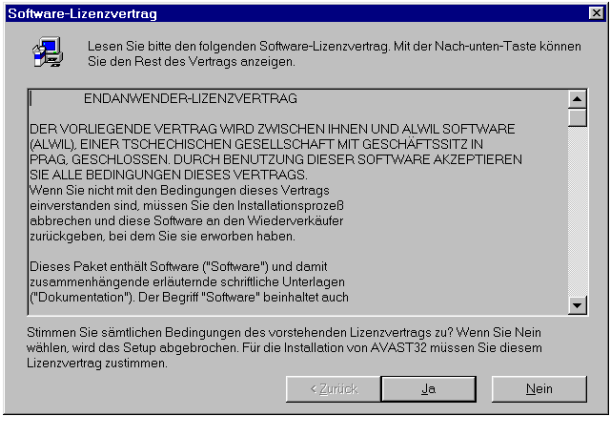

Abb. 5

Das folgende Programmfenster beinhaltet die Lizenzvereinbarung zwischen Ihnen und der Firma ALWIL Software (Abb. 5). Die Lizenz-

vereinbarung beinhaltet die durch Sie als den AVAST32-Benutzer einzuhaltenden Bedingungen und alle Rechte, die sie als Programmbenutzer haben. Wenn Sie mit der Lizenzvereinbarung und allen ihren Bestandteilen einverstanden sind, die Taste "Ja" betätigen. Der Begleiter läßt Sie dann zum weiteren Installierungsschritt übergehen. Sollten Sie mit der Lizenzvereinbarung nicht einverstanden sein, wird das Installierungsprogramm durch das Klopfen der "Nein"-Taste beendet. Das AVAST32-Programmpaket wird dann nicht installiert werden.

Weil der Umfang der Lizenzvereinbarung größer ist, als das Begleiterfenster, kann sie nicht in ihrer Gesamtgröße angezeigt werden.

Auf der rechten Seite des Fensters befindet sich eine Schiebeleiste, die eine Bewegung der Lizenzvereinbarung ermöglicht. Der Schiebeleistereiter bildet die Position ab, in der man sich befindet. Für die Abbildung der übrigen Lizenzvereinbarungbestandteile kann man auch die Tasten für die Kursorbewegung nach oben und nach unten benutzen, bzw. die mit "PgUp" und "PgDn" bezeichneten Tasten für den Übergang zu der vorhergehenden oder der nachfolgenden Seite der Lizenzvereinbarung benutzen.

Das dem Fenster der Lizenzvereinbarung folgende Fenster zeigt die Datei README.TXT an. Diese Datei beinhaltet wichtige Informationen, die nicht in dieser Dokumentation erfaßt worden sind. Diese Informationen können das eigene Programm betreffen, können aber auch Anleitungen über das Vorgehen im Fall von Problemen geben. Man sollte die README.TXT-Datei gründlich durchlesen - dadurch kann man mögliche Komplikationen vermeiden.

In dem angezeigten Text kann man sich in der gleichen Art und Weise bewegen,wie im Fall der Liezenzvereinbarung in dem vorhergehenden Begleiterfenster. Auch die Fensterbetätigung ist sehr ähnlich. Nachdem man die README.TXT-Datei durchgelesen hat, geht man durch das Klopfen der "Ja"-Taste zu dem folgenden Fenster des Begleiters über. Die Taste "< Zurück" bringt Sie zu dem vorhergehenden Fenster mit der Lizenzvereinbarung zurück und durch die "Nein"-Taste wird die Installierung des AVAST32-Programms beendet.

Abb. 6

Im folgenden Fenster (Abb. 6) werden Sie aufgefordert, Ihren Namen und den Namen Ihrer Firma einzugeben (bzw. Ihre Anschrift, sollte die Installierung für die Haushaltsbenutzung bestimmt werden). Der Begleiter wird versuchen, die notwendigen Informationen selber zu ermitteln, und so wird eine Mehrheit von Benutzern die voreingestellten Informationen bestätigen können. Sollten die Angaben der Wirklichkeit nicht entsprechen, wird es möglich, sie zu korrigieren. Wenn man mit der linken Maustaste in den Raum des Textfeldes mit der zu korrigierenden Angabe klopft, ermöglicht man die Aufbereitung. Auf der angegebenen Stelle wird der Kursor angezeigt und durch die Tastatur wird dann die eigene Änderung vorgenommen.

Wenn die angeführten Angaben der Wirklichkeit entsprechen, werden durch das Klopfen auf die Taste "Weiter >" bestätigt und man geht zu dem folgenden Fenster des Fensterführers über. Die Taste "< Zurück" dient der Rückkehr zum Fenster mit der README.TXT-Datei und durch die Taste "Abbrechen" kann die Installierung unterbrochen werden.

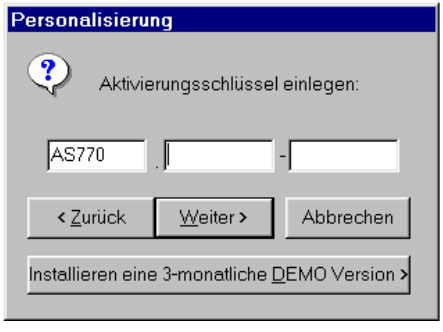

Abb. 7

In der Abb. 7 wird das Fenster des Fensterführers dargestellt, in das die Seriennummer Ihrer Programmkopie eingetragen werden muß. Die Aktivierungsschlüßel hat folgende Form: AABBB.CDDDDDDEEEEEE. Der erste Teil der Aktivierungsschlüßel (AABBB) wird duch den Be-

gleiter voreingestellt, es bleibt also, die restlichen zwei einzutragen. Der Teil CDDDDDD wird in die Mitte des Textfeldes und der Teil EEEEEE in das restliche Textfeld eingetragen.Durch das Klopfen der linken Maustaste auf das entsprechende Feld wird ermöglicht, Angaben in die einzelnen Textfelder einzutragen oder zu ändern. Ein Übergang zu dem gegebenen Textfeld kann auch durch das wiederholte Drücken der "Tab"-Taste erreicht werden.

Nach der Eintragung des Aktivierungsschlüssels sollte er sicherheitshalber noch einmal überprüft werden. Ohne seine richtige Eintragung wird das Programm nicht richtig installiert! Sollen Sie den Aktivierungsschlüssel nicht kennen, so können Sie eine dreimonatliche Demoversion des Programms installieren - auf die Taste “Installieren eine 3-montliche DEMO Version >" klopfen.

Durch die Taste "Weiter >" wird der eingetragene Aktivierungsschlüssel bestätigt und wenn er richtig eingegeben wurde, werden Sie durch den Assistent zum nächsten Fenster durchgelassen. Im Gegenfall erhalten Sie eine Fehlermeldung und der Aktivierungsschlüssel wird korrigiert werden müssen. Durch Betätigung der Taste "< Zurück" kehren Sie ins Fenster mit dem Namen des Benutzers und der Firma zurück. Die Betätigung der Taste "Abbrechen" beendet das Installierungsprogramm.

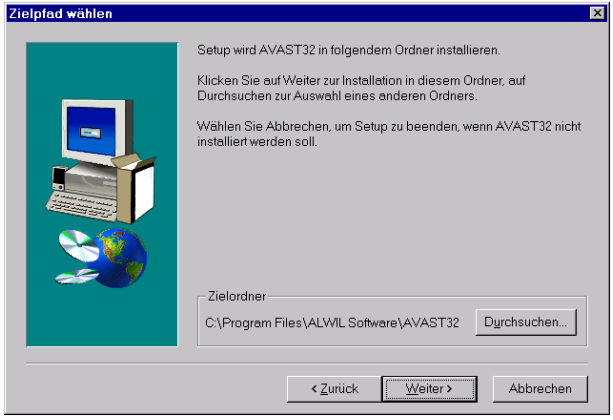

Abb. 8

Ist der eingegebene Aktivierungsschlüssel richtig, erscheint ein Fenster, in dem der Assistent die Aufforderung zur Festlegung der Zielmappe presäntiert, in die AVAST32 installiert werden soll (Abb. 8). Diese Mappe ist im Rahmen des "Zielordner" gegeben. Die Standardmappe ist die Mappe "ALWIL Software\AVAST32", die auf Ihrer Systemplatte in der Mappe "Programm Files" generiert wird. Für die meisten Benutzern wird diese Standardmappe ausreichen, die anderen können die Taste "Durchsuchen..." betätigen und mit der

Hilfe vom Dialog (in der Abb. 9), die Zielmappe auswählen. Den weniger erfahrenen Benutzern empfehlen wir die Standardmappe zu benutzen; dadurch kann möglichen Problemen ausgewichen werden.

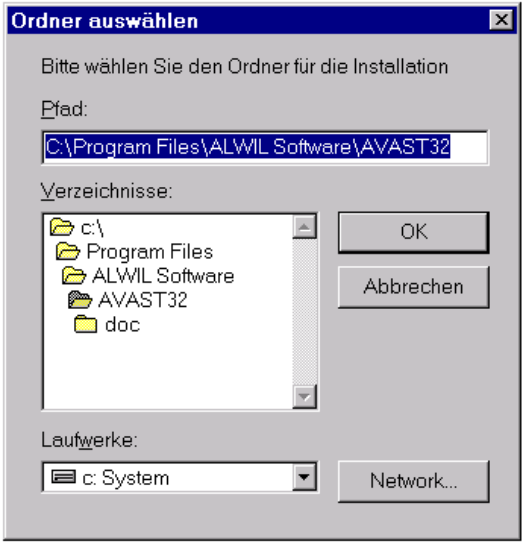

Abb. 9

Das Fenster in der Abb. 10 folgt nach dem Fenster mit der Auswahl der Zielmappe für die Programminstallierung. In seinem oberen Teil ist eine Liste von Elementen, die mit dem eigentlichen Programm AVAST32 installiert werden können. Auf diese Weise kann z.B. die Unterstützung der englischen Sprache ausgewählt werden. Bei der Arbeit mit dem Programm kann dann jeder Benutzer wählen, welche Sprache er benutzen will.

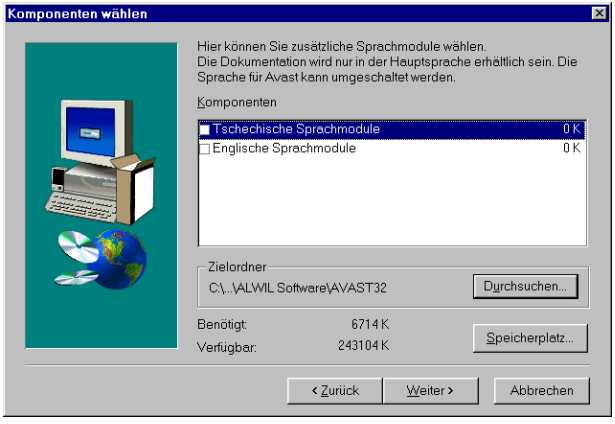

Abb. 10

Das Fenster ermöglicht auch, das Zielverzeichnis für die Installierung des Programms AVAST32 zu verändern und zwar nach dem Klopfen auf die Taste "Durchsuchen..." (Abb. 9). Der Benutzer kann auch die Informationen über die freie Kapazität auf einzelnen Festplatten des Computers abbilden lassen. Durch die Betätigung der Taste "Wei-

ter >" bestätigen Sie die ausgewählten Komponenten und die Zielmappe.

Das folgende Fenster stellt alle Informationen dar, die man dem Begleiter angegeben hat. Es beinhaltet also den Benutzernamen, die Benutzerfirma oder die Benutzeranschrift, die Seriennummer der Programmkopie und die Zielmappe, in die das AVAST32-Programm installiert werden soll. Wir bitten Sie, die angegebenen Daten zu prüfen und sollten sie Ihnen oder der Wirklichkeit nicht entsprechend sein, kann man durch das Klopfen auf der Taste "< Zurück" zu den vorhergehenden Fenstern des Fensterführers zurückkehren und die entsprechenden Daten korrigieren. Sollte alles vorstellungsmäßig sein, kann man durch das Klopfen auf der Taste "Weiter >" zu der eigenen Installierung der Dateien des AVAST32-Programms auf Ihre Festplatte übergehen. Die Taste "Abbrechen" kann die Installierung unterbrechen.

Über die Anzahl der kopierten Dateien informiert der Indikator auf dem Bildschirm des Installierungsprogramms. Die Installierung der Dateien kann durch Klopfen auf die Taste im rechten unteren Bereich des Bildschirms oder durch die Betätigung der Taste "F3" unterbrochen werden. Sobald alle Dateien installiert werden, geht der Assistent automatisch zum nächsten Fenster über.

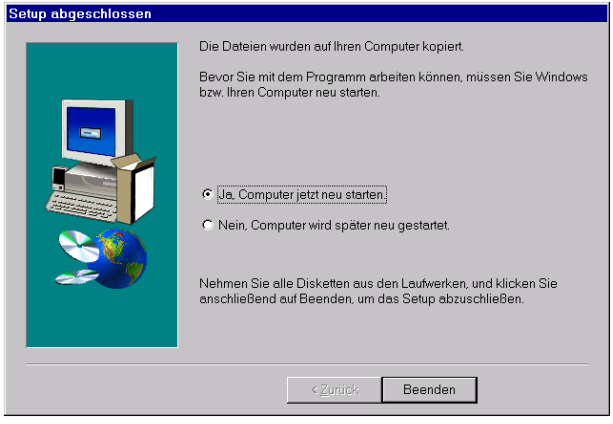

Abb. 11

Das letzte Fenster des Begleiters wird in der Abb. 11 dargestellt. Es beinhaltet Umschaltetasten, mit deren Hilfe man bestimmen kann, ob der Rechner wieder angelaufen werden soll oder ob das Installierungsprogramm ohne den Rechneranlauf beendet werden soll. Das Klopfen auf der Taste "Beenden" beendet das Installierungsprogramm und in der Abhängigkeit von der Wahl der Umschaltetaste wird auch Ihr Rechner wieder gestartet werden.

Nach der Installierung des AVAST32-Programms und vor seinem ersten Anlauf muß der Rechner wiedergestartet werden. Wenn man es nicht mit der Hilfe des Begleiters im seinem letzten Fenster ge-

tan hat, wird man es später selber machen müssen. Im Angebot der "Start" - Taste die Stelle "Beenden..." wählen. In dem abgebidleten Fenster dann die Stelle "Rechner restarten" anhaken und durch die "Ja" - Taste den Rechner neu starten.

1.3.4 Installierungsprobleme

Die bekanntesten Installierungsprobleme des AVAST32-Programms werden im folgenden beschrieben:

- man kann wegen einem Aktivierungsschlüßelfehler nicht installieren. Der Aktivierungsschlüßel wurde falsch eingetragen. Die Aktivierungsschlüßel hat folgendes Format:
  AABBB.CDDDDDD-EEEEEE (seine Bedeutung ist in der Anlage D erklärt). Man soll sich vergewissern, ob diese Nummer wirklich richtig eingetragen wurde. Wenn man sich hundertprozentig sicher ist, daß ja, auch daß der Buchstabe "O" nicht als Null niedergeschrieben wurde und daß man in ein Textfeld keinen Trennungspunkt oder -strich eingetragen hat, ist es die höchste Zeit, mit der Firma **ALWIL Trade GmbH** in Konstakt zu kommen und eine Prüfung der Aktivierungsschlüßel von ihr zu verlangen.
- Das AVAST32-Programm kann man nicht installieren, weil auf ihrer Festplatte nicht genügend Platz ist. In diesem Fall gibt es nur einen Rat - das Installierungsprogramm zu beenden, genügend Raum auf Ihrer Festplatte freizulegen, d.h den Korb auszukippen, nicht benutzte Programme , alte Dokumente u.ä. zu löschen (es wird empfohlen, die zu löschenden Dateien zuerst auf eine Diskette zu übertragen und erst dann auszulöschen). Für eine erfolgreiche Installierung des AVAST32-Programmes wird man etwa 10 + 2 MB freien Raum auf der Festplatte, auf die das Programm installiert wird, benötigen. Danach wird das Installierungsprogramm wieder angelaufen und der Installierungsprozeß wird wederholt.
- das Programm kann wegen mangelhaften Rechten nicht installiert werden (nur in Windows NT). Unter dem Operationssystem Windows NT muß man für die Installierung von AVAST32 Programm die Administratorrechte haben. Es folgt also eine Abmeldung und dann die Anmeldung als Administrator oder man nimmt Kontakt mit dem Netzesadministrator an.

Sollte es zu einem anderen Installierungsfehler kommen, muß man feststellen, ob es sich hier um Ihren Fehler oder um einen Fehler des Systems handelt. Nachdem Sie alle Probleme Ihrerseits völlig ausgeschlossen haben, treten Sie in Kontakt mit unserer technischen Unterstützung. Sie sollten aber alle Fehlermeldungen wortwörtlich notiert haben.

1.3.5 Installierung von anderen Medien

Das AVAST32-Programm kann auch von einem anderen Medium als CD-ROM und Disketten installiert werden. Dieses Verfahren kann man für die Beschleunigung der Installierung (sogar um einige Größendordnungen, je nach dem benutzten Medientyp) oder für den Fall der Installierung in Netzstationen benutzen. In diesem Fall muß man die Mappen DISK1, DISK2 usw. von der Installierungsplatte CD-ROM in das Medium kopieren, von dem dann die Installierung abgewikkelt wird (bei der Diskettennutzung müssen die Mappen zuerst gebildet werden, dann müssen die Distributionsdisketten oder ihre Kopien in sie kopiert werden, wobei die erste Installierungsdiskette in die Mappe DISK1 kopiert wird, usw.) und die Installierung von diesem Medium in der im Kapitel 1.3.2 angeführten Weise starten.

1.3.6 Administratorische Installierung

Das Installierungsprogramm für das AVAST32-Programm unterstützt in einem begrenzten Maße die sg. "administratorische Installierung", deren Inhalt in der Vorbereitung einer eigenen Kundeninstallierung in die gemeinsam genutzte Mappe des Servers besteht. Die eigene Kundeninstallierung kann dann ohne Benutzereingriffe ganz automatisch erfolgen. Diese Weise der Installierung kann durch Administratoren einer größeren Rechneranzahl vorteilhaft angewendet werden.

Die administratorische Installierung wird folgenderweise erstellt. Der Administrator erstellt Kopien der Installierungsdisketten in die Mappen DISK1 ... DISKn in den Mappenserver, ähnlicherweise wie bei der Installierung von anderen Medien. Dann werden Werte der Datei ADMIN.NI in der neuerstellten Mappe DISK1 modifizeirt und auf sie wird die Datei AVAST32.CNF mit den vorher vorbereiteten Aufgaben kopiert. Es muß klar verstanden sein, da es nicht günstig ist, einen absoluten Weg zu den Dateien (z.B. Klangdateien) anzuwenden.

Wenn Sie mehr über die administratorische Arbeit wissen möchten, in der ersten Installierungsdiskette finden Sie die Datei **ADMIN.TXT**, die nähere Informationen zu diesem Installierungstyp beinhaltet.

1.4 Programmdeinstallierung

Das AVAST32-Programm kann jederzeit vom System deinstalliert werden. Diese Operation beseitigt unwiderruflich (mit der Ausnahme der wiederholten Installierung) das AVAST32-Programm von der Festplatte des Rechners und bringt das System in den ursprünglichen Zustand zurück. Die Deinstallierung löst auch solche Probleme wie die Deinstallierung von gemeinsam geführten Biblio-

theken und die Erneuerung der internen Informationen in den Registern des Operationssystems.

In den folgenden Kapiteln werden die einzelen Schritte der Deinstallierung beschrieben.

1.4.1 Deinstallierungsvorbereitung

Vor der Deinstallierung des AVAST32-Programms sollte man sich überzeugen, daß kein von den Programmen läuft. Gegenteilfalls wird die Deinstallierung nicht ordungsgemäß erfolgen und Reste des AVAST32-Programmes können auf der Festplatte verbleiben, bzw. kann das Starten der Deinstallierung abgelehnt werden. Die Erneuerung der internen Systemdaten kann dann nicht vollständig erfolgen. Das kann (und meistens auch ist) eine Ursache von **ERNSTEN** Problemen bei der Installierung weiterer Versionen des Antivirenprogramms AVAST 32 sein.

Schauen Sie auf das Hauptkonsole auf der unteren Bildschirmkante. Wenn Sie hier ein von den Programmen das AVAST32-Systems sehen, beenden Sie es. Die rechte Maustaste betätigen und das Befehl "**Ende**" für die eingeschalteten Programme des AVAST32-Programmes wählen.

1.4.2 Anlauf der Deinstallierung

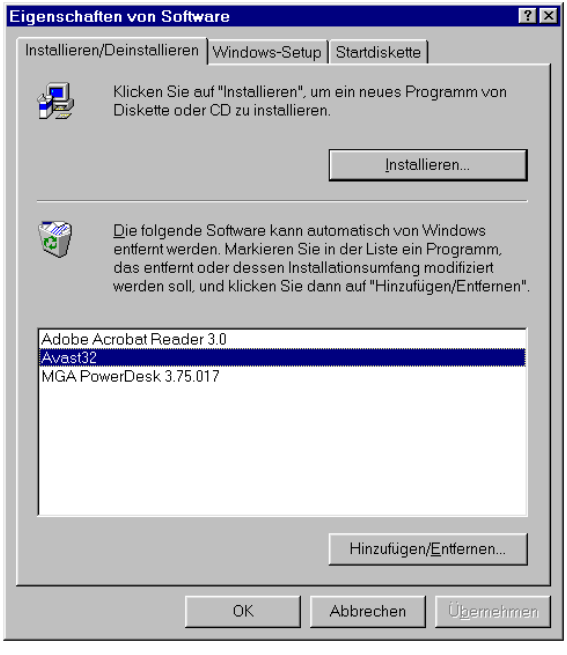

Abb. 12

Bei dem Anlauf der Deinstallierung empfiehlt sich, grundsätzlich ein standartes in das Operationssystem implementiertes Mittel anzuwenden. Man findet es in der Mappe "**Systems-**

teuerung" unter der Bezeichnung "**Software**" (das Finden und Starten dieses Mittels wurde im Kapitel 1.3.2 beschrieben).

Im Fenster dieses Mittels befindet sich in unterem Teil eine Liste der installierten Programme (Abb. 12), die eine automatische Deinstallierung unterstützen (das AVAST32-Programm gehört zu ihnen). Will man ein Programm, hier das AVAST32-Program, deinstallieren, klopft man mit der linken Maustaste auf den Namen des entsprechenden Programms. Auf diese Weise wird die Deinstallierung des AVAST32-Programms gestartet.

1.4.3 Verlauf der Deinstallierung

Der eigene Deinstallierungsverlauf ist voll automatisch, außer der ersten Anfrage, ob die Deinstallierung wirklich vorgenommen werden soll. Beantwortet man "**Ja**", wird das AVAST32-Programm deinstalliert und das System wird in seinen ursprüngichen Zustand gebracht. Sollte das Deinstallierungsprogramm nicht in der Lage sein, alle AVAST32-Bestandteile zu deinstallieren, wird diese Tatsache kurz vor dem Abschluß mitgeteilt. Diese Situation entsteht ziemlich oft, weil das AVAST32-Programm bei seiner Arbeit neue Dateien erstellt und Informationen über Systemvariablen für sich registriert (sg. "**registr**").

1.5 Originalsoftware benutzen

Soll der Virenschutz wirksam sein, muß man einige Regeln einhalten. Außer der regelmäßigen Anwendung des Antivirenprogramms ist ein der Programme für die Reservenkopienbildung anzuwenden, um mindestens die Kopien der wichtigsten Daten aufzubewahren. Daten kann man nämlich auch ohne einen Virenbefall verlieren.

Eine weitere wichtige Gewohnheit ist die auschließliche Anwendung von Originalsoftware, wo ein minimales Risiko des Virennbefalls besteht. Schwarz besorgtes Software konnte auf seinem Weg vom Produzenten mehrere Viren aufnehmen und die Mittel für die Virenbeseitigung können dann mehrmals den Preis der Originalsoftware überschreiten. Darüberhinaus übeschreitet man durch die Nutzung solcher Programme das Gesetz und es besteht die Möglichkeit der Strafverfolgung.

Ein Virenparadies sind auch die verschiedenen öffentlichen Archive vom Shareware und Freeware, wo man nie wissen kann, wer mit ihnen manipuliert hat. Sollte man sich zur Anwendung eines solchen Programms entscheiden, sollte es durch ein Antivirenprogramm geprüft werden.

1.5.1 Wie erkennt man das Originalsoftware

Eine allgemeine Anleitung zur Unterscheidung der Originalsoftware von Schwarzkopien gibt es nicht, wir können nur einige Ratschläge liefern. Man sollte das Software nur bei glaubwürdigen Verkaufsleuten kaufen und man sollte sich immer diesen Kauf bestätigen lassen. Ein Bestandteil der Verpackung sollte auch eine Bestätigung des Softwareursprungs sein, wie z.B. ein Lizenzvertrag oder -vereinbarung, Echtheitszertifikat u.ä.

Sollte man anstelle der Dokumentation z.B. nur einige durch einen Nadeldrucker gefertigte A5-Blätter erhalten, ist es mindestens verdächtig. Ähnlich gilt es auch für die Installierungsdiskettenschilder oder auch für den CD-ROM-Druck.

Das AVAST32-Programm wird auf einer **silbernen** CD-ROM geliefert, auf der das Logozeichen des AVAST32-Programms gedruckt wird und auf deren Datenseite sich ein Hologram mit der Anschrift "ALWIL" befindet. Das AVAST32-Programm kann auch auf eine Spezialbestellung auf einigen Disketten gekauft werden. Die Diskettenschilder beinhalten dann das Logozeichen der Firma ALWIL Software und den Namen des Programmes.

Sollten Sie Zweifel über den legalen Ursprung Ihrer Lieferung des AVAST32-Programms haben, wenden Sie Sich direkt an die Firma ALWIL Trade GmbH.

1.6 Der AVS-Dienst

Das Gebiet der Rechnerviren ist heutzutage das dynamischste Gebiet in der Rechnerwelt überhaupt, deswegen müssen die neuesten Versionen der Antivirenprodukte angewendet werden. Für den Benutzer heißt es, sich oft und selbst um die Aktuallisierung seines Antivirenprogramms zu kümmern.

Um unseren Kunden diese Täitkgeit möglichst viel erleichtern zu können, stellen wir seit einer längeren Zeit den AVS-Antivirendienst zur Verfügung. Im Rahmen dieses Dienstes stellen wir im Laufe eines Jahres automatisch nicht nur die neuesten Versionen der Virendatabasis (sg. kleine Aktualisierung), sondern auch die möglichen neuen Programmversionen zur Verfügung und sichern auch einen technischen und Beratungsdienst.

Das AVAST32-Programm wird im Rahmen des AVS-Dienstes jeden Monat, die Programme selbst dann einmal oder zweimal jährlich aktuallisiert. Weitere Informationen über den AVS-Dienst nehmen Sie dann den Mitarbetern der Firma ALWIL Trade GmbH ab. Die aktuellen Versionen der VPS-

Datei kann man auch mittels unserer WWW-Seiten erhalten.

2.Erste Schritte

2.1 Programmstarten

Nach einer erfoglreich durchgeführten Installierung kann man gleich mit der Anwendung des AVAST32-Programms beginnen. Das Installierungsprogramm hat für Sie eine Installierungsstelle unter dem Namen "Avast32" im Angebot der Taste "Start" geschaffen. Durch ihre Wahl kann das Programm angelaufen werden. Diese Stelle befindet sich im Angebot der "Start"-Taste (es wird nach dem Klopfen mit der linken Maustaste auf dieser Taste angezeigt), in der Mappe "Programme". Die Gestalt des Angebots der "Start"-Taste hängt von der Einstellung der Umgebung des Operationsystems und der bereits installierten Programmen ab - eine mögliche Darstellung wird in der Abb. 13 gezeigt.

Wenn man in der Umgebung des Operationssystems Windows NT 3.51 arbeitet, hat das Installierungsprogramm die Gruppe "AVAST32 Antivirus" erstellt, die den AVAST32-Vertreter beinhaltet. Das Programmstarten durch diesen Vertreter ist völlig equivalent mit jeder anderen Weise des Programmstartens.

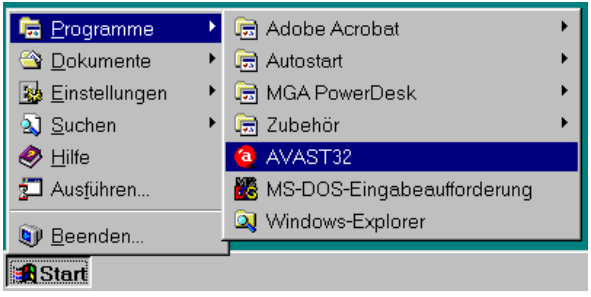

Abb. 13

Wir empfehlen Vertreter des AVAST32-Programmes in der Arbeitsfläche des Rechners zu bilden. Wenn man das AVAST32-Programm starten will, muß man dann nicht die komplizierte Struktur des "Start"-Angebots durchgehen. Will man einen Vertreter bilden, startet man das Programm "Explorer" - z.B. so, daß man mit der rechten Maustaste auf der Taste "Start" klopft und aus dem dargestellten Angebot dann die Stelle "Untersuchen" wählt (Abb. 14).

Abb. 14

In dem Programm "Explorer" die Mappe einstellen, in die das AVAST32-Programm installiert worden ist (Abb. 15). Sollte man die Einstellung der Zielmappe nicht geändert haben, dann ist es die Mappe "Program files\ALWIL Software\Avast32" in der Systemfestplatte. Dann die linke Maustaste auf dem Dateinamen "Avast32.exe" drücken und gedrückt festhalten. Den Mauszeiger zu der Arbeitsfläche gleiten lassen, d.h. zu der Fläche, die zu keinem Fenster gehört, und die Maustaste freilassen.

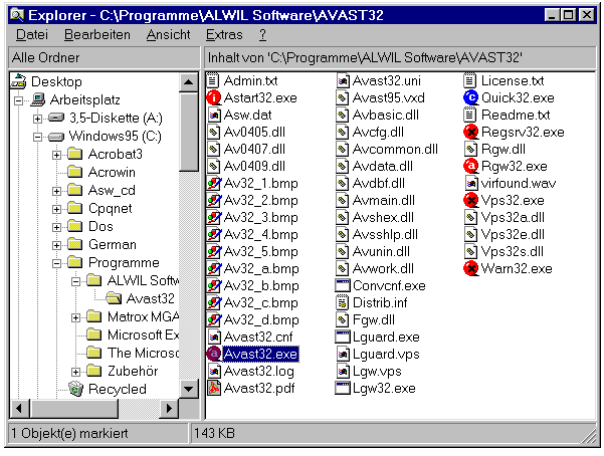

Abb. 15

Nach dieser Operation wird auf der Stelle, wo man die Maustaste freigelassen hat, der Vertreter für das AVAST32-Programm geschaffen (Abb. 15). Sollte man die Maustaste über diesen Vertreter zwei mal nacheinander schnell klopfen, wird das AVAST32-Programm gestartet.

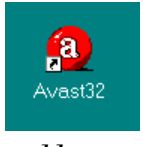

Abb. 16

Das Starten des AVAST32-Programms ist auf mehrere Weisen möglich und alle Weisen sind gleichwertig. Es ist gleichgültig, ob man die AVAST32-Stelle in dem Angebot der ”Start”-Taste gewählt hat, auf den gerade gebildeten Vertreter in der Arbeitsfläche geklopft hat oder auf die Avast32-Stelle des "Explorer"-Programmes geklopft hat, wie es die Abb. 15 zeigt. Es gibt auch andere Methoden des Programmstartens, aber die will man jetzt hier nicht behandeln.

2.2 Was sollte zuerst gestartet werden

Nach dem Starten des AVAST32-Programmes wird zuerst das Hauptfenster auf dem Bildschirm angezeigt (Abb. 17), das eine Liste von Stellen beinhaltet. Diese Stellen stellen Aufgaben dar, die in dem gegebenen Moment erreichbar sind. Nach der Installierung des AVAST32-Programms wird eine Virenanwesenheitprüfung der Festplatten des Rechners empfohlen. Um die in den einzelnen Dateien durchgeführten Änderungen verfolgen zu können und so auch einen neuen und unbekannten Virus entdecken zu können, muß man eine Dateiendatabasis erstellen. Beide diese Tätigkeiten werden durch die Aufgabe unter dem Namen "Suchen+Kontrollieren: alle lokale Laufwerke" durchgeführt.

Abb. 17

Die Aufgabe wird gestartet indem man die linke Maustaste auf dem Aufgabennamen zweimal kurz nacheinander betätigt (Anklopfen). Daß die Aufgabe wirklich gestartet worden ist, erkennt man an der Ikone - die Ikoneneben dem Aufgabennamen ändert sich wie in der Abb. 18 abgebildet. Wenn sich die Ikone nicht geändert hat, hat man wahrscheinlich die linke Maustaste nicht schnell genung nacheinander betätigt.

Abb. 18

Die gestartete Aufgabe "Suchen+Kontrollieren: alle lokale Laufwerke" wird alle Mappen in den Festplatten untersuchen und die gefundenen Dateien werden geprüft, ob Viren beinhaltet sind oder nicht. Gleichzeitig wird jede gefundene Datei gespeichert und der Zustand notiert, in welchem sie sich auf der Festplatte befindet. Die Aufgabe kontrolliert auch den Arbeitsspeicher des Rechners.

Abb. 19

Wird ein Virus in den Dateien oder im Arbeitsspeicher gefunden, wird eine Warnmeldung angezeigt (Abb. 19). Wie man in solchem Fall vorgeht, wird in der Anlage B beschrieben. In jedem Fall sollte man nicht in Panik geraten und wenn man sich mit seinen Rechnerfähigkeiten nicht sicher ist, ist es zu empfehlen, die Virusbeseitigung einer erfahrener Person zu überlassen. Wenn die Aufgabe keinen Virus gefunden haat, wird im Velauf ihrer Tätigkeit keine Meldung angezeigt.

Die Aufgabendauer ist von der Dateienanzahl und -typen in den Festplatten und von der Rechnergeschwindigkeit abhängig. Sie kann sich in der Zeitspanne von einigen Zehnten Sekunden bis zu einigen Minuten bewegen. Ihre Durchführung lohnt sich in jedem Fall, weil man nach dem Aufgabenalauf feststellen kann, ob ein Virenbefall besteht und ob eine Dateiendatabasis zur Verfügung steht, mit derer Hilfe man bei Virenbefall des Systems eine Dateienerneuerung versuchen kann.

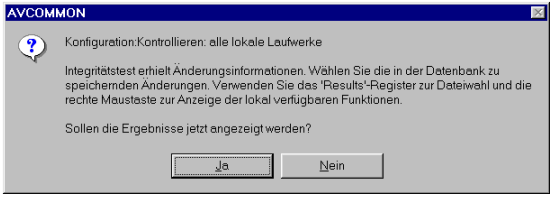

Abb. 20

Nach der Aufgabenbeendigung wird durch das Programm ein Dialog abgebildet, das in der Abb. 20 dargestellt ist, und das Symbol neben dem Aufgabennamen nimmt wieder seine ur-

sprüngliche Form an (siehe Symbolen bei den Aufgabennamen in der Abb. 17). Drücken Sie die Taste "Ja" im Dialog und die Struktur der Festplatten Ihres Computers mit allen gefundenen Mappen und Dateien erscheint. Jetzt ist es notwendig, die Datenbank der Dateien zu füllen. Klopfen Sie mit der rechten Maustaste auf das Element "Mein Rechner". Im erscheinenden Lokalmenü wird die Funktion "Akzeptieren" in der Mappe “Dateiverarbeitung“ gewählt (Abb. 21). Damit haben sie dem Programm mitgeteilt, daß es Angaben über alle Dateien auf die Festplatten in die Dateiendatenbank eintragen soll.

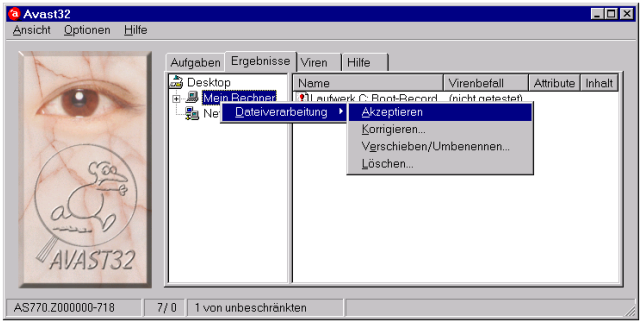

Abb. 21

Ist das Fenster, das nach der Durchführung der vorherigen Vorgänge vor Ihnen auf dem Bildschirm geblieben ist, zu kompliziert (Sie befinden sich nämlich in der sogenannten erweiterten Systemsteuerung - siehe das Kapitel 3.3 und 5), dürfen Sie zu der ursprünglichen einfachen Steuerung zurückkehren. Falls Sie es tun wollen, wählen Sie das Element "Einfache Benutzerschnittstelle" aus dem Menü "Ansicht" (Abb. 22) aus. So wird wieder in die einfache Steuerung umgeschaltet, die in der Abb. 17 gezeigt wird.

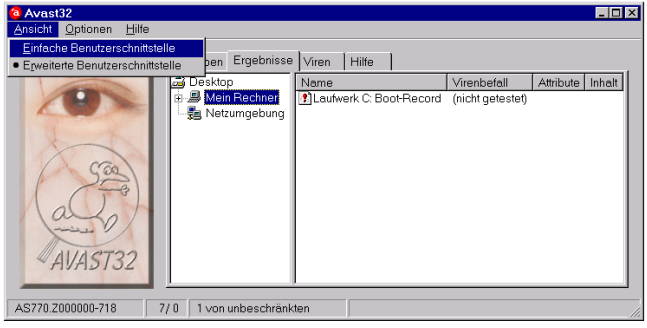

Abb. 22

2.3 Hat man hier Viren?

Wenn man nur feststellen wird, ob sich im Rechner Viren befinden, klopft man mit der linken Maustaste auf der Stelle "Suchen: alle lokale Laufwerke". Damit wird eine Aufgabe anlaufen, die alle Dateien auf den Festplatten überprüft und läßt dabei auch den Arbeitsspeicher des Rechners nicht aus.

Daß die Aufgabe wirklich angelaufen ist, erkennt man nach der Gestalt der Ikone neben dem Aufgabennamen, die wie ind der Abb. 18 abgebildet aussehen wird.

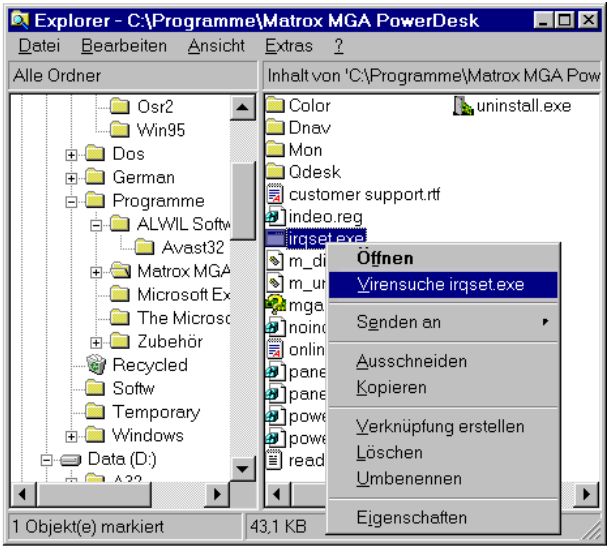

Abb. 23

Zur Feststellung, ob eine Datei durch Viren befallen ist, braucht man nicht das ganze AVAST32-Programm zu starten. Es genügt, wenn man im "Explorer"-Programm (im Kapitel 2.1 beschrieben) in die Mappe mit der entsprechenden Datei greift und auf derer Bezeichnung dann mir der rechten Maustaste klopft. Im lokalen Stellenangebot dann die Stelle "Virensuchen <Programmbezeichnung> ..." (Abb. 23) wählen. Die entsprechende Datei wird nach der Virenanwesenheit überprüft. Wenn sie Viren enthält, wird man eine Warnmeldung erhalten, wie in der Abb. 23 abgebildet (die Warnmeldung wird im Kapitel 10 beschrieben).

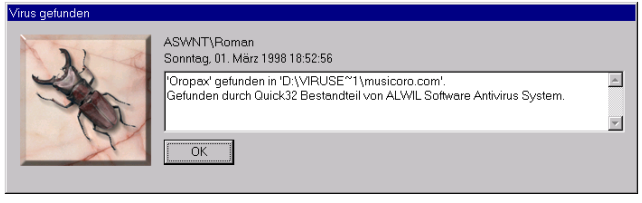

Abb. 24

In der gleichen Weise kann man auch ganze Mappen und Dateien untersuchen, ohne da es nötig ist, das gesamte AVAST 32-Programm anlaufen zu lassen. Wiederum klopft man mit der rechten Maustaste auf dem Namen der entsprechenden Mappe und sucht man aus dem lokalen Stellenangebot die Funktion "Virensuchen <Mappenbezeichnung> ..." aus. Wenn die untersuchte Mappe verdeckte Mappen beinhaltet, werden auch Dateien in diesen Mappen untersucht.

2.4 Wie man Makroviren vermeidet

Ein ernstes Problem stellen in der letzten Zeit sg. "Makroviren" dar. Es geht um Viren, die sich in der Makro-Gestalt in Dokumenten der Applikationen wie MS Word, MS Excell u.ä., verbreiten. Vor der Dokumenteneröffnung, auch wenn das Dokument in einem fremden Rechner nur geöffnet war, muß man die Makrovirenanwesenheit testen.

Wenn man ein Dokument auf einer Diskette hat, ist es günstig, die Aufgabe "Suche: Diskette A:" starten, die alle Dokumente und Dateien nach der Virenanwesenheit untersucht. Wenn man einen Virus in einem Dokument oder in einer Datei gefunden hat, wird eine Warnmeldung angezeigt (Abb. 19). Wie man weiter in diesem Fall vorgeht, wird in der Anlage B beschrieben.

Will man nur ein bestimmtes Dokument nach der Virenanwesenheit untersuchen, wird es auf die im Kapitel 2.3 beschriebene Weise durchgeführt.

Wenn man Dokumente z.B. vom Netz speichern will und man keine Sicherheit über die Dokumentensauberkeit hat (und hat man praktisch nie), müssen diese Dokumente auch geprüft werden. Mit der linken Maustaste auf dem Aufgabennamen "Suchen: interaktive Auswahl" klopfen. Nach dem Starten der Aufgabe, das durch eine Ikonenänderung indiziert wird, erscheint ein Dialog, durch das man die Mappe mit den zu überprüfenden Dateien bestimmen muß (Kapitel 5.5). Das Dialog und seine Bedienung sind dem standarten Systemdialog für die Dateieneröffnung sehr ähnlich.

2.5 Wie man auch einen unbekannten Virus entdecken kann

Weil die größte Mehrheit der Viren auf eine bestimmte Art und Weise Daten auf der Festplatte ändert, ist es geeignet, Änderungen auf den Festplatten laufend zu überwachen. Will man feststellen, ob irgendeine Datei auf der Festplatte geänder worden ist, startet man die Aufgabe "Kontrollieren: alle lokale Laufwerke" (mit der linken Maustaste auf dem Aufgabennamen anklopfen). Die angelaufene Aufgabe untersucht alle Fesplatten und erfaßt jede gefundene Datei und den Zustand, in dem sie sich auf der Festplatte befindet.

Wenn dann eine Datei geändert worden ist, wird das Programm nach der Aufgabenbeendigung eine Meldung mit der Frage, ob man die Aufgabenergebnisse darstellen soll, abgegeben (Abb. 18). Nach der Betätigung der "Ja"-Taste wird dann die Struktur Ihres Rechners mit allen Dateien, die ab

letzte Kontrolle geändert worden sind, angezeigt. Eine nähere Beschreibung der dargestellten Ergebnisse wird im Kapitel 5.3.2 gegeben; die Interpretierung der dargestellten Ergebnisse gibt das Kapitel 7.

Damit das Programm ermitteln kann, welche Datei geändert worden ist und welche nicht, muß man eine Dateiendatabasis zu schaffen. Wie man es macht, wurde im Kapitel 2.2 beschrieben.

Eine regelmäßige Kontrolle der Datenintegrität auf Ihren Festplatten ist sehr wichtig, wichtiger als die Virensuche. Man spart sich dadurch eine Reihe von Problemen, und wir empfehlen, ihr eine angemessene Aufmerksamkeit zu widmen!!!

2.6 Wie man das Vireneindringen in das System vermeidet

Damit der Rechner am besten geschützt wird, ist es empfehlenswert vor dem Beginn der eigenen Arbeit mit dem Rechner die Aufgabe "Resident: voller Schutz" anlaufen zu lassen (wiederum durch das Anklopfen auf die Aufgabenbezeichnung mit der linken Maustaste). Diese Aufgabe wird fast alle im Rechner stattfindende Tätigkeiten überwachen. Im Fall, daß eine "verdächtige" Operation durchgeführt werden sollte oder wenn das Programm einen Virus im laufenden Programm oder im Systembereich der geladenen Diskette findet, werden Warnmeldungen angezeigt (sie können die gleiche Gestalt wie die in den Abb. 25 und Abb. 26 abgebildete Meldung haben). Die Aufgabe verhindert jedoch das Eindringen des Viren in das System nur in dem Fall, daß sie angelaufen worden ist und läuft (neben dem Aufgabennamen ist die in der Abb. 18 abgebildete Ikone). Nach der Aufgabenbeendigung ist das System nicht mehr geschützt.

Abb. 25

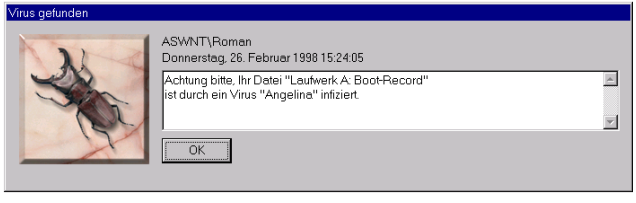

Abb. 26

Nach der Installierung des AVAST32 Programms auf Ihren Computer ist die Aufgabe "Resident: voller Schutz" nach jedem Anfahren des Operationssystems automatisch angelaufen, so daß die Notwendigkeit, sie "manuell" vor der eigentlichen Arbeit anzulaufen, wegfällt. Wie diese Möglichkeit ausgeschaltet werden kann, finden Sie im Kapitel 2.8 (allerdings empfehlen wir den normalen Benutzern den residenten Schutz eingeschaltet zu lassen!!!).

2.7 Bevor man eine fremde Diskette anwendet

Soll der Rechnerschutz wirksam sein, muß man sich außer dem regelmäßigen Anlaufen der virensuchenden Aufgaben, der regelmäßigen Aktuallisierung der Dateiendatabasis und der regelmäßigen Sicherstellung von wichtigen Daten bestimmte Gewohnheiten für die Arbeit mit dem Rechner aneignen. Eine von diesen Gewohnheiten besteht darin, daß man vor jeglichem Kopieren von einer Diskette, über die man nicht hundertprozentig weiß, ob sie in Kontakt mit einem Virus gekommen war oder nicht (und das sind alle Disketten, die auch nur eine kurze Weile in einem fremden Rechner waren), diese Diskette nach der Virenanwesenheit überprüft.

Diese Tätigkeit wird durch die Aufgabe "Suchen: Diskette A:", die wie jede andere Aufgabe angelaufen wird, dh.h. durch das Anklopfen auf dem Aufgabennamen mit der linken Maustaste. Die Aufgabe "Suchen: Diskette A:" prüft zuerst das Systembereich der Diskette (sg. Bootsektor), ob hier Viren enthalten sind oder nicht, und dann prüft alle Diskettenmappen und kontrolliert alle Dateien und Dokumente, die hier gefunden werden. Enthält eine Datei Viren (Virus) (gleichgültig ob einen Makrovirus oder einen Programme befallenden Virus), zeigt das AVAST32-Programm eine Warnmeldung an (Abb. 19). Gegenteilfalls beendet die Aufgabe ihre Tätigkeit normal.

Eine weitere wichtige Gewohnheit besteht darin, die Disketten in der Mechanik nur für die notwendigste Zeit behalten. Auf diese Weise vermeidet man das Übertragen des Systems von der virenbefallenen Diskette und die "Rechnereinsteckung". Die Mehrheit von den heutzutage hergestellten Rechnern ermöglicht die Ausschaltung des Systembootens von der Diskette im sg. SETUP. Wenn der Begriff SETUP für Sie fremd ist, kontaktieren Sie Ihren Netzadministrator.

2.8 Vorschläge für die Arbeit mit dem AVAST32-Programm

Dieses Kapitel enthält einige Ratschläge hinsichtlich der Ausnutzung des AVAST32 Programms.

Bildung eines Vertreters auf der Arbeitsfläche

Wenn man regelmäßig eine Aufgabe startet, kann man für sie einen Vertreter auf der Arbeitsfläche bilden. Nach dem Anklopfen auf dem Vertreter mit der linken Maustaste wird das AVAST32-Programm mit der entsprechenden Aufgabe automatisch angelaufen. Man wird also nicht das AVAST32-Programm und die entsprechende Aufgabe starten müssen. Der Aufgabenvertreter wird auf der Arbeitsfläche erstellt, in dem man auf dem entsprechenden Aufgabennamen mit der rechten Maustaste klopft und aus dem Lokalangebot dann die Funktion "Shortcut erstellen" wählt (Abb. 27).

Abb. 27

Auf der Arbeitsfläche wird ein Vertreter erstell, der den gleichen Namen wie die Aufgabe, auf der man die Maustaste betätigt hat, haben wird. Die Gestalt des Vertreters für die Aufgabe "Suchen +Kontrollieren: alle lokale Laufwerke" wird in der Abb. 28 abgebildet.

Abb. 28

Wegen der neuen Architektur des AVAST32-Programms muß man mit dem Anlaufen für eine neue Aufgabe nicht bis zu der Beendigung der laufenden Aufgabe warten. Das Programm ist fähig, mehrere Aufgabengleichzeitig zu verarbeiten. Die Geschwindigkeit der Aufgabenverarbeitung hängt von der Rechnerausstattung ab.

Aufgabenanlauf nach dem Systemanlauf

Zuerst die Aufgaben, die Sie nach jedem Anmelden ins System anlaufen (ähnlich der Aufgabe "Resident: voller Schutz", siehe das Kapitel 2.6), automatisch anlaufen zu lassen. Im Menü "Ansicht" suchen Sie das Element "Erweiterte Benutzerschnittstelle". Schalten Sie hier auf die Seite “Aufgaben“ um (klicken Sie auf die gleichnamige Anschrift im oberen Bereich des Fensters).

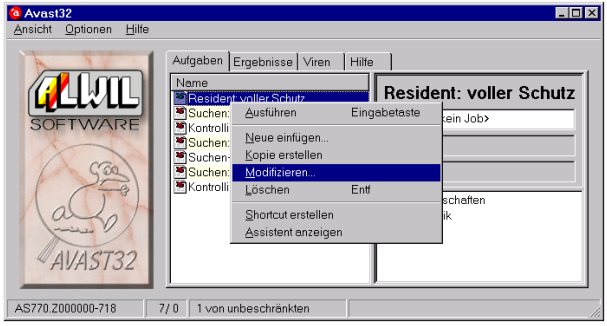

Abb. 29

Die rechte Maustaste auf dem Namen der Aufgabe, die automatisch angelaufen soll, betätigen und aus dem erscheinenden Menü die Funktion "Modifizieren..." wählen (Abb. 29). Es erscheint das Fenster des sogenannten Assistenten. Es enthält die Taste "Weiter >>", durch derer mehrfache Betätigung Sie bis auf die Seite gelangen, die in ihrem oberen Bereich das Text "Gemeinsame Bediengselemente für ..." enthält (Abb. 30). Hier das Feld "Aufgabe mit dem OS starten lassen" abhaken und die Taste "OK" betätigen (Eine detailliertere Beschreibung der Seite ist im Kapitel 4.4.6 zu finden). Nach Ihrer nächsten Anmeldung ins System wird diese Aufgabe automatisch angelaufen.

Wenn Sie den automatischen Aufgabenanlauf verhindern wollen, gehen Sie auf dieselbe Weise

vor und löschen Sie das Abhaken des erwähnten Feldes.

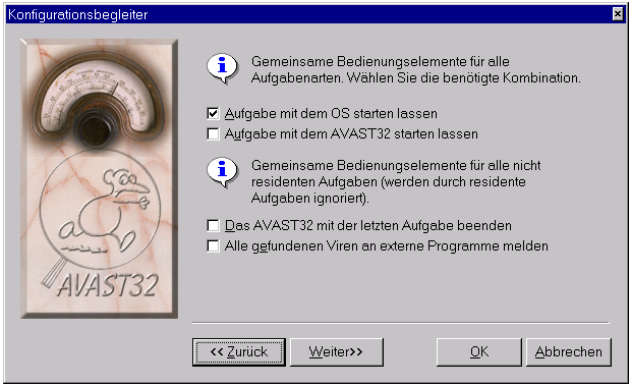

Abb. 30

Die Programmsteuerung ist allerdings wieder in ihre "erweiterte" Form umgeschaltet, deswegen wenn Sie erneut in der ursprünglichen einfachen Steuerung arbeiten wollen, wählen Sie das Element "Einfache Benutzerschittstelle" aus dem Menü "Ansicht" aus (Abb. 22).

3.Programmbeschreibung

Das AVAST32-Programm bietet einen vollständigen Antivirenschutz der Personalrechner, die unter den Operationsystemen Windows 95 oder Windows NT arbeiten. Das Programm ermöglicht die Durchführung von Tätigkeiten, die praktisch alle Gebiete des Antivirenschutzes betreffen.

Außer des heutzutage schon klassischen Programms der Suche nach bekannten Viren werden im AVAST32-Programm auch Mittel enthalten, die auch sg. Makrovire und polymorfe Viren oder sogar unbekannte Viren entdecken können.

Mit Hilfe von Residentüberprüfungen kann man kontrollieren, ob im Rechner Operationen gelaufen sind, die ein Ergebnis der Virentätigkeit sein könnten. Das AVAST32-Programm ermöglicht auch alle im System velaufenden Operationen zu überwachen und bei Verdacht dann diese Operation zu blockieren und auf diese Weise den Virenbefall zu verhindern.

Die Benutzerspanne des AVAST32-Programms enspricht der Umgebung der Operationsysteme Windows 95 und Windows NT und ist völlig den eingeführten Standarts unterordnet. Der in dieser Umgebung operierende Benutzer wird keine Probleme mit der Aneignung dieses Programms haben.

Damit der Benutzer eine angenehme Arbeit mit diesem Programm haben kann, beinhaltet dieses Programm breite Möglichkeiten der Einstellung und zwei Bedienungsarten. Diese Bedienungsarten werden in den Kapiteln 3.3, 3.4, 3.5 und 5 behandelt.

3.1 Eigenschaften und Vorteile des AVAST32-Programms

Das AVAST32-Programm ist ein für die Operationssysteme Windows 95 und Windows NT bestimmte Programm. Die Unterschiede in der Tätigkeit dieser beiden Systeme sind sehr gering und ergeben sich ausschließlich aus der unterschiedlichen Architektur beider Systeme. Der AVAST32-Benutzer wird folglich keine Probleme mit der Bedienung unter beiden Systemen haben.

Der Hauptvorteil des AVAST32-Programms besteht in einer schnellen und vor allem gründlichen Prüfung des Rechnersystems und seiner Bestandteile. Die angewendeten Algorhitmen sind in dem Maße wirkungsvoll, daß der Virus bis zu einem

Hundert von Fällen von einem Hundert von Fällen erkannt wird - das wurde durch unabhängige Tests bewiesen! Man kann nicht nur die Virenanwesenheit prüfen, sondern auch die Tatsache, ob ab letzte Kontrolle Veränderungen gegenüber dem vorherigen Zustand aufgetreten sind. Man kann auf diese Weise auch einen noch unbekannten Virus entdecken! Wird eine Datei befallen oder beschädigt und eine Dateiendatabasis besteht, kann man versuchen, diese Datei mit Hilfe des AVAST32-Programms zu erneuern. Der Erfolgsgrad der Erneuerung beträgt bis zu 95% und die Richtigkeit der Erneuerung kann bis zu 100% gewährleistet werden!

Das AVAST32-Programm kann Netzkommunikationsmittel benutzen. Im Fall vom Virenauftritt kann man also alle gewählten Netzbenutzer zeitig benachrichtigen. Diese Eigenschaft ermöglicht, das Risiko des Datenverlustes auf eine entscheidende Weise zu vermindern und der Einsteckungsverbreitung vorzubeugen.

Das AVAST32-Programm nutzt alle Vorteile der modernen Operationssysteme, wie z.B. lange Dateinamen (bis zu 256 Zeichen), neue Bedienungselemente oder die Möglichkeit mehrere Rechnertätigkeiten auf einmal durchzuführen. Der Benutzer wird also nicht eingeschränkt und kann seine Zeit am Rechner und die Rechnerkapazität voll ausnutzen.

Die Programmbedienung kann voll den Benutzerbedürfnissen und -fähigkeiten angepaßt werden. Anfänger werden bestimmt die Möglichket der Arbeit am Rechner ohne die Notwendigkeit einer detaillierten Kenntnis begrüßen und Fortgeschrittene werden dann die Möglichkeit eine detaillierten Einstellung der Programmtätigkeiten und -reaktionen auf bestimmte Ereignisse haben.

Das AVAST32-Programm benutzt das Programm Acrobat Reader zu der Anzeige der Hilfe, das sehr qualitätsgerecht und benutzerorientiert und zur Zeit sehr beliebt ist. Das Programm Acrobart Reader wird jedoch so angewendet, das es als ein Bestandteil des AVAST32-Programms erscheint. Es ermöglicht sehr schnell die Hilfe durchzugehen und schnell zu dem Teil zu gelingen, das gebraucht wird.

3.2 Grundlegende Programmfunktionen

Ein klassischer Bestandteil aller Antivirenprograme einschl. des AVAST32-Programms ist die Suche nach bekannten Viren (diese Tätigkeit wird als Scanieren bezeichnet). Das Programm überprüft die getestete Datei im Bezug auf die Anwesenheit einer bestimmten Reihenfolge von Bytes, durch die einzelne Viren identifiziert werden können.

Das AVAST32-Programm identifiziert auf diese Weise eine große Anzahl von Viren. Neue Viren tauchen jedoch sehr oft und regelmäßig auf und es ist notwendig, daß die Databasis bereits erkannter Viren aktuallisiert wird (siehe Kapitel 1.6). Das AVAST32-Programm kann auch polymorfe Viren erkennen, die bei ihrer Wirkung sich selbst modifizieren und folglich sehr schwierig zu erkennen sind. Unser Produkt kann auch sg. Makroviren erkennen, d.h. solche Viren, die sich in der Gestalt von Makren in OLE Dokumenten verbreiten (z.B. Dokumente der Applikationen MS Word oder MS Excel).

Eine weniger verbreitete Methode der Virensuche ist der sg. Datenintegritätstest. Dieser Test geht von der Voraussetzung aus, daß der Virus in der Zeit , in der der Rechner außer Betrieb ist, in einem permanenten Rechnerspeicher gespeichert werden muß. Ein solcher Speicher ist heutzutage am meisten die Festplatte des Rechners. Daraus ergibt sich, daß wenn man Änderungen in den Dateien verfolgen wird, kann man sowohl einen Virus, der noch nicht bekannt ist , als auch einen schon gut bekannten Virus entdecken.

Wenn z.B. eine Textdatei geändert wurde (Datei mit dem Suffix TXT), kann man mit 99%-iger Sicherheit behaupten, daß kein Virus die Ursache war. Wenn aber ein Programm oder eine Systemdatei geändert wurde, ist die Wahrscheinlichkeit des Virenbefalls sehr hoch.

Um Änderungen in den einzelnen Dateien verfolgen zu können, muß man Informationen über den Stand aufbewahren, in dem sich die Dateien vor einer bestimmten Zeit befanden. Der Vergleich des aktuellen Standes mit dem in der Databasis sichergestellten Stand kann man zuverlässig ermitteln, ob diese Datei geändert worden ist oder nicht. Wenn der Benutzer diesen Test jede Woche durchführt, wird er über alle Änderungen wissen, die im Laufe dieser einen Woche eingetreten sind.

Die Informationen über Dateien, die in der Dateiendatabasis erfaßt sind, kann man außer des Integritätstests auch für den Versuch der Wiedererneuerung der Dateien im Fall von ihrem Virenbefall benutzen. Man kann auf der Grundlage dieser Databasis ganz genau bestimmen, ob eine Datei erfogreich wiederhergestell worden ist.

Das AVAST32-Programm bietet auch die Möglichket der Verfolgung von allen verdächtigen Operationen mit Dateien und mit den Systembereichen der Platten im System und der Benachrichtigung des Benutzers vor ihrer Durchführung. Der Benutzer hat dann die Möglichkeit, diese Operationen zu erlauben oder zu verbieten. Dieser Residenzschutz wird als "Residente Blöcke" bezeichnet und geht davon aus, daß die Mehrheit

von Viren während ihrer Tätigkeit Operationen mit Dateien durchführt, sei es in der Form des Befalls oder einer Beschädigung.

Der Virus kann im Rechner anwesend sein, aber der Rechner muß nicht infiziert werden. Damit der Virus aktiv wird, muß er angelaufen werden. Die Mehrheit von Viren greift folglich Dateien, die gestartet werden müssen, vor allem Programme an. Das AVAST32-Programm bietet eine residente Tätigkeit an, die als "Schutz von ausführbaren Dateien und OLE-Dok." bezeichnet wird und die Prüfung aller im Rechner gestarteten Programme durchführt. Bevor man eine Programm anlaufen läßt, wird es durch das AVAST32-Programm untersucht, ob es Viren enthält. Ist alles in Ordnung, wird das Programm gestartet. Wurde ein Virus im Programm entdeckt, erhält man eine Warnmeldung und das Programm wird nicht ohne eine Erlaubnis gestartet.

Eine weitere verbreitete Virengruppe sind Viren, die sich in den Systembereichen der Platten, d.h. vor allem in den Bootsektoren der Disketten verbreiten.Der Rechner kann zwar durch das Einschieben der Diskette nicht "eingesteckt" werden, kann aber durch das ungewollte Eintragen des Systems von der in der Mechanik vergessenen Diskette infiziert werden. Das AVAST32-Programm beinhaltet eine residente Tätigkeit unter der Bezeichnung "Bootsektor Überwachung", die beim Herangehen an eine Diskette zuerst das Boostsektor prüft. Ist ein Virus gefunden worden, informiert man den Benutzer mittels einer Warnmeldung. Ist kein Virus gefunden worden, kann die Arbeit mit der Diskette fortgesetzt werden.

3.3 Einfache versus erweiterte Benutzerschnittstelle

Die Bedienung des AVAST32-Programms kann zwei grundlegende Formen haben, die sich vor allem in der Anzahl der angewendeten Elemente und folglich in der Kompliziertheit der eigenen Bedienung unterscheiden. Darus ergibt sich dann die Benutzerzielgruppe, für die die jeweilige Bedienung bestimmt ist.

Die erste mögliche Bedienungsart des AVAST32-Programm wird in der Abb. 31 dargestellt. Diese Bedienung wird als "einfach" bezeichnet, weil sie nur die wichtigsten Bedienungselemente des Programms beinhaltet und den Benutzer vor einer Reihe von Bedienungselementen schützt, mit den in meisten Fällen nicht operiert wird.

Abb. 31

In der einfachen Bedienung kann man nur die grundlegensten Tätigkeiten und Operationen mit den Aufgaben durchführen.

Die Bedienung des AVAST32-Programms kann auch die in der Abb. 32 dargestellte Art haben. Diese erweiterte Bedienung enthält alle Bedienungselemente des Programms. Der Benutzer kann dann zu allen Funktionen und Einstellungen des AVAST32-Programms zurückgreifen.

Die erweiterte Bedienung ist wegen ihrem Umfangs in einige grundlegende Seiten aufgeteilt, die die eigentlichen Funktionen und Parameter beinhalten. Unter den einzelnen Seiten kann man sich durch das Betätigen der linken Maustaste auf dem Namen der entsprechenden Seite bewegen.

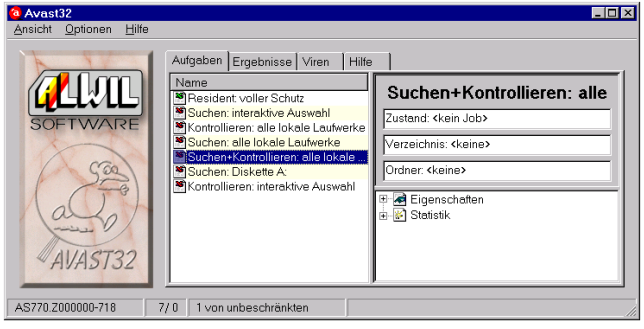

Abb. 32

Die benutzte Bedienungsart hängt von der aktuellen Programmeinstellung ab: implizit wird die einfache Bedienung eingestellt. Eine detaillierte Beschreibung der einzelnen Bedienungsarten des AVAST32-Programms und der Umschaltung wird im Kapitel 5 beschrieben.

3.4 Welche Bedienung anwenden?

Zu dieser Unterscheidung in der Bedienung des AVAST32-Programms hat die Tatsache geführt, daß man die Programmbenutzer nach Tätigkeiten aufteilen kann, die sie ausführen. Einerseits gehören zu ihnen Fachleute (z.B. Netz-

administratore, die den richtigen Netzbetrieb und -einstellung gewährleisten) und anderrerseis die normalen Benutzer.

Der normale Benutzer braucht nicht eine große Parameteranzahl - seine Hauptanforderung besteht in der möglichst einfachen Bedienung, ohne die Notwendigkeit, die Programmeinstellung und -bewältigung detailliert kennenzulernen. Diesen Benutzern wird die einfache Bedienung empfohlen, weil sie diesen Anforderungen absolut entspricht.

Die Netzadministratore und erfahrenere Benutzer brauchen im Gegenteil eine genaue Einstellung der Tätigkeit und des Programmverhaltens. Für diese Gruppe ist die erweiterte Bedienung des AVAST32-Programms bestimmt, die alle Funktionen und Bedienungselemente des Programms zugänglich macht und dadurch eine Anpassung an die Benutzeranforderungen ermöglicht.

Jeder der mit dem gegebenen Rechner arbeitende Benutzer hat die Wahl der ihm entsprechenden Bedienung und der Arbeit mit dieser Bedienungsart. Das Programm "merkt" sich nämlich die angewendete Bedienungsart für jeden Benutzer einzeln.

3.5 Möglichkeiten der einzelnen Bedienungsarten

Die Möglichkeiten der einzelnen Bedienungsarten werden durch ihre Bestimmung gegeben. Die einfache Bedienung ist für den einfachen Benutzer bestimmt, der braucht, eine Aufgabe durchführen zu können (d.h. einen bestimmten Systembestandteil zu überprüfen), ohne daß er sich mit den Details dieser Tätigkeit und der Programmeinstellung beschäftigt. Diese Anforderungen wurden berücksichtigt und die einfache Bedienung ermöglicht folglich eine sehr einfache Durchführung der grundlegenden Aufgabenoperationen.

Bei der einfachen Bedienung kann der Benutzer Aufgaben starten, beenden oder anhalten. Wird durch die Aufgabe ein Virus gefunden, wird der Benutzer benachrichtigt. Die einfache Bedienung ermöglicht nicht die Darstellung der Details der Aufgabenergebnisse und folglich kann nicht ermitteln, welche von den geprüften Dateien befallen oder geändert wurde.

Weiter ermöglicht die einfache Bedienung die Durchführung von grundlegenden Funktionen wie das Beenden von einem Programm, die Programmhilfeanzeige oder Erstellung eines Vertretrs auf der Arbeitsfläche. Die einfache Be-

dienung ermöglicht natürlich auch das Umschalten zu der erweiterten Bedienung.

Die Aufgabe der erweiterten Bedienung besteht darin, alles was das AVAST32-Programm bietet, zugänglich zu machen. Außer der grundlegenden Aufgabenoperationen, wie sie bei der einfachen Bedienung erwähnt worden sind, kann der Benutzer die Parameter der einzelnen Aufgaben ändern oder sie sogar löschen. Man kann selbstverständlich auch neue Aufgaben gestalten.

Der Benutzer hat komplette Ergebnisse der bereits durchgefühten Aufgaben und die Mittel für die Reaktion auf diese Ergebnisse zur Verfügung. Man kann also die Aufgabenergebnisse akzeptieren, man kann aber auch versuchen, die geänderten Dateien zu korrigieren. Man kann verdächtige oder befallene Dateien löschen oder umnennen oder sie in eine andere, dazu bestimmte Mappe übertragen.

Die erweiterte Bedienung ermöglicht auch die Einstellung der Umgebung von einzelnen Programmelementen und von dem AVAST32-Programm in seiner Gesamtheit. Es sind auch Bedienungselemente zur Verfügung, die dem Benutzer die Möglichkeit geben, die Programmeigenschaften dem eigenen Bedarf anzupassen. Die Einstellung der Programmumgebung enthält auch die Möglichkeit der Umschaltung des Programms zu ihrer einfachen Form.

Ein Bestandteil der erweiterten Bedienung sind auch kurze Virencharakteristiken aus der aktuellen VPS-Datei, Informationen über die Virenversion, die Programmversion und den Lizenzbesitzer. Diese Informationen sind vor allem beim Kontaktieren der Mitarbeiter unserer Frima wichtig.

3.6 Aufgabe als das Hauptelement

Das Hauptelement für die Arbeit des AVAST32-Programms ist die "Aufgabe". Unter diesem Begriff versteht man eine detaillierte Beschreibung aller Tätigkeiten, die nach dem Anlaufen der Aufgabe durchgeführt werden. Man kann bei einzelnen Tätigkeiten auch eine Reihe von Parametern einstellen, die das Aufgabenverhalten bestimmen.

Jede Aufgabe muß ihren Namen haben und muß eine bestimmte Tätigkeit enthalten. Die Tätigkeit kann z.B. in der Prüfung der Dateiien auf der Festplatte mit dem Ziel, Viren zu finden, oder in der Systemüberwachung, bestehen. Die Aufgabe kann auch mehrere Tätikgeiten geliechzeitig durchführen, man kann z.B. die Virenanwesenheit prüfen und dabei die Kontrolle der Datenänderung durchführen (sg. Dateintegritätstest).

Aufgaben können privat oder gemeinsam genutzt werden. Die gemeinsam genutzten Aufgaben sind allen mit dem gegebenen Rechner arbeitenden Mitarbeitern zugänglich, im Gegenteil zu

den privat genutzten Aufgaben, die ausschließlich dem Besitzer zugänglich sind, d.h. dem Benutzer, der sie gestaltet hat. Der Benutzer bestimmt bei der Aufgabenerstellung, ob die Aufgabe privat oder gemeinsam genutzt wird.

Alle Aufgaben, die momentan zugänglich sind, werden in einem Aufgabenverzeichnis angeführt, die ein Bestandteil sowohl der einfachenals auch der erweiterten Bedienung ist.

Die Gestaltung neuer Aufgaben wird im Kapitel 4 beschrieben.

3.7 Gelieferte Aufgaben

Zu der Installierung des AVAST32-Programms gehören auch einige schon gestalteten Aufgaben, die dem Benutzer ermöglichen, das Programm gleich nach seiner Installierung zu benutzen. Diese Aufgaben werden in den nächsten Paragraphen einzeln beschrieben.

Aufgabe "Suchen: alle lokale Laufwerke"

Diese Aufgabe untersucht alle analaufbaren Dateien und OLE-Dokumente in allen lokalen Festplatten des Rechners. Wird durch das AVAST32-Programm ein Virus gefunden, folgt eine Warnmeldung mit Klangeffekten (wenn im Rechner eine Klangkarte eingebaut ist). Jeder gefundene Virus wird durch die Aufgabe gemeldet. Auch komprimierte Dateien und der Arbeitsspeicher des Rechners werden untersucht. Auch das Systembereich bei jeder Platte wird untersucht.

Aufgabe "Suchen: interaktive Auswahl"

Diese Aufgabe führt die gleichen Untersuchungen wie die vorangegangene Aufgabe durch, der Benutzer wird jedoch vor der eigenen Prüfung die Möglichkeit haben, Bereiche auszuwählen, die untersucht werden sollen. Man kann auch mehrere Bereiche in einem Schritt wählen (siehe Kapitel 5.5).

Bei den gewählten Mappen kann bestimmt werden, daß auch die verdeckten Mappen untersucht werden sollen, falls sie vorhanden sind.

Aufgabe "Suchen: Diskette A:"

Diese Aufgabe führt die gleichen Kontrollen wie die zwei vorhergehenden Aufgaben durch, aber auf der Diskette in der Mechanik A:. Es wird empfohen, diese Aufgabe mit allen potentiell infizierten Disketten durchzuführen. Es geht vor allem um Disketten, die in anderen Rechnern oder durch andere Benutzer angewendet waren. Die Aufgabe untersucht auch das Systembereich der Diskette, d.h. das Bootsektor.

Wenn man sich gewöhnt, jede fremde Diskette vor der Anwendung zuerst zu Prüfen, wird man auf eine wesentliche Weise das Risiko der Rechnereinsteckung vermindern können.

Aufgabe "Kontrollieren: alle lokale Laufwerke"

Diese Aufgabe prüft, ob anlaufbare Dateien und OLE-Dokumente nach der letzten Kontrolle geändert worden sind oder nicht. Der Dateieinhalt wird nur dann geprüft, wenn es ab der letzten Kontrolle zu Änderungen in Dateienparametern kam, z.B. in den Attributen, Größe, usw.. Die Ergebnisse werden in einer übersichtlichen bauförmigen Form dargestellt (siehe Kapitel 5.3.2). Die Aufgabe kontrolliert auch, ob es seit der letzten Untersuchung zu Änderungen in den Systembereichen der kontrollierten Platten kam.

Aus der vorhergehenden Beschreibung ergibt sich, daß man Dateienänderungen nur zwischen zwei Integritätsunteruchungen überwachen kann. Das Ergebnis der ersten Untersuchung wird eine Meldung über die “Zunahme” der gesamten Dateien auf der kontrollierten Platte sein. Deswegen muß der Dateienzustand in einer internen Databasis erfaßt werden, damit man bei weiteren Untersuchungen den aktuellen Dateienzustand mit dem vorherigen Zustand vergleichen kann. Die Erstellung einer Dateiendatabasis wurde im Kapitel 2.2 beschrieben.

Aufgabe "Kontrollieren: interaktive Auswahl"

Diese Aufgabe führt gleiche Kontrollen wie die vorheregehende Aufgabe durch, sie fragt jedoch den Benutzer über die zu kontrollierenden Bereiche ab. Der Wahl der zu kontollierenden Mappen dient das im Kapitel 5.5 beschriebene Dialog. Auch bei dieser Untersuchung gilt es, daß zuerst die Dateiendatabase ertstellt werden muß, sollen die Ergebnisse anwendbar sein.

Aufgabe "Resident: voller Schutz"

Der durch diese Aufgabe durchgeführte Schutz geht von zwei Tatsachen aus. Soll ein Virus den Rechner befallen, muß der Rechner zuerst angelaufen werden (d.h. die Steuerung muß an den Rechner übergeben werden). Folglich ist es geeignet, alle anzulaufenden Dateien und einzulesenden Sektoren (sg. Bootsektoren) der eingegebenen Disketten zu kontrollieren. Die zweite Voraussetzung besteht darin, daß der Virus im Rechner bestimmte Tätigkeit aufweist, d.h. er ändert anlaufbare Dateien, Diskettenbootsektore oder versucht sogar einen Plattenbereich neu zu formatieren.

Alle angeführten Tätigkeiten werden durch diese Aufgabe überwacht und sollte eine potentiell gefährliche Operation durchgeführt werden, wird der Benutzer gefraget, ob diese Operation durchgefüjrt werden darf. Ohne die Benutzererlaubnis wird diese Operation nicht durchgeführt.

Es wird die Durchführung dieser Aufgabe gleich nach dem Anlauf des Operationssystems oder sogar noch mehr ihr automatischer Anlauf mit dem

Start des Operationssystems oder die Positionierung eines Aufgabenvertreters in die Mappe "Beim Start anlaufen lassen" empfohlen . Sollen die Aufgabe und ihr Schutz wirksam sein, muß diese Aufgabe laufen!

Aufgabe "Suchen+Kontrollieren: alle lokale Laufwerke"

Diese Augabe ist eine Kombination von den Aufgaben "Suchen: alle lokale Laufwerke" und "Kontrollieren: alle lokale Laufwerke". Wenn man beide Aufgaben durchführen will, ist es schneller die Aufgabe "Suchen+Kontrollieren: alle lokale Laufwerke" anlaufen zu lassen (auch aus der Sicht der Durchführung). Über diese Aufgabe gilt alles, was zu den beiden Enzelaufgaben angeführt wurde.

3.8 Grundlegende Programmbedienungsarten

Die Bedienung des AVAST32-Programms wurde unter der Berücksichtigung von Standarts auf diesem Gebiet vorgeschlagen. Für die Bedienung des AVAST32-Programms wurden folglich nur standarte Bedienungselemente genutzt.

Man kann das Programm grundsätzlich wie folgt bedienen: entweder durch die Tastatur oder durch die Maus. Für eine schnellere Bedienung wird die Maus empfohlen, die Tastatur sollte nur für die Texteingabe benutzt werden. Eine genaue Beschreibung der Maus- und Tastaturanwendung wird im Handbuch oder in der Hilfe des Operationssystems gegeben.

Im folgenden Text versteht man unter dem Begriff "aktives Element" ein solches Element, das auf eine bestimmte Weise hervorgehoben wird. Z.B. in der Abb. 31 ist die Taste "Start" aktiv, in der Abb. 32 ist die Aufgabe "Suchen + Kontrollieren: alle lokale Laufwerke" aktiv. Welche Farbe für die Hervorhebung genutzt wird, hängt von der aktuellen Einstellung des Operationssystems (Mappe "Systemsteurung", Element "Anzeige") ab.

Der Programmbedienung dienen Bedienungselemente. Zu den wichtigsten gehört das sg. Lesezeichenverezichnis, das in der Abb. 33 abgebildet wird. Es beinhaltet immer einige Seiten mit unterschiedlichen Inhalten und Funktionen. In dem gegeben Moment wird nur eine von diesen Seiten sichtbar. Andere Seiten kann man durch das Klopfen mit der linken Maustaste auf dem Namen der entsprechenden Seite.

Abb. 33

Mit der Hilfe der Tastatur kann man sich in den einzelnen Seiten durch die Aktivierung des Lesezeichenverezichnisses und durch die Benutzung der Tasten für die Kursorbewegung links und rechts bewegen. Auf diese Weise wird die Seite links oder rechts aktiviert.

Ein weiteres und sehr wichtiges Bedienungselement ist der sg. Baum. Er stellt in einer hierarchischen Darstellung eine Struktur dar, die verschiedene Inhalte haben kann. Er kann z.B. die baumförmige Struktur der auf der Platte gespeicherten Mappen darstellen (so wird der Baum durch den "Explorer"-Programm benutzt) oder Informationen über den aktuellen Stand liefern (Abb. 32).

Die baumförmige Struktur enthält Stellen. Wenn man eine Stelle "aufmachen" will, klopft man mit der linken Maustaste auf die Ikone neben der Bezeichnung der entsprechenden Stelle an. Bei der Tastaturanwendung muß diese Stelle zunächst aktiviert werden und dann durch die "Enter"-Taste bestätigt werden. Die Stelle wird auf die gleiche Weise "zugemacht". Man kann auch die Kursorbewegungtasten betätigen - Kursor für die Bewegung nach links für die "Stellenzumachung", Kursor für die Bewegung nach rechts für die "Stellenaufmachung".

Ein Element, mit dem das AVAST32-Programm auch arbeitet, ist ein Verzeichnis. In der Abb. 31 wird das Verzeichnis der erreichbaren Aufgaben dargestellt, aber dieses Verezichnis kann auch auf anderen Stellen benutzt werden. Es kann auch mehrere Spalten enthalten, derer Bedeutung immer in der ersten Zeile beschrieben wird. Die Breite der einzelnen Spalten im Verzeichnis kann beliebig geändert werden. Die Arbeitsweise ist folgend: zuerst drückt man auf der rechten Seite des Spaltennamnens mit der linken Maustaste und hält man sie gedrückt. Durch die Bewegung der Mausanzeige wird dei benötigte Spaltenbreite eingestellt. Dann wird die Maustaste freigelassen.

Ein Verzeichniselelment wird hervorgehoben - es wird als aktiv bezeichnet. Damit ein Element aktiv wird, muß auf ihm mit der linken Maustaste geklopft werden oder muß es mit Hilfe der Tastaturtasten für die Kursorbewegung nach oben und nach unten hervorgehoben werden. Enthält das Verzeichnis zu viele Elemente, man kann sich in ihm "seitenweise" mit Hilfe der Tasten "PgUp" und "PgDn" bewegen.

Abb. 34

Die rechte Maustaste dient in den Operationssystemen Microsoft Windows dem Aufruf des sg. Lokalangebots (Abb. 34). Das gleiche gilt auch für das AVAST32-Programm. Die Funktionen des Lokalangebots betreffen. immer das Element, auf dem die rechte Maustaste betätigt wurde (in der Abb. 34 ist es die Aufgabe "Suchen: alle lokale Laufwerke") und das solche Operationen enthält, die man mit dem gegebenen Element durch führen kann. Die zu startende Funktion wird durch das Betätigen der linken Maustaste über ihrem Namen gewählt. Das Angebot kann nicht nur Funktionen enthalten, sondern auch andere Mappen, in denen wiederum Funktionen oder weitere Mappen, usw. aufbewahrt werden.

Für die AVAST32-Programmbedienung wird das Lokalangebort ziemlich oft angewendet und wir empfehlen, vor allem den beginnenden Benutzern, sich an die Betätigung der rechten Maustaste zu gewöhnen. Einige Programmbestandteile kann man nämlich nur mittels des Lokalangebots oder durch die Tastatur bedienen.

4.Erstellung neuer Aufgaben

Ein Bestandteil des AVAST32-Programms sind auch einige bereits erstellte Aufgaben (Kapitel 3.7), die eine direkte Anwendung des Programms für seine Installierung und die Ausnutzung einer Mehrheit seiner Funktionen ermöglichen. Nach einer bestimmten Zeit wird aber die Mehrheit von Benutzern das Bedürfnis haben, neue Aufgaben für sich gestalten zu wollen, die den eigenen spezifischen Bedürfnissen entsprechen werden.

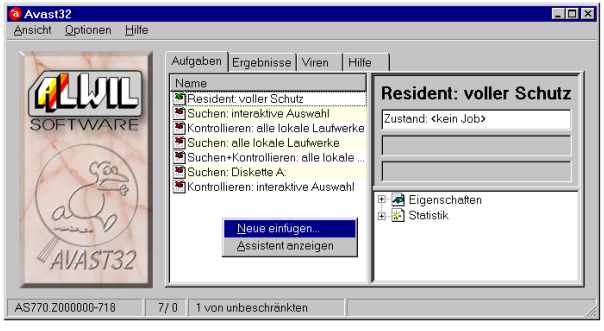

Abb. 35

Eine neue Aufgabe kann man nur in der erweiterten Umgebung oder mit Hilfe von "Steuerungssystem" erstellen (siehe das Kapitel 6.7). Wenn Sie also in der einfachen Umgebung arbeiten, das Element "Erweiterte Benutzerschnittstelle" aus dem Menü "Ansicht" wählen. In der einfachen Umgebung schalten Sie auf die Seite "Aufgaben" um, wo Sie auf der Aufgabenliste die rechte Maustaste betätigen. Im Lokalmenü wählen Sie dann die Funktion "Neue einfügen..." (Abb. 35).

Wenn die Einstellung beliebiger Aufgabe geändert oder eine neue Aufgabe erstellt werden soll und das Programm AVAST32 nicht angelaufen ist, dann können Sie das durch "Steuerungssystem" durchführen. Eine detaillierte Beschreibung ist im Kapitel 6.7 zu finden.

Eine detaillierte Beschreibung der Erstellung von neuen Aufgaben wird man gerade in diesem Kapitel finden. Dabei wird nicht nur eine Beschreibung der einzelne n Bedienungslemente gegeben, sondern auch Empfehlungen, die vor allem durch alle weniger erfahrenen Benutzer respektiert werden sollten.

4.1 Privat oder gemeinsam genutzte Aufgabe?

Vor der eigenen Augabenerstellung sollte der Benutzer bestimmen, zu welchem Zweck die neue Aufgabe dienen soll und durch wen sie benutzt werden soll. Einige Aufgaben müssen allen Benutzern des konkreten Rechnersystems zugänglich sein, z.B. die Diskettenüberprüfung in der Mechani A:, oder eine Systemüberprüfung. Gegenteilfalls gibt es Aufgaben, die nur für einen Benutzer bestimm sind. Als Beispiel soll die Überprüfung persönlicher Dokumente und Applikationen angegeben werden.

Eine solche Aufgabenaufteilung ist sehr günstig, weil dabei die Erstellung von völlig identischen Aufgaben für jeden Benutzer entfällt und gleichzeitig für jeden einzelnen Benutzer die Möglichkeit erhalten bleibt, für sich eine eigene, seinen Bedürfnissen ensprechende, Aufgabe zu erstellen.

Aufgaben, zu denen alle Benutzer des gegebenen Systems Zugang haben, werden als gemeinsam genutzte Aufgaben bezeichnet. Es geht um Aufgaben, die im Aufgabenverzeichnis aller Benutzer angezeigt werden. Ihre Dienste können also durch alle Benutzer ausgenutzt werden. Die gemeinsam genutzten Aufgaben werden im Aufgabenverzeichnis durch eine Ikone gekennzeichnet, die in der Abb. 36 abgebildet wird.

Abb. 36

Die gemeinsam genutzten Aufgaben sollten auf einem Computer (Computernetz), auf dem mehrere Benutzer arbeiten , durch eine Person erstellt werden, die das Computer (Computernetz) betreut. Diese Person ist in den allermeisten Fällen der Netzadministrator. Mit dieser Problematik hängt auch die Möglichkeit zusammen, mehrfach genutzte Aufgaben durch ein Kennwort zu schützen. Ist der Kennwortschutz eingestellt, wird für den Benutzer, der das Kennwort nicht kennt, nur möglich, die Aufgabe anlaufen zu lassen, ihr Vorgang zu beenden und eine Privatkopie der Aufgabe zu erstellen. Bei allen anderen Manipulationen wird der Benutzer ums Kennwort gebeten (siehe das Kapitel 6.1.2).

Als "privat" genutzte Aufgaben werden solche Aufgaben bezeichnet, die ausschließlich nur dem einen Benutzer zugänglich sind, der sie erstellt hat. Diese Aufgaben werden nicht in den Aufgabenverzeichnissen anderer Benutzer angezeigt und kein anderer Benutzer kann mit ihnen ope-

rieren. Die privaten Aufgaben haben im Aufgabenverzeichnis neben ihrem Namen die in der Abb. 37 dargestellte Ikone.

Abb. 37

Der Benutzer bestimmt bei der Erstellung der Aufgabe (siehe Kapitel 4.4.1), ob sie privat oder gemeinsam genutzt wird. Später kann diese Einstellung jederzeit geändert werden (bei gemeinsam genutzten Aufgaben und dem angeschalteten Schutz muß die Kennwortkenntnis bestehen).

4.2 Mit oder ohne Begleiter?

Die Bedienug des AVAST32-Programms wurde unter der Berücksichtigung aller Programmbenutzer gestaltet. Wie man schon erwähnt hat, kann mit dem Programm in einer einfachen oder in einer erweiterten Bedienung gearbeitet werden. Der Zweck dieser Aufteilung besteht vor allem darin, den einfachen Benutzern mit der Programmbedienung zu helfen und sie nicht mit zu vielen Details zu belasten einerseits und andererseits den Fachleuten eine komplexe Programmbedienung und Einstellung zu ermöglichen.

Ähnlich ist es auch bei der Erstellung von einer neuen Aufgabe, wo man entweder den sg.Begleiter oder das klassische Lesezeichenverzeichnis anwenden kann. Der Unterschied von beiden Erstellungsbedienungen besteht vor allem im Herangehen zum Benutzer. Während der Begeleiteranwendung dient der Begleiter als Hilfe, das Lesezeichenverzeichnis ist ausschließlich ein Instrument für die Erstellung einer neuen Aufgabe. Die Bedienungselemente sind für beide Bedienungsarten identisch.

Der Assistent für das Erstellen einer neuen Aufgabe kann durch das Abhakfeld "Assistenten für Erstellung der neuen Aufgabe anwenden" auf der Seite "Grundlege Informationen" im Menü "Optionen/Hauptkonsolle ..." eingeschaltet werden (siehe das Kapitel 6.1.1).

Benutzt man den Begleiter (Abb. 38), wird man durch das Programm für die Erstellung von neuen Aufgaben geführt. Seite nach Seite geht man den ganzen Prozeß der Aufgabenerstellung durch und man stellt die Bedienungselemente auf den einzelnen Seiten ein. Der Benutzer kann jederzeit zur weiteren Seite übergehen, wenn er mit der Einstellung zufrieden ist, oder kann zu der vorangehenden Seite zurückkehren. Dazu werden die Tasten "Weiter >>" und "<< Zurück" benutzt. Die Aufgabenerstellung kann durch die Betätigung der "Abbrechen"-Taste oder des Tastaturknopfes

"Esc" unterbrochen werden. Die Aufgabe kann auch auf der Grundlage der bis jetzt eingestellten Parametern durch die "OK"-Taste erstellt werden. In diesem Fall werden für die nicht eingestellten Paramter ihre implizite Werte angewendet.

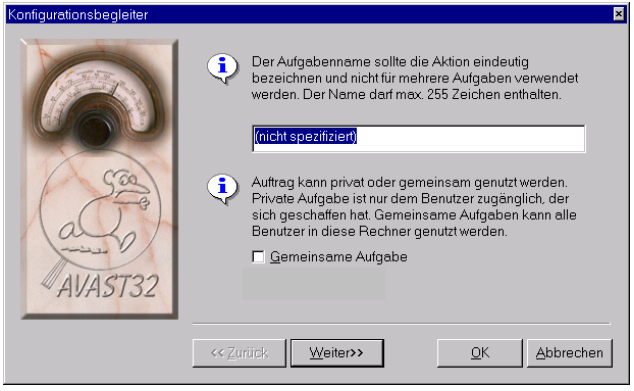

Abb. 38

Die Begleiteranwendung wird vor allem den Benutzern, die erst lernen, das AVAST32-Programm zu bedienen, empfohlen. Die Begleiteramwendung ist einfach und das Übersehen von einem wichtigen Parameter wird praktisch ausgeschlossen. Der Benutzer lernt die einzelnen Einstellungsmöglichkeiten und ihre Verteilung auf den einzelnen Seiten kennen.

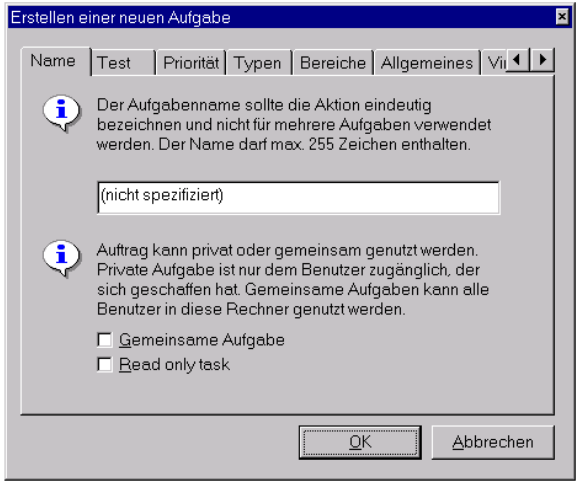

Abb. 39

Wenn der Begleiter ausgeschaltet ist, werden sich alle ereichbaren Seiten nacheinander im klassischen Lesezeichenverzeichnis befinden (Abb. 39), dessen Bedienung im Kapitel 3.8 beschrieben worden ist. Dieses Verezichnis ermöglicht dem Benutzer einen direkten Übergang zu der Seite mit den benötigten Bedienungselementen ohne alle vorangehenden Seiten durchgehen zu müssen. Gleich wie bei der Begeleiteranwendung kann die Aufgabenerstellung jederzeit durch die "Abbrechen"-Taste unterbrochen werden oder kann um die Aufgabenerstellung mit den bereits eingegebe-

nen Werten durch die "OK"-Taste gebeten werden. Für die nicht eingegebenen Parameter werden ihre implzite Werte angewendet.

Das Lesezeichenverzeichnis werden wahrscheinlich die erfahreneren Benutzer anwenden, vor allem wegen seiner schnelleren Bedienung. Der Benutzer stellt nur das ein, was er einzustellen braucht und kann direkt zu der Erstellung von einer neuen Aufgabe übergehen (diese Art wird den weniger erfahreneren Benutzern nicht empfohlen). Das Lesezeichenverzeichnis ist sehr günstig für die Parameteremodifizierung einer bereits bestehenden Aufgabe.

Als Standard ist die Ausnutzung des Assistenten für die Erstellung einer neuen Aufgabe sowie auch für Änderung einer Aufgabe, die schon existiert, eingestellt.

Die Parameteränderung der bestehenden Aufgaben erfolgt in der gleichen Umgebung wie die Erstellung neuer Aufgaben. Folglich gilt alles über die Aufgabenerstellung auch für ihre Änderungen. Der einzige Unterschied besteht darin, daß wenn man während der Aufgabenparameteränderung die "Abbrechen"-Taste betätigt, werden alle Parameter ohne Änderung erhalten bleiben und die Aufgabe als solche auch erhalten bleiben wird.

Der Assistent für die Veränderung bereits vorhandener Aufgaben kann durch das Abhaken des Feldes "Assistenten bei der Aufgabeänderung anweden"auf der Seite "Grundlege Informationen" im Menü "Optionen/Hauptkonsolle..." des Hauptfensters eingeschaltet werden (siehe das Kapitel 6.1.1).

4.3 Was beinhaltet eine Aufgabe?

Das grundlegende Element für die Arbeit des AVAST32-Programms ist eine Aufgabe. Jede Aufgabe hat eine Bezeichnung und beinhaltet eine detaillierte Beschreibung aller Tätigkeiten und Eigenschaften, die nach dem Augabenanlauf durchgeführt werden. Die Aufgabe beinhaltet auch Informationen über ihre Wichtigkeit, bzw. Priorität.

Die Aufgabe kann drei Tätigkeiten durchführen: Prüfung der Anwesenheit von bekannten Viren, Datenintegritätstest und verschiedene residente Tests. Die angeführten grundlegenden Tätigkeiten können meistens noch weiter unterteilt werden, aber im Prinzip ist es nicht notwendig. Jede von den angeführten Tätugkeiten kann genau nach den Benutzerbedürfnissen eingestellt werden.

Die angeführten Tätigkeiten sind untereinander kombinierbar, was letzendlich die Beschleunigung des gesamten Prüfungsprozesses bedeutet. Z.B. eine gemeinsame Einstellung der Virenanwesenheitprüfung und des Datenintegritätstests

heißt, daß diese Tests in den einzelnen Dateien gleichzeitig ablaufen werden und die Dateien nicht mehrmals gespeichert werden müssen, usw.

Ein Bestandteil der Aufgabe ist auch die Information über ihre Anlaufzeit. Die Einstellung kann sichern, daß die Aufgabe automatisch nach dem Start des Operationssystems anläuft und den Rechner während seiner gesamten Tätigkeitsdauer schützt. Das kann bei den residenten Tests sehr praktisch sein, wenn der Rechner möglichst am längsten "unter Kontrolle" sein muß. Der Aufgabenanlauf kann auch mit dem AVAST32-Programmanlauf eingestellt werden oder kann vom Benutzer entschieden werden.

Die Aufgabe beihaltet auch die Bestimmung, wie man den Benutzer über mögliche Viren benachrichtigt. Das AVAST32-Programm ermöglicht das Einfügen des Fehlermeldungtexts und auch die Wahl des Klanges, der die Meldung begleiten wird.

4.4 Beschreibung der Seiten der Aufgabenkonfiguration

Im folgenden Text werden die einzelnen Seiten mit den Bedienungselementen beschrieben. Zuerst werden immer alle Bedienungselemente auf einer Seite und ihre vorgegebenen Werte beschrieben. Abbildungen bei einzelnen Seiten stellen die Seiten bei der Begleieteranwendung dar. Bei der Anwendung des Lesezeichensverzeichnisses ist die Gestalt des Fensters anders, die Bedienungselemente und ihre Beduetung sind die gleichen (siehe Unterschied zwischen den Abb. 38 und Abb. 39).

Es ist hervorzuheben, daß die Anzahl der aktuell erreichbaren Seiten von den ausgewähletn Aufgabentätigkeiten abhängt und kann bei der Aufgabenerstellung variieren. Der Benutzer muß also nicht die Seiten “überspringen”, die keinen Einfluß auf den Aufgabenablauf haben.

4.4.1 Seite "Name"

Auf der Seite "Name" verlangt das Programm die Eingabe des Namens der zu erstellenden Aufgabe (Abb. 38 und Abb. 39). Dieser Name sollte treffend und nicht identisch mit dem Namen einer schon bestehenden Aufgabe sein - das Programm kann zwar mit den gleich bezeichneten Aufgaben arbeiten, eine gleiche Bezeichnung sollte jedoch der Übersichtlichkeit wegen vermieden werden. Wird kein Name angegeben, wird eine neue Aufgabe nicht erstellt. Implizit beinhaltet das Textfeld den Namen "(nicht spezifiziert)".

Durch das Anhakfeld "Gemeinsame Aufgabe" kann eingestellt werden, ob eine Aufgabe gemeinsam oder privat genutzt werden soll. Gemeinsam genutzte Aufgaben können durch alle Benutzer des

gegebenen Rechners genutzt werden, im Unterschied zu den privat genutzten Aufgaben, die nur durch ihren Ersteller genutzt werden können. Bleibt das Feld nicht angehakt, wird die neu erstellte Aufgabe privat, das ist die implizite Einstellung.

Diese Seite ist bei jeder Variante der erstellten Aufgabe vorhanden.

4.4.2 Seite "Test"

Die Seite "Test" beinhaltet Bedienungselemente, durch die die eigene Aufgabentätigkeit bestimmt wird (Abb. 40). Auch eine gleichzeitige Ausführung mehrerer Tätigkeiten kann eingestellt werden. Die Einstellung der Bedienungselemente auf dieser Seite hat einen entscheidenden Einfluß auf die Anzahl der daraufolgend zugänglichen Seiten. Soll keine Tätigkeit ausgewählt werden, wird die Erstellung einer neuen Aufgabe nicht erlaubt.

Abb. 40

Das Anhakfeld "Virensuche" schaltet die Prüfung der Anwesenheit von bekannten Viren ein. In jeder der gewählten Dateien werden dann unter anderem alle bekannten Viren gesucht und ihre eventuelle Anwesenheit wird dem Benutzer mitgeteilt. Die Virensuche ist implizit eingeschaltet.

Das Anhakfeld "Integritätstest" dient dem Anlauf des Dateintegritätstests. Jede ausgewählte Aufgabe wird in der Hinsicht geprüft, ob sie seit der letzten Kontrolle geändert worden ist oder nicht, wenn ja, wird gesagt wie. Das Feld ist implizit angehakt.

Das Anhakfeld "Vereinfacter Integritätstest" schaltet gleich wie das vorheregehende Feld den Dateiintegritätstest ein. Es werden aber nur vereinfachte Kontrollsummen der Inhalte berechnet,

die Dateienattribute werden nicht überprüft. Die Dateienänderungskontrolle wird so schneller verlaufen. Die einfache Prüfung ist nicht implizit eingeschaltet.

Die erwähnten Vorgänge nennen wir nonresident. Die folgenden Aufgaben werden den residenten Aufgaben zugeordnet. Nach dem Typ des durchgeführten Vorgangs sprechen wir über residenten und nonresidenten Aufgaben. Ob die gerade erstellende Aufgabe resident sein wird oder nicht, hängt davon ab, ob irgendwelcher nonresidenter Vorgang erlaubt ist. Wenn es der Fall ist, die Aufgabe wird nonresident sein und die Einstellung der Steuerungselemente der residenten Vorgänge wird ignoriert werden. Ist kein residenter Vorgang abgehakt, wird die Aufgabe resident.

Das Feld "Intergritätstest" kann nicht gleichzietig mit dem Feld "Vereinfacter Intergritätstest" angehakt werden (das würde keine Bedeutung haben). Werden beide Felder angehakt, das AVAST32-Programm betrachtet das letzte angehakte Feld als angehakt. D.h. es ändert die Einstellung der Anhakfelder in der Weise, damit sie zulässig bleibt.

Das Anhaken des Feldes "Residente Blöcke" schaltet die residente Blockierung verdächtiger Operationen für die gegebene Aufgabe ein. Sie besteht in der Systemüberwachung und folgender Blockierung der potentiell gefährlichen Aktionen. Sie beinhaltet einige Dateioperationen und den Schritt der Diskettenformatierung. Ist die Blokkierung erlaubt, wird der Benutzer über solche Aktion benachrichtigt und gefragt, ob die angeführte Operation tatsächlich durchgeführt werden soll. Das Feld ist implizit angehakt.

Das Anhakfeld "Bootsektor Überwachung" ermöglicht, die Überwachung des Bootsektors der eingegebenen Disketten zu den durch die Aufgabe durchgeführten Tätigkeiten zu zuordnen. Das Feld ist implizit angehakt.

Das Anhakfeld "Schutz von ausführbaren Dateien und OLE-Dok." schaltet die Kontrolle der zu startenden Programme und Dokumente für die gegebene Aufgabe ein. Jedes Programm muß vor seinem Anlauf untersucht werden, ob es bekannte Viren enthält oder nicht. Wird der Virus gefunden, wird das Programm nicht gestartet und der Benutzer erhält eine Warnmeldung. Sonst wird das Programm normal angelaufen. Die Programmverfolgung ist implizit eingeschaltet.

Diese Seite ist bei jeder Variante der zu erstellenden Aufgabe vorhanden.

4.4.3 Seite "Priorität"

Jede nicht residente Aufgabe ermöglicht, ihre Durchführungspriorität einzustellen. Der Benutzer teilt dem Operationssystem mit, inwieweit die jewilige Aufgabe für ihn wichtig ist. Je höher die

Aufgabenpriorität, desto mehr Prozessorzeit bekommt sie zugeordnet und desto schneller wird sie ablaufen. Die Geschwindigkeit der Aufgabendurchführung hängt nicht nur von ihrer Priorität, sondern auch vom aktuellen Systemzustand und von den Prioritäten der gerade laufenden Programme ab. Implizit wird die Aufgabepriorität niedriger als die AVAST32-Priorität eingestellt.

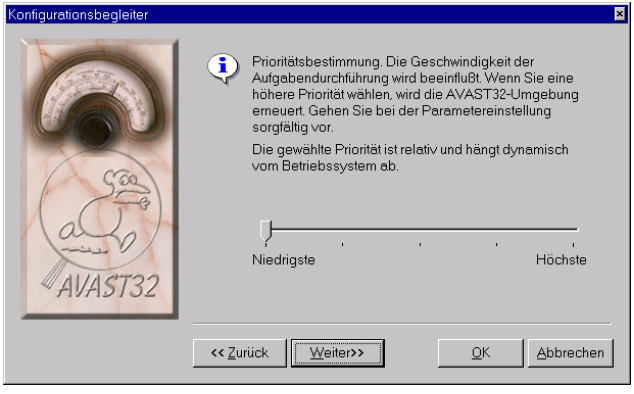

Abb. 41

Gerade diese Seite (Abb. 41) dient der Prioritätseinstellung. Sie beinhaltet nur einen Schiebereiter, durch deren Einstellung die Aufgabenpriorität geändert werden kann. Nach links ist die Aufgabenpriorität niedriger und umgekehrt. Weil es sich hier um einen Eingriff in die Aufgabenplanung des Opertionssystems handelt, wird die Positionsänderung des Schiebreiters nur den Benutzern empfohlen, die ganz genau seine Aufgabe kennen. Der einfache Benutzer kann mit dem vorgegeben Prioritätswert zufriedengestellt werden. Wenn die angegebene Aufgabenpriorität zu hoch ist, kann eine verlangsamte Erneuerung der Benutzerumgebung des Programms verursacht werden. Es ist kein Programmfehler, sondern die Folge dessen, daß die Aufgabe eine höhere Priorität als die Benutzerumgebung des AVAST32-Programms bekommen hat.

Die Seite "Priorität" ist nur dan vorhanden, wenn eine Virensuche oder ein Datenintegritätstest erlaubt worden sind - normal oder vereinfacht, d.h. wenn die Aufgabe nicht residente Tätigkeiten beinhaltet.

4.4.4 Seite "Typen"

Diese Seite dient der Bestimmung von Dateientypen, die in den ausgewählten Mappen kontrolliert werden sollen (Abb. 42). Meistens müssen nicht alle Dateien geprüft werden, weil Viren nur einige Dateien befallen. Z.B. ist die Überprüfung der Textdateien überflüssig (Dateien mit dem TXT-Zuffix) - wäre hier ein Virus vorhanden , das Operationssystem würde das Anlaufen dieser Textdatei nicht erlauben und der Virus könnte nie aktiv werden. Durch die Einschränkung der Anzahl

der zu überprüfenden Dateien kann der Aufgabenablauf beschleunigt werden.

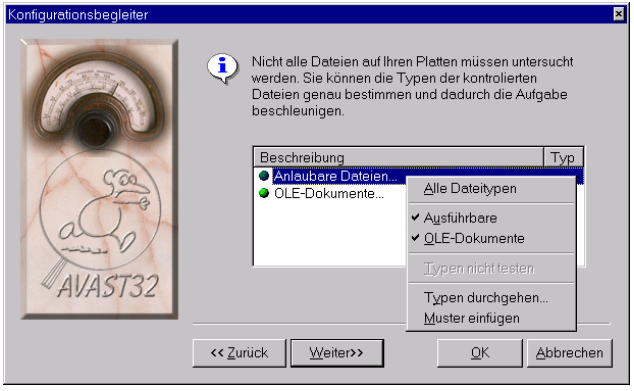

Abb. 42

Alle Dateientypen, die geprüft werden, werden im Verzeichnis auf deiser Seite angeführt. Das Verzeichnis enthält auch eine kurze Beschreibung des Dateientyps, bzw. das Dateisuffix. Das Suffix kann auch Vertretungszeichen wie "*" (Sternchen) und "?" (Fragezeichen) beinhalten, die die gleiche Bedeutung wie bei der Anwendung im Operationssystem haben.

Das Einfügen von einem weiteren Typ in das Verzeichnis der kontrollierten Typen kann durch das Lokalangebot durchgeführt werden (Abb. 41). Das Lokalangebot erscheint nach der Betätigung der rechten Maustaste auf dem Typenverezichnis. In den ersten drei Angebotstellen werden die voreingestellten Typen dargestellt - durch das Anhaken wird der ausgewählte Typ in das Typenverzeichnis überführt. Es sind folgende Stellen: "Alle Dateitypen" - Einschaltung der Kontrolle aller ausgewählten Dateien, "Ausführbare"- Kontrolle der anlaufbaren Dateien (einschl. Bibliotheken) und "OLE-Dokumente" - Einschaltung der durch die OLE-Technologie geschaffenen Dokumente. Wird das Anhaken aufgehoben, werden die Dateientypen automatisch im Verzeichnis der zu überprüfenden Typen gelöscht.

Auch Typen aus der Databasis der bekannten Typen können in das Typenverzeichnis eingefügt werden. Dazu dient die Funktion "Typen durchgehen..." im Lokalangebot. Nach der Wahl dieser Funktion wird das die Databasis aller bekannten Dateientypen enthaltende Dialog angezeigt (Abb. 43). Diese Databasis kann entweder die wichtigsten Dateientypen erfassen oder kann nach dem Anhaken des Feldes "Alle Erweiterungen anzeigen" gesamte bekannte Dateientypen erfassen. Will man einen Dateientyp zu dem Verzeichnis der zu überprüfenden Dateinen einfügen, wird dieser Typ zuerst aktiviert und dann wird die "OK"-Taste betätigt. Das Betätigen der "Abbrechen"-Taste schließt das Dialog und das Verzeichnis bleibt ungeändert.

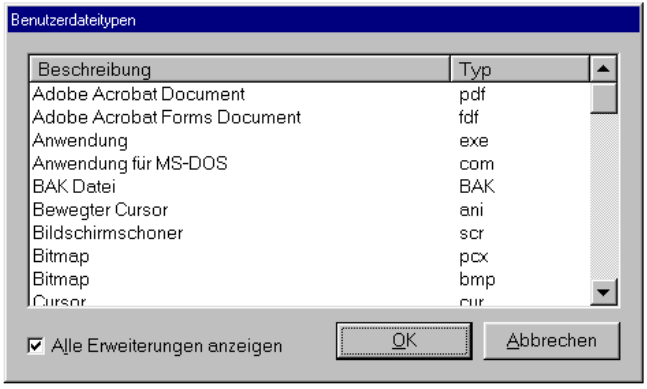

Abb. 43

Die Funktion "Muster Einfügen" dienr der direkten Eingabe des Typs der kontrollierten Dateien. Nach der Wahl dieser Funktion kann der Nutzer das Typsuffix eingeben - das Suffix kann auch Vertretezeichen "*" (Sternchen) und "?" (Fragezeichen) beinhalten. Nach der Eintragung und Bestätigung durch den "Enter"-Tastaturknopf wird der neue Typ zum Verzeichnis zugeordnet.

Neben der Bezeichnung der kontrollierten Datei befindet sich eine Ikone, die die Art der Arbeit mit dem Datentyp anzeigt:

- Dateien diesen Typs werden kontrolliert werden. Auf diese Weise werden alle neu zugefügten Dateien implizit bezeichnet , einschließlich der vorgewählten Dateien,
- auf diese Weise bezeichnete Dateientypen werden nicht kontrolliert werden. Dem Programm kann man befehlen, daß es z.B. "Alle Dateitypen" außer der TXT-Dateien kontrollieren soll. Die Typnebezeichnung wird durch das Anhaken der Stelle "Typen nicht testen" im Lokalangebot durchgeführt. Die voreingestellten Typen können nicht aus der Kontrolle ausgenommen werden.

Wenn die Überprüfung eines Typs nicht stattfinden soll und er als socher im Verzeichnis bezeichnet wird, kann eine geringe Verlangsamung des Aufgabenablaufes die Folge sein. Das Programm überprüft nicht nur, ob eine Datei vom solchen Typ kontrolliert werden soll, sondern auch ob sie aus der Kontrolle ausgenommen werden soll. Andererseits kann durch die Ausnahme eines Dateientyps aus der Kotrolle der Aufgabenablauf wesentlich beschleunigt werden. Die konkrete Situation ergibt sich aus dem Muster der kontrollierten Dateien, im allgemeinen kann gesagt werden, daß wegen z.B. der Kontrolle einer zusätzlichen Datei lohnt es sich nicht, ihren Typ aus dem Verzeichnis der kontrollierten Typen auszunehmen.

Bei der Durchführung einer Aufgabe wird bei jeder gewählten Datei zunächst ihr Typ geprüft. Ist der Typ in der Liste auf dieser Seite aufgeführt

und mit einer gelben Kugel bezeichnet, werden alle gewählten Vorgänge mit diesem Programm durchgeführt. Sonst wird die Datei einfach umgesprungen. Als Standard ist die Prüfung der Programme (bzw. der durchführbaren Dateien) und OLE Dokumente eingestellt.

Bei der Aufgabendurchführung wird bei jeder ausgewählten Datei zuerst ihr Typ überprüft. Wenn dieser Typ im Verzeichnis dieser Seite angeführt ist und durch einen grünen Punkt gekennzeichnet ist, werden mit ihm alle gewählten Tätigkeiten durchgeführt. Ansonsten wird die Datei einfach übersprungen werden. Implizuit ist die Überprüfung aller Dateientypen eingestellt.

Wenn die Aufgabe residente Blöcke durchführen wird, werden nur solche Dateienoperationen kontrolliert, derer Typ auf dieser Seite angeführt wird. Die Stellen "Alle Dateitypen", "OLE-Dokumente" und Typen, die ausgenommen werden sollen (d.h. die mit einem roten Punkt bezeichnete Typen) werden nicht wahrgenommen werden, d.h. daß ihre Anwesenheit im Verzeichnis gar keinen Einfluß auf die residenten Blöcke haben wird.

4.4.5 Seite "Bereiche"

Diese Seite ermöglicht dem Nutzer einzustellen, welche Platten, bzw. Mappen sollen durch die neu zu erstellende Aufgabe kontrolliert werden (Abb. 44). Auf diese Weise können ganz genau nur die zu kontrollierenden Mappen ermittelt werden und der Aufgabenablauf beschleunigt werden, da die nicht zu kontrollierenden Mappen übersprungen werden.

Abb. 44

Alle kontrollierten Bereiche oder Mappen werden im Verzeichnis auf dieser Seite dargestellt. Bereiche können über das Lokalangebot eingefügt werden.Das Lokalangebot beinhaltet vorgewählte Bereiche "Alle Platten", "Laufwerk A:", "Andere Laufwerke", "Lokale Festplatten", "Laufwerke entfernen" und "Im Lauf einfügen". Die letzte Stelle bedeutet, daß der Benutzer vor dem Beginn der eigenen Aufgabe nach weiteren zu kontrollierenden

Stellen gefragt wird, die gemeinsam mit den im Verzeichnis angeführten Stellen kontrolliert werden. Durch das Anhaken dieser Stelle im Lokalangebot wird diese auch im Verzeichnis der untersuchten Bereiche angezeigt.

Durch die Nutzung der Anhakstelle "Prozeßunterverzeichnis" im Lokalangebot kann ermittelt werden, ob in dem ausgewählten Bereich auch alle verdeckten Mappen untersucht werden sollen. Ist die Stelle nicht angehakt, werden nur Dateien in der ausgewählten Mappe oder Platte kontrolliert, eventuelle verdeckte Mappen werden nicht kontrolliert werden. Diese Stelle kann auch für jeden untersuchten Bereich einzeln eingestellt werden. Implizit ist die Untersuchung der verdeckten Mappen erlaubt.

Neben dem Namen des kontrollierten Bereichs befindet sich eine Ikone, die die Art der Arbeit mit dem Bereich darstellt:

- der Bereich wird kontrolliert werden. Auf diese Weise werden alle neu eingefügten Bereiche, einschl. der voreingestellten implizit bezeichnet,
- die auf dise Weise gekennzeichneten Bereiche werden nicht kontrolliert werden. Dem Programm kann man befehlen, daß es z.B. "Lokale Festplatten" **außer** der Mappe "C:\Bekannte_Viren" u.ä. kontrollieren soll. Die Typenbezeichnung wird durch das Anhaken der Stelle "Bereich nicht testen" im Lokalangebot durchgeführt. Die voreingestellten Bereiche können nicht aus der Kontrolle ausgenommen werden.

Die Funktion des Lokalangebotes "Bereiche durchgehen" dient der direkten Auswahl von Mappen oder Platten, die untersucht werden sollen. Nach ihrer Bestätigung erscheint ein standartes Dialog, das auch eine gleichzeitige Wahl von mehreren Mappen ermöglicht. Die in diesem Dialog gewählten Mappen werden dem Verzeichnis beigefügt.

Die Funktion "Muster einfügen" dient der direkten Bereichseingabe aus der Tastatur. Nach der Eingabe wird dem Verzeichnis der kontrollierten Bereiche die Stelle "Bereichbezeichnung eingeben..." beigefüft und ihre Aufbereitung wird ermöglicht. Nach der Bereicheingabe die "Enter"-Taste betätigen. In der Bereichsbeziechnung können auch Vertreterzeichen "*" (Sternchen) und "?" (Fragezeichen) angewendet werden und auf diese Weise mehrere Mappen spezifiziert werden.

Will man einen Bereich aus dem Verzeichnis beseitigen, wählt man zuerst diesen Bereich mit der linken Maustaste und dann betätigt man die "Del"-Taste in der Tastatur. Die vorausgewähltten Bereiche können aus dem Verzeichnis auch durch die Annullierung des Anhakens im Lokalangebot beseitigt werden.

Die Seite "Typen" ist nur dann vorhanden, wenn die Virensuche oder der Datenintegritätstest erlaubt sind, sei es in der normalen oder in der vereinfachten Form.

4.4.6 Seite "Allgemeines"

Diese Seite beinhaltet Bedienungselemente von solchen Parametern, die aufgrund ihrer Charakteristik nicht zu einer anderen Seite zugeordnet werden können (Abb. 45).

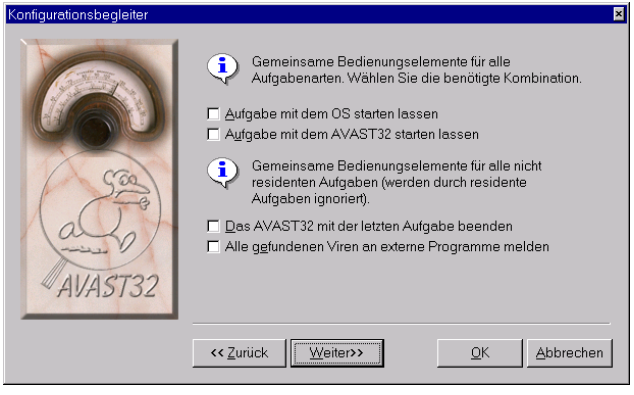

Abb. 45

Durch das Anhaken des Feldes "Aufgabe mit dem OS starten lassen" teilt der Benutzer dem Programm mit, daß die zu erstellende Aufgabe gleich nach der Benutzeranmeldung angelaufen werden soll. Implizit wird dieses Feld nicht angehakt. Wenn die Aufgabe eine gemeinsam genutzte Aufgabe ist, wird diese Aufgabe für jeden Benutzer des gegebenen Rechners nach seiner Anmeldung im System angelaufen werden.

Das Anhakfeld "Aufgabe mit dem AVAST32 starten lassen" schaltet die Aufgabe automatisch nach dem Anlauf des AVAST32-Programms ein. Wenn die Aufgabe eine gemeinsam genutzte Aufgabe ist, wird sie automatisch für alle Benutzer anlaufen, ansonsten wird sie nur für den Benutzer anlaufen, der sie erstellt hat. Der Aufgabenanlauf gemeinsam mit dem AVAST32-Programm ist implizit ausgeschaltet.

Die folgenden zwei Anahkfelder haben Einfluß nur auf die nicht residenten Aufgaben, d.h. die die Virensuche oder den Integritätstest (normal oder vereinfacht) beinhaltenden Aufgaben. Ihre Einstellung wird durch die residenten Aufgaben ingnoriet werden.

Das Anhakfeld "Das AVAST32 mit der letzten Aufgabe beenden" schaltet eine automatische Beendigung des AVAST32-Programms nach der Beendigung der letzten laufenden Aufgabe ein. Die Ausnutzung dieser Möglichkeit ist vor allem bei solchen Aufgaben vorteilhaft, die anders als direkt aus dem AVAST32-Programm eingeschaltet werden, z.B. mit der Hilfe eines Vertreters auf der Arbeitsfläche. Das Feld wird nicht implizit angehakt.

Das Anhakfeld "Alle gefundenen Viren an externe Programme melden" ermöglicht dem Benutzer einzustellen, ob externe Programme (d.h. Programme, die nicht ein Bestandteil des AVAST32-Programms sind) über den ersten gefundenen Virus während einer Aufgabe (das Feld wird nicht angehakt) oder über alle gefundenen Viren (das Feld wird angehakt) informiert werden sollen. Implizit wird das Feld nicht angehakt. Nähere Informationen über das Informationssystem der externen Programme über die gefundenen Viren werden in der Anlage F.1. beschrieben.

Die Seite "Allgemeines" ist bei jeder Variate der zu erstellenden Aufgabe vorhanden.

4.4.7 Seite "Virensuche"

Eine der wichtigsten Tätigkeiten des AVAST32-Programms ist die Suche nach bekannten Viren. Diese Seite (Abb. 46) dient der Einstellung des Programmbstendteiles des AVAST32-Programms, das für die Virensuche verantwortlich ist.

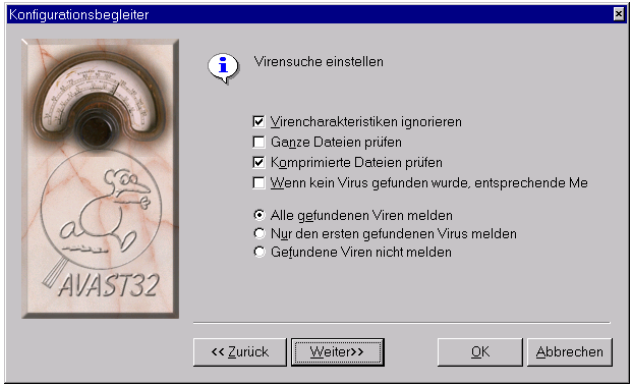

Abb. 46

Durch das Anhakfeld "Arbeitsspeicher testen" kann der Benutzer einstellen, ob bei der Virensuche auch der Arbeitsspeicher des Rechners untersucht werden soll. Auf diese Weise kann man einen Virus entdecken, der den Rechner schon befallen hat. Implizit wird die Untersuchung des Arbeitsspeichers durchgeführt.

Unter dem Operationssystem Windows NT, durch seinen Aufbau bedingt, hat der Test des Arbeitsspeichers keine Bedeutung. Deswegen wird bei der Arbeit unter diesem Operationssystem keine solche Möglichkeit angeboten. Die Seite "Virensuche" für das Operaionssystem Windows NT beinhaltet kein Anhakfeld "Arbeitsspeicher testen".

Das Anhakfeld "Virencharakteristiken ignorieren" dient der Einschaltung der Kontrolle der Dateien nach der Virenanwesenheit in der Databasis. Wenn das Feld nicht angehakt wird, werden die Dateien nur nach den Viren untersucht, die den gegebenen Dateientyp befallen. D.h. daß eine COM-Datei nicht nach der Anwesenheit solcher Viren untersucht wird, die nur EXE-Dateien befallen u.ä.

Durch das Anhaken dieses Feldes wird gewährleistet, daß Dateien nach Viren untersucht werden, ohne Berücksichtigung des Dateientyps, der durch diese Viren befallen wird. Implizit wird das Feld angehakt.

Da Anhakfeld "Ganze Dateien prüfen" bestimmt, ob ganze Dateien anch Viren untersucht werden sollen. Wenn das Feld nicht angehakt ist, wird das AVAST32-Programm nur einige Dateibereiche kontrollieren. Das ist für die Aufgabengeschwindigkeit vorteilhaft. Das Programm geht dabei davon aus, daß die Mehrheit von Viren am Dateienende auftaucht oder ihren Beginn löscht, so daß die Überprüfung der ganzen Datei überflüssig ist. Das Feld wird implizit angehakt.

Durch das Anhakfeld "Komprimierte Dateien prüfen" kann die Kontrolle komprimierter dateien eingeschaltet werden. Komprimierte Dateien können in zweirlei Arten infiziert werden: vor und nach der Komprimierung. Wenn die Datei erst nach der Komprimierung befallen worden ist, wird sie durch das AVAST32-Programm ohne die Notwendigkeit der Dekomprimierung entdeckt . Damit ein Virus, der eine Datei vor der Komprimierung befallen hat, entdeckt werden kann, muß die Datei zuerst dekomprimiert und dann kontrolliert werden.

Nach dem Feldanhaken werden zuerst die kompromierten Dateien durch das AVAST32-Programm kontrolliert, dann werden diese Dateien intern dekomprimiert (Dateien bleiben auf der Platte im komprimierten Zustand) und das Ergebnis wird nochmals kontrolliert.

Das AVAST32-Programm unterstützt zur Zeit die Koprimierungsprogramme Diet, Lzexe, Pklite und Ice. Die Prüfung der komprimierten Dateien wird implizit erlaubt.

Abb. 47

Das Abhaken des Feldes "Informationen abbilden, wenn kein Virus gefunden wurde" verursacht, daß AVAST32 eine Meldung über das Be-

enden der Virussuche auch in dem Fall abbildet, wenn kein Virus gefunden wurde, (Abb. 47). Diese Möglichkeit ist in der standarden Einstellung ausgeschaltet.

Weiter kann gewählt werden, ob man über das Finden eines Viren informiert werden will. Die Auswahl wird duch die Wahl von einem der folgenden Schalter durchgeführt:

- die Wahl des Schalters "Alle gefundenen Viren melden" verusacht, daß das AVAST32-Programm für jeden gefundenen Virus eine Warnmeldung abgibt (Kapitel 5.4) und die Benutzerreaktion abwartet,
- Schalter "Nur den ersten gefundenen Virus melden" schaltet die Anzeige der Warnmeldung wie in dem vorhergehenden Fall ein, aber nur für den ersten gefundenen Virus. Wenn der Benutzer eine Information darüber braucht, ob sein Rechner durch Viren befallen wurde oder nicht, kann es günstig sein, diesen Schalter zu wählen. Wenn man nach der Testbeendigung alle infizierten Dateien ermitteln muß, kann man nur die Seite "Ergebnisse" der erweiterten Bedienung durchgehen,
- Schalter "Gefundene Viren nicht melden" dient der Unterdrückung der Anzeige von Warnmeldungen. Ist dieser Schalter gewählt worden, wird der Benutzer über keinen der gefundenen Viren informiert werden. Weil hier die Gefahr des Übersehens eines Viren im Systems besteht, wird diese Möglichkeit in Wechselwirkung z.B. mit der Meldung über das Finden eines Viren bei der Benutzeranmeldung empfohlen (Kapitel 6.5.1, Anhakfelder "Virenmeldung nach Anmeldung anzeigen").

Seite "Virensuche" ist nur dann erreichbar, wenn die Aufgabe Viren suchen soll, d.h. die Tätigkeit der Virensuche auf der Seite "Test" gewählt worden ist (siehe Kapitel 4.4.2).

4.4.8 Seite "Integrität"

Diese Seite dient der Einstellung der Parameter für die Prüfung der Datenintegrität auf den Rechnerplatten (Abb. 48). Unter dem Begriff des Datenintegritätstests kann man die Überwachung von Änderungen verstehen, die seit der letzten Kontrolle aufgetreten sind. Der Benutzer kann auf diese Weise Virentätigkeit entdecken, einschl. der Tätigkeit von noch unbekannten Viren.

Abb. 48

Durch das Anhaken des Feldes "Attribut ARCHIVE ingnorieren" wird das Programm informiert, daß es eine Änderung des ARCHIVE-Attributes in den kontrollierten Dateien ignorieren soll. Dieses Attribut wird vor allem durch Sicherstellungsprogramme zur Unterscheidung der zu archivierenden Datien angewendet. Das Operationssystem stell dieses Attribut bei jeglicher Dateieintragung ein.

Wenn das Feld angehakt ist, wird die Integritätsprüfung keine Änderung dieses Attributes melden, d.h. daß eine Datei, bei der seit der letzten Kontrolle nur das Attribut ARCHIVE geändert worden ist, nicht in das Verzeichnis der geänderten Dateien eingetragen wird. Dieses Feld ist nicht implizit angehakt.

Das Anhakfeld "Dateieninhalt nicht testen" kann die Prüfung der Änderung der Dateieninhalte verbieten.Dateien werden dann nur nach Parametern wie das Datum der letzten Änderung, Größe, Attribute usw. untersucht, es werden aber keine Kontrollsummen des Dateieninhalts durchgeführt. Durch das Anhaken wird der Aufgabenablauf beschleunigt. Wir empfehlen jedoch aus den Gründen der Sicherheit ihres Systems, die Prüfung der Dateieninhalte eingeschaltet lassen. Der Dateieninhalt wird implizit kontrolliert.

Durch das Anhakfeld "Dateieninhalt nur bei Zustandsänderung testen" kann der Benutzer so einstellen, daß der Dateieninhalt nur dann geprüft wird, wenn es zu einer Änderung der grundlegenden Dateieigenschaften kam (Attribute, Datum der letzten Änderung u.ä.). Diese Möglichkeit geht von der Voraussetzung aus, daß wenn eine Manipullieung mit dem Dateiinhalt vorliegt, wurden auch die Dateiparameter geändert. Durch das Feldanhaken kann man den Aufgabenablauf bechleunigen. Das Feld wird implizit nicht angehakt.

Diese Seite wird nur dann vorhanden sein, wenn eine von den durchzuführenden Tätigkeiten die Datenintegritätsprüfung ist, in ihrer normalen oder vereinfachten Form (siehe Kapitel 4.4.2).

4.4.9 Seite "Fortfahren"

Seite "Fortfahren" ermöglicht dem Benutzer, die Aufgabe auszuwählen, die nach der Beendigung der gerade erstellenden Aufgabe gestartet werden soll (Abb. 49).

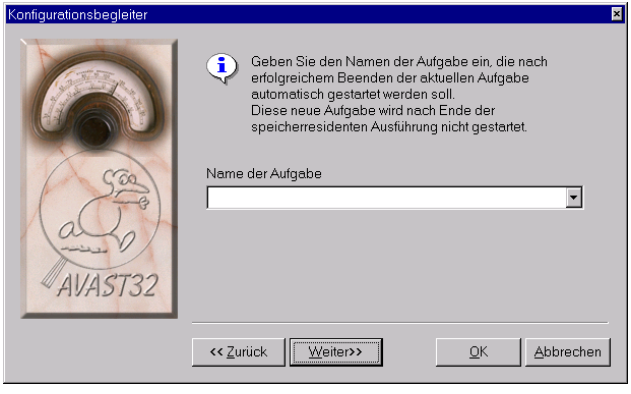

Abb. 49

Es ist notwendig den Namen einer solchen Aufgabe in das Textfeld "Name der Aufgabe" einzutragen oder die Möglichkeit besteht, ihn aus der Liste der bisher erstellten Aufgaben auszuwählen. Die Aufgabenliste erscheint nach dem Klopfen mit der linken Maustaste auf den Pfeil rechts vom Textfeld. In standarder Einstellung enthält das Textfeld keinen Aufgabennamen.

Die Seite "Fortfahren" ist nur für nonresidente Aufgaben zugreifbar, d.h. wenn auf der Seite "Test" mindestens ein nonresidenter Vorgang ausgewählt wurde.

4.4.10 Seite "Bericht"

Während der Aufgabendurchführung kann durch das AVAST32-Programm eine Datei mit einem detaillierten Bericht über ihre Tätigkeit und Ergebnisse zusammengestellt werden. Die Erlaubnis der Zusammenstellung dieses Berichtes und die Einstellung des Berischtsnamens werden in der Seite "Bericht" enthalten (Abb. 50). Der Bericht über den Aufgabenverlauf wird in der Gestalt eines reinen ASCII-Texts in die gewählte Datei eingetragen (siehe weiter). Er beinhaltet Informationen über die kontrollierten Dateien, über die gefundenen Viren und weitere wichtige Informationen, einschl. Statistiken der Dateienprüfung.

Das Anhakfeld "Bericht konfigurieren" schaltet die Erstellung der Datei mit dem Bericht über die Aufgabentätigkiet ein. Die Berichtsdatei wird implizit erstellt.

Unter dem vorhergehenden Bedienungselement befindet sich ein Textfeld, in das die Mappe und die Dateibezeichnung eingetragen werden können, in die der Bericht eingetragen wird. Wird durch den Benutzer anstelle einer Bezeichnung "*" (Sternchen)

eingegeben, wird die Berichtsdatei die gleiche Bezeichnung wie die Aufgabe haben - sie bekommt nur das Suffix RPT. Befindet sich in der Dateibezeicnung kein Suffix, wird automatisch das RPT-Suffix angewendet. Das Textfeld beinhaltet implizit das "*"-Zeichen.

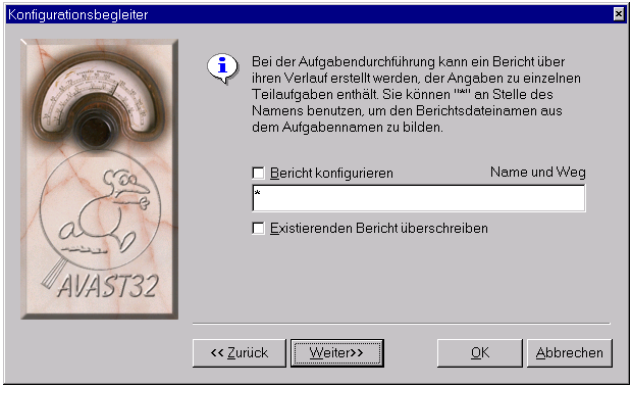

Abb. 50

Das Anhakfeld "Existierenden Bericht überschreiben" sagt dem Programm, daß wenn schon eine Berichtdatei unter der gegebenen Bezeichnung besteht, sollte sie überschrieben werden. Wenn das Überschreiben nicht erlaubt ist und eine Berichtsdatei schon besteht, wird der Bericht über die Tätigkeit dieser Aufgabe zu der schon bestehenden Datei eingefügt. Das Feld ist implizit nicht angehakt.

Diese Seite ist nur in dem Fall zugänglich, wenn die Aufgabe mindestens eine nicht residente Tätigkeit, d.h. mindestens die Virensuche oder den Datenintegritätstest beinhaltet.

4.4.11 Seite "Netzwarnung"

Diese Seite beinhaltet Bedienungselemente für die Einstellung von Parametern für die Sendung von Warnmeldungn im Netz (Abb. 51). Das AVAST32-Programm ermöglicht, wenn ein Virus gefunden wurde, eine Warnmeldung über die drohende Gefahr an die duch das Lokalnetz erreichbaren Rechner zu versenden und auf diese Weise eine Virenverbreitung zu vermeiden.

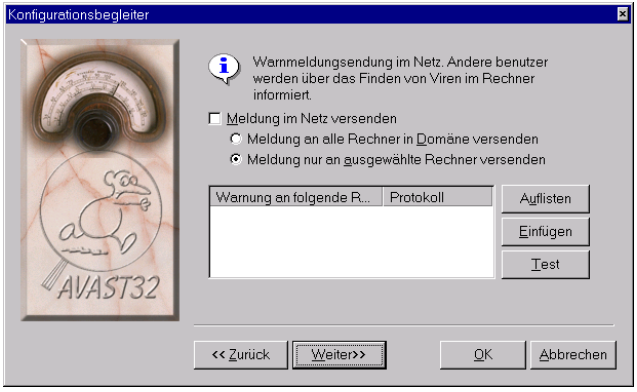

Abb. 51

Das Anhakfeld "Meldungen im Netz versenden" schaltet die Versendung einer Warnmeldung mittels des Netzes ein. Die Warnmeldungsversendung im Netz wird nicht implizit erlaubt.

Wurde die Warnmeldungsversendung im Netz erlaubt, muß man weiter bestimmen, an welche Rechner die Warnmeldung versendet werden soll. Dazu kann einer der fogenden Schalter verwendet werden:

- Schalter "Meldungen an alle Rechner in Domäne versenden" stelt die Versendung der Warnmeldung über die Virenanwesenheit an alle Rechner ein, die im gegebenen Moment zur aktuellen Domäne angeschaltet werden,
- Schalter "Meldungen nur an ausgewählte Rechner versenden" bewirkt, daß die Meldung nur an Rechner versendet wird, die im Verzeichnis dieser Seite erfaßt werden.

Implizit ist die Warnmeldungsversendung nur an gewählte Rechner eingestellt.

Ist die Warnmeldungsversendung im Netz erlaubt worden und die Warnmeldung nur an gewählte Rechner versendet werden soll, müssen diese Rechner bestimmt werden. Das Verzeichnis der ausgewählten Rechner befindet sich unter den angegebenen Bedienungselementen.

Der Computer, auf den die Meldung über den Virusfund geschickt werden soll, kann durch das direkte Eintragen seines Namen in die Liste der ausgewählten Computer gewählt werden. Durch die Betätigung der Taste "Einfügen" wird das Lokalmenü mit einigen Protokollen abgebildet:

- Das Element "Internet" bestimmt, daß der Computer, auf den die Warnmeldung geschickt werden soll, durch eine standarde URL Adresse gekennzeichnet ist. Für die Meldungszustellung wird das Internetprotokoll ausgenutzt,
- durch das "Microsoft" Element teilen Sie dem Programm mit, daß der Computer über die Post von Microsoft Exchange zugreifbar ist,
- das Element "Intern" heißt, daß für den Zugriff in den ausgewählten Computer ein Protokoll für das

lokale Netz besteht (der Computer muß selbstverständlich über das Lokalnetz zugreifbar sein).

Nach der Wahl des Protokolls wird das Element mit dem Namen "Gültige Rechnerbezeichnung angeben !!" hinzugefügt. Wenn Sie auf es mit der linken Taste klopfen, wird seine Bearbeitung ermöglicht. Nach der Eintragung des Computernamens drücken Sie die Taste "Eingabe".

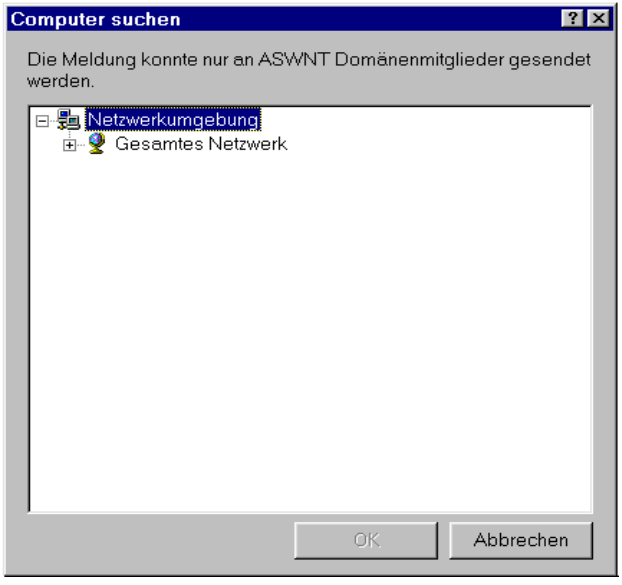

Abb. 52

Nach dem Drücken der Taste "Auflisten" erscheint erneut das Lokalmenü mit den Protokollen (gegenwärtig enthält es nur das Element "Intern", siehe oben). Der Computer, der durch das Lokalnetz zugreifbar ist, kann mittels Dialog, dargestellt in der Abb. 52, gewählt. Suchen Sie nacheinander alle Netzteile durch, bis Sie den gewünschten Computer finden. Sie reihen ihn in die Liste der gewählten Computer ein, indem Sie ihn zunächst markieren und dann die Taste "OK" drücken. Durch das Drücken von "Abbrechen" werden Sie das Dialog schließen und die Computerliste bleibt ohne Änderung.

Sie können den Computer von der Liste entfernen, indem Sie ihn zunächst aktivieren und dann die Taste "Del" drücken.

Die Elementenparameter in der Liste, bzw. den gewählten Computer, kann man nachträglich ändern. Wenn Sie das Zugriffsprotokoll für den gegebenen Computer ändern wollen, klopfen Sie in die Spalte "Protokoll" des entsprechenden Computers. Aus dem Lokalmenü wählen Sie dann ein neues Protokoll aus. Auf eine ähnliche Weise verändern sie auch den Namen oder die Adresse des Computers: nach dem Klopfen mit der linken Maustaste wird Ihnen seine Bearbeitung ermöglicht.

Ist man sich mit der Ankunft der Warnmeldung nicht sicher, kann die Verbindung durch Betäti-

gung der "Test"-Taste überprüft werden. An jeden ausgewählten Rechner wird dann eine Testmeldung versendet.

Wenn Sie im Operationssystem Windows NT arbeiten, müssen Sie die Dienste "Alerter" und "Alerter" angelaufen haben (die Mappe "Systemsteuerung", das Element "Services"), so daß Netzmeldungen absgeendet und empfangen werden können. Wenn Sie über die dazu notwendige Rechte nicht verfügen, nehmen Sie Kontakt mit Ihrem Netzadministrator auf. Wenn Sie unter Windows 95 arbeiten und wollen, daß die Sendung von Warnmeldungen über das Netz arbeitet, muß das Programm "WinPopup" angelaufen werden.

Eine Warnmeldung kann an den gewähleten Rechner auch mehrmals versendet werden. Es handelt sich um keinen Programmfehler, sondern um eine Systemangelegenheit. Die Anzahl der abgesendeten Kopien hängt von der Anzahl der installierten Netzprotokolle ab.

Diese Seite ist bei jeder variante der zu erstellenden Aufgabe vorhanden.

4.4.12 Seite "Meldung"

Diese Seite dient der Aufbereitung des Textes der Meldung, die beim Finden von Viren angezeigt wird (Abb. 53). Ist die Meldungsversendung im Netz erlaubt, wird diese Meldung auch an alle ausgewählten Rechner versendet (sieh Kapitel 4.4.11).

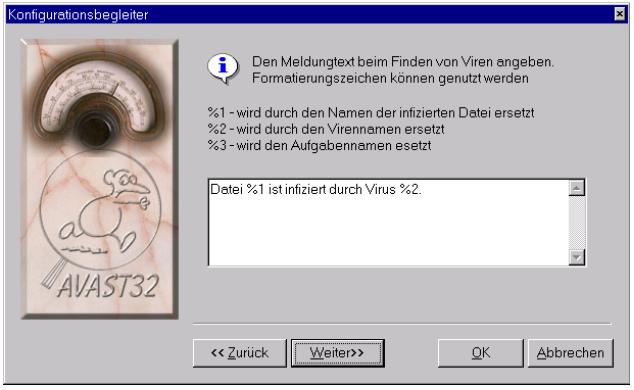

Abb. 53

Ein Textfeld steht zur Verfügung, das die Eintragung des eigenen Textes der Meldung ermöglicht. Mit Hilfe von Formatierungszeichen können auch variable Parameter eingegeben werden, wie z.B. die Dateibezeichnung, die Aufgabenbezeichnung. Das jeweilige Formatierungszeichen wird dann durch die gegebene Bezeichnung ersetzt. Die Bedeutung der Formatirungszeichen ist folgend:

%1 - Bezeichnung der infizierten Datei,
%2 - Virenbezeichnung,

%3 - Bezeichnung der Aufgabe, die den Virus endeckt hat.

Wenn z.B. durch die Aufgabe "Eigene" der Virus "OneHalf" in der Datei "D:\PRG.EXE" gefunden wurde und das eingegebene Text folgende Gestalt haben wird:"Achtung! Virus%2 wurde in Datei %1 gefunden. Aufgabe %3 benutzt.", wird die Ergebnismeldung folgende Gestalt haben: “Achtung! Virus OneHalf wurde in Datei D:\PRG.EXE gefunden. Aufgabe Eigene benutzt."

Das Textfeld enthält implizit eine Meldung in der folgenden Gestalt:

Datei %1 ist infiziert durch Virus %2.

Die Seite "Meldung" ist nur dann anwesend, wenn sie ein der gewählten Vorgänge der Aufgabe und auch der Virensuche ist.

4.4.13 Seite "Klang"

Das Finden eines Virus kann das Programm AVAST32 auch durch einen Klang offenbaren. Wenn Sie diese Möglichkeit ausnützen wollen, dann drücken Sie die Taste "Setup" auf der Seite "Klang" (Abb. 54) und stellen Sie in dem abgebildeten Dialog den entsprechenden Klang ein (eine detaillierte Beschreibung ist weiter gegeben).

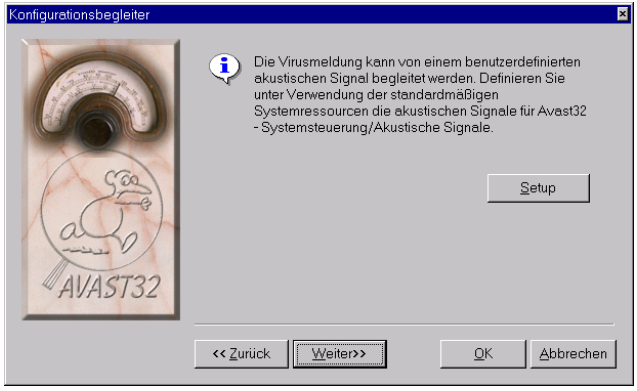

Abb. 54

Das Programm AVAST32 benutzt für die Einstellung der Audioparameter der Meldung über den Virusfund die Systemsteuerung "Akustische Signale" (Abb. 55).

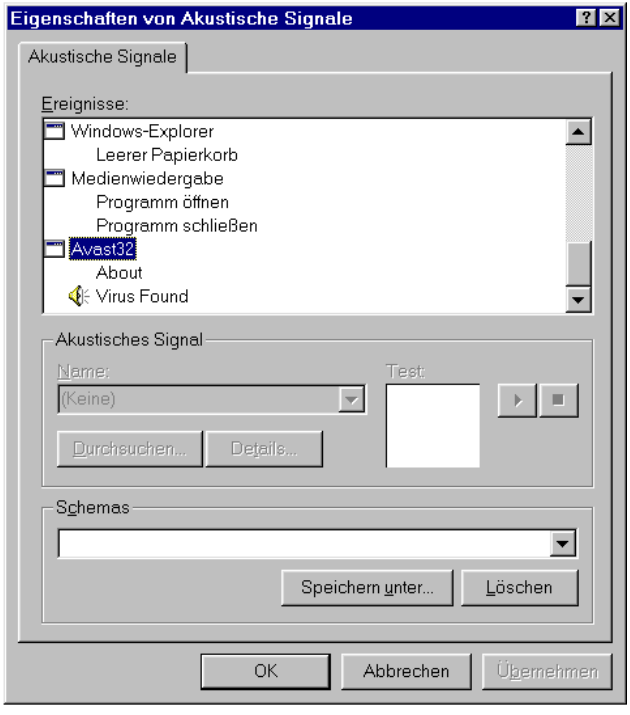

Abb. 55

Zunächst finden Sie das Element "Avast32" in der Liste "Ereignisse" und markieren Sie sein Subelement "Virus gefunden".

Die Mappe und den Dateinamen mit dem Klang können Sie entweder direkt in das Textfeld eintragen oder sie mit Hilfe von Standarddialog für die Öffnung der Dateien auswählen. Das Dialog wird nach dem Drücken der Taste "Durchsuchen ..." abgebildet. Eine ähnliche Beschreibung dieses Dialogs ist im Handbuch oder in der Hilfe des Operationssystems aufgeführt.

Die entsprechende Klangdatei kann auch aus dem Menü ausgewählt werden, das nach dem Drücken des Pfeils neben dem Textfeld "Name:" erscheint.

Klänge des AVAST32 Programms für verschiedene Ereignisse können mittels Systemsteuerung "Akutische Signale" eingestellt werden auch wenn das AVAST32 Programm nicht läuft - siehe Kapitel 6.7.3.

Damit die Datei auf Ihrem Computer gespielt werden kann, muß Ihr Computer mit einer Audiokarte und mit entsprechenden Treibern versehen werden! Bloße Anwesenheit der Audiokarte und ihrer Treiber im Computer genügt allerdings nicht! Es ist notwendig, daß die Karte sowie die Treiber richtig installiert werden und arbeiten. Wenn Ihr Operationssystem die Klänge spielt (z.B. beim Start, wenn sie nicht ausgeschaltet sind), werden diese Klänge auch vom AVAST32 Programm problemlos wiedergegeben!

Die Seite "Klang" ist anwesend, wenn für die entsprechende Aufgabe einer der folgenden Vorgän-

ge ausgewählt wurde: Virensuche, Überwachung des Boot-sektors oder die residente Überwachung.

4.4.14 Seite "Überwachung"

Diese Seite beinhaltet Bedienungselemente, die einer näheren Bestimmung der Dateien dienen, die vor ihrem Anlauf kontrolliert werden müssen (Abb. 56). In der letzten Zeit ist ein neuer Virentyp entdeckt worden, der nicht die anlaufbaren Dateien oder die Bootsektore der Platten, sonder neu dattierte Dateien, konkret die OLE-Dokumente, angreifen. Es sind Makroviren. Das AVAST32-Programm enthält die Möglichkeit einer laufenden Prüfung auch von den zu öffnenden OLE-Dokumneten. Durch die Einschränkung der Anzahl der kontrollierten Dateien kann das Anlaufen der einzelnen Programme und das Öffnen der OLE-Dokumente beschleunigt werden.

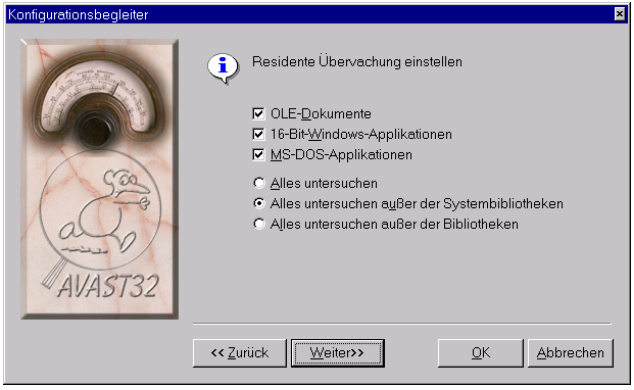

Abb. 56

Bei jedem Versuch, ein Programm zu starten oder ein Dokument zu öffnen, werden diese durch das AVAST32-Programm untersucht, ob sie durch einen bekannten Virus infiziert worden sind oder nicht. Wenn kein Virus entdeckt wird, wird die Datei gestartet, im engegengesetzten Fall wird der Benutzer infomiert. Dateien, die OLE-Dokumente enthalten, werden nur dann kontrolliert, wenn sie mittels der OLE-Funktionen geöffnet werden. Daraus ergibt sich, daß es zu einer schwachen Verlangsamung der Geschwindigkeit nur beim Anlaufen der kontrollierten Applikation oder bei der schon erwähnten Öffnung der OLE-Dokumente kommen kann - nicht bei der eigenen Arbeit mit der schon

angelaufenen Applikation oder mit dem geöffneten Dokument.

Man kann OLE-Dokumente, 16-bit-Applikationen für Windows 3.1, Applikationen des MS-DOS und 32-bit-Programme kontrollieren. Ob der entsprechende Dateientyp kontrolliert wird, wird durch das Anhaken des entprechenden Feldes bestimmt. 32-bit-Applikationen (d.h. Applikationen für die Operationssysteme Windows 95 und NT) werden immer kontrolliert. Man kann eine beliebige Kombination der überwachten Programme bestimmen. Implizit sind alle Stellen angehakt.

Weiter kann der Benutzer bestimmen, ob beim Programmstart alle seine Dateien geprüft werden, d.h. einschl. Bibliotheken, oder alle Dateien mit der Ausnahme von Systembibliotheken oder alle Dateien mit der Ausnahme von Bibliotheken. Die Auswahl erfolgt durch die Wahl von einem der angezeigten Schalter.

Die Wahl der Einstellung hat einen großen Einfluß auf die Geschwindigkeit des Applikationsanlaufs, vor allem wenn immer gleiche Bibliotheken benutzt werden. Wenn also eine regelmäßige Prüfung des Systems erfolgt, ist aus der Sicht der Geschwindigkeit die Ausschaltung von Systembibliotheken vorteilhaft. Im Gegenteil, wenn ein Programm mit unbeknanntem Ursprung installiert werden soll, wird die Einschaltung der Kontrolle von allen anlaufbaren Dateien, einschließlich Bibliotheken, empfohlen.

Die Kontrolle durchaus aller durchführbaren Dateien ist als vorgegeben eingestellt, inbegriffen der Bibliotheken mit der Ausnahme von Systembibliotheken.

Die Seite "Überwachung" ist nur in dem Fall vorhanden, wenn zu den Aufgabentätigkeiten auch die Überwachung der gestarteten Programme gehört (siehe Kapitel 4.4.2).

4.4.15 Seite "Residente Blöcke"

Diese Seite beinhaltet Bedienungselemente für die Einstellung von einer weiteren möglichen Aufgabentätigkeit, die in der Blockierung potentiell gefährlicher Operationen besteht (Abb. 57). Bei jedem Versuch um die Durchführung von einer solchen Operation wird der Benutzer benachrichtigt und Operation wird nur mit seiner Einverständnis durchgeführt.

Abb. 57

Bei diesem Herangehen kann der Benutzer oft durch überflüssige Fragen gestört werden. Das AVAST32-Programm bietet also die Möglichkeit, nur die zu überwachenden Operationen zu wählen.

Das Anhaken des Feldes "DOS-Dateioperationen" wird bewirken, daß das AVAST32-Programm alle potentiell gefährliche Dateienoperationen kontrollieren wird, die die für das Operationssystem MS-DOS bestimmte Applikationen auszuführen versuchen.

Das Anhakfeld "Windows-Dateioperationen" dient der Einschaltung der Kontrolle von potentiell gefährlichen Dateienoperationen, die die für die Operationssysteme Windows 95 und Windows NT bestimmte Applikationen auszuführen versuchen. Das Feld ist implizit angehakt.

Arbeitet man unter dem Operationssystem Windows 95, enthält die Seite "Residente Blöcke" auch das Anhakfeld "Formatierung". Durch sein Anhaken wird die Kontrolle der Formatierungsoperationen im Rechnersystem eingeschaltet. Wir empfehlen, das Feld angehakt zu lassen, weil die diesen Systemdienst angreifende Viren besonders gefährlich sind - man kann einen Teil oder den ganzen Inhalt der Festplatte verlieren. Das Feld ist implizit angehakt.

Unter dem Operationssystem Windows NT beinhaltet diese Seite nur die Anhakfelder "DOS-Dateioperationen" und "Windows-Dateioperationen".

Diese Seite ist nur in dem Fall erreichbar, wenn eine der Aufgabentätigkeiten auch die Blockierung von potentiell gefährlichen Operationen ist (siehe Kapitel 4.4.2).

4.4.16 Seite "Ignorieren"

Diese Seite ermöglicht dem Benutzer, die Dateien zu spezifizieren, mit denen alle Operationen (MS-DOS und Windows-Operationen) durch das AVAST32-Programm bei eingeschalteter Blockierung von gefährlichen Operationen völlig ignoriert werden sollen (Abb. 58). Diese Möglichkeit wurde vor allem deswegen in das Programm ein-

gegliedert, weil es eine Reihe von Programmen gibt, über die man weiß, daß sie während ihrer Tätigkeit verschiedenste Informationen in sich speichern. Die Meldung von solchen Programmtätigkeitn kann unangenehm und sehr zeitaufwendig sein.

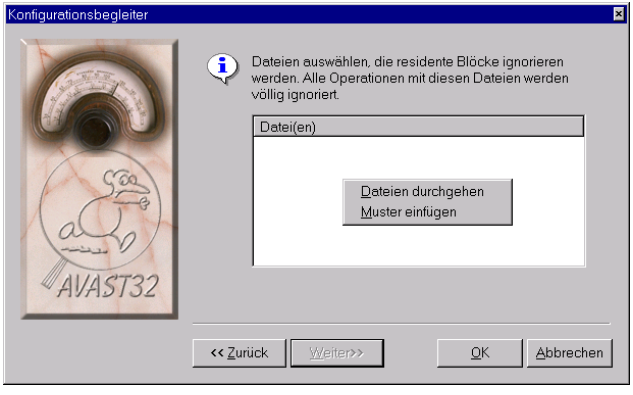

Abb. 58

Diese Seite beinhaltet ein Verzeichnis von Dateien, bei den keine Operationen überwacht werden. Wenn die Aufgabe auch andere Tätigkeiten als Blockierung umfaßt, werden diese Tätigkeiten auch mit den in diesem Verzeichnis angeführten Dateien durchgeführt. Das Verzeichnis ist implizit leer. Will man eine Tätigkeit zum Verzeichnis zuordnen, nutzt man das Lokalangebot:

- Funktion "Muster einfügen" fügt eine Stelle mit der Bezeichnung "Gültigen Dateinamen eingeben..." in das Verzeichnis ein und ermöglicht ihre Editierung. Nach der Bezeichnungseintragung wird die "Enter"-Taste betätigt,
- Funktion "Dateien durchgehen" öffnet ein Standartdialog für die Dateienöffnung (Abb. 89) und emöglicht die Auswahl der entsprechenden Datei. Die ausgewählte Datei wird dann in das Dateienverzeichnis überführt.

Die Dateibezeichnung darf keine Vertretezeichen wie "*" (Sternchen) und "?" (Fragezeichen) beinhalten. Die Datei kann aus dem Verzeichnis auf eine übliche Weise beseitigt werden, d.h. sie muß zuerst gewählt werden und dann durch die "Del"-Taste gelöscht werden.

Diese Seite ist nur in dem Fall erreichbar, daß eine der Aufgabetätigkeiten auch die Blockierung der potentiell gefährlichen Operationen ausgerichtet ist (siehe Kapitel 4.4.2).

4.5 Kontrolle der eingetragenen Daten

Das AVAST32-Programm verlangt bei der Aufgabenerstellung die Eintragung von einigen Daten und auch die Kontrolle der Richtigkeit und Vollständigkeit dieser Daten. Wenn die eingetragenen Daten nicht richtig sind, wird der Benut-

zer darauf aufmerksam gemacht. Ist die Anwendung des Begeleiters eingeschaltet, kann der Benutzer ohne die Eintragung von richtigen Daten nicht zu der folgenden Seite übergehen.

Der Aufgabenname sollte möglichst treffend sein und sollte aus dem Grund der Übersichtlichkeit nicht für mehrere Aufgaben benutzt werden. Das Programm hindert jedoch nicht die Erstellung von Aufgaben mit dem gleichen Namen. Ist der Aufgabenname nicht eingetragen worden, erlaubt das AVAST32-Programm keine Aufgabenerstellung.

Damit die Aufgabenerstellung sinnvoll ist, muß diese Aufgabe Tätikeit(en) enthalten. Einzelne Tätigkeiten der Aufgabe werden auf der Seite "Test" (Kapitel 4.4.2) eingetragen. Wenn keine Tätigkeit der Aufgabe eingetragen ist, wird die Aufgabenerstellung nicht erlaubt.

Das AVAST32-Programm erlaubt auch nicht, eine neue Aufgabe zu erstellen, wenn sie die Tätigkeit der Virensuche oder des Datenintegritätstests enthält und der Typ der zu kontrollierenden Dateien (Kapitel 4.4.4) oder die zu kontrollierenden Bereiche (Kapitel 4.4.5) nicht bestimmt wird. D.h., daß die Verezeichnisse auf den Seiten "Typen" und "Bereiche" leer sind.

Das AVAST32-Programm kontrolliert jedoch nicht, ob die eingetragenen Dateien (z.B. eine Klangdatei oder die zu ignorierenden Dateien) existieren. Der Benutzer wird über die Tatsache ihrer Nichtexistenz erst im Bedarfsfall benachrichtigt. Auch die Erreichbarkeit der auf der Seite "Netzwarnung" erwähnten Rechner (Kapitel 4.4.11) wird nicht kontrolliert - sie kann durch die "Test"-Taste auf dieser Seite geprüft werden.

5.Programmsteuerung

Bedienung des AVAST32 Programmes kann zwei Formen annehmen. Die erste Form ist die sgn. einfache Bedienung, die ihrem Charakter nach besonders für die Benutzer geeignet ist, die übliche Funktionen durchzuführen brauchen, ohne Kentnisse über Einzelheiten der Programmarbeit und -fuktionen zu haben.

Die andere Bedienung, die sgn. erweiterte, enthält Interface für sämtliche Funktionen und Möglichkeiten, die das AVAST32 Programm bietet. Sie wird vor allem von den Fachleuten ausgenutzt, weil sie ermöglicht das Programm eigenen Bedürfnissen anzupassen und, auf diese Weise, alle seine Funktionen und Vorteile auszunutzen.

Außer des Zeichens der Firme ALWIL Software und des Fenstermenüs, das in dem nächsten Kapitel beschrieben ist, ist die Zustandszeile gemeinsames Element beider Steuerungssysteme. Sie befindet sich am unteren Fensterrand. Sie enthält vier Kolonnen. In der ersten Kolonne ist die genaue Versionszahl des Programms AVAST32 mit seiner Zahl der Übersetzung angegeben. Im Fall irgendwelcher Probleme werden Sie die erwähnten Zahlen brauchen, wenn sie mit den Mitarbeitern unserer Firma Kontakt aufnehmen wollen werden.

Die zweite Zelle enthält die Anzahl der verfügbaren Aufgaben und die Anzahl der gerade laufenden Aufgaben. Die Anzahl der gekauften Lizenzen ist in der dritten Zelle angegeben. Die letzte Zelle ist zur Zeit nicht genützt.

Nach dem ersten Programmanlauf zeigt sich die einfache Bedienung des AVAST32 Programms.

5.1 Das Hauptfenstermenü

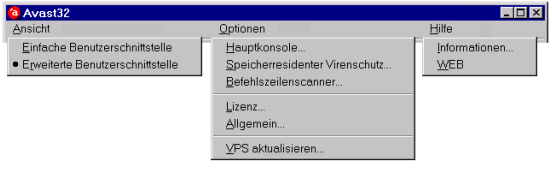

Abb. 59

Weiteres Element, das für die einfache und erweiterte Steuerung gemeinsam ist, ist das Fenstermenü (Abb. 59). Es befindet sich unter der Leiste des Hauptfensters und ist jederzeit während des Programmbetriebs verfügbar.

Das Menü "Ansicht"

Es ist für die Steuerungsumschaltung AVAST32 vorgesehen. Sein Inhalt sind die Elemente "Einfache Benutzerschnittstelle" und "Erweiterte Benutzerschnittstelle", durch dessen Wahl Sie zum entsprechenden Steuerungsteil des Programms umschalten.

Die zur Zeit benutzte Steuerung ist mit einer Kugel markiert (Abb. 59 zeigt die Nutzung der erweiterten Steuerung).

Das Menü "Optionen"

Mit Hilfe von Elementen dieses Menüs kann das Verhalten des Programm AVAST32 und aller seiner Teile den Bedürfnissen einzelner Benutzer angepaßt werden. Sie enthalten z.B. die Ausnutzung der Assistentenhilfe bei der Erstellung und bei den Änderungen der Aufgaben usw. Ein Bestandteil der Programmeinstellung ist auch die Möglichkeit der Aktualisierung der Datei mit den Charakteristiken aller bisher bekannten Viren, der sogenannten VPS Datei.

Wegen des Umfangs und der Wichtigkeit dieser Elemente haben wir entschieden, ihnen ein selbständiges Kapitel zu widmen. Eine eingehende Beschreibung aller Teile der Programmeinstellung kann der Benutzer im Kapitel 6 finden.

Das Menü "Hilfe"

Das einzige Element "Informationen" dieses Menüs ist für die Abbildung der Informationen über das Programm bestimmt (Abb. 60).

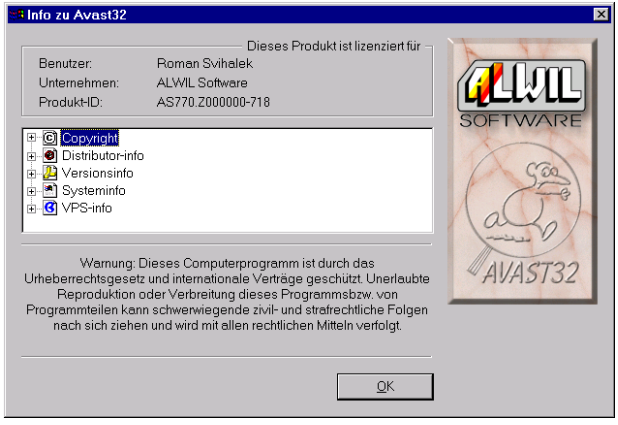

Abb. 60

Sie sollten eine gewisse Aufmerksamkeit diesen Informationen widmen, weil Sie irgendwelche gebrauchen können, im Fall, daß Sie sich auf unsere Firma mit dem Antrag für die technische Unterstützung wenden. Die Mitarbeiter der technischen Unterstützung dürfen die Beantwortung Ihrer Fragen ablehnen, wenn Sie ihnen diese Informationen nicht geben!

Fogende Informationen sind enthalten:

- Inhaber der Autorrechte,
- Lizenzinhaber und über das Netz zugreifbare Lizenzenanzahl,
- Version des Programms AVAST32 und der angewendeten Komponenten, einschließlich detaillierter Informationen über die Programmübersetzung,
- Informationen über das Operationssystem, seine Version und verfügbaren Speicher,
- Version der VPS Datei (Virendatenbank) und Informationen über ihre Übersetzung.

Die Nummer der Version des AVAST32 Programms und die Nummer seiner Übersetzung ist auch in der ersten Kolonne der Zustandszeile des Programmhauptfensters angegeben.

5.2 Einfache Benutzerschittstelle

Einfache Steuerung ist in der Abb. 61 dargestellt. Sie enthält die Liste von verfügbaren Aufgaben und einige Steuerungstasten.

Abb. 61

Die Liste der verfügbaren Aufgaben enthält die Aufgaben, die der Benutzer zur Zeit ausnutzen kann. An dem Namen der jeweiligen Aufgabe ist eine Ikon, die ihr aktuellen Zustand darstellt. Sofern die Aufgabe nicht angelaufen ist, stellt die Ikon den Aufgabentyp dar (an der Abb. 61 die Aufgaben sind "Gemeinsam genutzt" und "Privat"). Ist die Aufgabe angelaufen, ist eine grüne Kugel neben ihrem Namen (an der Abb. 61 die Aufgabe ist "Angelaufen"). Ist die Aufgabe angehalten, ist eine rote Kugel neben ihrem Namen (an der Abb. 61 die Aufgabe ist "Angehalten").

Die Taste "Start" dient zum Anlauf oder zur Anhaltung des Aufgabenlaufs. Ihre Bedeutung ändert sich je nach der aktiven Aufgabe, das heisst der Aufgabe, die in der Liste der verfügbaren Aufgaben hervorgehoben wird. Ist die aktive Aufgabe nicht angelaufen, hat die Taste ein Namen "Start" und dient zum Programmanlauf. Ist die aktive Aufgabe angelaufen, hat die Taste ein Namen "Stop" und dient in diesem Fall zur Programmbeendigung.

Die Aufgabe kann angelaufen oder angehalten (nicht beendet) werden auch so, daß sie sie zunächst aktivieren und dann die Taste "Enter" drükken oder mit der rechten Maustaste an ihrem Namen klopfen. Das AVAST32 Programm wird durch drücken der Taste “Ende“ beendet. Gleichzeitig damit werden auch alle nicht residente Aufgaben beendet.

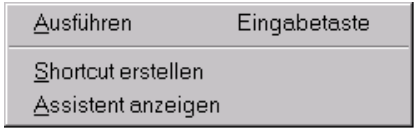

Abb. 62

Das Lokalangebot, das durch das Drücken der rechten Maustaste am Aufgabennamen hervorgerufen wird, wird die Abb. 62 zeigen. Die ausgewählte Funktion wird mit der Aufgabe durchgeführt, auf deren Namen wurde die rechte Maustaste gedrückt.

Das Lokalangebot kann folgende Funktionen enthalten:

- Die Funktion "Ausführen" startet die Durchführung der Aufgabe. Sie ist zugänglich nur aus den Aufgaben, die zur Zeit nicht laufen,
- Die Funktion "Stop" beendet die Aufgabendurchführung. Sie ist zugänglich nur aus den Aufgaben, die zur Zeit laufen oder angehalten werden,
- Die Funktion "Pause" hielt die Aufgabe an. Sie ist zugänglich nur aus den Aufgaben, die zur Zeit laufen,
- Die Funktion "Shortcut erstellen" bildet einen Aufgabenvertreter auf der Arbeitsfläche. Der Vertreter kann dann zur direkten Anlauf der Aufgabe ausgenutzt werden,ohne zunächst das AVAST32 Programm anlaufen zu müssen. Die Funktion ist im Angebot immer enthalten.
- Die Funktion "Hilfe" ruft zunächst die Hilfe des AVAST32 Programms. Zum Hervorrufen der Hilfe des AVAST32 Programms kann auch die Taste "F1" ausgenutzt werden. Die Funktion ist im Angebot immer enthalten.

5.3 Erweiterte Benutzerschittstelle

Die erweiterte Bedienung enthält einen für den Benutzer angenehmen Interface für den Zugriff zu sämtlichen Funktionen und Einstellungen, die

Das AVAST32 Programm bietet. Weil die Funktionen und Einstellungen zu viele sind, ist die erweiterte Bedienung in einigen Seiten organisiert. In dem folgenden Kapiteln beschreiben wir ausführlich einzelne Seiten.

5.3.1 Seite "Aufgaben"

Die Seite ist in zwei Teile untergeteilt (Abb. 63). Der linke Teil enthält eine Liste der verfügbaren Aufgaben so, wie sie bei der einfachen Bedienung beschrieben wurden. Ihre Nutzung sowie auch ihre Eigenschaften, bis auf das Lokalangebot, sind durchaus identisch.

Abb. 63

Im linken Seitenteil sind Informationen über den Zustand der aktiven Aufgabe untergebracht. Die Informationen sind in einer Baumstruktur angeordnet.

Die Informationen über den Zustand der aktiven Aufgabe sind in Textfeldern im oberen Teil untergebracht. Das erste Textfeld ist das Feld "Zustand", das den aktuellen Zustand der Aufgabe abbildet. Es gibt drei mögliche "Zustand:" die Aufgabe ist nicht angelaufen ("<kein Job>" - arbeitet nicht), die Aufgabe ist angelaufen ("LÄUFT" - arbeitet) oder die Aufgabe ist angelaufen, aber momentan ist ihr Lauf angehalten ("<unterbrochen>" - Pause). Einen kompletten Zugriffsweg zu der zur Zeit durchsuchten Mappe zeigt das zweite Textfeld - "Verzeichnis:" und das letzte Textfeld enthält das Name der Datei, die zur Zeit getestet wird. Solange die aktive Aufgabe resident ist (siehe Kapitel 4.4.2), ist nur die Information über den Zustand abgebildet.

Die Eigenschaften und Statistiken über den Aufgabenablauf sind in einer Baumstruktur angeordnet, die sich unter den erwähnten Textfeldern befindet. Zugriff zu einzelnen Daten erhalten sie durch "Entfaltung" des zuständigen Eintrags. Das wird durch Anklopfen mit der linken Maustaste auf das Zeichen vor dem Eintragsnamen gemacht.

Informationen über dem Aufgabeneigentümer, Tätigkeiten, die während des Aufagbenlaufes durchgeführt werden, über das Erstellungsdatum

und über das Datum der letzten Aufgabennutzung sind im Eintrag "Eigenschaften" angegeben. Hier gibt es auch die Information über die gesamte Anzahl der Aufgabenanläufe seit ihrer Erstellung.

Der letzte Eintrag ist "Statistik" (die auf der Abb. 63 entfaltet ist), die den Benutzer über die Anzahl der gefundenen Dateien, getesteten Dateien, Dateien, die auf Anwesenheit von Viren getestet wurden, Dateien, bei den ihre Integrität getestet wurde, über die Anzahl der nicht getesteten Dateien, infizierten Dateien und über die Anzahle der gefundenen Viren informiert. Alle Einträge beziehen sich zur aktiven Aufgabe. Kontrolliert die aktive Aufgabe, zum Beispeil, nur die Datenintegrität, wird der Eintrag der gefundenen Virenanzahl immer Null seín!

Läuft die aktive Aufgabe (d.h. die Aufgabe, die aus der Liste gewählt wurde) zur Zeit, sind die Informationen aktuallisiert und der Benutzer hat auf diese Weise einen Übersicht über ihr Verlauf.

Das Lokalangebot

Gleicherweise wie die einfache Bedienung enthält die erweiterte Bedienung ein Lokalangebot, der sich nach Drücken der rechten Maustaste auf dem entsprechenden Aufgabennamen (Abb. 64) abbildet. Ausser den Funktionen zum Anlauf, zur Anhaltung und zum Beenden der Aufgabe enthält es die folgenden Funktionen.

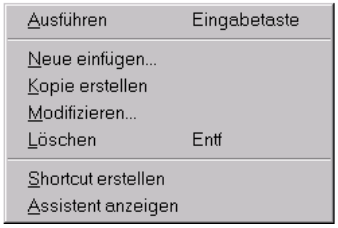

Abb. 64

- Die Funktion "Neue einfügen..." dient zur Erstellung neuer Aufgaben. Ihre Beschreibung is in Kapitel 4 angeführt.
- Mit der Funktion "Kopie erstellen" kann man eine genaue Kopie der gegebenen Aufgabe erstellen. Die neue Aufgabe enthält durchaus identische Parametereinstellung wie die gewählte Aufgabe. Das Name der neuen Aufgabe wird allerdings in der Form "Kopie <Name der gewählten Aufgabe>" erscheinen. Eine Kopie kann man allerdings nur aus einer Aufgabe erstellen, zu der der Benutzer Zugriff hat, das heißt aus einer privaten Aufgabe, oder auch aus einer mehrfach ausgenutzten Aufgabe wenn sie nicht durch Kennwort geschützt wird oder wenn der Benutzer das Kennwort kennt.
  Will der Benutzer eine Kopie der gemeinsam genutzten Aufgabe erstellen und die gemeinsam genutzten Aufgaben durch ein ihm unbekanntes Kennwort geschützt sind, wird die neu erstellte

Aufgabe privat. Sämtliche andere Einstellungen bleiben erhalten.

- Die Funktion "Modifizieren..." ermöglicht dem Benutzer die Parametereinstellung der Aufgabe zu verändern. Die Aufgabenänderung verläuft in einer durchaus identischen Umgebung wie die Aufgabenerstellung. Daher alles, was in der Kapitel 4 über die Neuaufgabenerstellung geschrieben wurde gilt auch für ihr Verändern. Wenn sie im Fenster der Veränderung der Bedienungselemente die Taste "OK" drücken und wenn die durchgeführte Veränderungen die Bedingungen, die in der Kapitel 4.5 aufgeführt sind, erfüllen, dann die Veränderung durchgeführt wird. Wenn sie, allerdings, die Taste "Abbrechen" drücken, wird die Veränderung nicht durchgeführt und die Einstellung aller Parameter der Aufgabe bleibt unverändert.
- Die Funktion "Löschen" dient zur Beseitigung der Aufgabe aus der Aufgabenliste und zugleich auch aus der Festplatte. Nach ihrer Wahl wird der Benutzer gefragt, ob er das mit der Beseitigung ernst nimmt (Abb. 60). Nach dem Drücken der Taste "Ja" wird die Aufgabe unwiederaufnehmbar aus der Liste der verfügbaren Aufgaben und von der Festplatte des Computers beseitigt.

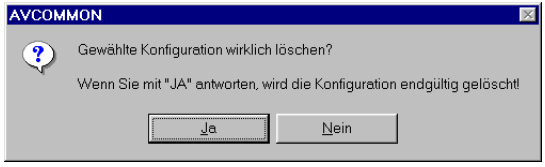

Abb. 65

- Die Funktion "Shortcut erstellen" erstellt, wie bei der einfachen Bedienung, einen Aufgabenvertreter auf der Arbeitsfläche. Dieser Vertreter kann dann zum direkten Anlauf der Aufgabe ausgenutzt werden ohne zunächst das AVAST32 Programm anlaufen zu müssen.
- Die Funktion "Hilfe" bilded Hilfstexte des AVAST32 Programmes ab. Die Hilfstexte können auch mittels Taste "F1" hervorgerufen werden.

5.3.2 Seite "Ergebnisse"

Die Seite "Ergebnisse" enthält Resultate aller Aufgaben, die die Tätigkeiten der Suche nach bekannten Viren oder Prüfung der Datenintegrität beinhaltet haben (Abb. 66). Die Bedienung dieser Seite ist sehr ähnlich der Bedienung des Programms "Explorer". Dieses Kapitel beschreibt nur die Bedienung und Bedeutung einzelnen Tatsachen, die die Seite "Ergebnisse" beinhaltet. Die Interprätation dieser Tatsachen ist erst im Kapitel 7 behandelt.

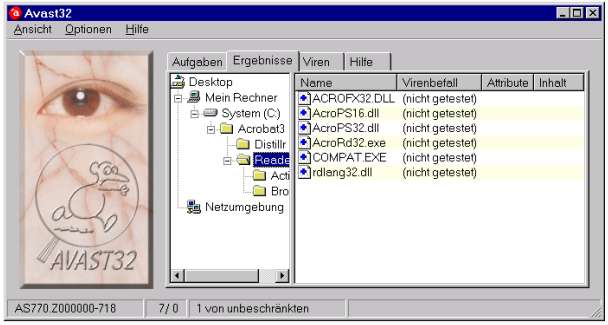

Abb. 66

Die Aufgabenresultate sind in einen Eintragsbaum zusammengestellt und dank diesem Fakt hat der Benutzer Übersicht über die Resultate aller Aufgaben, die vor dem Programmanlauf durchgeführt wurden. In den Eintragsbaum werden vom AVAST32 Programm nur die Aufgaben eingeordnet, die Zeichen einer Virusinfektion aufweisen oder wurden seit der letzten Kontrolle irgendwie verändert. Mit anderen Worten, hier werden alle verdächtigen Dateien angeführt.

Hier werden auch die neuen Dateien eingeordnet, genauer gesagt die, die vom AVAST32 Programm in seiner internen Dateidatenbank nicht gefunden hat. Hier werden sie auch die Namen der Dateien finden, die ausgelöscht oder umgelagert wurden. Mit den Bootsektoren und mit dem Speicher behandelt man wie Dateien, so daß im Fall ihrer Veränderung sie auch in die Baumstruktur eingeordnet werden. Sie werden direkt in die Mappe "Mein Rechner" eingeordnet.

Verdächtige Dateien sind in die Baumstruktur nach ihrem wirklichen Zugriffsweg eingeordnet. Wenn also der Baum irgendeine Mappe enthält, dann enthält diese Mappe (oder irgendeine verschachtelte Mappe) eine verdächtige Datei. Wenn sie also den Inhalt einer von diesen Mappen feststellen vollen, aktivieren sie sie und im rechten Teil der Seite kommen die verdächtigen Dateien (wenn es da irgendwelche gibt) zum Vorschein. Vor dem Namen jeder Datei kann sich eine Ikone, die die Aktion darstellt, die mit der Datei durchgeführt wurde.

Abb. 67

Erscheint da ein blaues Pluszeichen (Abb. 67) heißt es, daß die Datei neu ist, ist hier also seit der letzten Kontrolle angelangt. Wenn sie den Integritätstest zum erstenmal angelaufen haben, werden alle gefundene Dateien als neue bezeichnet, weil die interne Dateidatenbank bisher leer ist und es ist notwendig sie zunächst zu füllen.

Abb. 68

Erscheint da ein grünes Minuszeichen (Abb. 68) signalisiert es umgekehrt, daß die Datei mit dem Namen fehlt. Es ist gut zur Kentniss zu nehmen, was sie mit dem Computer gemacht haben. Wenn sie, zum Beispiel, seit der letzten Kontrolle den Korb ausgechüttet haben, ist es selbstverständlich, daß das Programm fehlende Dateien auf der ensprechenden Festplatte in der Mappe "RECYCLED" meldet. Gleichermaßen werden sie wahrscheinlich über das Verschwinden der temporären Dateien, usw. informiert.

Abb. 69

Ein weiteres Zeichen, das an dem Dateinamen zum Vorschein kommen kann, ist ein rotes Ausrufszeichen (Abb. 69). AVAST32 gibt an dieser Weise bekannt, daß es bei der Arbeit mit der Datei zu einem Fehler gekommenn sei. Er könnte aus verschiedenen Ursachen vorkommen, am häufigsten, allerdings, handelt sich um einen Fehler der Dateiteilung, d.h., daß die Datei durch eine andere Applikation geblockt ist.

Abb. 70

Wenn sie eine Korrektur eines OLE Dokumentes vorgenommen haben (siehe weiter), kann an dem Namen der korrigierten Datei ein gelbes Fragezeichen zum Vorschein kommen (Abb. 70). AVAST32 signalisiert auf diese Weise, daß nach der Korrekturoperation bzw. nach dem entfernen des Makroviren aus der Datei, ihr Zustand unbekannt ist. Wenn sie festzustellen brauchen, ob sich der Zustand einer so markierten Datei von dem Zustand, der sich in der inneren Datenbank befindet, unterscheidet, führen sie nochmals den Dateiintegritätstest durch.

Abb. 71

Eine Kugel (Abb. 71) kann erscheinen, ähnlicherweise wie beim Fragezeichen, bei der Dateien, die repariert wurden. Im Gegensatz zum Fragezeichen erscheint es nur bei den Dateien, die nicht OLE Dokumente sind und deren Korrektur erfolgreich abgeschlossen wurde. So markierte Dateien befinden sich also im Zustand, der in der Dateidatenbank aufgezeichnet ist.

Ist am Dateinamen keine Ikone, wurde die Datei irgendwie verändert. Genauere Informationen über die Dateiveränderung sind in den Spalten hinter seinem Namen aufgeführt. Die Spalten sind wie folgt:

- die Spalte "Infektion" enthält das Name des Virus, mit dem die Datei wahrscheinlich infiziert ist. Die Spalte ist nur dann von Bedeutung, wenn die Datei auf das Vorkommen des Virus getestet wurde. Ist es der Fall und die Spalte leer ist, wurde in der Datei kein von den bekannten Viren entdeckt. Enthält die Spalte, allerdings, den Virennamen, ist die Datei mit größten Wahrscheinlichkeit infiziert! War die Datei nicht getestet, enthält die Spalte ein Text "(nicht getestet)",
- Die Spalte "Attribute" informiert den Benutzer über Veränderungen der Attribute und über die Änderung der Daten und der Zeit der letzten Dateieintragung. War die Dateiintegrität getestet und die Spalte leer ist, dann sind die angeführten Parameter seit der letzten Kontrolle nicht verändert worden. Im entgegengesetzten Fall die Spalte enthält "!!!" (drei Ausrufszeichen).

Wir machen sie nochmals darauf aufmerksam, daß solange die Spalte "Infektion" leer ist, muß es nicht unbedingt heißen dab die Datei nicht infiziert ist. War die gegebene Datei auf das Virusvorkommen getestet und die Spalte leer ist, dann heißt es, daß in der Datei bei der gegebenen Einstellung kein bekannter Virus entdeckt wurde!

Das Lokalangebot

Das Lokalangebot (Abb. 72) bezieht sich immer auf die Dateien, die markiert wurden. Das gleiche Angebot ist auch für die Mappen des rechten Seitenteils benutzt. Die für die gegebene Mappe ausgewählte Funktion wird mit allen Dateien durchgeführt, die sie enthält, sowie mit allen Dateien in allen verschachtelten Mappen.

Abb. 72

Die Funktion "Einzelheiten" dient zur Abbildung des Dialogs mit genaueren Informationen über den Charakter der Veränderung (Abb. 73). Da sind Informationen über die ausgewählte Datei, wie ihr Zustand, Attribute, Datum der Erstellung und der letzten Modifikation sowie auch Dateilänge bzw. das Name des Virus, der die Datei angegriffen hat, gegeben. Alles das ist für den ursprünglichen Dateizustand (wie gespeichert in der internen Datenbank) sowie auch für den aktuellen Dateizustand, in dem sie auf der Festplatte befindet, abgebildet.

Für die Abbilding des Dialogs kann man auch Tastenabkürzung "Alt+Enter" benützen.

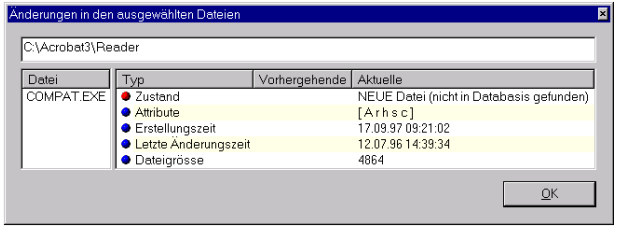

Abb. 73

Das Lokalangebot enthält die Mappe "Dateiverarbeitung", die die Funktionen, notwendig für die Arbeit mit verdächtigen Dateien, enthält:

Akzeptieren der Dateien

Die Funktion "Akzeptieren" teilt dem AVAST32 Programm mit, daß sie über die Dateiveränderungen wissen und daß sie sie nicht mehr melden soll. Die auf diese Weise behandelten Dateien verschwinden aus der Liste der verdächtigen Dateien und, wenn die Mappe, in der sie sich befanden, leer wurde, verschwindet sie auch. Die Funktion eigentlich trägt die aktuellen Dateizustände in die interne Datenbank ein, so daß sie bei der nächsten Kontrolle als Ausgangszustände erscheinen werden.

Reparieren der Dateien

Die Funktion "Korrigieren..." versucht die markierten Dateien in den Ausgangszustand zu bringen. Nach ihrer Auswahl kommt ein Dialog zum Vorschein, der auf der Abb. 74 zu sehen ist. Ist die reparierte Datei ein OLE Dokument, dann liegt für den Benutzer eine Möglichkeit vor, einige Parametr zu ändern. In dem gegengesetzten Fall hat ihre Einstellung keinen Sinn und sie wird ignoriert werden.

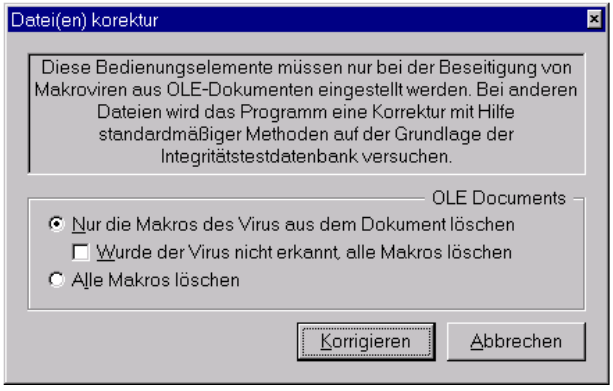

Abb. 74

Durch die Betätigung des Schalters "Nur die Makror des Virus aus dem Dokument löschen" ist es möglich einzustellen, daß nur die Makra, in de-

nen das Virus entdeckt wurde, entfernt werden. Alle andere Makra bleiben unberührt.

Durch die Betätigung des Schalters "Wurde der Virus nicht erkannt, alle Makros löschen" wird es verursacht, daß alle Makra aus dem OLE Dokument entfernt werden, ob sie das Virus enthalten oder nicht.

Die vorgegebene Einstellung ist nur die Makra, die Virus enthalten, zu entfernen.

Duch das Abhakfeld "Alle Makra auszulöschen, wenn das Virus nicht ganz erkannt wurde" teilen sie dem Programm mit, daß wenn das Virus nicht ganz erkannt wurde (bei einigen Maktroviren kann die Detektion sehr schwierig sein), alle Makra sollen aus dem Dokument entfernt werden.

Wenn eine Datei, die kein OLE Dokument enthält, repariert werden soll, dann versucht das AVAST32 Programm die Datei mit einem Verfahren, dem der Datenintegritätstest zugrunde liegt, zu reparieren. Das AVAST32 Programm verwaltet eine interne Dateidatenbank, in der wichtige Informationen über den Zustand einzelner Dateien und, mit Hilfe der Kontrollsummen, auch über ihr Inhalt gespeichert werden. Durch Ausnutzung dieser Informationen versucht AVAST32 die gewählte Datei zu reparieren. Es ist möglich bis fünfundneunzig Prozent der infizierten Dateien zu reparieren. AVAST kann mit einer hundertprozentigen Sicherheit feststellen, ob die Datei erneuert wurde.

Aus dem vorherigen Text geht hervor, daß wenn sie die Dateien erfolgreich reparieren wollen, brauchen sie eine regelmäßig aktualisierte Dateidatenbank auf ihren Festplatten. Diese Dateidatenbank muß verwaltet werden, mit anderen Worten, ist es notwendig durchlaufend Datenintegritätskontrolle durchzuführen und die legale Dateiveränderungen mit Hilfe der Funktion "Akzeptieren" in die interne Datenbank einzutragen.

Die Algorithmen für die Dateierneuerung, die im AVAST32 Programm angewendet werden, sind ausschließlich für die Erneuerung der Dateien bestimmt, die durch irgend ein Virus angegriffen wurden. Für die Erneuerung der überschriebenen oder aufbereiteten Dateien können sie nicht benützt werden. Die Einstellung der Bedienungselemente des Dialogs wird für die Dokumente, die nicht OLE Dokumente enthalten, ignoriert.

Durch Drücken der Taste "Korrigieren" wird der eigene Prozeß der Dateireparatur angelaufen. Durch Betätigung der Taste "Abbrechen" schließen sie den Dialog und es kommt zu keiner Manipulation mit den markierten Dateien.

Umbenennung und Umlagerung der Dateien

Die Funktion "Verschieben/Umbennen..." ermöglicht die verdächtigen Dateien in eine andere Mappe umzulagern oder sie umzunennen. Die Funktion bildet ein Dialog ab, der auf der Abb. 75 zu sehen ist. Das Dialog enthält drei Bedienungselemente:

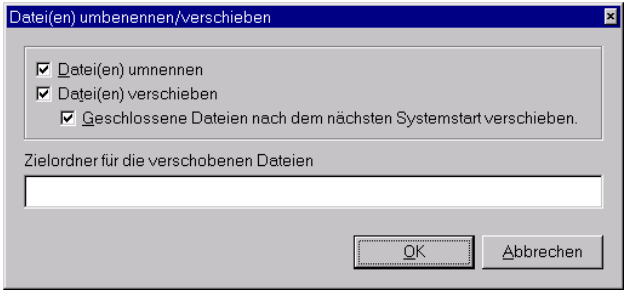

Abb. 75

Das Anhakfeld "Datei(en) umnennen" ermöglicht bei den markierten Dateien ihren Suffix zu verändern. Auf diese Weise umgenannt Dateien werden von den anderen unterschieden und bei den anlaufbaren Dateien wird so ihr unfreiwilliges Anlaufen verhindert. Das würde, wenn die Datei ein Virus enthält, zum Infizieren des Computers führen (wenn es dazu noch nicht gekommen ist). Bei der Datei wird der bisherige Suffix durch einen vorgewählten Suffix ersetzt (siehe Kapitel 6.1.3). Der eigene Dateiname bleibt unberührt.

Findet das Programm während der Umnennung einen unbekannten Dateityp, fragt es den Benutzer, wie der Suffix der gefundenen Datei verändert werden soll. Der eingetragene Suffix wird vom Programm gemerkt und, wenn er eine andere Datei des gleichen Typs findet, benützt er automatisch denselben Suffix.

Durch Anhaken des Feldes "Datei(en) verschieben" schalten sie das Umlagern der markierten Dateien in die ausgewählte Mappe. Das Name der Mappe, in die die markierten Dateien umgelagert werden und ihr Zugriffsweg wird in das Textfeld „Zielordner für die verschobenen Dateien“ eingetragen.

Ist die Umlagerung der Dateien eingeschaltet, ist es möglich durchs Anhaken des Feldes „Geschlossene Dateien nach dem nächsten Systemstart verschieben“ festzustellen, daß wenn die Datei in dem Moment nicht manipulierbar ist (z.B. ist sie von einer anderen Applikation benützt), ist es möglich ihre Umlagerung bis den nächsten Operationssystemanlauf zu verschieben. So kann es ihnen nicht passieren, daß sie die gegebene Datei umzulagern vergessen - das Programm kümmert sich selbst dafür.

Implizit ist Dateiumnennung sowie ihre Umlagerung eigeschaltet einschließlich der Möglichkeit

ihre Umlagerung bis zum nächsten Operationssystemanlauf zu verschieben.

Auslöschung der Dateien

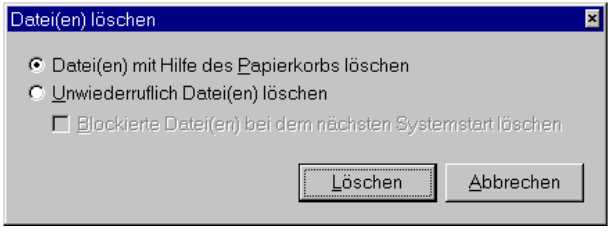

Abb. 76

Die letzte Funktion in der Mappe "Dateiverarbeitung" ist die Funktion "Löschen...". Nach ihrer Wahl wird ein Dialog abgebildet, in dem der Benutzer die Weise der Dateiauslöschung wählen kann (Abb. 76).

Durch die Wahl des Schalters "Datei(en) mit Hilfe des Papierkorbs löschen" stellen sie fest, daß die markierten Dateien duch die Umlagerung in den Abfallkorb ausgelöscht werden. So können die ausgelöschten Dateien jederzeit ohne Probleme erneut werden und deswegen empfehlen wir diese Weise besonders für die weniger erfahrenen Benutzer der Personalcomputer.

Wenn sie das Operationssystem Windows NT Version 3.51 benützen, dann wird dieser Schalter wird für sie unverfügbar. Sie müssen dann die folgende Methode anwenden.

Der Schalter "Unwiederruflich Datei(en) löschen" schaltet das direkte Auslöschen der Dateien aus den Festplatten ohne jede Möglichkeit ihrer Wiederherstellung ein.

Wenn der Schalter angewählt ist, können sie durchs Anhakfeld "Blockierte Datei(en) bei dem nächsten Systemstart löschen" feststellen, daß, wenn man mit der Datei zur Zeit nicht manipulieren darf (es ist z.B. in einer anderen Applikation verwendet), ist es möglich ihr Auslöschen bis zum nächsten OS Anlauf zu verschieben. Das Feld ist implizit nicht angehakt.

Der Schalter "Datei(en) mit Hilfe des Papierkorbs löschen" ist implizit vorgewählt.

Nach dem Drücken der Taste "Löschen" wird die Auslöschung aller markierten Dateien auf die gewählte Weise vorgenommen. Die Taste "Abbrechen" schließt das Dialog.

5.3.3 Seite "Viren"

Wenn sie nähere Informationen über alle Viren, die das AVAST32 Programm zur Zeit kennt, klopfen sie auf die Name der Seite "Viren". Auf der Seite haben sie eine komplette Liste der grundsätzlichen Viren in alfabetischer Ordnung zur Verfügung gestellt (Abb. 77).

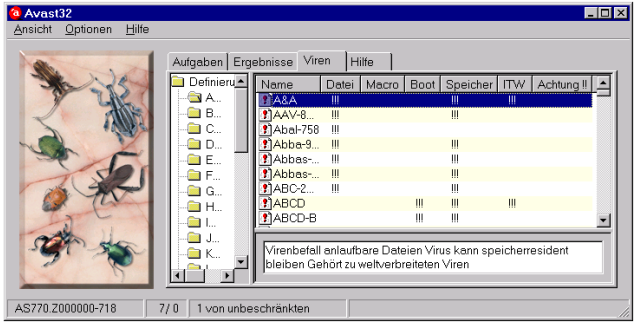

Abb. 77

Ähnlich vie alle anderen Seiten ist auch diese Seite in zwei Teile unterteilt. Links hat der Benutzer die Möglichkeit den Anfangsbuchstaben oder die Namennummer des Virus zu wählen, über die er ausführlichere Informationen erfahren will. Die Viren, dessen Namen mit dem gewählten Zeichen beginnen, kommen mit ihrer Charakteristik im rechten Seitenteil zum Vorschein.

Die Viren können sich grundsätzlich auf folgende Weisen verbreiten: als eine Komponente einer anlaufbaren Datei, als ein Makro eines bestimmten Dokumentes (die sogenannten Makroviren) oder durchs Überschreiben des sogenannten Bootsektors (das ist der Sektor, das bei der Systeminitialisierung eingelesen wird) einer Platte.

Den obengenannten Weisen entsprechen die ersten drei Spalten die hinter dem Virennamen vorhanden sind. Wenn eine Spalte bei einem Virus "!!!" (drei Ausrufszeichen) enthält heißt es, daß dieses Virus das Computersystem auf diese Weise angreift.

Die Spalte "Speicher" sagt, ob das Virus im Operationsspeicher des infizierten Computers langfristig anwesend sein kann (man sagt, daß es resident ist). Die weitere Spalte enthält die Information, ob das Virus in der ITW Liste steht, was die Liste der verbreitetesten Viren ist. Die letzte Spalte, die durch "Achtung !!" bezeichnet ist, informiert über die Gefährlichkeit des Virus. Wenn si bei einem Virus Bezeichnung "!!!" (drei Ausrufszeichen) finden, ist es besser mit ihm nicht zu spaßen. Auf diese Weise bezeichneten Viren kann man als Regel nur sehr schwierig aus dem Computer entfernen oder sie können große Schäden in ihren Daten machen. Das Entfernen solcher Viren sollte ein wirklich erfahrener Fachmann vornehmen!

Wenn sie irgendein Virus in der Liste auf dem rechten Teil der Seite "Viren" markieren, kommt seine Charakteristik in dem unteren Teil zum Vorschein.. Es handelt sich eigentlich um eine verständliche Darstellung des Inhalts der einzigen Spalten so, wie wir sie beschrieben haben.

Der linke Teil der Seite "Viren" enthält ausser der Buchstaben des Alfabets, der Ziffern und anderen Zeichen auch zwei spezielle Einträge. Durch den Eintrag "ITW" kann in dem rechten Teil der Seite eine Liste aller Viren aus der VPS Datei, die in der ITW Liste enthalten sind, abgebildet werden. Ähnlich arbeitet auch der Eintrag "Achtung !!" wobei in dem rechten Seitenteil besonders gefährliche Viren zum Vorschein kommen. Die Viren werden in beiden Fällen in alfabetischer Ordnung sein.

Weil es zum Finden der Viren aus den obengenannten zwei Einträgen notwendig ist die ganze VPS Datei durchzusuchen, kann ihre Abbildung eine Weile dauern.

Eine ausführlichere Beschreibung aller bekannten Viren, ihrer Tätigkeit und ihrer Besonderheiten ist nicht vorhanden. Es ist weder erträglich noch sinnvoll sämtliche Umständlichkeiten über die Viren hauptsächlich wegen ihrer Anzahl zu ermitteln. Potenzielle Interessenten um ausführlichere Informationen über ein bestimmtes Virus sollen einen Blick in den Anhang B werfen bzw. sich an Mitarbeiter unserer Firma wenden, die ihnen die Informationen gerne bieten.

5.3.4 Seite "Hilfe"

Abb. 78

Die Seite "Hilfe" (Abb. 78) dient dem Benutzer als Zufluchtsort vor etwaigen Problemen bei der Arbeit mit dem Programm. Sie enthält nämlich die Hilfe des AVAST32 Programms.

Bei irgendwelchen Problemen mit dem Programm bitten wir sie zunächst einen Blick in die AVAST32 Programmhilfe zu werfen und erst dann, wenn sie da nicht das finden, was sie suchen, mit unserer technischen Unterstützung Kontakt aufzunehmen.

Ist in ihrem Computer das Programm Acrobat Reader nicht installiert, wird es nicht möglich sein

die AVAST 32 Programmhilfe abzubilden: In diesem Fall müssen sie AVAST32 beenden, das programm Acrobat Reader installieren (siehe Kapitel 1.3.3) und dann AVAST32 wieder anlaufen.

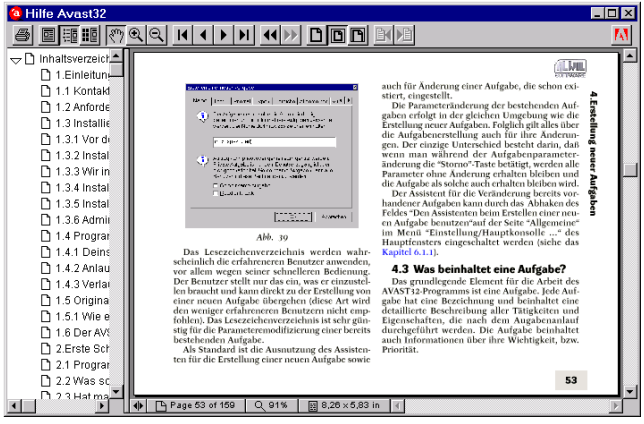

Abb. 79

Die AVAST32 Programmhilfe kann entweder ein Teil der Seite "Hilfe" sein, wie auf der Abb. 78 gezeigt wird oder kann "fliegend" sein. Unter dem Begriff "fliegende" ist ein Fenster mit der Hilfe versteckt, die frei beweglich auf der Arbeitsfläche ist (Abb. 79). Ist also die Hilfe nicht an die Seite "Hilfe" gebunden sondern kann wohin immer untergebracht werden und kann immer zur Verfügung stehen.

Die fliegende Hilfe kann jederzeit während der Tätigkeit des AVAST32 Programms aufgerufen werden und zwar enweder vom lokalen Angebot oder auf die Weise die in der Umgebung der Operationssysteme Windows 95 und NT üblich ist, das heißt durchs Betätigen der Taste F1. Geschlossen wird sie mit der "Esc" Taste.

Ist die fliegende Hilfe abgebildet, enthält die "Hilfe" Seite keine Hilfe mehr, das heißt es ist möglich nur eine Hilfe geöffnet zu haben.

Mag die Hilfe auf der obengenannten Seite sein oder fliegend sein, die Bedienung ist immer dieselbe, weil zur Abbildung der Hilfe wird in beiden Fällen das beliebte Programm Acrobat Reader angewendet. Es ist aber auf solche Weise angewendet, daß es scheint eine untrennbare Komponente des AVAST32 Programms zu sein.

In den folgenden Absätzen wird die Bedienung der Hilfe beschrieben.

Die Taste dient zum Druck der Hilfe oder ihres Teiles. Nach ihrer Betätigung kommt ein Dialog zum Vorschein, der Parmeter und Druckqualität und -umfang einzustellen ermöglicht.

Die folgenden drei Tasten bestimmen die Möglichkeiten der Bewegung duch die Programmhilfe:

Ist diese Taste betätigt, enthält das Fenster mit der Hilfe nur den Teil, der die eigene

Hilfe enthält. Der Teil, der die Bewegung durch die Programmhilfe erleichtert, wird nicht abgebildet.


Ist diese Taste betätigt, muß das Fenster mit der Hilfe ausser des Teils, der die eigene Hilfe abbildet, auch einen Teil enthalten, in dem der Hilfeinhalt abgebildet wird (Abb. 79). Durch Drücken der linken Maustaste über dem Eintrag kann man sich in den notwendigen Teil der Hilfe übertragen.


Die Taste schaltet die Abbildung einzelner nummerierten Seiten neben der eigenen Hilfe. Durch Drücken der linken Maustaste über der entspechenden Seite kann man sich auf die notwendige Seite der Hilfe übertragen.

Die folgenden drei Tasten bestimmen die Arbeitsweise mit der Hilfe (die Mausanzeige nimmt eine Form an, die die ausgewählte Taste zeigt).


Ist diese Taste betätigt, ist es möglich durchs Drücken der linken Maustaste über die Hilfe mit der Seite der Hilfe frei zu bewegen und den ihr Teil abzubilden, die der Benutzer zu sehen braucht.


Ist diese Taste betätigt, wird der gegebene Teil der Hilfe nach dem Drücken der linken Maustaste zweimal vergrössert.


Ist diese Taste betätigt, wird der gegebene Teil der Hilfe nach dem Drücken der linken Maustaste zweimal vermindert, d.h. man kann einen gröseren Teil sehen, aber mit kleineren Ausführlichkeiten.

Die weiteren vier Tasten dienen zur Bewegung in der Hilfe (die anderen Parameter, z. B. die Luppe, bleiben unverändert):


Diese Taste dient zum Transfer auf die erste Seite der Hilfe.


Durch Drücken dieser Taste kann man auf die vorherige Seite kommen.


Durch Drücken dieser Taste kommt man auf die nächste Seite.


Nach dem Drücken dieser Taste wird die letzte Seite der Hilfe abgebildet.

Die weiteren zwei Tasten ermöglichen die bisher durchgeführten Schritte wieder durchzugehen:


Diese Taste hebt die zuletzt durchdgeführte Anweisung auf, d.h.kehrt das Fenster mit der Hilfe in den Zustand zurück, in dem es war vor ihrer Durchführung. So kann man z. B. auf alle vorher gegesehenen Hilfeseiten zurückkehren.


Wenn sie mit der vorherigen Taste ein Schritt zurückgemacht haben, ist es möglich mit dieser Taste siech ein Schritt nach vorne zu bewegen. In anderen Worten, wird

dieselbe Operation durchgeführt, die sie mit der vorherigen Taste abgerufen haben. Diese Taste kann nur dann benützt werden wenn sie nach dem Drücken der vorherigen Taste keine Operation vorgenommen haben.

Die folgenden drei Tasten dienen zur schnellen Einstellung der Luppe nach der abgebildeten Seite:

Die Taste stellt die Seitenabbildung in ihrer wirklichen Grösse, d.h. stellt den Wert der Luppe auf hundert Prozent. Es ist möglich, daß die abgebildete Seite grösser oder umgekehrt kleiner wird als der Fensterteil, der zu ihrer Abbildung reserviert wurde.

Nach dem Drücken dieser Taste wird der Luppenwert so eingestellt, daß man die komplette Seite sehen kann. Bei der Änderung von der Fenstergrösse wird auch die Seitengrösse verändert.

Mit dieser Taste können sie das Luppenwert so einstellen, das die Seitenbreite der Breite des Fensters mit der Hilfe entspricht. Keine Rücksicht wird auf die Seitenhöhe genommen. Bei der Änderung der Fensterbreite wird auch die Seitenbreite verändert.

5.4 Meldung zur Entdeckung eines Virus

Wenn ein Virus während des Aufgabenlaufs entdeckt wurde, dann erstellt das AVAST32 Programm eine Warnmeldung (Abb. 80). Der Text dieser Meldung hängt von der Einstellung der Aufgabe, die das Virus entdeckt hat (siehe Kapitel 4.4.12) ab.

Abb. 80

Durch Betätigung der Taste "Fortsetzen" teilen sie dem Programm mit, die Aufgabe fortzusetzen. Die infizierte Datei kann man dann später auf der Seite "Ergebnisse" behandeln (Kapitel 5.3.2).

Die Taste "Korrigieren..." dient zur unmittelbaren Reparatur der infizierten Datei. Es wird der gleiche Dialog hervorgerufen wie es bei der Funktion "Korrigieren..." in dem Lokalangebot auf der Seite "Ergebnisse" der erweiterten Bedienung der

Fall war. Eine ausführliche Dialogbeschreibung gibt es im Kapitel 5.3.2. Nach der Reparatur der Datei wird die Aufgabendurchführung fortgesetzt.

Die Taste "Umbenennen/Verschieben..." ermöglicht dem Benutzer die infizierte Datei in eine andere Mappe umzulagern und/oder ihr Suffix zu ändern. Eine ausführliche Beschreibung der gleichnamigen Funktion gibt es im Kapitel 5.3.2. Nach der Umlagerung und Umnennung der Datei wird die Aufgabendurchführung fortgesetzt.

Die Taste "Löschen..." dient zum Auslöschen der infizierten Datei von der Platte. Eine ausführliche Dialogbeschreibung gibt es im Kapitel 5.3.2. Nach seinem Abschluß wird die Durchführung der Aufgabe fortgesetzt, die das Virus entdeckt hat.

Durch die Betätigung von der "Stop" Taste beenden sie den Lauf der Aufgabe, die das Virus entdeckt hat.

Die Meldung zur Entdeckung eines Virus enthält auch zwei Bedienungselemente.

Durch Anhaken des Feldes "Diese Meldung nicht wieder anzeigen" teilen sie dem Programm mit, daß wenn es ein weiteres Virus entdeckt, soll es keine Meldung abbilden. Implizit ist das Feld nicht angehakt.

Durch Anhaken des Feldes "Für sonstige Dateien wiederholen" teilen sie dem Programm mit, daß wenn es ein weiteres Virus entdeckt, soll es mit ihr dieselbe Operation durchführem, die mit dieser Datei gemacht wurde. Das Feld ist zugänglich nur wenn das Feld "Diese Meldung nicht wieder anzeigen" angehakt ist. Diese Möglichkeit ist nicht implizit erlaubt.

5.5 Auswahl der getesteten Bereiche

Das AVAST32Programm braucht in einigen Plätzen zu bestimmen, welche Bereiche, also Dateien, Mappen bzw. ganze Platten, kontroliert werden sollen. Deswegen enthält es ein Dialog, das diese Tätigkeit erleichtert (Abb. 81). Es ermöglicht sogar mehrere Mappen oder Platten auf einen Ruck auszuwählen, womit es die Arbeit mit dem Programm sehr erleichtert.

Der obere Teil des Dialogs ist praktisch identisch mit dem Standarddialog für die Dateieröffnung, das ein Bestandteil des Operationssystems ist. Der Benutzer wählt hier die Datei, Mappe bzw. die ganze Platte, die er auswählen will, auf eine geläufige Weise und durch Betätigung der Taste "Einfügen" fügt er die gewählte Eintragung in die Liste zu, die sich in dem unteren Dialogteil befindet. So wird der Benutzer fortsetzen bis die Liste alle Bereiche enthält, die zu kontrollieren sind.

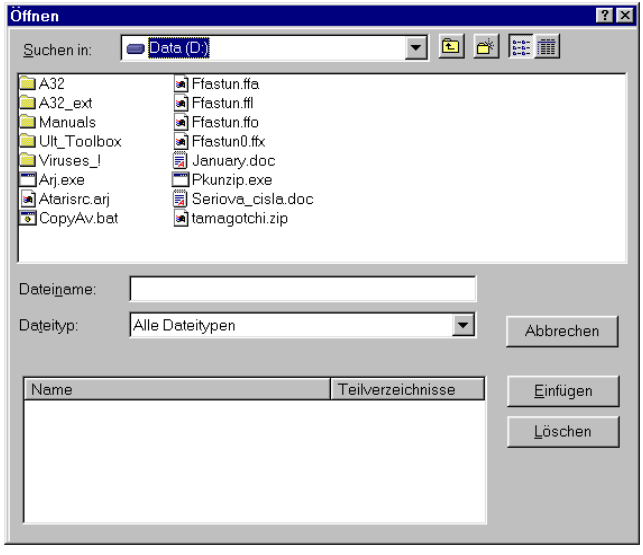

Abb. 81

Haben sie sich bei der Auswahl geirrt oder wollen sie einfach einen aus den gewählten Bereichen nicht mehr kontrollieren, dann entfernen sie ihn einfach aus der Liste. Das wird so gemacht, daß sie ihn zunächst auswählen und dann durch die Betätigung der Taste "Löschen" aus der Liste der gewählten Bereiche entfernen. Mit dem Bereich, der aus der Liste enfernt wurde, wird die ensprechende Operation nicht durchgeführt.

Wenn sie alle gewünschte Bereiche ausgewählt haben, können sie durch Betätigung der Taste "OK" die Durchführung der entsprechenden Operation anlaufen. Wenn sie die Taste "Abbrechen" drücken (oder das Dialog auf eine andere Weise schließen), wird die Durchführung der gewählten Operation aufgehoben und die ausgewählten Dateien werden ignoriert werden.

6.Programmeinstellungen

Das Menü "Optionen" (Abb. 82) dient zur Anpassung der Funktionen und Eigenschaften des AVAST32 Programms.

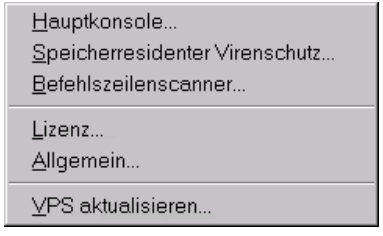

Abb. 82

Nach der Auswahl jedes beliebigen Elementes erscheint ein Dialog, in dem man die entsprechenden Steuerelemente nach Bedarf einstellen kann. Alle Dialoge sind, ähnlich dem Hauptfenster des AVAST32 Programms, in einige Seiten unterteilt, unter denen mit Hilfe von Lesezeichenliste umgeschaltet werden kann.

Die Seiten sind durch Kugeln in verschiedenen Farben markiert. Hat die Kugel blaue Farbe, sind die Steuerelemente auf der entsprechenden Seite auch für den normalen Benutzer bestimmt - ihre Einstellung hat keine grundlegende Bedeutung für den Betrieb und Funktionsfähigkeit des Programms. Ist die Kugel allerdings rot, sollten die Steuerelemente nur durch ein enerfahrenen Benutzer verändert werden, der genau weiß, was er durch diese Veränderung verursacht.

In den folgenden Kapiteln werden die einzelnen Elemente des Menüs "Optionen" des Hauptfensters eingehend beschrieben.

6.1 Element "Hauptkonsole..."

Das Dialog, das nach der Auswahl dieses Elementes erscheint, enthält auf einigen Seiten die Steuerelemente für die Einstellung des AVAST32 Programms und seiner Umgebung.

6.1.1 Seite "Grundlegende Informationen"

Die Seite "Grundlegende Informationen" ermöglicht dem Benutzer, das Programmverhalten den eigenen Bedürfnissen anzupassen (Abb. 83). Alle Steuerelemente auf dieser Seite sind getrennt für jeden Benutzer gespeichert, was eine individuelle Einstellung des AVAST32 Programms ermöglicht.

Ihre Veränderung macht sich erst nach dem nächsten Start des Programms bemerkbar.

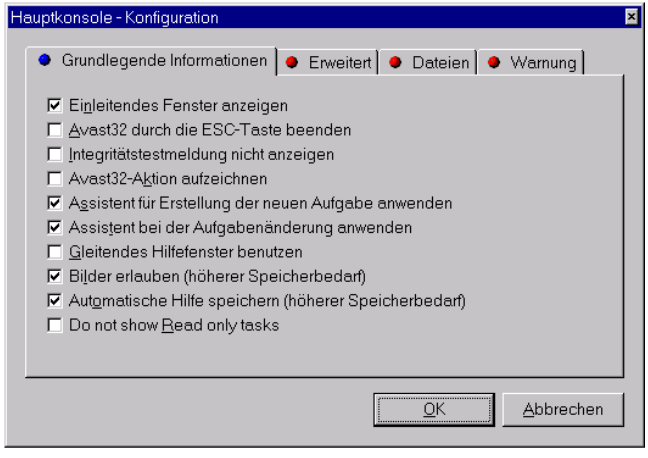

Abb. 83

Durch das Abhaken des Feldes "Einleiten des Fenster anzeigen" schalten Sie das Abbilden von dem Zeichen des AVAST32 Programms nach seinem Start ein. Stört Sie das Zeichen, oder wollen Sie den Programmstart etwas schneller haben, dann haken Sie das Feld nicht ab. Das Feld ist als abgehakt vorgegeben.

Das Abhakfeld "Avast32 durch die ESC-Taste beenden" bestimmt, daß es möglich ist, das Programm AVAST32 durch das drücken der "Esc" Taste zu beenden. Das ist besonders für erfahrenere Benutzer vorteilhaft, die die Programme lieber mit Hilfe von Zugriffstasten steuern. Der normale Benutzer sollte das Feld nicht abhaken, um eine ungewollte Programmbeendigung zu verhindern. Das Feld ist als nicht abgehakt vorgegeben.

Das Abhakfeld "Integritätstestmeldung nicht anzeigen" schaltet die Abbildung der Meldungen über die Beendigung des Datenintegritätstests ab (Abb. 84). Dabei ist es egal, ob es sich um einen normalen oder einen vereinfachten Test handelt.

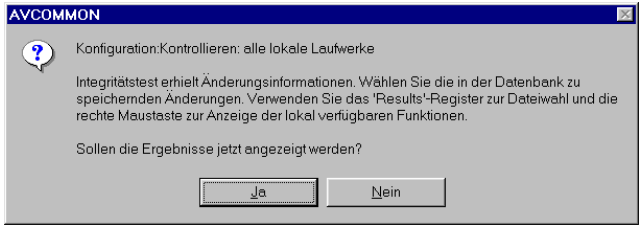

Abb. 84

Die Meldung wird nur dann abgebildet, wenn eine von den getesteten Dateien verändert wurde. Sie enthält auch die Frage, ob der Benutzer wünscht, die Resultate der Aufgabe abzubilden. Nach einer positiven Antwort, d.h. nach der Betätigung der "Ja" Taste, wird die Seite "Ergebnisse" der erweiterten Steuerung aktiviert (wenn Sie in der einfachen Steuerung arbeiten, schaltet das

Programm automatisch in die erweiterte Steuerung um). Die Abbildung der Meldungen ist als zugelassen vorgegeben.

Das Abhakfeld "Avast32-Aktion aufzeichen" schaltet die Anmeldung an. In Windows 95 besteht die Anmeldung darin, daß sich in der Mappe des AVAST32 Programms eine Textdatei mit dem Namen "AVAST32.log" bildet, in die alle durch das Programm vorgenommenen Vorgänge eingetragen werden. Weiter werden hier Informationen über gefundene Viren, über die mit dem Programm arbeitenden Benutzer,usw. eingetragen. Die Größe der Anmeldedatei ist durch die Angabe, die auf der Seite "Dateien" (Kapitel 6.1.3) in das Textfeld "Größe der Protokolldatei" eingetragen wurde, gegeben. Die Anmeldung ist als ausgeschaltet vorgegeben.

Unter dem Operationssystem Windows NT versucht das Programm, die Anmeldeinformationen in die Systemanmeldedatei einzutragen. Die kann mit Hilfe von Programm "Event Viewer" angesehen werden, das durch Auswahl des gleichnamigen Elementen aus der Mappe "Programme/Administratorsmittel" angelaufen werden kann. Wenn die Anmeldeinformation aus irgendwelchem Grund nicht in die erwähnte Datei eingetragen werden kann, wird wie in Windows 95 verfahren.

Die Anmeldung ist besonders in der Netzumgebung geeignet, wo auf dieser Weise das Vorgehen einzelner Benutzer kontrolliert werden kann.

Das Abhakfeld "Assistent für Erstellung der neuen Aufgabe anwenden" aktiviert den sog. "Assistenten", der Sie durch die Erstellung einer neuen Aufgabe begleiten wird (siehe Kapitel 4). Wir empfehlen, dieses Feld abzuhaken, besonders für die anfangenden Benutzern. Das Feld ist als abgehakt vorgegeben.

Das Abhakfeld "Assistent bei der Aufgabeänderung anweden" aktiviert, ähnlich wie bei dem vorangegangenen Feld, den Assistenten, diesmal allerdings für die Änderung existierender Aufgaben (siehe Kapitel 4). Die Ausnutzung des Assistenten ist als eingestellt vorgegeben.

Durch das Abhakfeld "Gleitendes Hilfefenster benutzen" kann man einstellen, das die Hilfe vom AVAST32 Programm eine beliebige Position auf dem Bildschirm einnehmen kann und nicht auf die Seite "Hilfe" gebunden ist (Kapitel 5.3.4). Das Feld ist als nicht abgehakt vorgegeben.

Das Abhakfeld "Bilder erlauben (höher Speicherbedarf)" schaltet die Abbildung von Bildern im Hauptfenster des AVAST32 Programms ein. Die Bilder illustrieren den durchgeführten Vorgang und machen die Arbeit mit dem Programm bequem. Ihre Anwendung beanspruch jedoch den

Operationsspeicher des Computers, und wenn Sie nicht genug Speicher haben, oder wenn Sie die Bilder einfach nicht wollen, haken Sie das Feld nicht ab. Die Anwendung von Bildern ist als zugelassen vorgegeben.

Das Abhakfeld hat nur auf das Programm AVAST32 Einfluß - die Bilder aus den Dialogen der Programme WARN32 und QUICK32 werden nicht entfernt.

Das Abhakfeld "Automatisch Hilfe speichern" dient dazu, die Dateien mit der Hilfe des AVAST32 Programms nach seinem Start automatisch einzuführen. Es ist also nicht notwendig, sie bei jedem Aufruf der Hilfe erneut vom Disk einzuführen. Ist das Feld nicht abgehakt, wird die Hilfedatei auf Ersuchen des Benutzers, das heißt nach dem Abhaken des entsprechenden Menüelements oder nach der Betätigung der Taste "F1", eingeführt. Das Feld ist abgehakt vorgegeben.

Wenn Sie genug Operationsspeicher haben und oft Hilfe benutzen, empfehlen wir Ihnen, das Feld abzuhaken. Auf dieser Weise wird die Hilfeabbildung beschleunigt.

6.1.2 Seite "Erweitert"

Die Steuerelemente auf der Seite "Erweitert" werden in der Abb. 85 dargestellt. Ihre Änderung beeinflußt alle Benutzer, die mit dem Programm arbeiten, weil die Einstellung dieser Einstellungselemente für das Programm AVAST32 als Ganzes gespeichert wird.

Die Veränderung der Steuerelemente kommt nur nach dem nächsten Programmstart zum Vorschein.

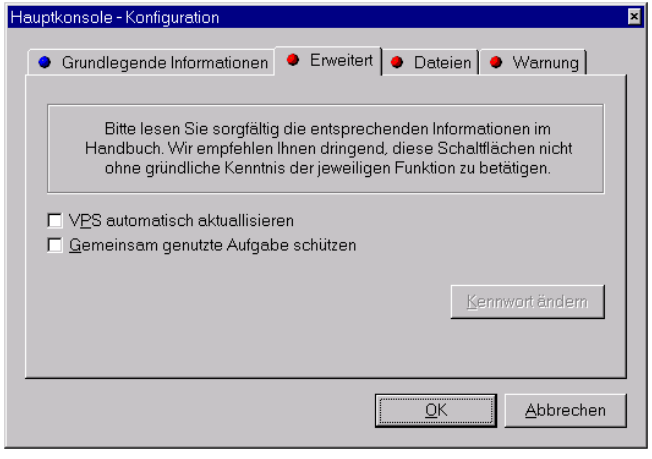

Abb. 85

Das Abhakfeld "VPS automatisch aktualisieren" dient zur Zulassung des automatischen Aktualisieren der VPS Datei, die die Datenbank der bekannten Viren enthält. Ist das Feld abgehakt, sucht das AVAST32 Programm nach seinem Start automatisch die eingestellte Mappe (Kapitel 6.6, Textfeld "Name der Quelldatei:"). Wenn das Pro-

gramm eine VPS Datei findet, die neuer als die bestehende ist, wird die bestehende VPS Datei automatisch durch die neuere ersetzt. Im entgegengesetzten Fall wird mit der bestehenden VPS Datei nichts getan.

Eine automatische Aktualisierung der VPS Datei ist nicht zugelassen.

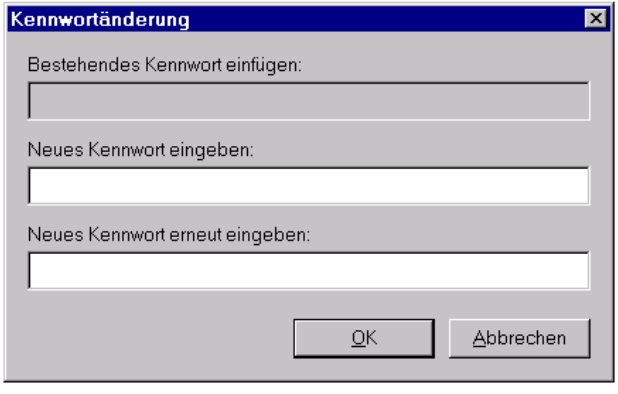

Abb. 86

Das Abhakfeld "Gemeinsam genutzte Aufgabe schützen" ermöglicht die gemeinsam genutzten Aufgaben vor Veränderung durch ein Kennwort zu schützen. Nach seinem Abhaken kommt ein Dialog zum Vorschein, das die Kennworteingabe ermöglicht (Abb. 86). Es ist notwendig, das Kennwort zweimal einzutragen und zwar zunächst in das Textfeld "Neues Kennwort eingeben" und für die Kontrolle auch in das Textfeld "Neues Kennwort erneut eingeben". Wenn das Kennwort in beiden Feldern gleich eingetragen wurde, wird es genutzt. Im entgegengesetzten Fall werden Sie darauf aufmerksam gemacht und Sie werden noch eine Möglichkeit bekommen, das Kennwort erneut einzutragen. Das Abhaken des Feldes kann nur mit dem Kenntnis des jetzt gültigen Kennworts aufgehoben werden.

Sind die gemeinsam genutzten Aufgaben durch Kennwort geschützt, werden ohne seine Kenntnis keine weiteren Vorgänge außer Aufgabenstarts, -anhalten, -beendigung, Erstellen einer Privatkopie und Erstellen eines Vertreters auf des Fläche mit den gemeinsam genutzten Aufgaben zugelassen.

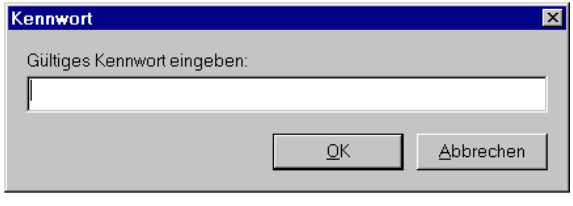

Abb. 87

In der Abb. 87 ist ein Dialog dargestellt, das immer abgebildet ist, wenn das Kennwort eingegeben werden muß. Ist das Kennwort richtig, wird dem

Benutzer der entsprechende Vorgang mit der Aufgabe ermöglicht. Die Eingabe des Kennworts wird beim Benutzer nur einmal abgefragt - Das Programm merkt sich das **richtige** Kennwort und seine wiederholte Eingabe wird er erst nach dem nächsten Start vom AVAST32 Programm oder nach der Änderung des Kennworts gebeten.

Zur Änderung des bestehenden Kennworts dient die Taste "Kennwort ändern". Nach ihrer Betätigung kommt das gleiche Dialog zum Vorschein wie in dem Fall der Einstellung des Schutzes der gemeinsam genutzten Aufgaben. Vor dem Eintragen des neuen Kennworts ist es notwendig, in das Textfeld "Bestehendes Kennwort einfügen" das bestehende Kennwort einzutragen, und zwar auch in dem Fall, daß der Benutzer schon das Kennwort während des Programmbetriebes eingegeben hat. Ohne die richtige Eingabe des Kennworts wird das Kennwort nicht verändert!

6.1.3 Seite "Dateien"

Die Seite "Dateien" gibt dem Benutzer die Möglichkeit, die Dateien näher zu bestimmen, mit denen das Programm AVAST32 arbeitet (Abb. 88).

Die Einstellungen der Steuerelemente auf dieser Seite werden für das Programm als Ganzes gespeichert, so daß durch ihre Änderung alle Benutzer beeinflußt werden. Die durchgeführten Veränderungen werden nur nach dem nächsten Start des AVAST32 Programms berücksichtigt.

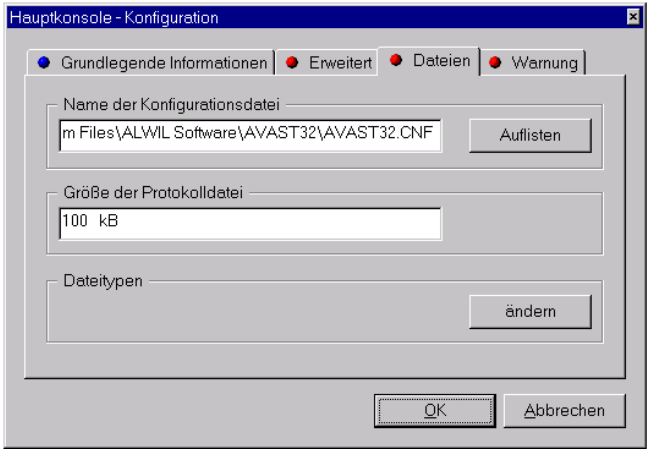

Abb. 88

Durch das Textfeld "Name der Konfigurationsdatei" hat der Benutzer die Möglichkeit, den Konfigurationsdateinamen (*.CNF) des AVAST32 Programms inklusive ihres Pfads einzutragen. Auf diese Weise spezifizierte Konfigurationsdatei wird anstatt der bestehenden Datei genutzt.

Die Taste "Auflisten" dient zur Bestimmung der Konfigurationsdatei mit Hilfe von einem standarden Systemdialog für die Öffnung von Dateien (Abb. 89). Der Name der ausgewählten

Datei wird automatisch in das obengenannte Textfeld eingegeben. Die Konfigurationsdatei aus der Mappe des Programms AVAST32 wird als genutzt vorgegeben.

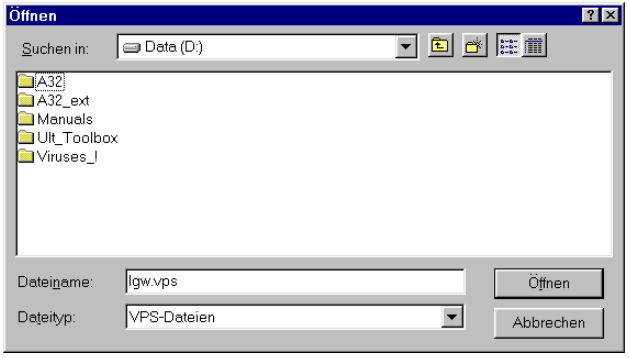

Abb. 89

Im Textfeld "Größe der Protolldatei" kann die maximale Größe der Anmeldedatei eingestellt werden. Die Größe der Anmeldedatei wird in KB (in Killobytes) angegeben. Wenn die Anmeldedatei die gegebene Größe erreicht, wird etwa ihr erstes Drittel gelöscht. Damit werden die ältesten Angaben aus der Datei entfernt und zur Platz für neue Angaben geschaffen. Vorgegeben ist eine maximale Anmeldedatei von 64 KB.

Die Angabe im Textfeld hat nur unter Windows 95 Sinn und das dann, wenn die Anmeldung erlaubt ist (nähere Informationen siehe Kapitel 6.1.1, Abhakfeld "Anmeldung des AVAST32 Programms erlauben").

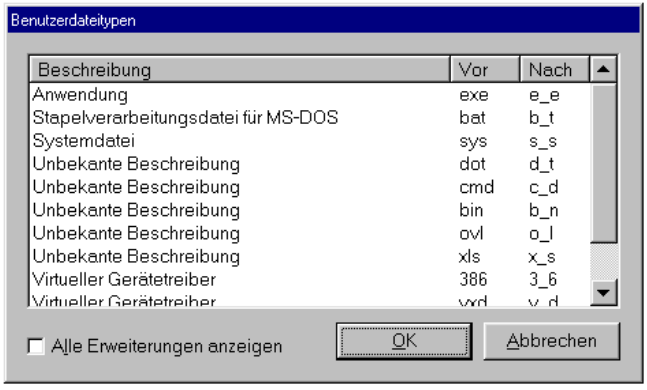

Abb. 90

Die Taste "Ändern" dient zum Aufruf eines Dialogs, in dem es möglich ist, die neue Erweiterung für den gegebenen Dateityp einzustellen (Abb. 90). Das Dialog enthält eine Liste von bekannten Dateitypen und ihrer Erweiterungen (Spalte "Vor"). Die Spalte "Nach" enthält die Erweiterungen, die bei der Umbenennung des gegebenen Dateityps die bestehende Erweiterung ersetzt. Das Dialog kann nur die wichtigsten Erweiterungen oder alle bekannten Erweiterungen

enthalten - es kann durch Abhaken des Feldes "Alle erweiterungen anzeigen" gewählt werden.

Die in diesem Dialog enthaltenen Erweiterungen werden bei der Umbenennung der Datei auf der Seite "Ergebnisse" genutzt (Kapitel 5.3.2). Die Dateien, die in der Baumstruktur auf dieser Seite aufgeführt sind, wurden irgendwie verändert oder das Programm hat in einer von den Dateien sogar ein Virus erkannt. In dem Fall ist es geeignet, (besonders bei den ausführbaren Dateien), die datei umzunennen, damit es nicht zu ihrer ungewollten Ausführung kommen kann.

Wenn Sie die Erweiterung eines Dateityps ändern wollen, wählen Sie sie zunächst aus und dann klopfen Sie auf sie mit der linken Maustaste. Iihre Bearbeitung wird ermöglicht. Die neue Erweiterung wird mit der Taste "Enter" bestätigt.

Sind Sie mit den Veränderungen zufrieden, die Sie mit den Dateierweiterungen durchgeführt haben, drücken Sie die Taste "OK". Die neuen Dateierweiterungen werden bei einer neuen Umbenennung der Dateien ausgenutzt, ohne das Programm erneut starten zu müssen. Wenn Sie lieber die Erweiterungen ausnutzen wollen, die bisher genutzt wurden, betätigen Sie die Taste “Abbrechen”.

6.1.4 Seite "Warnung"

Die Seite "Warnung" dient zur Auswahl von Computern (Abb. 91), zu den im Fall eines Virusfundes eine Warnmeldung geschickt werden soll. Die Benutzer dieser Computer werden zusammen mit denen informiert werden, die den Computer während der Erstellung der Aufgabe ausgewählt haben, wo das Virus gefunden war (Kapitel 4.4.11).

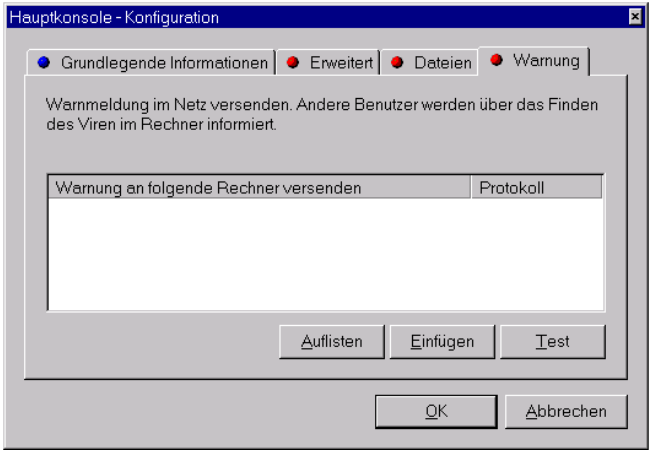

Abb. 91

Die Liste der ausgewählten Computer wird im Programm AVAST32 als Ganzes gespeichert, so

daß ihre Veränderung alle Benutzer beeinflußt. Die Veränderungen treten nach dem nächsten Start des AVAST32 Programms in Kraft.

Es ist möglich, den Computer, auf den die Meldung über den Virusfund geschickt wird, durch direkte Eintragung seines Namens in die Liste der ausgewählten Computer zu bestimmen. Durch die Betätigung der Taste "Einfügen" bilden sie das Lokalmenü mit einigen Protokollen ab:

- das Objekt "Internet" bestimmt, daß der Computer, auf den die Warnmeldung geschickt werden soll, durch eine standarde URL Adresse bestimmt ist. Für die Nachrichtzustellung wird das Internetprotokoll ausgenutzt,
- durch das Objekt "Microsoft" teilen Sie dem Programm mit, daß der Computer mittels Microsoft Exchange Post zugreifbar ist,
- das Objekt "Intern" heißt, daß für den Zugriff zu dem ausgewählten Computer das Protokoll für das Lokalnetz ausgenutzt werden kann (der Computer muß allerdings über das Lokalnetz verfügbar sein).

Nach der Wahl des entsprechenden Protokolls wird das Element mit dem Namen "Gültige Rechnerbezeichnung angeben !!" in die Liste beigefügt. Wenn Sie auf sie mit der linken Maustaste klopfen, wird ihre Bearbeitung ermöglicht. Nach dem Eintragen des Namens in den Computer betätigen Sie die Taste "Eingabe".

Nach dem Drücken der Taste "Auflisten" erscheint wieder das Lokalmenü mit Protokollen (zur Zeit enthält sie nur den Objekt "Intern", siehe oben). Sie können den Computer, der über das Lokalnetz verfügbar ist, mittels Dialogs auswählen, das auf der Abb. 52 gezeigt wird.

Sie können den Computernamen aus der Liste entfernen, indem Sie ihn zunächst auswählen und dann die Taste "Del" drücken.

Die Parameter der Objekte in der Liste, bzw. der ausgewählten Computer, können nachträglich verändert werden. Wenn Sie das Zugriffsprotokoll auf den Computer in Frage ändern wollen, klopfen Sie in der Spalte "Protokoll" des entsprechenden Computers. Dann wählen sie ein neues Protokoll aus dem Lokalmenü. Auf eine ähnliche Weise können Sie auch den Namen oder die Adresse des Computers ändern: nach Betätigung der linken Maustaste wird seine Bearbeitung ermöglicht.

Sollen Sie nicht über die Zustellung der Warnmeldung sicher sein, können Sie “die Kommunikation“ mit der Taste "Test" prüfen. Auf jeden ausgewählten Computer wird eine Testmeldung geschickt. Die Liste der Computer, auf die die Warnmeldungen geschickt werden sollen, ist als leer vorgegeben.

6.2 Element "Speicherresidenter Virenschutz..."

Durch die Auswahl dieses Objektes wird das Dialog eröffnet, das in der Abb. 92 dargestellt ist. Es enthält Steuerungselemente für die Einstellung der Teile, die den residenten Schutz sichern (es handelt sich um das Programm RGW32, siehe Kapitel 9).

Die Veränderung tritt nur nach dem nächsten Programmstart in Kraft.

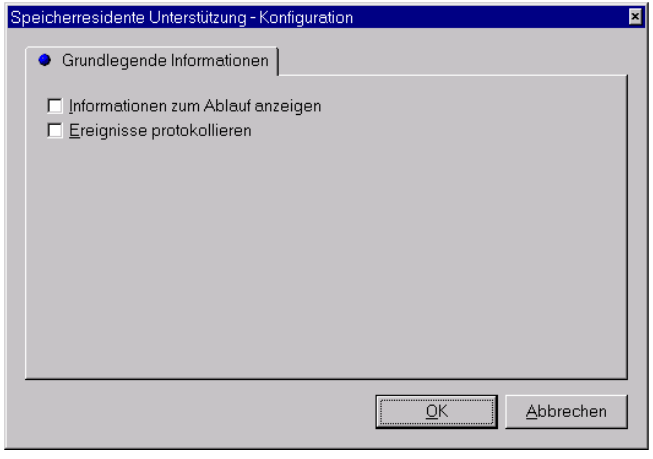

Abb. 92

Das Abhakfeld "Informationen zum Ablauf anzeigen" bestimmt, ob der Benutzer wünscht, über die verlaufenden residenten Vorgänge informiert zu sein. Ist das Feld abgehakt, wird links unten auf der Arbeitsfläche eine kurze Information über den gerade durchgeführten residenten Vorgang abgebildet. Ist das Feld nicht abgehakt, keine Information wird abgebildet, was auch die vorgegebene Eistellung ist.

Durch das Abhaken des Feldes "Ereignisse protollieren" kann der Benutzer dem Programm seinen Wunsch mitteilen, daß die Informationen über den Vorgang der residenten Schutze in die sog. Anmeldedatei eingetragen werden sollen (eine eingehendere Beschreibung ist im Kapitel 6.1.1, bei dem Abhakfeld "Avast32-Aktion aufzeichen" aufgeführt).

6.3 Objekt "Befehlszeilenscanner..."

Nach der Auswahl des Objektes "Befehlszeilenscanner..." erscheint das Dialog, das in der Abb. 93 dargestellt ist. Es enthält Steuerelemente für die Grundeinstellung des sog. Zeichenscanners, d.h. eines Programms für die Virussuche, das von der Anweisungszeile gestartet wird (es handelt sich um Programm LGW32, siehe Kapitel 8).

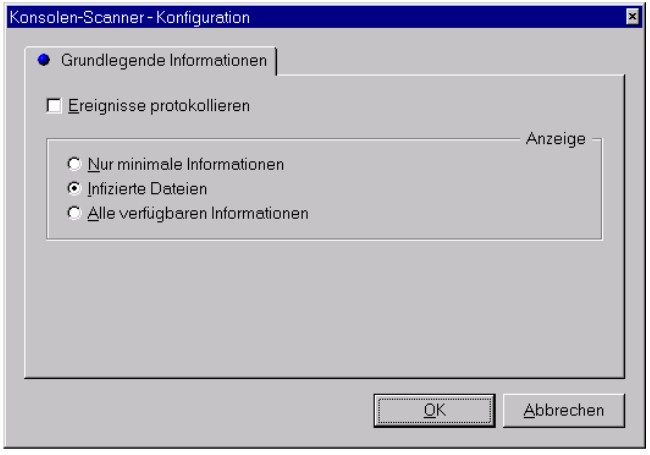

Abb. 93

Mit Hilfe des Abhakfelds "Ereignisse Protollieren" kann der Benutzer dem Programm seinen Wunsch mitteilen, daß Informationen über den Vorgang des Zeichenscanners in die Anmeldedatei eingetragen werden sollen (eine eingehendere Beschreibung ist im Kapitel 6.1.1, am Abhakfeld "Avast32-Aktion aufzeichen").

Das Dialog enthält auch Optionen, mit Hilfe von denen der Benutzer eine Menge von Informationen einstellen kann, die in der Standardausgabe sind (gewöhnlich geht es um ein Fenster der Anweisungszeile):

- Option "Nur minimale Informationen" bewirkt, daß der Zeichenscanner nur seine Titelzeile schreiben wird,
- Nach der Auswahl der Option "Infizierte Dateien" wird die Titelzeile des Zeichenscanners, Informationen über eventuellen infizierten Dateien und Viren, mit denen sie infiziert sind, abgebildet. Auch eine Tafel mit sämtlicher Statistik über den Testverlauf wird abgebildet,
- Durch die Option "Alle verfügbaren Informationen" teilt der Benutzer dem Zeichenscanner, daß er wünscht, über alles informiert zu werden, was gerade durchgeführt wird und auch über die Resultate seines Vorganges.

Die Menge der Informationen, die durch den Zeichenscanner abgebildet werden, kann auch mit Hilfe von Parametern auf der Anweisungszeile einstellen (siehe Kapitel 8, Parameter /V). In einem solchen Fall wird auf die Einstellung auf dieser Seite keine Rücksicht genommen.

6.4 Element "Lizenz..."

Das Dialog, das mit dem Objekt "Lizenz" verbunden ist , ermöglicht dem Benutzer, den Programmaktivierungsschlüssel zu ändern (Abb. 94). Es enthält unter anderem auch die Information über die Anzahl der gekauften Lizenzen, wenn Sie sich für den Kauf von weiteren Lizenzen entscheiden.

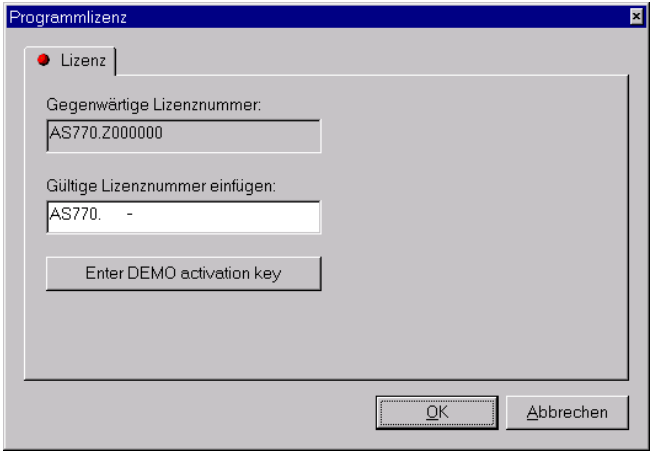

Abb. 94

Die Seite enthält oben den bestehenden Aktivierungsschlüssel. Unter ihm befindet sich ein Textfeld, das ermöglicht, einen neuen Aktivierungsschlüssel einzutragen. Durch die Betätigung der Taste "OK" führen Sie die eigentliche Änderung des Aktivierungsschlüssels ein. Soll der eingetragene Aktivierungsschlüssel ungültig sein, bekommen Sie eine Fehlermeldung und der Aktivierungsschlüssel wird nicht verändert.

Die Bedeutung einzelner Teile des Aktivierungsschlüssel ist im Anhang D erklärt.

6.5 Element "Allgemein..."

Das Dialog, das nach der Wahl dieses Objekts zum Vorschein kommt, enthält Seiten mit Steuerelementen, die gemeinsam für alle Teile des AVAST32 Programms sind.

6.5.1 Seite "Grundlegende Informationen"

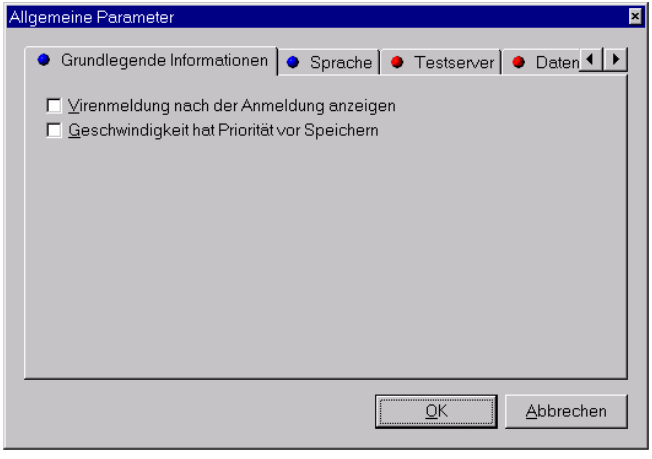

Abb. 95

Diese Seite enthält Steuerelemente für die standarde Einstellung aller Teile des AVAST32

Programms (Abb. 95). Die Einstellung der Steuerelemente auf dieser Seite wird für das Programm als Ganzes gespeichert, so daß ihre Änderung alle Benutzer beeinflußt. Die Änderungen, die auf dieser Seite vorgenommen wurden, treten allerdings nur nach dem nächsten Start des AVAST32 Programms in Kraft.

Das Abhakfeld "Virenmeldung nach der Anmeldung anzeigen" dient zum Erlaubnis von Abbildung einer Warnmeldung nach dem Benutzeranmelden in das System. Die Warnmeldung wird nur dann abgebildet, wenn ein Virus während des letzten Starts gefunden wurde. Der Benutzer ist auf dieser Weise informiert, daß er mit einem infizierten Computer arbeitet. Das Feld ist als nicht abgehakt vorgegeben.

Für das Abbilden von Warnmeldungen wird das Programm WARN32 genutzt, das detaillierter im Kapitel 11 beschrieben ist.

Das Abhakfeld "Geschwindigkeit hat Priorität vor Speicher" sagt dem Programm, unter welchen Bedingungen der Testserver (Datei "VPS32.DLL", siehe Anhang A) im Speicher anwesend sein soll. Ist das Feld nicht abgehakt, wird der Testserver seit seiner ersten Ausnutzung im Speicher anwesend und wird nicht einmal nach der Beendigung seines letzten Vorgangs entfernt. Ist das Feld abgehakt, wird der Testserver aus dem Operationsspeicher entfernt, sobald er nicht benötigt wird, d.h. nach der Beendigung der letzten durchzuführenden Aufgabe. Nach dem Start der nächsten Aufgabe wird der Testserver von der Festplatte erneut geladen.

Wenn Sie genug Platz im Operationsspeicher haben, empfehlen wir Ihnen, das Feld nicht abzuhaken. Sie werden auf diese Weise den Lauf des AVAST32 Programms beschleunigen. Sollen Sie nicht genug Operationsspeicher haben, dann haken Sie das Feld lieber nicht ab - Sie müssen aber mit einer langsameren Programmreaktion rechnen. Das Feld ist als nicht abgehakt vorgegeben.

6.5.2 Seite "Sprache"

In die Seite "Sprache" kann dem Benutzer unter Sprachen umschalten, die das Programm AVAST32 unterstützt (Abb. 96). Die Sprachen befinden sich in der Liste im rechten Bereich der Seite. Die Sprache, in der das Programm gerade kommuniziert, ist mit einer gelben Kugel und die anderen mit blauen Kugeln versehen.

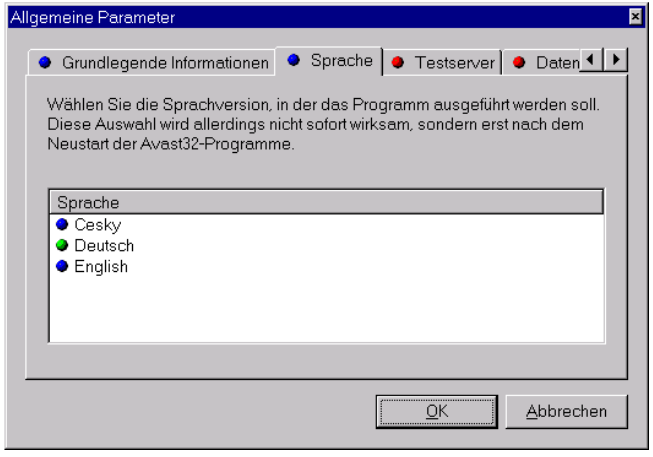

Abb. 96

Wenn Sie die Sprache des AVAST32 Programms ändern wollen, klopfen Sie sie mit der linken Maustaste. Die Änderung der Sprache kommt erst nach dem nächsten Programmstart zum Ausdruck. AVAST32 "merkt sich" die eingestellte Sprache für jeden Benutzer getrennt, so daß die Änderung nur die Einstellung des Benutzers beeinflußt, der sie durchgeführt hat.

Die Sprache ist als vorgegeben eingestellt, die der Benutzer vor der eigentlichen Installierung gewählt hat (Abb. 3).

6.5.3 Seite "Testserver"

Die Seite "Testserver" ermöglicht dem Benutzer, die Grundparameter des sog. Testservers einzustellen (Abb. 97). Er wird von allen Teilen des AVAST32 Programms benutzt, so daß die hier durchgeführten Änderungen jeden von seinen Teilen sowie auch jeden Benutzer beeinflussen, der mit dem Programm AVAST32 auf dem Computer arbeitet (nähere Informationen über den Testserver sind im Anhang A).

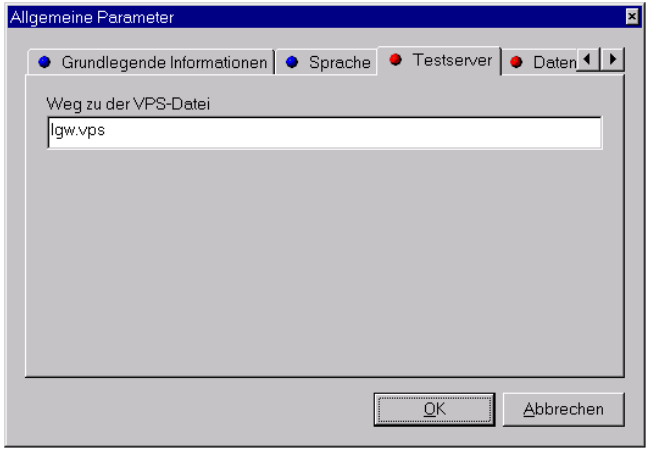

Abb. 97

Das Textfeld "Feg zu der VPS-Datei" enthält die VPS Dateiname, d.h. den Namen der Datei mit der Datenbank der bekannten Viren, einschließlich des kompletten Pfads. Weil es sich um eine sehr wichtige Datei handelt, sollte dem Benutzer bewußt sein, daß er sich durch Angabe einer nicht richtigen VPS Datei in Gefahr der Nichterkennung der Viren setzt oder umgekehrt, daß er falsche Alarmmeldungen bekommt. Das Textfeld enthält den Dateinamen "lgw.vps" aus der Mappe des AVAST32 Programms.

6.6 Element "VPS Aktualisieren..."

Das Programm AVAST32 ermöglicht eine einfache Aktualisierung der Datenbank der bekannten Viren. Es genügt, nur die bestehende Datei LGW.VPS durch eine neuere zu ersetzen; es ist also nicht notwendig, das Programm selbst umzuinstallieren.

Sie können die Datei LGW.VPS manuell kopieren (wir jedoch empfehlen dieses Vorgehen nicht sehr) oder Sie können dieses Objekt wählen. Nach seiner Auswahl erscheint ein Dialog, das man in der Abb. 98 dargestellt ist.

Abb. 98

Das Textfeld "Name der Quelldatei" enthält den Pfad zur Mappe, wo eine neuere VPS Datei gesucht wird. Die Aktualisierung der VPS Datei kann auch automatisch durchgeführt werden, (siehe Kapitel 6.1.2, das Abhakfeld "Automatisch VPS aktualisieren"). Wenn Sie das Programm AVAST32 aus dem CD-ROM installiert haben, dann wird das Textfeld den vorgegebenen Pfad "<cd>:\AVS\LGW.VPS" enthalten, wo anstelle von <cd> die Markierung Ihrer CD-ROM Einheit steht. Bei der Installierung von Disketten ist der Pfad "A:\LGW.VPS" vorgegeben.

Die notwendige Mappe kann man auch mit Hilfe eines Standarddialogs für das Öffnen der Dateien finden (Abb. 89), das nach dem Klopfen auf die Taste "Blättern" erscheint.

Das Textfeld "Letzte Aktualisierung" enthält das Datum und die Zeit der zuletzt durchgeführten

Aktualisierung der VPS Datei (wenn eine durchgeführt wurde).

Durch Betätigung der Taste "Aktualisieren" starten Sie die eigentliche Aktualisierung der LGW.VPS Datei. Die Aktualisierung wird jedoch nur dann durchgeführt, wenn die angegebene LGW.VPS Datei neuer ist als die, die jetzt benutzt wird.

6.7 Programmeinstellung über "Systemsteuerung"

Die Einstellung aller Teile des AVAST32 Programms kann auch ohne die Notwendigkeit des Anlaufs des Hauptprogramms durchgeführt werden. Es genügt, aus der Mappe "Einstellung" des Menü der Taste "Start" das Objekt "Systemsteuerung" zu wählen.

Im erscheinenden Fenster auf das Objekt "AVAST32 Konfiguration" anklopfen (doppelklicken) (Abb. 99). Es erscheint ein Fenster mit Seiten, unter denen Sie mit Hilfe von Lesezeichenliste umschalten können. In den folgenden Kapiteln werden einzelne Seiten beschrieben.

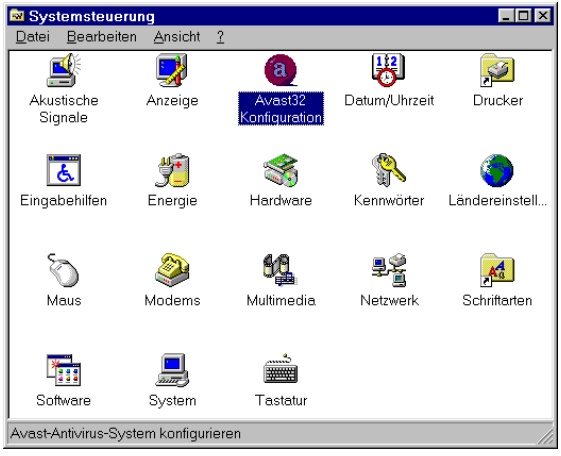

Abb. 99

6.7.1 Seite "Programme"

Die Seite "Programme" dient der Auswahl des Programmteils, den Sie einstellen wollen (Abb. 100). Durch das Doppelklicken auf das entsprechende Objekt rufen Sie ein Dialog hervor, in dem Sie mit Hilfe von Steuerelementen die Einstellung des entsprechenden Teils des Programms verändern.

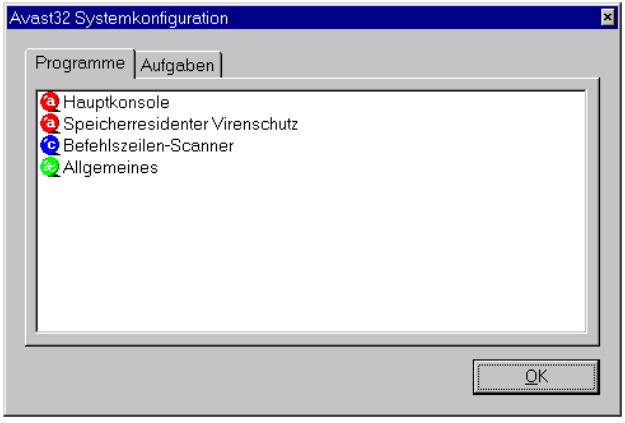

Abb. 100

Die Liste auf dieser Seite enthält folgende Objekte:

- Das Objekt "Hauptkonsolle" ruft ein Dialog für die Einstellung des AVAST32 Programms als solches hervor. Das abgebildete Dialog ist ausführlich im Kapitel 6.1 beschrieben,
- Durch das Objekt "Speicherresidenter Virenschutz" können Sie die Einstellung des Teils des Programms ändern, der residente Vorgänge betreut (Programm RGW32, siehe Kapitel 9). Die Beschreibung des abgebildeten Dialogs finden Sie im Kapitel 6.2,
- Das Objekt "Befehlzeilen-Scanner“ dient zur Grundeinstellung des Programms für die Suche der bekannten Viren, das für die Anweisungszeile bestimmt ist (Programm LGW32, siehe Kapitel 8). Das entsprechende Dialog ist im Kapitel 6.3 beschrieben,
- Mit Hilfe des Objekts "Allgemeines" ist es möglich, verschiedenste Parameter einzustellen, die für alle Teile des AVAST32 Programms gemeinsam sind. Nähere Informationen über das abgebildete Dialog finden Sie im Kapitel 6.5,
- Das letzte Objekt "Lizenz" ermöglicht, den Aktivierungsschlüssel der Programmkopie zu ändern. Auf diese Weise können Sie die Anzahl der verfügbaren Lizenzen ändern, ohne das ganze Programm erneut installieren zu müssen, siehe Kapitel 6.4.

6.7.2 Seite "Aufgaben"

Aus dieser Seite können Sie Dialoge für die Änderung einzelner Aufgaben des AVAST32 Programms hervorrufen (Abb. 101). Die Liste auf dieser Seite ist der Liste der Aufgaben der einfachen und erweiterten Steuerung sehr ähnlich. Auf den Aufgabennamen doppelklicken, den Sie ändern wollen. Ein Dialog erscheint, das ausführlich im Kapitel 4 beschrieben ist (die Beschreibung der einzelnen Dialogseiten enthalten das Kapitel 4.4.1 bis 4.4.16).

Abb. 101

Lokalmenü

Das Lokalmenü, das durch Betätigung der rechten Maustaste auf der Aufgabenliste der Seite "Aufgaben" erscheint, zeigt Abb. 102.

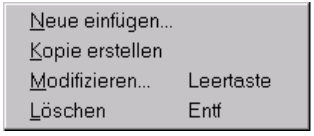

Abb. 102

- Das Objekt "Neue einfügen..." dient der Erstellung einer neuen Aufgabe des AVAST32 Programms (siehe Kapitel 4), ohne das Programm anlaufen zu müssen,
- Mit Hilfe des Objekts "Kopie erstellen" kann der Benutzer eine Aufgabenkopie erstellen. Die Aufgabenkopie kann genau diesselbe Einstellung von Parametern haben, wie die Aufgabe, auf der die rechte Maustaste betätigt wurde. Nur wenn die Aufgabe gemeinsam genutzt ist und der Benutzer das richtige Kennwort kennt, wird die neu erstellte Aufgabe privat sein,
- Das Objekt "Modifizieren", gleich wie beim Doppelklicken auf dem Aufgabennamen, ruft das Dialog für die Änderung der Einstellung der gegebenen Aufgabe (siehe oben) auf,
- Durch die Wahl des Objektes "Löschen..." kann die entsprechende Aufgabe permanent aus der Liste der Aufgaben entfernt werden. Zunächst ist allerdings notwendig, das Löschen der Aufgabe durch das Drücken der Taste "Ja" im Dialog, das nach der Auswahl des Objektes erscheint, zu bestätigen (Abb. 65).

Wenn Sie beliebige Änderungen in den Aufgaben durch die "Systemsteuerung" machen und das Programm AVAST32 dabei im Betrieb haben, werden die vorgenommene Änderungen im Programm erst bei seinem weiteren "Start" sichtbar!!!

6.7.3 Audioeinstellung

Das AVAST32 Programm ermöglicht auch eine Audiodatei für seine Ereignisse einzustellen, deren Wiedergabe immer gestartet wird, wenn das ausgewählte Ereignis kommt.

Klänge kann man in der Systemsteuerung "Akustische Signale" wählen, die in der Abb. 55 dargestellt ist. Weil für die Audioeinstelleung ein standarder Systemmittel ausgenutzt wird, ist zur Audioeinstellung nicht notwendig (wie bei der Einstellung von anderen Teilen des AVAST32 Programms), daß das Programm selbst gestartet wird.

In der Liste "Ergebnisse" das Element "Avast32" finden und das Ereignis wählen, für das die eingestellte Audiowiedergabe geändert werden soll. Die Weise, wie die Audiodatei für ein bestimmtes Ereignis einzustellen, ist im Kapitel 4.4.13 beschrieben.

7.Interpretation der Resultate

Wir empfehlen ihnen dieses Kapitel gründlich zu lesen und ein bißchen darüber nachzudenken. Mag sein, daß wir nur alte bekannte Wahrheiten wiederholen werden, aber Vorsicht kann nie schaden. Besonders die weniger erfahrenen Benutzer der Personalcomputer sollten die Ohren schärfen und entschieden dieses Kapitel nicht überspringen.

Ein grundsätzlicher Fakt, den sie folgen müssen, ist, daß es eine direkte Proportionalität zwischen der Arbeit, Kentnissen, Erfahrung und Sicherheit ihres Computers gilt. Es kann ihnen merkwürdig vorkommen, aber solange sie auf das, was sie tun auch vom Gesichtspunkt der möglichen Vireninfektion nicht ihr Augenmerk richten, kann ihnen kein Antivirusprogramm helfen. Wenn sie nicht in Computern interessiert sind und ein Artzt, Ökonome oder Jurist sind und keine Zeit haben sich um "unwesentliche" Sachen zu kümmern, wie die Sicherheit ihres Computers und ihren Daten ist, müssen wir sie enttäuschen. Tatsächlich, sie irren. Und wenn sie nichts auf unseren Rat geben wollen und wollen nicht einmal die Grundsätze lernen, empfehlen wir ihnen unser Programm dem Verkäufer zurückzugeben, der ihnen das Geld zurückzahlt. Sie sparen sich und uns sehr viel Sorgen. Damit sie ihre Arbeit gut machen können, müssen sie die tschechische Rechtschreibung und Grammatik beherrschen. Genauso auch die Arbeit mit dem Computer erfordert bestimmte Grundkentnisse, die sie nur schwierig entbehren können.

Es ist möglich ein Programm für die Textaufarbeitung, Datenbank oder Spreadsheet zu schreiben, die völlig benutzerfreundlich werden und werden praktisch keine spezielle Kentnisse erfordern oder sie gegebenfalls die notwendigen Sachen lernen. Die Problematik der Sicherheit und des Antivirusschutzes ist aber wirklich verschieden. Wir ersuchen sie dringend, widmen sie ihr die notwendige Zeit und Aufmerksamkeit.

7.1 AVAST32 hat Viren gefunden

Dieser Teil ist relativ einfach wenn auch nicht ganz trivial. Wenn Avast32 meldet, daß es Virus gefunden hat, bedeutet das noch nicht, daß es wirklich ein Virus ist. Und wenn auch das Virus da ist, heißt es noch immer nicht, daß sie den Computer infiziert haben. Auch dieser Text wurde auf einem Computer geschrieben, der Dutzen-

de von verschiedenen Viren enthält und doch ist der Author ganz ruhig , weil diese Viren nicht **aktiv** sind.

Eine ausführliche Beschreibung, was mit der Information über das gefundene Virus zu tun, das ist alles im Anhang B geschrieben, den wir ihnen empfehlen gründlich zu studieren.

7.2 AVAST32 hat Veränderungen in den Dateien gefunden

Da ist die Situation ein bißchen komplizierter aber nicht unlösbar. Nichtsdestoweniger, nur die Erfahrung mit einer regelmäßigen Arbeit mit dem AVAST32 Programm und mit dem Testen der Datenintegrität können ihnen erwartete Resultate bringen.

Die Interpretation der Resultate ist nicht einfach. Nicht vielleicht deswegen, daß das Programm komplizierte Informationen oder Chiffren bieten würde, aber weil jeder von ihnen bei jedem Anlauf der Integritätsteste andere Informationen bekommt und ihre Verarbeitung kann von Fall zum Fall unterschiedlich sein. Deswegen ist es nicht möglich ein allgemein gültiges Kochbuch zu schreiben, das alle Benutzer befriedigen würde. Wir können hier nur ein Paar allgemeine Ratschläge, Vorschläge und Verfahren geben,die wir empfehlen anzuwenden. Aber die Einzelheiten und Ausführlichkeiten müssen sie selbst ableiten.

7.2.1 Neue Dateien

Wenn das AVAST32 Programm meldet, daß es neue Dateien gefunden hat, kann es sich um mehrere Fälle handeln. Der einfachste von ihnen ist der, daß es sich um eine wirklich neue Datei handelt, die ihren Ursprung in einer legalen Quelle haben. Die Lösung ist einfach, einfach akzeptieren sie sie und so wird sie in die Dateidatenbank gespeichert. Allerdings, was eine legale Quelle ist komplizierter . Zum Beispiel, eine wirklich legale Quelle sind die Installationsmedien des Programms, das sie vor kurzem installiert haben. Das erwähnte Programm konnte von ihren Kollegen oder vom Netzadministrator installiert werden . Wenn sie in ihrer Firma gute Beziehungen haben, dann würden sie über diesen Fakt sicherlich informiert und sie konnen darüber entscheiden ob die Datei in Ordnung ist oder nicht.

Es kann sich auch um eine temporäre Datei handeln, die von einem Programm für seine Zwecke erstellt wurde und die von ihm zur Zeit benutzt wird oder er hat vergessen sie auszulöschen. Das ist auch wahrscheinlich in Ordnung , aber ein solcher Dateityp konnte auch ein Virus erstellen. Die Entscheidung kann schwierig sein und es ist an ihnen alleine.

Auch die Anwendung des „Korbs“ für das Löschen der Dateien bringt Detektion neuer Dateien in dem ensprechenden Verzeichnis.

Lassen sie sich nicht verwirren, daß die neue Datei in einem Verzeichnis mit einem bekannten Namen erstellt wurde, zum Beispiel im Verzeichnis des Operationsssystems. Die Authoren der Viren kennen diese Verzeichnisse auch und und nutzen sie mit Erfolg.

7.2.2 Veränderte Dateien

Gründe für eine Dateiveränderung kann wirklich sehr viele sein. Auch das eigentliche Operationssystem "lebt sein eigenes Leben" und nutzt die Dateien sehr intensiv aus. Jeder Programmanlauf oder Aufbereitung eines Dokuments hat die Folge in einer Spur die vom Avast32 endeckt und gemeldet wird. Da müssen sie entscheiden, welche Veränderung gültig ist und welche nicht . Zum Beispiel, Veränderung in den Textdateien wird zu neunundneunzig Prozent von ihnen verursacht, weil die Änderung der COMMAND.COM Datei zu neunundneunzig Prozent von einem Virus verursacht wurde. Beachten sie, daß nichts hundertprozentig ist, was zu gilt für die gesamte Virusproblematik. Zwischen den obengenannten Extremen liegen die restlichen Dateitypen. Zum Beispiel, über die Dokumente des Microsoft Word Programms (*.doc) ist es schwierig zu sagen, warum sie sich verändert haben. Es konnten sie sein, durch das einfache Lesen ihres Inhalts oder es konnte ein sogenanntes "Makrovirus", der dieses Dokument angegriffen hat.

Allgemein gilt es, daß wenn ein ablauffähiges Programm angegriffen wird (exe, sys, dll, bin, vxd, scr,...), ist die Veränderung viel mehr verdächtig, als wenn es ein Dokument oder Daten Datei ist. Aber Achtung, auch hier existieren Ausnahmen.

7.2.3 Ausgelöschte Dateien

Da hilft nichts sehr viel. Eine Erneuerung einer dolchen Datei ist möglich nur mit Hilfe eines speziellen Mittel des Operationssystems oder von den Reservekopien. Nebenbei, wann haben sie zuletzt ihre Daten sichergestellt? Wollen sie sich wirklich nur auf den Zufall verlassen?

7.2.4 Spezielle Fälle

Es existieren ein Paar Spezialfälle, wann es ihnen nicht gelingt mit den Dateien zu arbeiten. In diesen Fällen stellen sie fest, daß AVAST32 einen Fehler signalisiert bei der Arbeit mit der Datei (Kapitel 5.3.2).

Meistens können sie Dateien nicht kontrollieren, die von einem anderen Programm gerade ausgenützt wird. Diese Datei ist blockiert und das Operationssystem erlaubt ihnen zu ihr den Zugriff

nicht. Das gilt sowohl für das Operationssystem, das nützt Dateien selber als auch für die arbeitende Programme. Die müssen nicht jedesmal sichtbar auf dem Bildschirm ihres Computers sein. Wenn sie aber arbeiten und Dateien ausnützen, Avast32 kann diese Dateien nicht kontrollieren.

Wenn sie mit einem Operationssystem arbeiten, das die Sicherheit auf dem Niveau der Dateien unterstützt und ein System der Dateien ausnützen, das diese Eigenschaft auch unterstützt (Windows NT mit NTFS), müssen sie hinreichende Rechte haben, um einzelne Dateien kontrollieren zu dürfen. Sollen ihre Rechte nicht genügend sein, so bleibt die Datei unkontrolliert.

8.LGW32 Programm

Das Programm dient zur Aussuchung der bekannten Viren, einschließlich der polymorfen Viren und Makroviren. Es handelt sich um ein Equivalent der Aufgabe, wo wir nur Präsenz der bekannten Viren im AVAST32 Programm testen würden und es hat also sehr ähnliche Einstellungsmöglichkeiten.

Mit Rücksicht darauf, daß sowohl das AVAST32 Programm als das LGW32 Programm Dienste des Testservers VPS32 ausnützen, sind ihre Resultate absolut identisch. Die einzige Differenz zwischen ihnen ist in daß das LGW32 Programm für seine Tätigkeit nur die Möglichkeiten der Anweisungszeile, nützt zum Unterschied von der sehr benutzerfreundlichen Umgebung des AVAST32 Programms.

Die Anweisungszeile des LGW32 Programms sieht folgendermaßen aus:

```
LGW32 [@<Aufgabenname> | [+ | -]
<Bereichsname>[-][<Parameter>, ...]]
```

Wenn Sie eine mit dem AVAST32 Programm erstellte Aufgabe starten wollen, schreiben Sie hinter das Zeichen "@" ihr Name. Wenn der Aufgabenname ein Zwischenraumzeichen enthält, muß der Name zwischen Anführungsstrichen gegeben werden. Ist es nicht der Fall, wird das Programm die Aufgabe nicht ausführen!

Ist in der Anweisungszeile kein Aufgabenname gegeben, wird das LGW32 Programm vorgegebene Bereiche kontrollieren. Auf welche Weise die Kontrolle vorgenommen wird, wird mit Hilfe von Parametern, ähnlich den Anweisungen des Operationssystems, bestimmt.

Beim LGW32 Programm ist es möglich, einige Parameter einzustellen. Eine ausführliche Beschreibung dieser Parameter ist im Kapitel 6.3 gegeben. Soll in der Anweisungszeile auch entsprechende Option angeführt werden, ist der Parameter nach der Option eingestellt.

[+ | -]
- Vorzeichen vor dem Bereichsnamen bedeuten, ob auch die verschachtelten Mappen kontrolliert werden sollen. Das Plusvorzeichen bedeutet Erlaubnis für den Test der verschachtelten Mappen, das Minusvorzeichen wird es verbieten.

[-]
- Das Minusvorzeichen hinter dem Bereichsnamen verursacht, daß der Bereich nicht getestet wird. So

kann man dem LGW32 Programm z.B. mitteilen, daß es die Ganze Festplatte D: testen soll ausser der Mappe "D:\Viren". Es hat denselben Effekt die rote Kugel am Namen wie des kontrollierten Bereiches im AVAST32 Programm (siehe Kapitel 4.4.5).

Das LGW32 Programm unterstützt folgende Parameter:

/? /H, /HELP
- das Programm wird Hilfe abbilden. Hilfe beinhaltet einige Seiten, unter denen es möglich ist umzuschalten mittels numerischen Tasten, die immer die Seitennummer bedeuten, die abgebildet werden soll. Nach Betätigung einer anderen Taste kommt es zur Rückkehr in die Anweisungszeile.

/A
- schaltet die Kontrolle der Dateien für die Anwesenheit aller Viren ein, einschließlich derer, die den gegebenen Dateityp nicht angreifen. Dann wird z.B. eine Datei mit dem Suffix COM auch auf Anwesenheit der Viren kontrolliert, die nur EXE Dateien angreifen.

/C[+]
- schaltet die Kontrolle der ganzen Dateien (siehe Kapitel 4.4.7) ein. In diesem Regime schaltet das Programm automatisch nach Entdeckung eines beliebigen Virus um. Das Vorzeichen "+" (Plus) verursacht, daß auch die komprimierten Dateien kontrolliert werden.

/E[A|E|O|<Typen>]
- informiert das Programm, welche Dateitypen zu kontrollieren (siehe Kapitel 4.4.4). Der Buchstabe "A" bedeutet, daß alle Dateien kontrolliert werden, der Buchstabe "E" bedeutet anlaufbare Dateien und endlich der Buchstabe "O" bedeutet die OLE Dokumente. Es kann auch direkt die Typen der zu kontrollierten Dateien spezifizieren. Ihre Anzahl ist nicht begrenzt, sie müssen nur durch Kommas getrennt werden. Ist der Parameter gegeben, so werden nur die Anlaufdateien und OLE Dokumente getestet.

/X[Typen]
- die angegebene Dateitypen werden nicht kontrolliert. Auf diese Weise ist es möglich zu besorgen, daß alle Dateien kontrolliert werden ausser der Textdateien (Suffix TXT). Der Parameter hat denselben Effekt wie die rote Kugel am Typnamen in der Liste der zu kontrollierten Typen im AVAST32 Programm (siehe Kapitel 4.4.4).

/L[-]
- für den gegebenen Vorgang schaltet er die Anmeldung. Eine ausführliche Beschreibung des Anmeldungsmechanismus ist im Kapitel 6.1.1, bei dem Abhakfeld "Anmeldung des AVAST32 Programms erlauben", gegeben.

/M
- schaltet den Test des Operationsspeichers ein. Ausser des Speichers wird allerdings nichts anderes getestet.

/R[<Name>]
- bei der Durchführung der Kontrolle wird eine Datei mit der Nachricht über den Kontrollverlauf erstellt (siehe Kapitel 4.4.10). Ist der Dateiname nicht angegeben, wird das Protokol in die "LGW32.RPT" Datei in das aktuelle Verzeichnis geschrieben.

/S<Name>
- specifiziert die Datei, die den Klang beinhaltet, der nach der Entdeckung des ersten Virus durchgespielt werden soll. Um den Klang durchspielen zu dürfen, muß in dem Computer die Audiokarte und die entsprechenden Driver installiert werden.

/V[N|I|A]
- bestimmt, über welche Dateien Informationen auf dem Bildschirm geschrieben werden sollen. Der Buchstabe "N" schaltet die Ausgabe aus, "I" schaltet die Ausgabe nur für die infizierte Dateien ein und "A" schaltet die Ausgabe aller gefundenen Dateien ein.

/U<Name>[,<Name>]
- bestimmt das Computername oder Bereichsname, auf das die Meldung über die Entdeckung eines Virus geschickt werden soll. Hinter dem Parameter muß mindestens noch ein Name geschrieben werden.

/Z[+|V]
- schaltet eine automatische Beseitigung der gefundenen Makroviren in den OLE Dokumenten ein. Das Vorzeichen + verursacht, daß, sei das Virus im OLE Dokument ganz genau erkannt, alle Makra im Dokument ausgelöscht werden. Der Buchstabe V stellt eine automatische Beseitigung aller Makra aus dem infizierten Dokument sicher. Ist hinter dem Schalter kein Zeichen geschrieben, so wird aus dem OLE Dokument nur das Makro entfernt, daß das Virus enthält.

Im Moment der Tätigkeitsbeendigung schickt das LGW32 Programm dem Operationssystem den Rückkehrkod. Dieser Kod kann später ent-

weder durch das Programm, das es gestartet hatte, oder in der Anweisungszeile mittels Anweisung IF ERRORLEVEL getestet werden. Der Rückkehrkod des LGW32 Programm kann nur folgende Werte annehmen:

0	- das Programm ist normal beendet, kein Virus gefunden,
1	- ein Virus wurde bei dem Programm gefunden,
10	- Zeit, für die die Programmdemoversion genützt werden konnte, ist abgelaufen,
11	- das Programm kann nicht gestartet werden, offenbar eine schlechte Installation,
255	- schwerwiegender Fehler währed des Programmlaufs.

9.RGW32 Programm

Das Programm kümmert sich um alle residenten Tätigkeiten. Wenn sie also zum Beispiel im AVAST32 Programm irgendwelche residente Aufgaben anlaufen, sie wird vom Programm RGW32 gerufen. Seine Anwesenheit im Speicher ist durch die Ikone im rechten Teil des Hauptpanels indiziert (Abb. 103). Durch Klopfen der linken Maustaste auf diese Ikone wird das Programmfenster abgebildet.

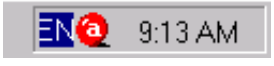

Abb. 103

Mittels dieses Fensters (Abb. 104) kann man das RGW32 Programm und somit auch die angelaufene Aufgabe beenden. Wenn sie das Feld "Ausführlichkeiten abbilden" abhaken, kommt in dem Fenster auch eine Liste der Tätigkeiten, die gerade von der residenten Aufagabe durchgeführt werden, in der Form von Baumstruktur zum Vorschein. Die einzelnen Tätigkeiten werden in zwei Grundgruppen: "Schutz von ausführbaren Dateien und OLE-Dok." und “Rezidente Blöcke” eingereiht. Durch ihre Entfaltung werden einzelne Tätigkeiten abgebildet.

Beim RGW32 Programm ist es möglich, einige Parameter einzustellen. Eine ausführliche Beschreibung dieser Parameter ist im Kapitel 6.2 angegeben.

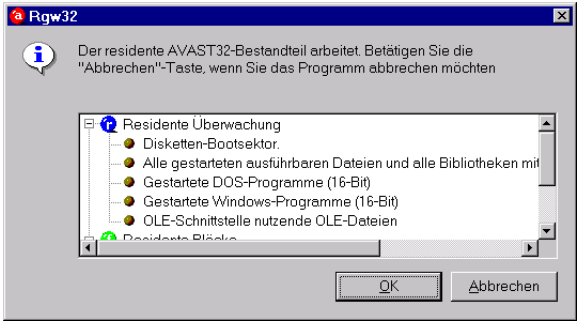

Abb. 104

Anweisungszeile des RGW32 Programms sieht wie folgt:

```
RGW32 <Name>
```

Der <Name> Parameter spezifiziert die residente Aufgabe, die anzulaufen ist. Ist der Parameter nicht angegeben oder die Aufgabe mit dem Na-

men existiert nicht, dann bildet das Programm eine Fehlermeldung ab. Nur eine einzige residente Aufgabe kann in einem Computer laufen. Beim Anlauf einer weiteren residenten Aufgabe wird die erste Aufgabe beendet.

Enthält die Aufgabe auch irgendwelche nonresidente Vorgänge, werden diese Vorgänge und ihre Einstellung ignoriert - stets werden nur die ausgewählten residenten Teste durchgeführt.

Das RGW32 Programm schickt keine Rückkehrkode zurück.

Das RGW32 Programm kann während seiner Tätigkeit einige weitere Dialoge abbilden. Diese Dialoge machen den Benutzer bekannt mit einer gefährlichen Operation mit der Datei, mit der Endeckung eines Virus im Bootsektor der eingelegten Diskette oder eines Virus im anzulaufenden Programm oder im OLE Dokument, das mittels der OLE Funktionen eröffnet wird. Ihre Beschreibung ist in den nächsten Kapiteln gegeben.

9.1 Meldung der gefährlichen Operationen

Wie schon gesagt, kümmert sich das RGW32 Programm um alle residente Tätigkeiten, die die Aufgaben durchführem können. Unter diese Tätigkeiten gehört auch das residente Blockieren der gefährlichen Operationen. Ist eine Aufgabe angelaufen, die in ihr auch eine Tätigkeit der residenten Blöcke enthält, sind dann sämtliche Operationen des gewählten Operationssystems verfolgt (Kapitel 4.4.15).

Abb. 105

Beim Versuch um die Durchführung einer belkiebigen verdächtigen Operation das RGW32 Programm gibt Warnung (Abb. 105) und hält die Durchführung der Operation an, bis ihm der Benutzer mitteilt, was weiterzumachen. Die Warnung enthält ein Textfeld, das den Namen der Datei enthält, mit der die verdächtige Operation durchgeführtr werden sollte. Weiter enthält sie drei Tasten:

- wenn sie die Taste "OK" anklopfen, so wird die Operation mit der Datei durchgeführt. Potenzielle weitere verdächtige Operationen mit der Datei werden auch gemeldet,

- die Taste “OK& Ignorieren" erlaubt die Operation und das RGW32 Programm bis seine Beendigung und seinen Wiederanlauf wird dem Benutzer keine Operationen mit jener Datei melden,
- die Taste "Abbrechen" wird dem Programm mitteilen, daß die Durchführung der Operation unterdrückt werden soll. Nach ihrer Betätigung erlaubt das Programm die Durchführung der Operation nicht, und selbstverständlich meldet es dem Benutzer auch jeden weiteren Versuch um die Durchführung einer gefährlichen Operation mit jener Datei.

9.2 Meldung eines Bootvirus und eines Virus im einer anlaufbaren Datei oder im Dokument

Das RGW32 Programm kann auch anlaufende Programme, OLE Dokumente, die mittels OLE Funktionen eröffnet werden, und Bootsektoren der eingelegten Disketten 3kontrollieren. Die erwähnten Tätigkeiten wird das RGW32 Programm durchführen, wenn sie auf der Seite "Test" (Kapitel 4.4.2) abgehakt wurden.

Wenn sie eine Diskette in die Mechanik einlegen, wird das Programm beim ersten Zugriff zu ihr das Bootsektor kontrollieren,ob es kein Virus enthält. Findet es ein Virus, wird eine Warnmeldung abgebildet (Abb. 106). Mit der Diskette können sie weiter abeiten, weil dazu, daß das Virus aktiv würde, muß es zunächst anlaufen und dazu kommt es bei den Bootviren nur bei der Ladung des Systems. Die Warnmeldung hat die Aufgabe, sie auf die lauernde Gefahr aufmerksam zu machen.

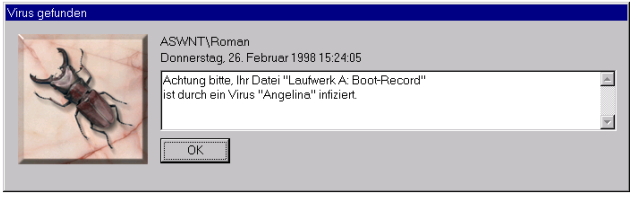

Abb. 106

Die Warnmeldung auf der Abb. 92 wird auch zum Vorschein kommen, wenn in irgendeinem anlaufbaren Programm ein bekanntes Virus entdeckt wurde oder der Benutzer versuchte ein OLE Dokument, das ein Virus enthalten hat, zu eröffnen. Damit das RGW32 Programm die Meldung abbildet, muß die Aufgabe laufen, die die Tätigkeit des residenten Verfolgung enthält und muß die Kontrolle der ensprechenden Dateien ausgewählen.

Wenn sie auf die Taste "OK" klopfen, können sie die Arbeit weitermachen.

10.Das QUICK32 Programm

Das QUICK32 Programm dient, ähnlich den AVAST32 und LGW32 Programme, zum Testen der Datei auf die Anwesenheit einen von den bekannten Viren. Zum Unterschied vom LGW32 Programm bietet es allerdings praktisch keine Eistellungsmöglichkeiten. Es kontroliert alle Dateien, die es findet, und kontroliert sie ganz.

Das QUICK32 Programm ist vor allem benützt für die Kontrolle der Datei, die durch das Lokalangebot hervorgerufen wurde (Abb. 107) z.B. im "Explorer" Programm. In anderen Fällen ist es bei weitem besser das AVAST32 oder LGW32 Programm zu benützen.

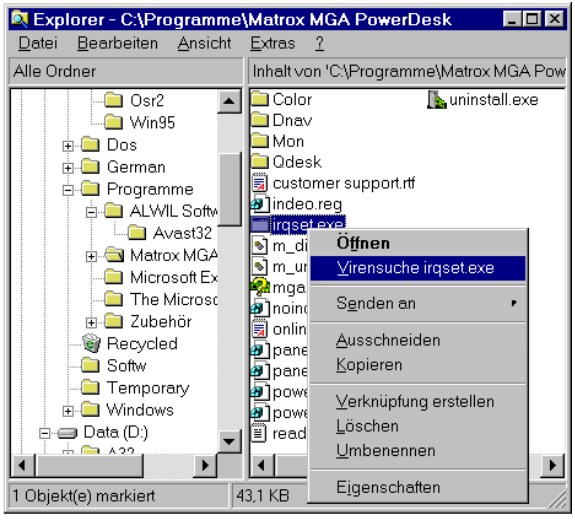

Abb. 107

Das QUICK32 Programm ist so eingestellt, daß es alle Dateien für die Anwesenheit aller Viren testet. Die komprimierten Dateien werden zunächst in ihrer komprimierten Form kontrolliert und dann werden sie intern dekomprimiert und wieder kontrolliert.

Die Anweisungszeile des QUICK32 Programms sieht so aus:

```
QUICK32 <Name>
```

Der Parameter <Name> gibt den Name der Mappe oder Datei, die wir kontrollieren wollen, einschließlich ihres Zugriffswegs. Falls eine Mappe als Parameter übergeben wurde, werden in ihr nur anlaufbare Dateien und OLE Dokumente kontrolliert und auch alle verschachtelten Mappen werden durchsucht.

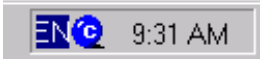

Abb. 108

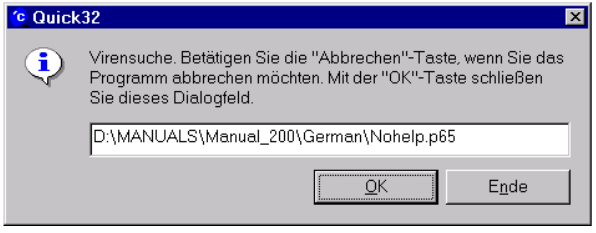

Abb. 109

Das Programm informiert den Benutzer über seinen Lauf durch eine kleine Ikone an der rechten Seite des Hauptpanels (Abb. 108). Nach Anklopfen auf der Ikone mit der linken Maustaste kommt ein Fenster mit dem Namen der gerade kontrollierten Datei zum Vorschein (Abb. 109). Wollen sie die Programmtätigkeit vorzeitig beenden, betätigen sie die Taste "Ende". Das Fenster kann durch Betätigung der Taste "OK" geschlossen werden.

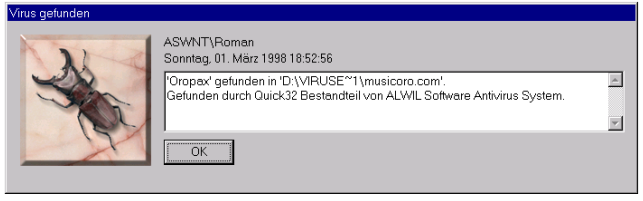

Abb. 110

Entdeckte das QUICK32 Programm ein Virus, informiert es darüber den Benutzer durch eine Warnmeldung (Abb. 110). Das Programm wird allerdings nach dem Entdecken und Anmeldung des Ersten Virus beendet, so daß wenn die kontrollierte Mappe mehr infizierten Dateien enthält, wird der Benutzer nur auf das erste Virus aufmerksam gemacht!

Das QUICK32 Programm schickt keinen Rückkehrkod zurück.

11.Das WARN32 Programm

Es ist die Aufgabe des WARN32 Programmms den Benutzer auf die Tatsache aufmerksam zu machen, daß in dem Computer ein Virus entdeckt wurde. Es ist automatisch angelaufen nach dem Start des Operationssystems, wenn es erlaubt ist Warnmeldungen abzubilden (siehe Kapitel 6.5.1, Abhakfeld "Virenmeldung nach der Anmeldung anzeigen").

Die Anweisungszeile des Programms sieht so aus:

```
WARN32
```

Wie man sehen kann, benötigt das Programm keine Parameter für seinen Anlauf und angesichts seiner Tätigkeit (siehe weiter) schickt es auch keinen Rückkehrkod zurück.

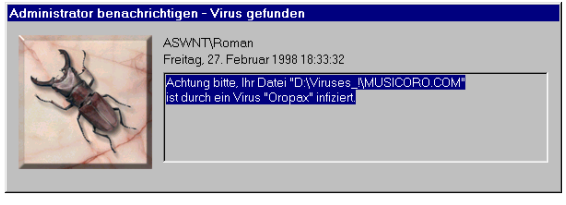

Abb. 111

Nach seinem Anlauf wirft das Programm einen Blick in das Register des Operationssystems, ob in diesem Computer irgendein Virus entdeckt wurde (diese Information wird für WARN32 in den Register von den Programmen AVAST32 , LGW32 und QUICK32 eingetragen). Wurde ein Virus entdeckt, bildet das Programm eine Warnmeldung ab (Abb. 111), die sich über die Arbeitsfläche bewegen wird. Die Warnmeldung informiert den Benutzer über die zuletzt gefundenen infizierten Datei und weiter über den Namen des Virus, das die Datei angegriffen hat, den und über den Name der Aufgabe, die das Virus entdeckt hat.

Soll kein Virus entdeckt werden, wird das Programm beendet, ohne über seine Tätigkeit auf irgendwelche Weise Bescheid zu geben. Der Benutzer muß gar nicht bemerken, daß es lief.

Hat das Programm eine Warnmeldung abgebildet, ist seine Beendigung nicht eine einfache Angelegenheit. Deswegen solte ein üblicher Benutzer das WARN32 Programm alleine nicht anlaufen (es hat in übrigen auch keinen Grund dazu).

Soll nach der Anmeldung des Benutzers in das System eine Warnmeldung in Vorschein kommen,

sollte er es unverzüglich dem Netzadministrator oder einem anderen Verantwortlichen melden!

Die Enfernung der Meldung des WARN32 Programms von der Arbeitsfläche genügt alleine dem nächsten Anlauf des Operationssystems die Meldung nicht abgebildet wird!

A.Implementierung der Virusroutinen

Informationen, die in diesem Anhang angeführt sind, sind besimmt vor allem den Benutzern, die díe Arbeit des Systems optimieren wollen, in dem das AVAST32 Programm zum Einsatz kommt. Da werden die Arbeitsgrundsätze des Programms und flüchtig einige Bibliotheken beschrieben. Gewöhnliche Benutzer werden die hier angeführten Informationen offensichtlich nicht ausnutzen.

A.1 Allgemeine Grundsätze

Angesichts der Tatsache, daß das Antiviruspaket AVAST32 einige Programme enthält, die die Viren suchen, ist das eigentliche Testen als ein selbständiger Teil implementiert, der von diesen Programmen angerufen wird. Damit ist eine Wiederholung des Programmes und der dazu gehörenden Daten verhindert, was würde die Dialoge unnötigerweise verlängern und Platz auf der Festplatte und Speicher ihres Computers besetzt. Alle Programme, die festzustellen, wollen, ob irgendwo nicht ein Virus ist, nutzen dasselbe Verfahren und dieselben Bibliotheken, was eine dramatische Verringerung der Forderungen für die Operationsspeicher des Computers bringt.

Auch die Ausnutzung der Daten ist optimiert. Wie schon angegeben, befinden sich alle Daten notwendig für die Virussuche in der LGW.VPS Datei. Diese Datei ist schon groß genug und die schlechte Nachricht für den Benutzer ist, daß es wegen der ständig wachsenden Anzahl der Viren sich diese Datei vergrössern wird. Wenn sie in sie einen Blick geworfen haben, ihr Inhalt ist auf den ersten Blick sehr sinnvoll, aber für die richtige Funktion des Programmes ist es lebenswichtig. Die Mehrheit der Informationen, die in ihr enthalten sind, ist statisch. Kann also von mehreren Programmen ausgenutzt werden ohne Gefahr der Überschreibung der dynamischen Daten.

A.2 Eigene Bibliotheken

Für die eigentliche Anrufung der Antivirusfunktionen sind einige Bibliotheken ausgenutzt. Die erste von ihnen ist die Bibliothek AvMain.DLL, was eine normale dynamische Bibliothek ist, die schon seit der Version Windows 3.x bekannt ist. Diese Bibliothek ist u.a. genutzt für die Initialisierung, "Aufräumen" und Generalisierung des Aufrufes der Antivirusdienste aus verschiedenen Programmtypen. Generell kann

man sagen, daß sie einen Umschlag der eigentlichen Implementation formt.

Die eigentliche Virensuche spielt sich in der Bibliothek Vps32s.DLL ab. Diese Bibliothek ist implementiert als "InProc server" arbeitende im Arbeitsmodel "Apartment". Es handelt sich um einen sogenannten COM server, der in den Addressraum, den er initialisiert, kopiert wird. Sagen ihnen diese Informationen gar nichts, das macht nichts. Sie können dieses Kapitel ruhig überspringen.

Zu der eigentlichen Arbeit nutzt diese Bibliothek noch einige Hilfsbibliotheken (Vps32a.DLL, Vps32e.DLL), die aber spezialisierte Tätigkeiten machen, die im Kontext dieses Kapitels nicht interessant sind.

Die angewendete Implementation hat eine Eigenschaft, die ihnen interessant vorkommen kann und sie werden sie gern ausnutzen. Die COM Server haben nämlich ein Interface, das vom Aussen sichtbar in einer lesbaren und verständlichen Form ist. Diese Tatsache verführt manchmal zu ihren Nutzung auf eine andere Weise als in einem Programm, das dazu befugt ist. Wir wollen sie davon warnen! Wir haben dazu zwei Gründe. Erstens, diese Vorgehensweise ist nicht im Einklang mit der Rechtsordnung und wenn wir es feststellen, werden wir gezwungen sein uns an unsere Juristen wenden. Der zweite, viel wesentlichere Grund, ist der, daß diese Funktionen nicht offiziell dokumentiert sind und ihre Nutzung kann ihnen **wirkliche Schadën** zufügen. Wenn sie sich auf die gegenwärtige Implementation verlassen, können sie in der Zukunft sehr unangenehm überrascht werden.

A.3 Nutzungsoptimierung

Aus der Weise der Implementation der Virusroutinen folgt direkt die Möglichkeit ihrer Nutzungsoptimierung. In Wirklichkeit jedes Programm, das diese Funktionen ausnutzt, muß Zugang zu allen Daten haben, die sich in der LGW.VPS Datei befinden. Diese Datei muß vor jeder Ausnutzung kontrolliert, gelesen und analysiert werden, was verhältnismäßig lange dauert. Deswegen werden die erwähnten Operationen nur dann durchgeführt, wenn die LGW.VPS Datei nicht mehr ausgenutzt ist.

Das heißt, daß solange die Datendatei von anderen Programmen ausgenutzt wird, wird der Anlauf eines weiteren Programms des Pakets AVAST32 schneller sein. Dazu liefern wir auch das Vps32.EXE Programm, das keine andere Aufgabe hat als die Virusdatendatei in dem Speicher zu halten und damit ihre Nutzung zu beschleunigen. Die genannte Eigenschaft werden sie vor allem in dem Fall schätzen, daß sie Dateikontrolle auf ihrem Computer mittels des Lokalangebots

des Programms "Explorer" anwenden werden, wenn die Initialisierung der ganzen VPS Datei für jede einzelne Datei frustrierend werden kann.

Die andere Seite dieser Beschleunigung ist weniger freien Platzes im Operationsspeicher in ihrem Computer, sogar in der Zeit wenn die LGW.VPS Datei durch keine Applikation genutzt ist.

B.Was mit dem gefundenen Virus

Sollte ihnen einer von den Programmen aus dem AVAST32 Paket eine Virusanwesenheit gemeldet haben, muß es nicht immer bedeuten das die Datei wirklich infiziert ist. Wie in einem solchen Fall vorgehen, das wird in den folgenden Kapiteln beschrieben. Auch hier aber gilt, daß die weiter beschriebene Operationen ein Benutzer machen sollte, der mit den Operationssystemen Windows 95 und NT Erfahrung hat und weiß, was nach der Durchführung der Operationen passieren wird und welche Folgen sie haben werden.

B.1 Was ist ein falscher Alarm?

Bevor sie der Panik verfallen und anfangen die erkannten Dateien auszulöschen, den Antivirusdienst anzurufen oder für einen unbegrenzten Urlaub ersuchen, müssen sie feststellen, ob die erkannte Datei wirklich angegriffen ist oder ob es sich um einen falschen Alarm handelt. Das kann durch verschiedene Ursachen verursacht werden, zum Beispiel:

- Alarm verursacht durch Nutzung von zwei Scannern gleichzeitig (Anlage B.1.1),
- Alarm verursacht durch Imunisierung der Dateien (Anlage B.1.2),
- Alarm verursacht durch Witzprogramme (Anlage B.1.3),
- Alarm verursacht durch Fehler der Technik, der Software oder des Benutzers (Anlage B.1.4),
- Alarm verursacht durch Arbeitsgrundsätze der Windows (Anlage B.1.5).

Das AVAST32 Programm ist erstellt mit Hinblick auf die Minimierung der falschen Alarme. Das regelmäßige Testen gegen sie involviert etwa 4 GB (4096 MB) von Dateien verschiedener Herkunft und Inhalt. Trotz des so gründlichen Testen kann passieren, daß jemand von den Programmen aus dem Paket falsche Meldung bietet. Wenn so was passiert, bitten wir, verbinden sie sich mit uns. Sie werden uns helfen unser Produkt zu verbessern und sie können sich sicherer fühlen.

Wenn sie die weitere Darlegung in diesem Kapitel nicht verstehen, machen sie sich nichts daraus. Erfahrung in der Arbeit mit dem Computer gehört nicht unter die angeborenen Eigenschaften. Nur im Fall der Virusendeckung wenden sie sich an wirkliche Fachleute.

B.1.1 Alarm verursacht durch Nutzung von zwei Scannern gleichzeitig

Wenn sie mehrere Scanner gleichzeitig oder eng nacheinander ausnutzen, kann es passieren, daß einer von ihnen einen Virus im Speicher melden wird. Der Grund dieser Meldung ist einfach. Jeder Scanner braucht mindestens für eine Weile die Informationen von Viren unkodiert und zugänglich im Speicher haben. Wenn in demselben Augenblick ein anderer Scanner diesen Speicher testet oder wenn der Speicher in den virtuellen Speicher umgeladen wird und später ohne Reinigung ausgenutzt, kann es passieren, daß diese Informationen Ursache eines falschen Alarms werden.

Die Situation ist einfacher, wenn die Scanner "schlecht" geschrieben sind, d.h., daß sie ihren Speicher nicht reinigen. In diesem Fall ist es sehr wahrscheinlich, daß sie im Speicher mehrere (z.B. 5 und mehr) verschiedene Virentypen finden. In diesem Fall ist die Situation klar, es handelt sich um einen falschen Alarm.

Schlimmer ist die Situation im Fall, daß die Scanner "gut" geschrieben sind und den Speicher hinter ihnen reinigen. Auch in diesem Fall kann passieren, daß sie ein Virus im Speicher finden.

Wie festzustellen, ob es sich um falschen Alarm handelt? Es ist ziemlich einfach, aber kann zeitaufwendig sein. Beenden sie die Arbeit mit allen Applikationen, beenden sie das Operationssystem und schalten sie den Computer mit dem Netzschalter aus. Schalten sie ihn wieder ein und laufen sie das Operationssystem an. Laufen sie den Scanner an der die Virusanwesenheit im Speicher gemeldet hat. Wenn er es wiederholt nicht meldet, versuchen sie die Arbeit zu reproduzieren (Anlaufen von Programmen), die sie vor dem Anlauf der Scanner gemacht haben und nach einer Weile laufen sie wieder das Testen gegen die Viren. Wenn auch in diesem Fall kein Virus im Speicher gefunden wurde, handelt es sich um einen falschen Alarm.

Das AVAST32 Programm reinigt konsequent sämtliche ausgenutzten Speicher und was mehr, speichert es alle Informationen und Virenmuster nur in kodierter Form. Nur im Augenblick des Tests dekodiert es die Information über ein Virus und nach seiner Nutzung löscht diese Information aus. Das heißt, daß in jedem Augenblick kann im Speicher maximal ein dekodierter Virenmuster sein.

B.1.2 Alarm verursacht durch Imunisierung der Dateien

Es existieren Antivirusmittel, die anbieten und arbeiten mit einer Funktion die man "**Imunisierung der Dateien**" nennt oder mit einer Funktion, die die Angliederung der Kontrollsumme zu der getesteten Datei anbietet. Beim nächsten Testen kontrollieren diese Mittel einfach die eingetragene Information gegen den aktuellen Zustand und aufgrund des Resultats können Verdacht an Angriff der Datei durch ein Virus mitteilen. Dieser Prozeß ist sehr schnell und verhältnismäßig einfach für die Implementation.

Allerdings dieser verhältnismäßig einfache und schnelle Prozeß trägt mit sich mehrere grundsätzliche Probleme. Stellen sie sich zwei auf diese Weise arbeitende Produkte ausgenutzt fürs Testen einer Datei vor. Ihre wechselartige Anwendung stört sich gegenseitig und beide Produkte werden melden, daß die Datei verändert wurde.

Ein weiteres Problem ist die Tatsache, daß ein bloßes Testen der Datei sie physisch ändert. Wenn wir die Probleme des Autorrechts der originellen Dateien, entsteht da die Frage, ob sie sich sicher sein können, daß die veränderte Datei auch weiter so arbeiten wird wie ihr Orignal. Wahrscheinlich ja, aber es existieren Programme, die sich vor dem Anlauf kontrollieren und im Fall jeglicher Veränderung nicht arbeiten werden. Das obenangeführte gilt nur für anlaufbare Dateien. Beliebige Veränderung der Datendateien trägt mit sich ein großes Risiko einer Havarie des Programms, das diese Dateien ausnutzt.

Wenn sie denken, daß sich die Viren in den Datedateien nich verbreiten können, dann hatten sie noch von kurzem recht. Heute existiert schon eine spezielle Virengruppe ("**Makroviren**"), die sich ausschließlich mittels Datendateien verbreitet.

Das AVAST32 Programm modifiziert auf keine Weise keine getestete Datei. Wegen einer größeren Sicherheit öffnet es sie nur fürs Lesen, damit es nicht einmal durch Zufall zu ihrer Beschädigung kommen konnte. Wenn einige Komponenten des AVAST32 Programms Informationen über Dateien speichern, dann machen sie es in eine selbstständige Datei.

Nur in einem speziellen Fall, und zwar bei der Entfernung der gefundenen Viren, sind die Dateien eingetragen, aber auch da ist dieser Prozeß auf einer Kopie durchgeführt und nur nach einer erfolgreichen Beendigung ist die reparierte Datei unter dem Originalnamen eingetragen.

B.1.3 Alarm verursacht durch Witzprogramme

Soll es ihnen vorkommen, daß sich der Computer beginnt abnormal bis verdächtig zu benehmen, muß es sich nicht um einen Virus handeln. Es kann um ein "Witzprogramm" gehen, das ihnen auf ihren Computer ihr Kollege installiert hat, oder der ihnen mit einer falschen oder irreführenden Information über seinen Zweck unterschoben wurde. Ein Beispiel kann die Installation von Vorführung "heikler" Bilder beim Computeranlauf sein. Schwächere Charaktere oder weniger erfahrene Benutzer können Probleme mit seiner Einführung in den originellen Zustand haben und einen ähnlichen "Witz" können sie für Wirkung eines besonders heimtükischen Virus halten.

Immerhin muß es nich wahr sein. Und wie soll man einen "Witz" von einem wirklichen Virus unterscheiden? Das kann schwierig sein. Es ist nicht möglich genaue Grenzen beider Gruppen festzustellen. Es ist notwendig aus einer konkreten Situation auszugehen. Zum Beispiel, die Viren können sich nicht leisten graphische Bilder vorzuführen (und dazu noch in Farben), weil sie ziemlich groß sind. Der wichtigste Unterschied, den es allerdings nich einfach ist zu entscheiden, ist der, daß sich die Viren mehren wogegen die "Witze" nicht.

B.1.4 Alarm verursacht durch Fehler der Technik, des Software oder des Benutzers

Probleme mit der Technik, mit den instalierten Programmen oder mit weiteren Einrichtungen können einfach mit einer Vireninfektion verwechselt werden. Zum Beispiel, häufige Probleme, die auf diese Weise oft verwechselt werden, sind Probleme mit dem Druck oder mit der Festplatte. Es existieren allerdings sehr wenige Viren, die diese Probleme verursachen können.

Andererseits, die Meldung "**Memory parity error**" kann nur ein Fachmann begreifen, weil diese Meldung kann durch einen fehlerhaften Speicherchip aber auch durch ein Virus verursacht werden, das die Meldung auf den Bildschirm schreibt. Da kann nur Erfahrung helfen.

B.1.5 Alarm verursacht durch Arbeitsgrundsätze der Windows

Windows nutzen eine solche Weise der Speicherverwaltung, aus die ihnen ermöglicht mehr Speicher zu nutzen als sie in Wirklichkeit haben. Das allerdings kann einen falschen Alarm hervorrufen,

weil die sgn. "Signaturen" der Viren sind in dem "physischen" Speicher anwesend, können allerdings auch auf der Festplatte in dem "virtuellen" Speicher erscheinen. Dann kann vorkommen, daß sie ein Virus z.B. in der Datei WIN386.SWP finden (im System Windows NT ist das die Datei PAGEFILE.SYS). Es passiert auch sehr häufig, daß das "normale" Virus in einer Datei .DOC gefunden wird. Auch das ist ein falscher Alarm, den kann man so loswerden, daß die Datei in Word eröffnet wird, man wählt "Eintragen als" aus und trägt sie unter demselben Namen ein. Achtung! Da muß man unterscheiden, ob es sich nicht um ein sgn. Makrovirus handelt.

B.2 Es ist wirklich ein Virus!!!

Wahrscheinlich das erste, was ihnen einfällt, kann sein "**Warum ausgerechnet ich?!**". Daran ist nichts Merkwürdiges, eine große Mehrheit der Benutzer hat sich mit einem Virus begegnet und die Gefahr droht nich nur den "Computereinsiedlern". Mit ein bißchen Glück muß die Infektion keine große Schade machen. **Andererseits, das Glück ist mehr günstig für die Vorbereiteten!!!**

- Die erste Aktion (Anlage B.2.1),
- Was für ein Virustyp hat meinen Computer infiziert? (Anlage B.3),
- Kombinierte (multipartite) Viren (Anlage B.3.1),
- Viren, die in dem Speicher installiert bleiben (Anlage B.3.2),
- Dateien angreifende Viren (Anlage B.3.3),
- Systembereiche der Festplatten angreifende Viren (Anlage B.3.4),
- Makroviren (Anlage B.3.5).

B.2.1 Die erste Aktion

Grundsästzlich ist es der Panik nicht zu verfallen. Der Schaden, den das Virus verursachen konnte, ist geringfügig im Vergleich mit dem, was sie durch ihre eigene übereilte Aktion verursachen können.

Die Panik ist ihr Feind. Wenn sie ein Typ sind, der leicht Panik macht, beim Finden des Virus lassen sie den Computer in Ruhe und lassen sie sich eine Tasse Kaffee machen. Dann rufen sie ihren Administrator . Sie werden sehen, daß das Problem nicht so ernst ist.

Wenn sie etwas ohne Hilfe der anderen machen wollen, beenden sie ruhig die Arbeit aller arbeitenden Programme und speichern sie ihre Daten. Es kann auch passieren, daß sie das gerade durchgeführte Programm beenden müssen. Das macht nichts, lassen sie das beenden, was notwendig ist. Sie haben Zeit, nur ein geringer Anteil der Viren ist von der Zeit abhängig, während der sie aktiv sind. Vermeiden sie nur Anlauf von weiteren Programmen (wenn es geht). Auf keinen Fall schal-

ten sie den Computer durch den Netzchalter aus. Die Folgen könten für ihre Daten auf der Festplatte katastrofal sein.

Das Ausschalten des Computers mit dem Netzschalter ohne vorheriger Beendigung der Arbeit des Operationssystem ("**shut down**"), was eine nicht schöne Gewohnheit ist, die sich ihnen ganz sicher rächen wird.

Wenn es ihnen gelungen ist das Operationssystem zu beenden, dann schalten sie den Computer durch den Netzschalter ab. Ruhen sie aus, weil es die Zeit gekommen ist nachzudenken, was weiter machen.

Es ist notwendig diese Zeit auszunutzen. Sie brauchen sich nicht nur vom Virus befreien, sondern brauchen sie genau oder mit einer großen Wahrscheinlichkeit die Quelle der Infektion festzustellen (wahrscheinlich ihr Freund mit einer neuesten Version des bekannten Spiels). Eine sehr wichtige Frage ist, wie lange dürfen sie das Virus im Computer haben.

Seien sie lieber pesimistisch, es zahlt sich aus. Unterschätzung dieser Zeit heißt den ersten Schritt zur widerholten Infektion zu machen!!!

Nicht weniger wichtig is es nachzudenken, ob sie das Virus nicht weiter verbreiten konnten. Es ist egal, ob sie einen Firmencomputer infiziert haben und ihre Firma tausende infizierte Disketten oder sie haben nur die neue Version eines Spieles ihrem Freund geschenkt. In beiden Fällen ist es am besten unverzüglich alle die zu informieren, die die potentielle Infektion betreffen kann. **Machen sie es gleich jetzt!!**

Die Schande, die mit der Verbreitung der Virenifektion verbunden ist, ist bei weitem erträglicher wenn sie auf die Gefahr selber aufmerksam machen. Im Fall einer Firma geht es ums Vertrauen der Kunden, das sie ganz verlieren können, wenn er die Infektion feststellt und stellt auch fest, daß sie davon gewußt haben und sie nicht informierten (kann sein, daß sie sich es leisten können).

Eine der wichtigsten Sachen, die sie beurteilen müssen ist das, ob sie wirklich alle wichtige Daten aus dem infizierten Computer reserviert haben.

Jede Entfernung eines Virus trägt mit sich ein Risiko des kompletten Datenverlustes auf ihren Festplatten auch dann wenn die Entfernung von einem ausgebildeten und sehr erfahrenen Fachmann durchgeführt wird.

Es ist uns klar, daß sie über die Notwendigkeit die Daten zu reservieren wissen. Aber Hand aufs Herz, wann haben sie zum letztenmal die Daten reserviert. Und wenn sie es regelmäßig machen, haben sie je versucht , die gespeicherten Daten wieder herzustellen? Und wenn sie auch beide Bedingungen erfüllen, haben sie eine Sicherungs-

kopie des Reservierungsprogramms woanders als in dem infizierten Computer? Was werden sie tun wenn sie in den Computer nie wieder eindringen können?

Also, wenn sie keine aktuelle Reservierungskopie haben, jetzt ist gerade die richtige Zeit sie zu machen. Da kann man nichts machen und sie müssen es mit dem Bewußtsein machen, daß die reservierten Daten auch Virus enthalten können und zugleich, daß jeder weitere Anlauf des Computers kann den Grad der Infektion des Systems es. Aber man kann nichts ander machen. Die Reservation ist wirklich notwendig auch in dem Fall, daß die weitere Arbeit von jemanden ganz anderem (besonders jemanden, der keine Verantwortung für ihre Daten trägt) gemacht wird.

Also, ein kleines Resumé. Im Falle einer Virusinfektion:

- beenden sie die Arbeit, beeilen sie sich nicht umsonst, aber säumen sie auch nicht mit weiteren Maßnahmen,
- ermitteln sie möglichst viel Informationen von dem Virus,
- beenden sie die Arbeit des Operationssystems,
- schalten sie den Computer mit dem Netzschalter aus,
- überlegen sie, wie lange sie den Computer infiziert haben können und woher die Infektion wahrscheinlich gekommen ist,
- informieren sie alle, den sie die infizierte Data oder Media senden konnten,
- sollte es notwendig sein, reserevieren sie die Daten. Überlassen sie nichts dem Zufall!!

Wenn sie diese Schritte erfüllt haben, können sie an die weitere Arbeit herantreten. Da müssen sie ihre eigene Fähigkeiten und ihre Erfahrung mit dem Computer kritisch bewerten. Wenn sie die Computer nicht viel verstehen empfehlen wir ihnen nicht die Entfernung des Virus mit eigenen Kräften vorzunehmen. Wenn sie aber die weitere Auslegung verstehen werden, können sie es ohne fachkundige Hile versuchen. Wie sollen sie herangehen? Auf diese Frage versuchen wir eine Antwort zu geben.

Geben sie auch auf verschiedene „Fachleute“ acht. Wenn sie von ihnen z. B. den Ausdruck “low level format”, hören, laufen sie schnell davon. In Wirklichkeit versucht er sie und ihre Daten zu vernichten.

Wenn sie in einer grösseren Firma arbeiten, nehmen sie als erste Kontakt mit ihrem Administrator oder mit dem Mann, der für die Computer sorgt, auf.

B.3 Was für ein Virustyp hat meinen Computer infiziert?

Es ist wichtig zu wissen, was für ein Virustyp in ihrem Computer anwesend ist. Das weitere Verfahren hängt direkt davon ab und zugleich manche feine Nuancen in der Bestimmug des Virustyps können das Verfahren der Virusentfernung wesentlich verändern.

Sollte die folgende Auslegung jemandem wenig fachkundig vorkommen, ist es durch die maximale Bestrebung um die Lesbarkeit dieses Kapitel auch für die Benutzer, die die Viren nicht regelmäßig begegnen, zu bewahren.

Die primären Virustypen also sind:

- kombinierte (multipartite Viren),
- Viren, die in dem Speicher installiert bleiben,
- Dateien angreifende Viren,
- Systembereiche der Festplatten angreifende Viren,
- Makroviren.

Wenn sie auf ein selten vorkommendes Virus, das die Dateien verändert oder modifiziert, andere als OLE Dokumente, haben sie wahrscheinlich Pech darin, daß diese Daten sehr unglaubwürdig oder sogar unbrauchbar sind. Zugleich existiert kein Mittel, wie die vernichteten Datendateien zu reparieren (vielleicht ausser der Reserve der statischen Daten).

Im weiteren Text werden wir annehmen, das sie das Operationssystem Microsoft Windows 95 oder Microsoft Windows NT benutzen. Die Entfernung der Viren im System MS-DOS kann von den hier angeführten Verfahren abweichen.

B.3.1 Kombinierte (multipartite) Viren

Kombinierte Viren sind einfach Viren, die eine der Kombination der Dateien, der Systembereiche der Festplatten und des Speichers auf einmal angreifen. Ihre Entfernung ist eine Kombination von Entfernung der einfachen Virentypen in einer genau festgestellten Reihenfolge. Für die Reihenfolge gilt es:

- es ist nicht möglich ein Virus aus der Festplatte zu entfernen, solange er im Speicher anwesend ist,
- bei der Entfernung der Viren aus den Festplatten ist es notwendig als erste die Viren aus den der Systembereichen der Festplatten zu entfernen,
- Die Viren in einzelnen Dateien werden als letzte entfernt.

B.3.2 Viren, die in dem Speicher installiert bleiben

Diese Viren sind nicht nur im Speicher installiert, sondern sind anwesend auch irgendwo auf der Festplatte.

Wenn ihnen einer von den "Fachleuten" behaupten wird, daß das Virus sich im Speicher befinden kann, ohne anderswo anwesend zu sein (auf der Festplatte, Diskette oder auf einem anderem Medium des ähnlichen Typs), wenden sie sich an jemanden anderen. Ihre Daten werden viel sicherer.

Ein Virus kann sich im Speicher befinden und zugleich inaktiv sein. Stellen sie sich folgende Situation vor, daß sie eine infizierte Datei von einer Diskette auf eine andere kopieren. Auch in diesem Fall ist der Operationsspeicher des Computers benutzt und die originellen sowie auch die resultierende Dateien sind in ihm eingetragen. Das heißt, das Virus kann in dem Speicher auch nach der Beendigung des Kopierens einfach deshalb existieren, weil es keinen Grund gibt, warum den so benutzten Speicher zu reinigen. Das allerdings bedeutet, daß das in dieser Form wie auch immer schaden kann.

Sie knnen nicht ein Virus zugleich aus ihrem System entfernen, wenn er im Operationsspeicher anwesend und aktiv ist. Der Grund ist einfach, das Virus greift jedes Programm oder den Systembereich der Festplatte, die sie zu heilen versuchen, gleich an. Damit kann man nichts machen. Allgemein gilt es, daß sie ein Virus im Speicher während der Zeit wenn es in ihm anwesend ist nicht eliminieren können. Selbstverständlich, es kann auch Ausnahmen geben, aber darauf kann man sich nicht verlassen.

Zugleich müssen wir betonen, daß die Viren speziell für die Operationssysteme Windows 95 und NT heute praktisch nicht existieren und keiner von den wenigen sehr raren Fällen ist unfähig im Speicher resident zu bleiben. Sollte sich die Situation ändern, werden wir sie darüber informieren.

Aus dem voherigen Absatz folgt es, daß nur ein für den MS-DOS System bestimmtes Virus sich im Speicher befinden kann, das dort nach dem Anlauf des Computers oder bei der Arbeit in dem DOS Fenster geraten ist. Sollte es sich zugleich um ein Virus halten, das die Systembereiche der Festplatten angreift, können sie gleich in das Kapitel über die Viren dieses Typs übergehen. Soll es sich um Viren handeln, die die Dateien angreifen, ist die Lösung, wie das Virus aus dem Speicher zu entfernen, nicht kompliziert.

Laden sie das System aus der Systemdiskette. Im Grunde genommen können sie beliebige System-

diskette für MS-DOS 5.0 oder höher benutzen. Wir allerdings empfehlen eine Systemdiskette für das System, das sie im Computer installiert haben, zu benutzen.

Setzen sie dem Virustyp nach fort.

Unter dem Operationssystem Windows NT gibt es im Grunde genommen keine Probleme mit den Viren im Speicher. Die einzigen Viren, die auf diese Weise Unfug treiben können, sind die Viren, die die Systembereiche der Festplatten angreifen.

B.3.3 Dateien angreifende Viren

Das Entfernen der Viren aus den Dateien ist eine einfache und ziemlich unverdauliche Arbeit. Das Hauptproblem besteht in der Entscheidung, wie das Virus entfernen. Da haben sie nochmals einige Möglichkeiten zur Auswahl.

Hundertprozentige Erneuerung sichert nur die Restaurierung der Dateien aus den Reservekopien (selbstverständlich, wenn sie eine Kopie haben und wenn auch sie nicht mit demselben oder einem anderen Virus angegriffen worden ist). Die Erneuerung aus den Reservekopien kann einfach und zuverlässig sein. Wenn sie regelmäßig Zeit für Reservierung opfern, werden sie feststellen warum es sich auszahlt. Es ist eine schnelle und bequeme Arbeit.

Wenn sie regelmäßig das Programm für die Integritätskontrolle benutzen und über die aktuelle Version der Datenbank verfügen, so haben sie praktisch keine Sorgen. Das AVAST32 Programm ermöglicht die Dateien, die praktisch von allen Viren angegriffen (etwa 95 Prozent von verschiedenen Virentypen) zu restaurieren. Die Zuverlässigkeit der Erneuerung ist diegleiche wie im Fall der Erneuerung der Dateien aus den Reservekopien, weil das AVAST32 Programm kontroliert, ob es ihm gelungen ist die Datei bis zum letzten Bit zu restaurieren.

Wenn sie nichts aus den obenangeführten Absätzen benutzen können, beginnt die Situation mehr ernst zu sein. Immer noch müssen sie keine Programme einbüßen. Sie müssen allerdings originelle Disketten oder ihre Kopien zur Verfügung haben. Das heißt allerdings erheblich mehr Arbeit, denn sie müssen die infizierten Programme abinstallieren und wieder installieren, was mit sich viele bekannte Probleme mit der Speicherung von mühsam erdachten Aufgaben und Konfigurationen trägt.

Das Deinstallieren der Programme bedeutet nicht ihr einfaches Löschen auf der Festplatte. Alle "soliden" Programme für die Operationssysteme Windows 95 und NT haben die Fähigkeir des Abinstallierens, die besorgt mehr als das einfache Löschen der Dateien.

Wenn sie weder dieses Verfahren benutzen können, dann haben sie ein Problem. Wirklich ein großes Problem, weil wir ihnen nur das Auslöschen der angegriffenen Dateien emfehlen. Es gibt zwar noch eine potenzielle Variante, die sie benutzen können, aber ihre Resultate können ziemlich trist sein. Es handelt sich darum, daß sie noch versuchen können die Viren aus den Dateien mittels einem von anderen Antivirus Programmen zu entfernen. Diese Entfernung hat einen großen Nachteil. Sie kann nicht sicherstellen, daß die reparierte Datei in identischen Zustand ist wie vor dem Angriff. Das ist auch der Hauptgrund, warum das AVAST32 Programm keine ähnliche Eigeschaft enthält.

B.3.4 Systembereiche der Festplatten angreifenden Viren

Es existiert eine große Menge von Viren, die fähig sind Systembereiche der Festplatten anzugreifen. Allerdings nur wenigen von ihnen sind die sgn. "kombinierten Viren", die fähig sind die Dateien anzugreifen und mit ihrer Hilfe sich zu verbreiten. Deswegen können wir, mit einem kleinen Vorbehalt, sagen, daß wenn sie das Virus im Systembereich einer Festplatte gefunden haben, passierte es so, daß sie versucht haben den Computer aus der Diskette anzulaufen. Es ist egal ob es gelungen ist oder nicht. War ein Virus auf der Diskette, hat er ihren Computer angegriffen ohne Rücksicht darauf, welches Operationssystem sie normalerweise ausnutzen.

Es ist ganz umsonst anzunehmen oder sogar jemanden überzeugen , daß zum Beispiel das Virus "J&M" oder "JiMi" in ihren Computer durch einfaches Lesen der Daten von der Diskette

eingedrungen ist. Das ist einfach nicht wahr , behaupte es wer will. Das ist einfach Unsinn.

Eine Ausnahme ist allerdings der Virus "OneHalf", der sich auch mit Hilfe der Dateien verbreiten kann , was bedeutet, daß durch Anlauf einer infizierten Datei es zum Angriff des Computers kommt von ähnlichen Viren gibt es allerdings ein reines Minimum.

Das Verfahren für die Entfernung: das System von der Systemdiskette anlaufen und das folgende Programm: **fdisk /MBR** des entsprechenden Operationssystems.

Es ist nur wichtig dab die Diskette nicht mit einem Virus angegriffen ist. Nach einer erfolgreichen Durchführung dieser Anweisungen wird das Virus aus den Systembereichen der Festplatte, die Microsoft Windows 95 and NT betreiben, entfernt.

Gelingt es ihnen das Operationssystem anzulaufen, haben sie praktisch gewonnen. Sie können die Fähigkeiten der Erneuerung des Operationssystems ausnutzen, die in ihm eingebaut sind und die wer-

den für den Rest sorgen. Sollen sie das System gar nicht anlaufen, ist es schlimm.

B.3.5 Makroviren

Es handelt sich um Viren, die die Dokumente verbreiten. Diese Viren gehören zur Zeit unter die meistverbreiteten Viren auf der Welt und dieser Trend kommt langsam auch zu uns. Am häufigsten greifen sie die Dokumente der Microsoft Word Application an, aber in der letzten Zeit übergehen sie auch auf andere Büroapplikationen.

Die Entfernung kann man flottheraus aus der Umgebung des AVAST32 Programms (Kapitel 5.3.2) vornehmen. Trotzdem empfehlen wir ihnen, dab sie die infizierten Dokumente irgendwohin reservieren, die Originale virusfrei gemacht haben und dann ihre Lesbarkeit in ihren Programmen getestet haben. Sind die so reparierte Dokumente in Ordnung, ist es möglich ihre mit Virus infizierten Reservedateien auszulöschen. Wenn nicht, nehmen sie Kontakt mit den Mitarbeitern unserer Firma auf.

Die Algorithme benutzt vom AVAST32 Programm für die Suche und darauffolgende Entfernung der Makroviren aus den OLE Dokumenten gehören zur Zeit zur Weltspitze, so daß ihre Dokumente wirklich in den richtigen Händen sind.

C.Implizite Einstellung einer neuen Aufgabe

Seite "Name"
Das Textfeld für die Eingabe des Aufgabenamens enthält das Text "(nicht spezifiert)". Die neue Aufgabe ist vorgegeben privat.

Seite "Vorgänge"
Aus den nonresidenten Vorgängen ist nur der Vorgang "Virensuche" gewählt. Weder "Integritätstest" noch "Vereifachter Integritätstest" ist ausgewählt. Keine von den residenten Vorgängen ist abgehakt.

Seite "Priorität"
Die Aufgabenpriorität ist auf einen Wert eingestellt, der niedriger als die Priorität der Umgebung des AVAST32 Programms liegt.

Seite "Typen"
Für eine neue Aufgabe ist die Kontrolle der Programme (bzw. der ausführbaren Dateien) und der OLE Dokumenten eingestellt.

Seite "Bereiche"
Als vorgegeben ist die Kontrolle aller lokalen Festplatten, d.h. aller Festplatten, die direkt in Ihrem Computer installiert sind, eingestellt. Auch die verschachtelten Elemente werden kontrolliert werden.

Seite "Allgemeines"
Kein von den Feldern auf diese Seite ist abgehakt, d.h. daß eine neue Aufgabe wird direkt durch den Benutzer gestartet, Das AVAST32 Programm wird nicht gleich mit der letzten Aufgabe beendigt und nur das erste Virus, das in der Aufgabe gefunden wird, wird externen Programmen gemeldet.

Seite "Virensuche"
Die Felder “Operationsspeicher testen“ (das Feld kann nur unter Windows 95 gesehen werden), "Virencharakteristiken ignorieren" und "Komprimierte Dateien prüfen" sind abgehakt.

Die Aufgabe wird unter dem Operationssystem Windows 95 den Operationsspeicher testen, wird die Virencharakteristik ignorieren, wird ganze Dateien prüfen. Komprimierte Dateien werden sowohl im komprimierten als auch im dekomprimierten Zustand kontrolliert. Wird kein Virus gefunden, wird keine Meldung abgebildet.

Aus den Optionen ist die Option "Alle gefundene Viren melden" als vorgegeben gewählt.

Seite "Integrität"
Auf dieser Seite ist nur das Feld "Attribut ARCHIVE ignorieren". Der Datenintegritätstest wird also bei den kontrollierten Dateien den Attribut ARCHIVE ignorieren und wird jedesmal den Dateiinhalt prüfen.

Seite "Fortfahren"
Das Textfeld "Aufgabenname" ist leer; nach der Beendigung dieser Aufgabe wird keine weitere Aufgabe anlaufen.

Seite "Bericht"
Das Feld "Bericht konfigurieren" ist nicht abgehakt, Das Textfeld "Dateiname und - Pfad" enthält "*" (Asterisk) und das Feld "Existierenden Bericht überschreiben" ist nicht abgehakt. Die neue Aufgabe wird folglich keine Nachricht über ihr Vorgang erstellen.

Seite "Netzwarnung"
Das Feld "Meldung im Netz versenden" ist nicht abgehakt, so daß die Nachrichtensendung durch das Netz nicht erlaubt ist und die Einstellung der weiteren Steuerelemente auf dieser Seite ignoriert wird. Die Option "Meldung nur an ausgewählte Rechner versenden" ist gewählt. Die Computerliste auf dieser Seite ist als leer vorgegeben.

Seite "Meldung"
Das Textfeld für das Nachrichtentext enthält folgendes Text vorgegeben:

Datei %1 ist infiziert durch Virus %2.

Seite "Klang"
Diese Seite enthält keine Steuerelemente.

Seite "Überwachung"
Die Felder "OLE-Dokumenten", "16-bit-Windows-Applikationen" a "MS-DOS-Applikationen" sind abgehakt, so daß alle Anwendungen, die in Ihrem Computer laufen, überwacht werden. Von den Optionen ist die Option "Alles untersuchen außer der Systembibliotheken" gewählt.

Seite "Residente Blöcke"
Die Felder "DOS-Dateioperationen" und "Windows-Dateioperationen" sind abgehakt. In Windows 95 ist das Feld "Formatieren" nicht abgehakt. Es werden also alle Vorgänge, außer Formatieren, überwacht.

Seite "Ignoriere"

Die Dateienliste auf dieser Seite ist als leer vorgegeben. Verdächtige Vorgänge mit allen Dateien in Ihrem Computer werden überwacht.

D.Aktivierungsschlüßel und Lizenzen

Der Aktivierungsschlüßel ist eine Folge der Zeichen in der Form AABBB.CDDDDDD-EEEEEE. Der erste Teil enthält die Programmidentifikation, Teil BBB setzt die Programversion fest und der Posten C ist ein Zeichen, das die Anzahl der verfügbaren Lizenzen bedeutet. Ist der Buchstabe "A", ist nur eine Lizenz gekauft, ist da "B", dann sind zwei Lizenzen gekauft usw. DDDDDD stellt die Aktivierungsschlüßel der Programmkopie und EEEEEE ist ein Kod, mit dem die Echtheit der ganzen Lizenznummer festgestellt wird.

Das AVAST32 Programm behütet die Anzahl der momentan angelaufenen Kopien im Netz. Wenn sie weniger als zehn Lizenzen gekauft haben, erlaubt ihnen das Programm immer um eine Kopie mehr anzulaufen, als die Anzahl der gekauften Lizenzen ist. Haben sie mindestens zehn Lizenzen gekauft, so können sie um zwei Kopien des AVAST32 Programms mehr betreiben, als sie Lizenzen gekauft haben.

Der Benutzer wird auf die Tatsache, daß er mehr Programmkopien angelaufen hat als die Anzahl der gekauften Lizenzen, durch eine Warnmeldung aufmerksam gemacht (Abb. 112).

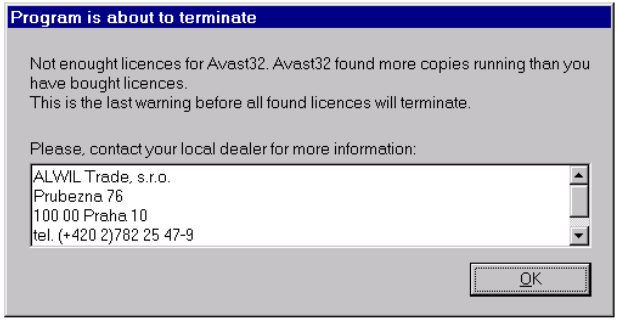

Abb. 112

Wenn der Benutzer, trotz diese Meldung, versucht weitere Kopien des AVAST32 Programms anzulaufen, werden alle seine bisher laufenden Kopien beendet.

E.Netzeigenschaften und Netzunterstützung

Das AVAST32 Programm unterstützt selbstverständlich die Arbeit im Netz, das ist heute eine ganz gewöhnliche Ausstattung einer Reihe von Arbeitsplätzen.

Das AVAST32 Programm ermöglicht beim Finden eines Virus eine Meldung jedem angeschlossenen Benutzer zu senden, am häufigsten offenbar dem Netzadministrator oder einer anderen verantwortlichen Person. Das AVAST32 Programm benutzt für diese Tätigkeit die Dienste, die ihm Operationssysteme Windows bieten, sodaß kein Bedürfniss auf eine zusätzliche Konfiguration besteht.

Bei der Arbeit im Netz ist es notwendig Lizenzabkommen einzuhalten. Das AVAST32 Programm behütet die Anzahl der momentan angelaufenen Kopien im Netz, damit ihre Anzahl nicht die Anzahl der gekauften Lizenzen übertrifft. Nähere Information ist im Anhang D.

Im Netz pflegt es ein Problem zu sein alle gebrauchten Programme in genügend aktuellen Versionen, bei den Antivirusprogrammen gilt es um so mehr. Damit der Netzadministrator die Virendatenbank nicht in jedem Computer extra aktualisieren muß, ist in das AVAST32 Programm die Automatisierung dieser Tätigkeit eingebaut.

Alles, was notwendig zu tun ist, ist eine Mappe zu erstellen, aus der alle Netzbenutzer lesen können. Diese Mappe ist es dann notwendig dem AVAST32 Programm als die Mappe anzugeben, die für die automatische Aktualisierung der VPS Datei benutzt sein soll (Kapitel 6.6, Textfeld "Name der Quelldatei") und selbstverständlich die eigene automatische Aktualisierung zu erlauben (Kapitel 6.1.2, Anhakfeld "VPS automatisch aktualisieren").

Dann genügt es, jede weitere Aktualisierung der VPS Datei (die sgn. kleine Aktualisierung) in die erstellte Mappe zu kopieren, und die Aktualisierung wird automatisch im ganzen Netz durchgeführt. Das AVAST32 Programm nämlich nach seinem Anlauf kontrolliert, ob die ausgewählte Mappe nicht eine neuere VPS Datei enthält. Wenn sie nicht enthält, dann wird die bisherige VPS Datei entfernt und mit einer neueren ersetzt.

F.Eigenschaften für die Programmierer

Das AVAST32 Programm ist hauptsächlich in die Benutzerrichtung orientiert, es hat aber auch mehrere Eigenschaften, die hauptsächlich die Programirer ausnutzen. Die wichtigste von ihnen ist in dem nächsten Kapitel beschrieben.

Wenn sie wo immer im AVAST32 Programm den Weg angeben, kann der Name auch der Name einer Systemveränderlichen, zwischen zwei Zeichen "%" (Prozent) sein. Man kann sich also auf die Rootmappe z.B. folgendermaßen beziehen: "%SystemRoot%". Soll die Systemveränderliche des angegebenes Namens nicht existieren, wird dieser Teil des Weges ignoríert.

F.1 Senden der Nachrichten über die gefundenen Viren

Das AVAST32 Programm disponiert über einen Mechanismus, der es ermöglicht die externen Programme über die gefundene Viren zu informieren. Zu diesem Zweck wurde ein Kasten mit dem Namen "\\\\.\\mailslot\\AVAST32\\VIRUSFOUND" erstellt, in den die Informationen über das erste durch das residente Programm gefundene Virus und Information über alle Viren, die durch die residente Programmegefunden wurden. Es ist möglich einzustellen, daß in den Kasten Informationen über alle gefundene Viren geschickt werden (Kapitel 4.4.6).

Die Nachricht über das gefundene Virus enthält den Bereichsnamen, Computernamen, Benutzernamen, Namen der infizierten Datei und des Virus, der die Datei angegriffen hat. Die Angaben sind in den Kasten im Kettenformat, gegenseitig mit einem Nullzeichen getrennt.

Register

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

V

W