VTC
VIRUS
TEST
CENTER

Computerviren auf dem Macintosh

Eine Einführung von
Ronald Greinke

Computerviren auf dem Macintosh

Mit zunehmender Verbreitung von Macintosh-Rechnern hat auch die Zahl der Viren zugenommen. Sie ist im Vergleich zur MS-DOS Welt zwar immer noch verschwindend gering und die verwendeten Mechanismen sind im Gegensatz zu PC-Viren noch sehr simpel, aber die existierenden Viren richten bereits genug Schaden an.

Dieser Artikel soll dem Anwender helfen, die Arbeitsweise von Viren zu verstehen um Gefahren frühzeitig zu erkennen und Schäden vorzubeugen. Er ist in drei Abschnitte gegliedert:

1. Aufbau und Arbeitsweise eines Macintosh-Programms
2. Typische Mechanismen von Viren zur Programminfektion
3. Bekannte und unbekannte Viren, Erkennung und Gegenmaßnahmen

1. Ein Typisches Macintosh-Programm:

Anders als in der MS-DOS Welt besteht ein Macintosh-Programm nicht aus einer Datei, in der alle Teile des Programms bunt zusammengewürfelt sind, sondern es gliedert sich in diverse Einzelteile, die separat ansprechbar sind.
Dies hat mehrere Vorteile: Ein Programm braucht weniger Speicher, da nicht immer alle Teile benötigt und nur bei Bedarf geladen werden müssen. Das Programm kann leichter an andere Sprachen angepaßt und geändert werden, da zum Beispiel Menüs ein separater Teil eines Programms sind.
Nachteile: Beim Betrieb ist eine Festplatte zu empfehlen, damit das Nachladen von Teilen nicht zuviel Zeit in Anspruch nimmt. Ferner kann das Aufleuchten der Laufwerks-Lampe jederzeit vorkommen und daher nicht als Verdachtsmoment für Virusaktivitäten benutzt werden.
Sehen wir uns nun einmal ein Programm näher an.

Abb. 1 zeigt ein Informationsfenster für das Programm WordPerfect.
Die dritte Zeile zeigt Typ und Creator von WordPerfect. Der "Typ" gibt die Art einer Datei an. Ein Typ "APPL" bedeutet daß es sich um ein Programm handelt. Andere Typen sind zum Beispiel "PICT" für Bilder oder "cdev" für Schreibtischprogramme. Der "Creator" beschreibt den

Erzeuger eines Dokuments und sorgt dafür, das der Finder WordPerfect startet, wenn der Benutzter einen Doppelklick auf ein Dokument vom Typ "TEXT" mit dem Creator "WPC2" macht. Jedes Programm besitzt einen individuellen Creator, damit Dokumente eindeutig zugeordnet werden können. Die weiteren Zeilen liefern ergänzende Informationen über das Programm, wie zum Beispiel das Erstellungsdatum und den Zeitpunkt der letzten Änderung.
Die Angabe "Size" gibt die Größe des Programms an. Dieses unterteilt sich in den Data- und den Resourceteil. Diese Teile werden als fork bezeichnet. Die Datafork enthält reine Daten und ist bei Programmen meist leer. In ihr wird bei Dokumenten der Text oder andere Daten gespeichert. Die Resourcefork enthält den eigentlichen Programmcode und alle weiteren benötigten Teile, wie zum Beispiel Menüs, Dialoge, Fenster. Der unterste Bereich legt das Aussehen und das Verhalten des Programms unter dem Finder fest, zum Beispiel ob das Programm ein eigenes Symbol hat oder nur das Standardsymbol - die Hand, die auf ein Tablett schreibt, dargestellt wird.

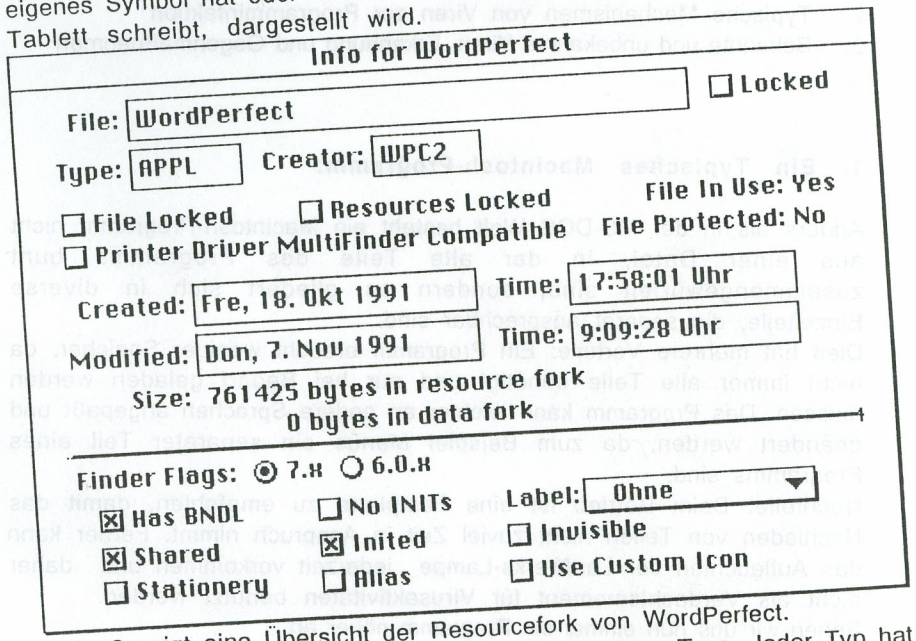


Abb. 2 zeigt eine Übersicht der Resourcefork von WordPerfect.
Eine Resource ist eine Ansammlung von Daten eines Typs. Jeder Typ hat einen Namen der aus vier Zeichen besteht. Resource-Typen werden im folgenden in *kursiv* dargestellt. Jede Resource eines Typs besitzt eine eindeutige Identifikationsnummer.
Die Resourcefork besteht aus verschiedenen Resource-Typen , wobei

solche existieren, die ein von Apple vorgeschriebenes Format besitzen und andere, die nur von diesem Programm und gegebenenfalls von weiteren Programmen benutzt werden. Uns interessieren nur die festgeschriebenen Typen. Hier sind zunächst die Typen, die Programmcode enthalten und damit für Viren geeignet sind. Der eigentliche Programmcode ist in den *CODE* Resourcen vorhanden und stellt den Teil des Programms dar, der als erstes gestartet wird. Resourcen vom Typ *CDEF* sind für das Aussehen von Kontroll-elementen, wie zum Beispiel Schieberegler, verantwortlich. Der Typ *LDEF* ist für die Darstellung von Elementen einer Liste zuständig. Ferner die Typen *MDEF* und *WDEF* (nicht im Bild) die Menüs bzw. Fenster beeinflussen. Alle diese Typen werden nur bei Benutzung der mit Ihnen verbundenen Elemente ausgeführt. Die nachfolgenden Typen enthalten keinen Code und werden nur zum allgemeinen Verständnis aufgeführt.
MENU und *MBAR* definieren die Einträge eines Menüs und ihr Erscheinen in der Menüleiste .
ALRT, *DLOG* und *DITL* Diese Typen bestimmen das Aussehen von Dialogboxen und Warnmeldungen.Der Typ *WIND* beschreibt das Aussehenneines Fensters und der Typ *PICT* enthält Bilder. *BNDL*, *ICON*, *icl8*, *icl4* und *FREF* enthalten die Symbole, die auf dem Desktop erscheinen, in Farbe und Schwarz-Weiß, sowie die Informationen, die der Finder braucht, um Dokumente einem Programm zuzuordnen.

WordPerfect

Type	Count	Size
ALRT	3	36
BITS	41	1850
Bmap	5	3387
Bmp#	7	7862
BNDL	1	140
CDEF	2	1930
CDSI	3	0
cMAP	23	3848
CNTL	5	119
CODE	89	669604
CURS	18	1224
DITL	3	210
FOND	1	84
FREF	15	105
icl4	13	6656
icl8	13	13312
ICN#	13	3328
ICON	5	640
LDEF	10	3734
Lmap	1	290
MDEF	2	7822
MENU	5	630
NFNT	2	864
PAT#	2	1028
PICT	2	2424

Abb. 3 Die Resource-Fork von Word Perfect

Die nächsten Bilder zeigen ein paar dieser Typen in graphischer Darstellung.

Abb. 3: *BNDL* und *FREF* sowie die Icontypen im Zusammenhang

FREF			Finder Icons		
local	res ID	Type	local	res ID	ICN# icl4 icl8 ics# ics4 ics8
0	128	APPL	0	128	
1	129	WPD1	1	129	
2	130	WPDF	2	130	
3	131	WPT1	3	131	

Abb. 4 und 5:*MENU und WIND* in graphischer Darstellung

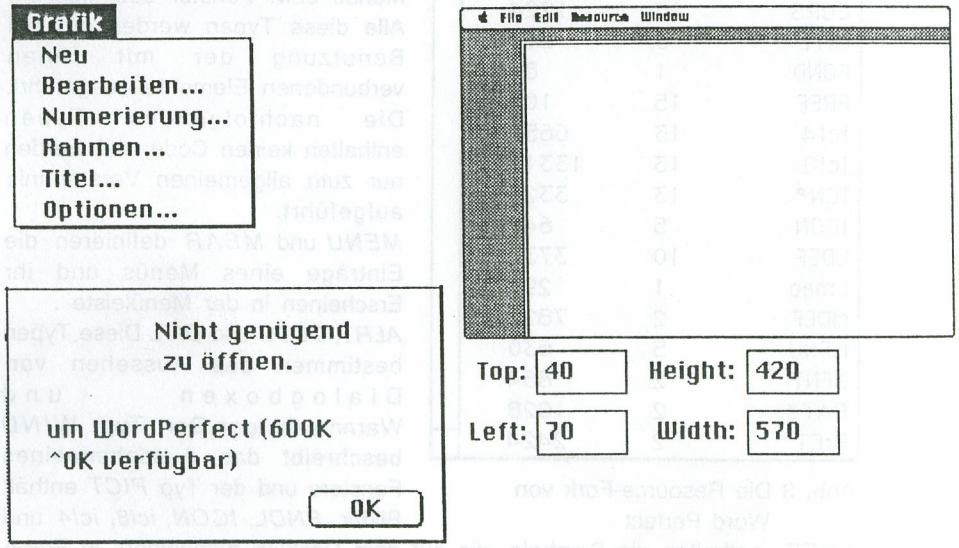


Abb. 6 *ALRT* Maske für eine Alarmbox (^0 wird zur Laufzeit durch eine Zahl ersetzt und in der linken oberen Ecke wird ein Stopsymbol eingesetzt).

2. Was ist ein Virus und wie infiziert er ein Programm ?

2.1 Was ist ein Virus ?

Ein Virus ist ein Programmcode, der die Fähigkeit besitzt sich selber zu vervielfältigen, indem er eine Kopie von sich selbst in ein anderes Programm einbaut. Dieser Code wird bei Start dieses Programms als erstes ausgeführt, erst dann erfolgt der Ablauf des ursprünglichen Programms. Viele Viren besitzen neben der Eigenschaft, sich zu duplizieren auch noch Code, der in irgendeiner Form das Arbeiten mit dem Rechner stört. Dieser Teil wird Wirkteil genannt. Dieser kann zum Beispiel dadurch bemerkbar machen, daß der Mauszeiger sich selbständig bewegt, wenn man die Maustaste drückt (Zuc-Virus) oder das alle Dateien in unsinnige Namen erhalten (INIT 1984-Virus). Der Wirkteil wird normalerweise durch ein bestimmtes Ereignis ausgelöst, zum Beispiel muß der Virus zunächst 16 Dateien infizieren oder ein bestimmte Datum muß erreicht sein.

2.2 Wie infiziert ein Virus ein Programm ?

Um ein Programm zu infizieren, muß der Virus erst einmal in den Speicher des Computers gelangen. Dies geschieht, indem ein bereits infiziertes Programm gestartet, eine Diskette mit einer infizierten Desktop-Datei eingelegt oder ein Programm gestartet wird, das einen Virus installiert .

2.2.1 Mechanismen

Wird ein infiziertes Programm gestartet, übernimmt der Virus die Kontrolle und sucht sich weitere Programme, die er infizieren kann. Dies kann in sehr unterschiedlicher Weise geschehen. Je nachdem welchen Mechanismus der Virus benutzt, werden andere Programme infiziert wenn sie gestartet werden, sie vom Finder kopiert werden, sie auf einer neu eingelegten Diskette vorhanden sind oder der Virus sie ausgewählt hat. In Fällen, in denen der Virus die Datei nicht selbst auswählt, muß er Funktionen des Betriebssystems auf sich umlenken, um sein Werk zu verrichten. Damit der Anwender hiervon nichts merkt, wird nach der Infektion die Originalfunktion ausgeführt, so daß dem Anschein nach alles normal abläuft. Um auch nach Beenden eines infizierten Programms weiter andere Programme verseuchen zu können, installieren sich manche Viren im Systemspeicher oder in der

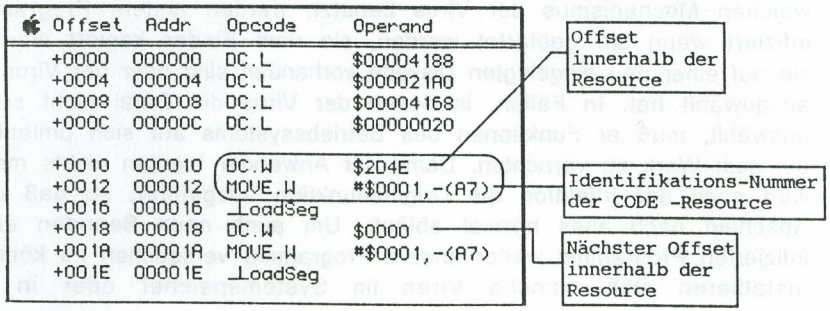
Systemdatei im Systemordner. Die Systemdatei ist immer in Betrieb und damit immer geöffnet (dazu mehr unter 2.2.4).
Eine Diskette mit einer infizierten Desktop-Datei wird eingelegt.
Die Destopdatei einer Diskette (auch jedes anderen Laufwerks wie Harddisk , CD-ROM , Wechselplatte) speichert Informationen über die auf dem Datenträger vorhandenen Dateien. Diese Informationen benötigt der Finder, um den Inhalt der Diskette anzuzeigen und Programme und Dokumente zu laden und zu starten. Diese Datei wird bei Einlegen einer Diskette automatisch vom Finder geladen. Befinden sich in der Datei Resourcen vom Typ *CDEF* oder *WDEF,* so werden diese gestartet. So gelangt der Virus in den Speicher. Danach kann er wie oben beschrieben weiter verfahren.

2.2.2 Programme, die Viren aussetzen.

Solche Programme werden Dropper (engl. fallenlassen) genannt. Diese Programme wurden von jemanden mit der Absicht programmiert, den in dem Programm untergebrachten Virus freizusetzen. Damit dies nicht auffällt, führen diese Programme auch sinnvolle Handlungen aus, nachdem sie den Virus - wie unter 2.2.1 erläutert - eingepflanzt haben.

2.2.3 Aufbau eines Programms vor und nach einer Infektion.

Hauptangriffspunkte bei Programmen sind die*CODE* Resourcen. Hierbei sind zwei Typen zu unterscheiden: die*CODE*-Resource mit der Identifikationsnummer 0 und alle anderen. *CODE* 0 ist die sogenannte "Jumptable" und definiert welcher Code bei Start eines Programms zuerst ausgeführt wird. Der erste Eintrag in der Tabelle definiert den Programmcode, der als erstes gestartet wird.
Abb. 8 *CODE* 0



Die ersten 4 Zeilen haben für Viren keine Bedeutung und werden vom Betriebssystem benötigt.
Die 6. Zeile besagt, daß als erstes der Code in der *CODE* 1 Resource gestartet wird und zwar an der Position hexadezimal 2D4E (11598 dezimal) Die weiteren Einträge definieren weitere Einsprungstellen für alle *CODE*-Resourcen.
In *CODE* 1 an der Position $2D4E beginnt der Computer mit der Programmausführung. Hier steht normalerweise der Startcode des Programms. Wird dieses Programm infiziert, so hat der Virus mehere Möglichkeiten, diesen Mechanismus zu nutzen. Entweder hängt sich der Virus an die bestehende *CODE* 1 Resource an und ändert die Einsprungaddresse entsprechend. Dies heißt, $2D4E wird durch die Startaddresse des Virus-Code ersetzt. Als zweite Möglichkeit kann der Virus eine zusätzliche *CODE*-Resource hinzufügen und ändert dann auch die Nummer der zu startenden Resource von eins in die Nummer der Virus-Resource. Eine weitere Methode besteht darin, die Nummer von *CODE* 1 zu ändern und eine neue *CODE* 1 Resource hinzuzufügen. Weitere Methoden sind denkbar. Weitere Angriffsziele von Viren sind die oben genannten Resourcen vom Typ *WDEF*, *MDEF*, *MBDF* und *CDEF*. Sie werden immer dann gestartet, wenn das infizierte Programm Fenster, Menüs, genauer: Kontrollelemente in Dialogen benutzt.

2.2.4 Aufbau eines Systemprogramms vor und nach einer Infektion.

Systemprogramme sind die Systemdatei (System) und andere Programme, die im Systemordner vorkommen (Kontrollfelder, Systemerweiterungen (Inits), Druckertreiber etc.) Der Finder und der Multifinder zählen nicht zu dieser Gruppe, da sie wie "normale" Programme aufgebaut sind. Alle diese Programme besitzen keine Resourcen vom Typ *CODE,* sondern solche vom Typ *INIT.* Diese Resourcen werden geladen und ausgeführt wenn der Computer eingeschaltet oder ein Neustart duchgeführt wird. Unter der Betriebssystemversion 7 gibt es in der Systemdatei keine *INIT* Resourcen mehr, so daß dieser Mechanismus in der Systemdatei selbst nicht mehr funktioniert. Die oben genannten Resourcen der Typen *WDEF, MDEF, MBDF* und *CDEF* werden auch in der Systemdatei von Viren benutzt. Aber Vorsicht, in der Systemdatei befinden sich auch die Standard-Resourcen, die für den Betrieb des Macintosh notwendig sind. Ein Systemprogramm wird durch Hinzufügen einer *INIT* Resource infiziert.

Eine Infektion mit den anderen Typen ist normalerweise mit einer zusätzlichen Änderung der Identifikations-nummer der vorhandenen Standard-Resource verbunden.

Dies ist notwendig, um diese Nummer von der Virus-Resource verwenden zu können. Auch hier wird der Virus dadurch getarnt, daß er nach einer Infektion die normale Arbeit des Wirtsprogramms wieder aufnimmt.

2.3 Tarnmechanismen von Viren

2.3.1 Einfache Tarnung

Der Virus infiziert ein Programm und führt dann das Wirtsprogramm aus. Dies funktioniert so schnell, daß der Anwender hiervon nichts bemerkt, ein Überwachungsprogramm im Speicher entdeckt die Virusaktivitäten jedoch mühelos.

2.3.2 Tarnung vor Überwachungsprogrammen

Überwachungsprogramme beobachten Aufrufe des Betriebssystem und warnen den Anwender, wenn Aktionen ausgeführt werden, die auf einen Virus hindeuten. Dies wird von Viren dadurch umgangen, daß sie das Betriebssystem im ROM direkt anspringen. Ferner "kennen" einige Viren die gängigen Überwachungsprogramme und können sie deshalb umgehen. Eine andere Methode der Viren ist es, sich als ein anderes Programm auszugeben, für daß ein Verhalten ähnlich dem des Virus normal ist.

2.3.3 Tarnkappenverfahren

Manche Viren machen sich "unsichtbar" für Virensuchprogramme, indem sie ihnen falsche Datei- und Speicherinhalte vorgaukeln. Diese Typen sind auf dem Macintosh noch nicht vorgekommen.

3. Erkennung von Viren und Gegenmaßnahmen

3.1 Erkennung von Viren

Deutliche Anzeichen für Viren sind:

- Die Länge und das Datum der letzten Änderung von Programmen verändern sich.
- Diskettenoperationen dauern länger als gewöhnlich.
- Programme stürzen häufiger ab als vorher oder funktionieren nicht mehr richtig.
- Es erscheinen Meldungen auf dem Bildschirm, es wird Musik gespielt oder die Maus verhält sich ungewöhnlich.

Alle oben genannten Symptome können jedoch auch andere Ursachen haben, zum Beispiel Unverträglichkeiten von Programmen mit einer Systemversion oder bestimmten Systemerweiterungen.

3.2 Gegenmaßnahmen

Besteht der Verdacht auf einen Virus, sollten die folgenden Regeln beachtet werden.

- Ruhe bewahren
- Zuerst eine andere Ursache annehmen.
  Haben vorher irgendwelche neuen Programme installiert oder die Systemkonfiguration geändert?
- Auf keinen Fall die Reset-Taste drücken oder den Rechner manuell ausschalten. Dies könnte zur Zerstörung der Verzeichnisstruktur führen. Außnahme: Der Rechner formatiert die Festplatte oder die eingelegte Diskette.
- Keine Dateien löschen, sie könnten zur Restauration des Originalzustandes oder zur Beweissicherung notwendig sein.
- Den Rechner über den Finder ausschalten.
- Falls vorhanden, alle Netzwerkverbindungen trennen.
- Von einer unverseuchten schreibgeschützten Systemdiskette den Rechner starten. Damit ist sichergestellt, daß kein Virus in den Speicher gelangen kann.
- Von einer unverseuchten schreibgeschützten Diskette ein aktuelles Antivirusprogramm starten und die Festplatte nach Viren absuchen.

- Wurde ein bekannter Virus gefunden, diesen entfernen und den Vorgang mit allen weiteren Datenträgern und mit den weiteren Computern im Netzwerk wiederholen, bis alle Kopien des Virus entfernt wurden.
- Sollte kein bekannter Virus gefunden werden, führen Sie die folgenden Schritte durch:
- Stellen Sie eine Liste der Symptome auf.
- Notieren Sie mit welchen Programmen Sie gearbeitet haben, seit Sie den Rechner eingeschaltet haben.
- Vergleichen Sie die Längen der Programme, mit denen Sie gearbeitet haben mit der Länge der Programme auf Ihren Originaldisketten.
  Sollte sich die Länge geändert haben, schicken Sie eine Kopie des Originals und der geänderten Datei an das Virus Test Center (Adresse: siehe letzte Seite)
- Sollten die geänderte Datei zu groß für eine HD-Diskette sein, können Sie auch das Programm "Vergleicher" benutzen um nur die Differenzen in eine Datei zu speichern.
  (Erhältlich beim Virus Test Center gegen Freiumschlag und Diskette)
- Für eine Analyse im Virus Test Center wird folgendes benötigt:
  - Die veränderten Dateien und falls vorhanden deren Original
  - Eine Beschreibung der Systemumgebung (Systemversion, installierte Systemerweiterungen), der Symtome und der Programme, mit denen Sie zuletzt gearbeitet haben.
  - Ferner wäre eine Kopie des Systemordners hilfreich.

3.3 Vorbeugende Maßnahmen

Bevor Sie neue Software installieren und ausprobieren, überprüfen Sie sie auf Viren.
Bewahren sie Originaldisketten immer mit Schreibschutz auf. Das Einlegen eine Diskette kann bereits zur Infektion führen, wenn diese nicht schreibgeschüzt ist.
Machen sie regelmäßig ein Backup von Ihren Daten. Es ist ratsam, mehrere Backupgenerationen aufzubewahren, da Viren oft mit Langzeitwirkung Schaden anrichten. Von Programmen ist kein Backup notwendig, wenn die Originaldisketten verfügbar sind.

4. Das Virus Test Center

4.1 Wir über uns

Das VTC (Virus Test Center) ist ein Arbeitsbereich des Fachbereichs Informatik der Universität Hamburg und beschäftigt sich mit Computersicherheit. Dies beinhaltet die Analyse von Computerviren, wie Viren, Würmern, trojanische Pferden, logische Bomben etc. Das VTC gibt den Virus-Katalog heraus, der eine Beschreibung bekannter Viren enthält. Der Katalog soll dem Anwender helfen, Viren aufzuspüren und zu beseitigen. Ein Katalogeintrag basiert auf der Analyse eines Virus durch das VTC. Ferner steht das VTC beratend zu Fragen der Virenbekämpfung zur Verfügung.

4.2 Ausstattung:

Zur Zeit arbeiten wir mit einen Mac IIcx und einen Mac LC mit zusammen 140MB Festplattenkapazität. Desweiteren haben wir Zugriff auf ein 44MB Syquest Wechselplattenlaufwerk sowie ein CD-ROM- Laufwerk.
Wir verfügen über die Systemversionen 6.04 , 6.05 , 6.07 , 6.08 ,7.0 , 7.01 mit System 7 Tuneup 1.1.1 und über System 7.1.

4.3 Anschrift

Virus Test Center
Fachbereich Informatik
Universität Hamburg
Vogt Kölln Straße 30
2000 Hamburg 54
(ab 01.07.1993: 22527 Hamburg)
Telefon: 040 / 54 71 5-405 (Sekretariat)
Telefon: 040 / 54 71 5-234 (VTC-Labor, nur DI und DO 10-12 Uhr)
Telefax: 040 / 54 71 5-226
Electronic Mail via Internet : greinke@informatik.uni-hamburg.de

4.4 Die VTC Mailbox

Unter der Telefonnummer 040 / 54 71 5-235 wird die VTC-Mailbox betrieben. Sie enthält aktuelle Informationen zu Viren, den Virus-Katalog sowie die neusten Versionen der verfügbaren Public-Domain- und Shareware-Antivirusprogrammen.

Ferner werden die Beiträge des Virus-L, einem Virendiskussionsforum im Internet, in der Box gespeichert.

Die Box ist öffentlich zugänglich und unterstützt Baud-Raten von 2400 bis 14.400.

Bitte beachten Sie: ein UPLOADEN ist nur nach vorheriger Absprache mit uns möglich, um die Gefährdung Dritter durch Virus-Infektionen weitgehend auszuschließen.