



Virenschutz

AN-
VIRUS-
SCHE-
RE

???



ES-
S-
VIRUS-
SCHE-
RE

j.meissburger@fz-juelich.de



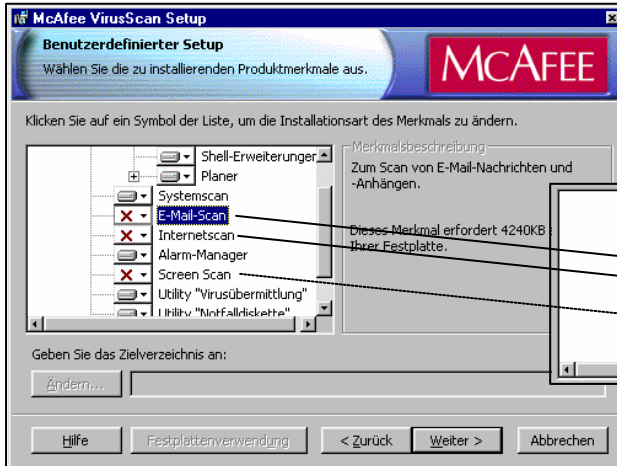
Typische Nutzungsarten von Antivirensoftware nach steigenden Systemanforderungen

1. Unter Windows, von Hand („on demand“) gestartet, und nur bei aktuellem Bedarf (spätestens vor einem Image-Backup!)
2. Boot-Block der Festplatte und Memory beim Starten des Systems automatisch überprüfen (DOS-Scanner)
3. Regelmäßige Scans in abgestimmten Zeitintervallen oder in der nicht interaktiv genutzten Zeit (Scheduler, Bildschirmschoner-Scanner)
4. Permanente Überwachung von E-Mail und anderen Downloads (Virenwächter)
5. Permanente Überwachung aller Dateioperationen (Virenwächter)

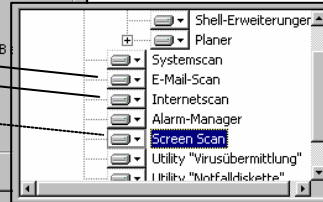


Installation von NAI VirusScan

- Unbedingt benutzerdefiniertes Setup im MS-Installer auswählen !

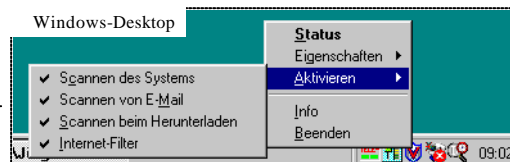


- E-Mail-Scan und Internetscan aktivieren!



Programmeigenschaften des NAI-Virenschanners

- Wird wie ein normales Windows-Programm installiert und kann jederzeit deaktiviert oder vollständig wieder deinstalliert werden
- Enthält ein im Hintergrund aktives Virenfiler (VShield) und einen Taskplaner zur automatischen, zeitgesteuerten Ausführung bestimmter Aktionen wie Scannen des Systems oder Update der Virensignaturen
- Kann bequem aus der Taskleiste heraus gesteuert werden
- Unterstützt
 - Scannen des Systems, d.h. der Festplatten, Bootsektoren und Dateien
 - Scannen von Email beim Herunterladen vom Mailserver
 - Scannen von Dateien beim Herunterladen von Web- oder FTP-Servern
 - Einfache Internet-Adreßfilter und Filter für aktive Inhalte Java & ActiveX





Scannen des Systems

Scannen des Systems Eigenschaften

Erkennung | Aktion | Warnung | Bericht | Ausschießung

Legen Sie die Ereignisse fest, durch die das Scannen ausgelöst wird, sowie die zu scannenden Dateitypen.

Scannen des Systems aktivieren

Dateien scannen auf: Ausführen Erstellen Kopieren Umbenennen

Disketten scannen in: Zugriff Herunterfahren

Zu scannende Elemente: Alle Dateien Nur Programmdateien Komprimierte Dateien

Allgemein: Scannen des Systems kann deaktiviert werden Symbol auf Desktop anzeigen

Buttons: Agsistent..., OK, Abbrechen, Anwenden

Callouts:

- Diese Dateien werden ignoriert
- Logging
- Art der Warnung
- Aktion beim Auffinden eines Virus (fragen, löschen ...)
- Was und wann wird gescannt ?



Scannen von Email und beim Herunterladen

Scannen von E-Mail Eigenschaften

Erkennung | Aktion | Warnung | Bericht

Geben Sie Ihr E-Mail-System sowie die zu scannenden E-Mail-Anhänge an. Klicken Sie mit der rechten Maustaste unter "E-Mail-System", um zusätzliche Informationen zu erhalten.

Scannen von E-Mail-Anhängen aktivieren

E-Mail-System: Erinnerung E-Mail aktivieren Microsoft Exchange (MAP) Lotus cc:Mail

Internet-Mail (Erfordert das Scannen beim Herunterladen)

Ordner: Alle neue Mail Ordner auswählen

Anhänge: Alle Anhänge Nur Programmdateien Komprimierte Dateien

Scannen beim Herunterladen Eigenschaften

Erkennung | Aktion | Warnung | Bericht

Aktivieren Sie das Scannen von vom Internet heruntergeladenen Dateien, und geben Sie die zu scannenden Dateitypen an. Klicken Sie mit der rechten Maustaste auf "Nur Programmdateien", um zusätzliche Informationen zu erhalten.

Scannen beim Herunterladen vom Internet aktivieren

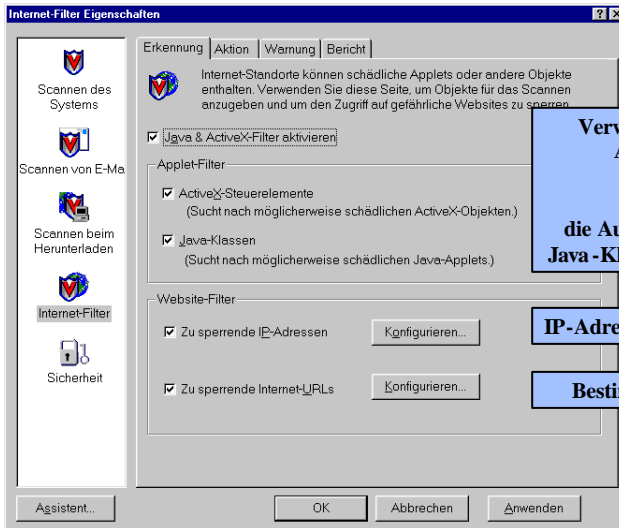
Zu scannende Elemente: Alle Dateien Nur Programmdateien Komprimierte Dateien scannen

Text:

- Scannen von Email und Attachments beim Herunterladen vom Mailserver
- Scannen von Dateien beim Herunterladen aus dem Internet



Internet-Filter



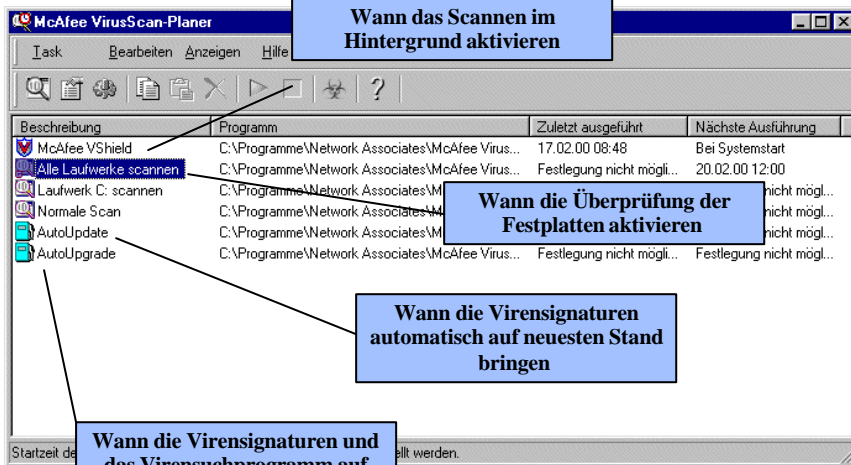
**Verwendung bestimmter
ActiveX-Klassen
und
die Ausführung bestimmter
Java -Klassen (Applets) sperren**

IP-Adressen und -Netze sperren

Bestimmte URL's sperren



McAfee Taskplaner



**Wann das Scannen im
Hintergrund aktivieren**

**Wann die Überprüfung der
Festplatten aktivieren**

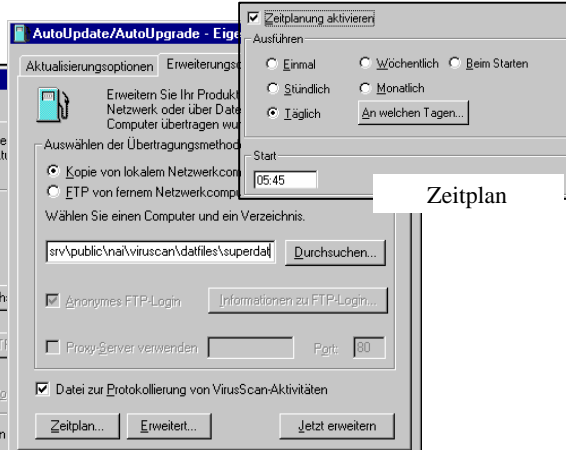
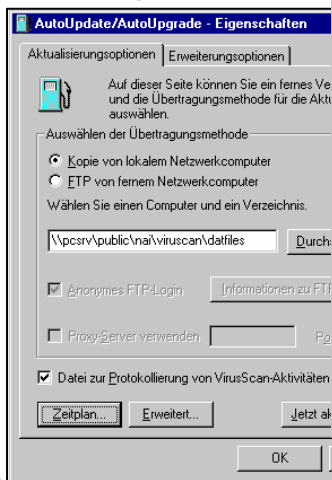
**Wann die Virensignaturen
automatisch auf neuesten Stand
bringen**

**Wann die Virensignaturen und
das Virensuchprogramm auf
den neuesten Stand bringen**



Automatische Aktualisierung im JuNet

Laden neuer Virenmuster
(Signaturen)



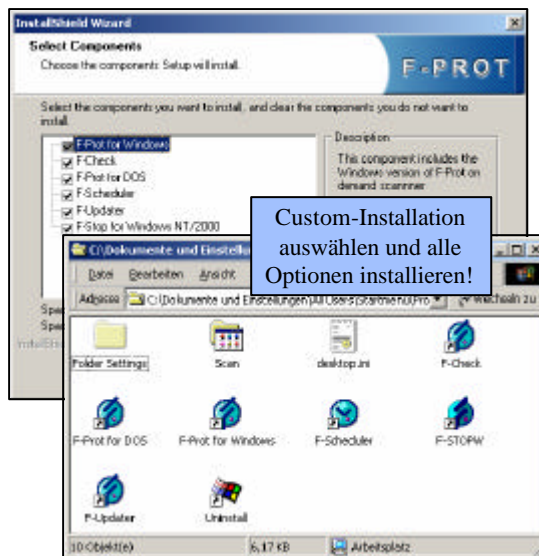
Zeitplan

Laden neuer Software und neuer
Virensignaturen



F-Prot für Windows und DOS

- F-Prot for Windows
 - Windows-Version des F-Prot „on demand“-Scanners
- F-Check
 - File Integrity Checker
- F-Prot for DOS
 - DOS-Version des F-Prot „on demand“-Scanners
(nicht für NTFS !)
- F-Scheduler
 - Zeitplaner zur automatischen Ausführung von F-Prot-Aktionen
- F-Stop for Windows
 - F-Prot „on access“-Scanner (Virenwächter)



Custom-Installation
auswählen und alle
Optionen installieren!



Minimaler Virenschutz beim Systemstart

F-Prot.exe für DOS (nicht für NTFS-Filesystem)

- Mit Texteditor Batch-Datei, z.B. C:\CLEANUP.BAT erstellen
- Link zu C:\CLEANUP.BAT im Autostart-Ordner erstellen
- Cleanup.bat:

```
@echo off
c:
cd \windows
if exist fff*_*.*.tmp del fffe*_*.*.tmp

rem *** F-Prot, nur Memory und Boot-Block
C:\Progra~1\FSI\F-Prot\f-prot.exe /BEEP /FREEZE /NOFILE C:

rem *** F-Prot, Windows-Directory
rem C:\Progra~1\FSI\F-Prot\f-prot.exe /BEEP /FREEZE /NOSUB C:\WINDOWS
@if not errorlevel 0 pause

rem *** McAfee VirusScan
rem C:\PROGRA~1\GEMEIN~1\NETWOR~1\VIRUSS~1\40~1.XX\scan.exe C:\
rem @IF ERRORLEVEL 1 PAUSE
```



Der Virenwächter F-StopW

- Alle Dateien
- Beim Erstellen und Download

- Zugriff verweigern

The image shows three screenshots of the F-STOPW Version 3.09A interface. The top screenshot shows the 'Properties' tab with options for what to do if a virus is found, such as 'Deny access', 'Rename automatically', 'Move automatically', 'Delete automatically', 'Disinfect automatically', and 'Report only'. The middle screenshot shows the 'What to scan' section with options for 'Program Files', 'Only macros', and 'All files', along with checkboxes for 'Inside archives', 'Compressed executables', 'Floppy boot sectors', and 'Heuristics'. The bottom screenshot shows the 'Log to file' section with a checkbox for 'Log to file' and a text field for the log file name, along with checkboxes for 'Append to log file', 'Virus infection', 'Virus disinfection', 'Delete', 'Move/Rename', 'User', 'Date and Time', 'Summary', and 'Settings'.

- Logging einschalten



F-Prot for Windows „on demand“-Scanner

- Scan-Optionen und Laufwerke können mit „Advanced“ ausgewählt und als (Default-) Profil abgespeichert werden (Default-Profil ist „HARDDISKS“)

Hinzufügen z.B. eines ZIP-Laufwerks
Unter „Settings“ noch Log-Datei und E-Mail-Adresse eintragen



F-Prot for DOS „on demand“-Scanner

- Der DOS-Scanner ist als Freeware auf dem PC-Server verfügbar
- Er benutzt die gleichen Virensignaturen wie der Windows-Scanner
- Er ist jedoch **nicht für das NTFS-Filesystem geeignet!**



Der Taskplaner F-Scheduler

- Festlegen des Scan-Profiles und des Zeitpunktes der Ausführung

• Scheduler beim Systemstart mitstarten!

Zuvor definiertes Default-Profil



Überprüfen der Systemintegrität mit F-Check

- Editieren der Datenbank und Hinzufügen von

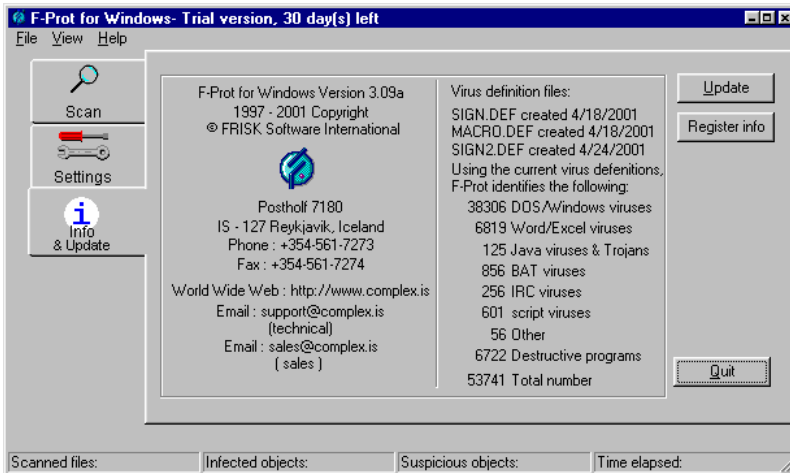
- Bootsektoren
- Ordnern
- Dateien

• Dateien auf Veränderungen prüfen und nach neuen Dateien suchen



Automatische Aktualisierung in F-Prot for Windows

- Anzeige des aktuellen Status und automatisches Update über Internet



Support im Forschungszentrum Jülich

- <http://www.fz-juelich.de/zam/net/security/infos/antiviren>
- Für das Forschungszentrum Jülich lizenzierte Software
- NAI Virus Scan (McAfee)
 - [\\pcsrv\public\NAI\viruscan](http://pcsrv/public/NAI/viruscan) und
 - <http://www.fz-juelich.de/zam/net/security/software/nai>
- F-Prot für Windows und DOS
 - [\\pcsrv\public\f-prot\zip](http://pcsrv/public/f-prot/zip) und
 - <http://www.fz-juelich.de/zam/net/security/software/f-prot>
 - fp-win_xxx.zip (Windows)
 - fpmimtt.zip (DOS)