



<http://bat-mail.de.vu>

◦ Gaijin's F-PROT PlugIn in TheBat! einbinden ◦

Diese Anleitung bezieht sich auf die Version 2.x von TheBat! – wenn das PlugIn unter TheBat! 1.6x eingebunden wird, ist der Vorgang bis auf die erweiterten Optionen der Anti-Virus Einstellungen und der etwas anderen Menüpunkte identisch.

Die aktuelle Version des »Gaijin's F-PROT PlugIns« bekommt ihr hier:

<http://www.gaijin.at/download/thebat/gfprotplugin.zip>

<http://bat-mail.de.vu/zip/gfprotplugin.zip>

Weiter Infos findet ihr auf der Homepage des Autors:



<http://www.gaijin.at/tbpgfp.shtml>

Voraussetzungen:

Das F-PROT-PlugIn setzt die Produktversion **F-PROT 3.14e** voraus, sollte eine ältere Version vorhanden sein muss diese aktualisiert werden. Die aktuelle F-PROT Version für DOS gibt es hier:

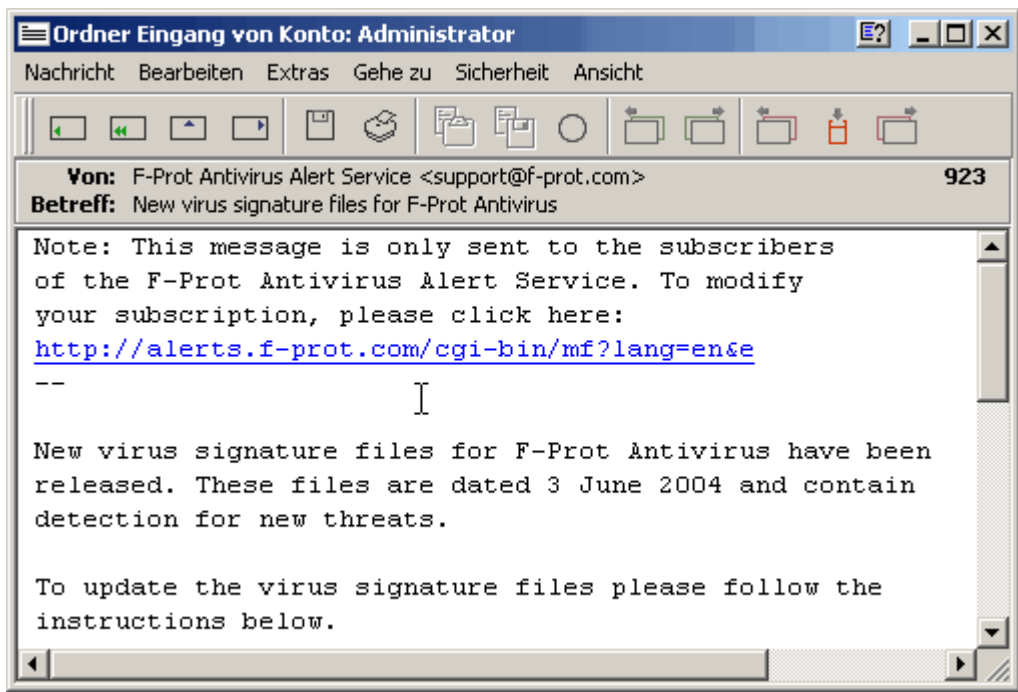


http://www.f-prot.com/download/download_fpdos.html

Um das Update zu automatisieren muss man sich zuerst beim »**F-PROT Antivirus Alert-Service**« anmelden um eine Benachrichtigungs-Mail zu bekommen, diese wird einem zugestellt sobald eine neue Virensignatur verfügbar ist.

Dies erfolgt über folgende Webseite: <http://alerts.f-prot.com/>

Nachdem man sich dort registriert hat, bekommt man nun bei Erscheinen einer neuen Virensignatur folgende Benachrichtigungs-Mail:

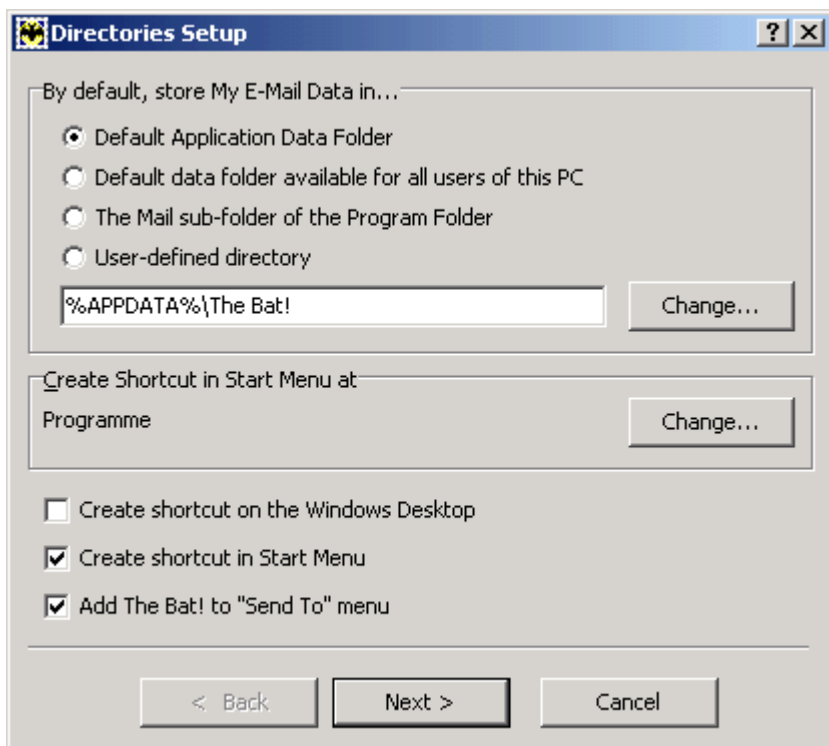


Das F-PROT PlugIn in das Arbeitsverzeichnis speichern

Ihr entpackt den Inhalt der Datei »gfpotplugin.zip« in das Arbeitsverzeichnis von TheBat!. Das Arbeitsverzeichnis ist jener Ordner, in dem TheBat! die allgemeinen Einstellungen speichert. Bei der Installation von TheBat! wurde man aufgefordert diesen Pfad anzugeben, dieser weicht auf den verschiedenen Betriebssystem etwas von einander ab z.B.:

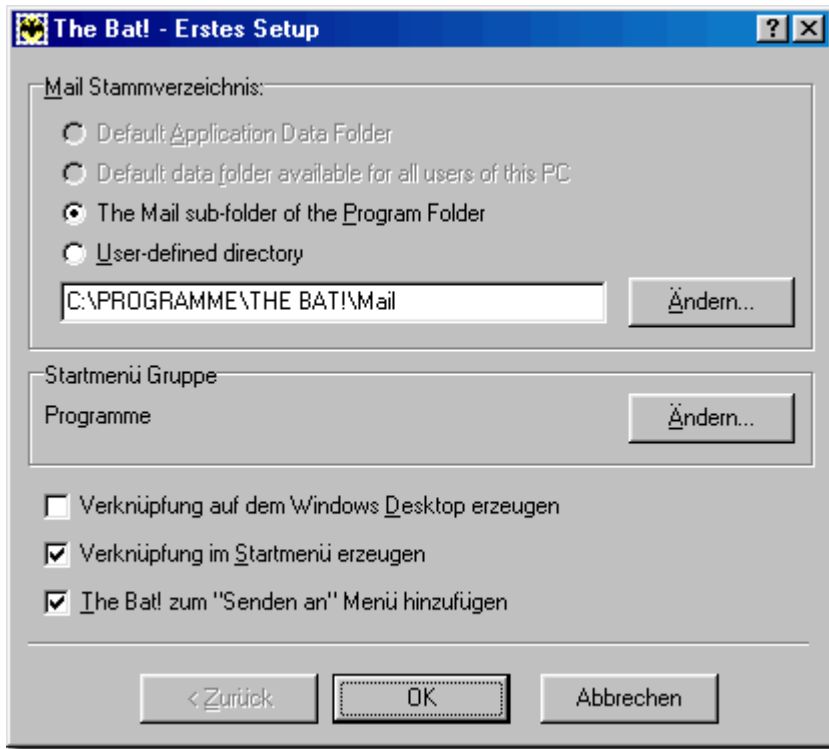
Unter Windows XP ist dies der Standard-Pfad:

C:\Dokumente und Einstellungen\[BENUTZERNAME]\Anwendungsdaten\The Bat!



Unter Windows 98/SE ist dies der Standard-Pfad:

C:\Programme\The Bat!\Mail



Die Update-Dateien integrieren

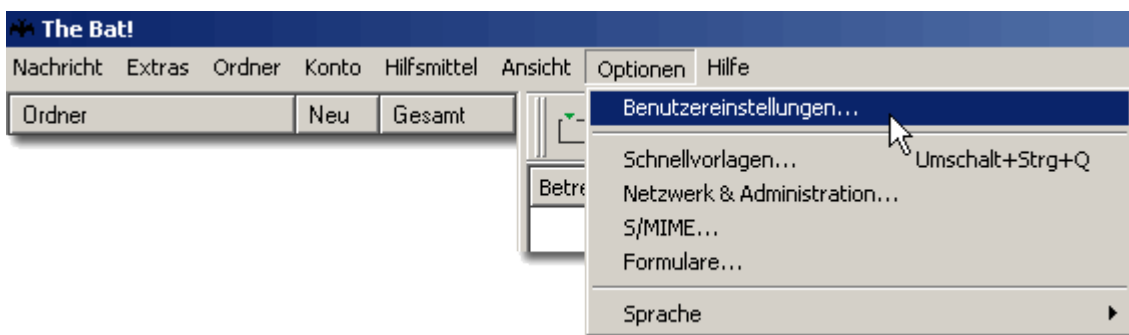
Die Dateien »**fprot-update.bat**«, »**WGET.exe**« und »**UNZIP.exe**« sollten nun auch in den gleichen Ordner gelegt werden in der auch die »f-prot.exe« liegt. Solltet ihr diese Dateien noch benötigen, findet ihr sie hier:

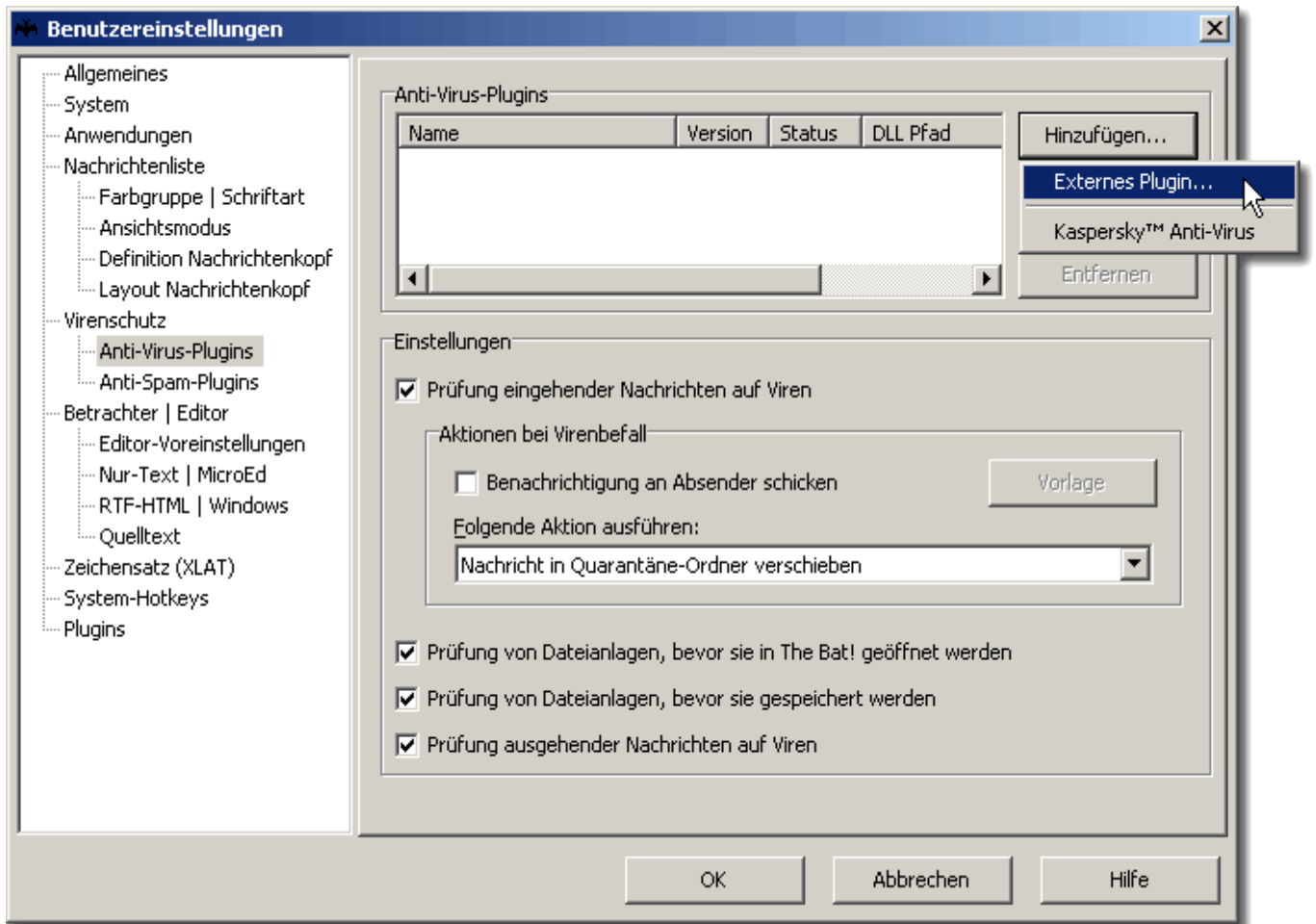
<http://bat-mail.de.vu/pdf/fprot-update.rar>

Das F-PROT Plugin in TheBat! einbinden

Nachdem das Plugin nun im Arbeitsverzeichnis von TheBat! auf dem Rechner gespeichert ist startet ihr TheBat!, und geht in der Menüleiste auf:

Optionen » Benutzereinstellungen » Virenschutz » Anti-Virus-Plugins

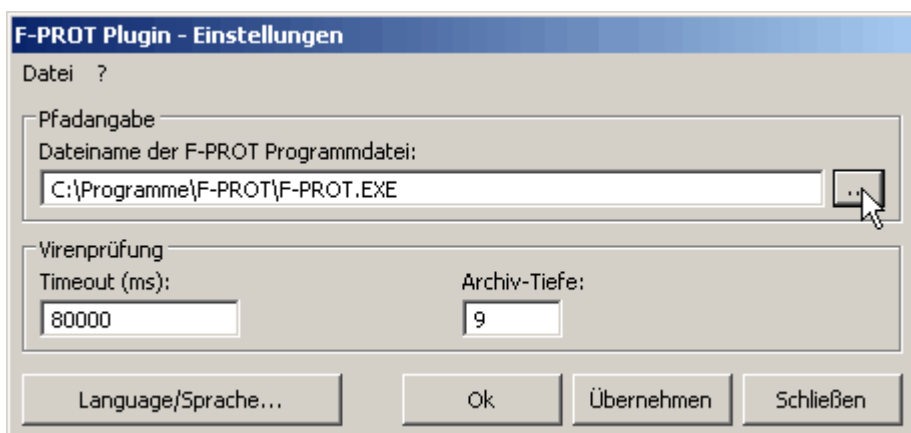




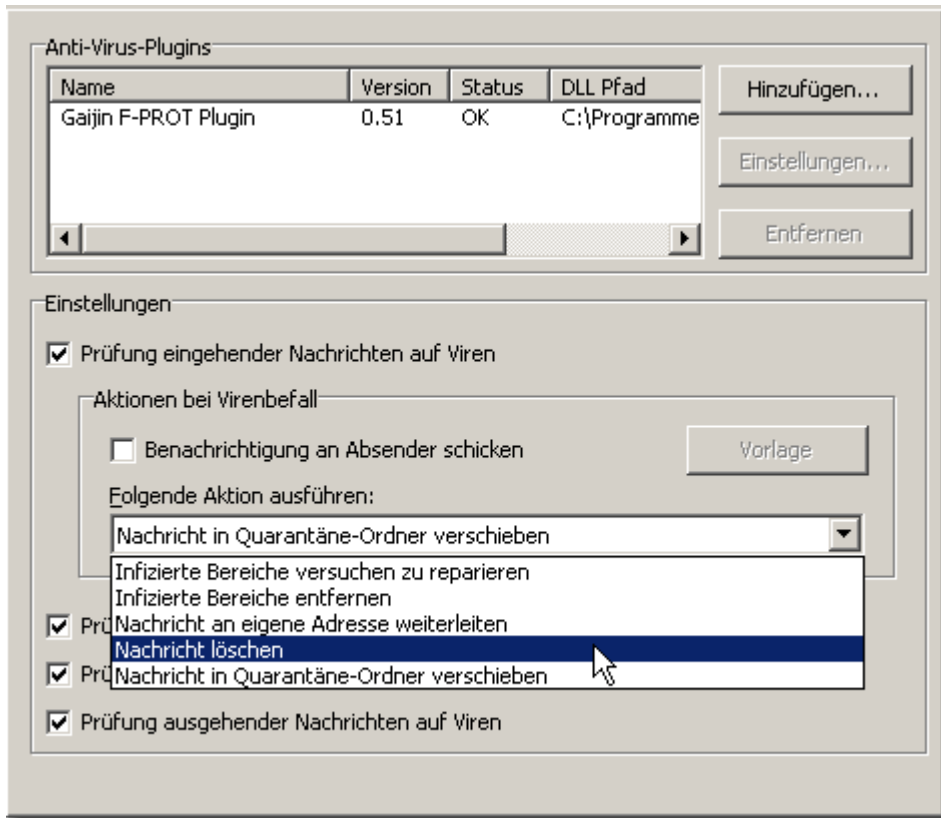
Über den Button »Hinzufügen« bindet ihr nun das F-PROT PlugIn ein, hier wählt ihr die Datei "gFProtPlugin.bav" aus und bestätigt mit »OK«. Jetzt öffnet sich das Einstellungsfenster - über den rechten Button navigiert man zur F-PROT.exe und bestätigt den Pfad.

Als »Timeout« sollte eine ausreichend lange Zeitspanne gewählt werden, z.B. 8000 Millisekunden. Dieser Wert bestimmt die maximale Laufzeit von F-PROT und ist nur dann relevant, wenn F-PROT abstürzen sollte.

Der Eintrag »Archiv-Tiefe« gibt die Tiefe der Ordnerstruktur an, in denen nach Viren gesucht werden soll.



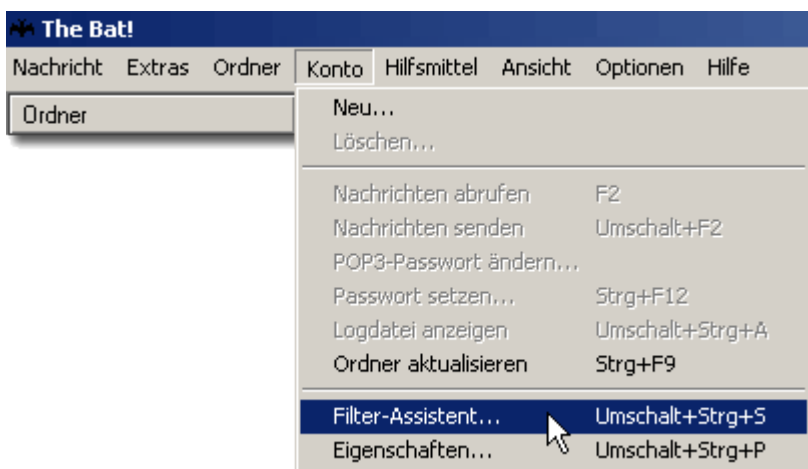
Jetzt müssen noch die Optionen in den Anti-Virus Einstellungen in TheBat! aktiviert werden.



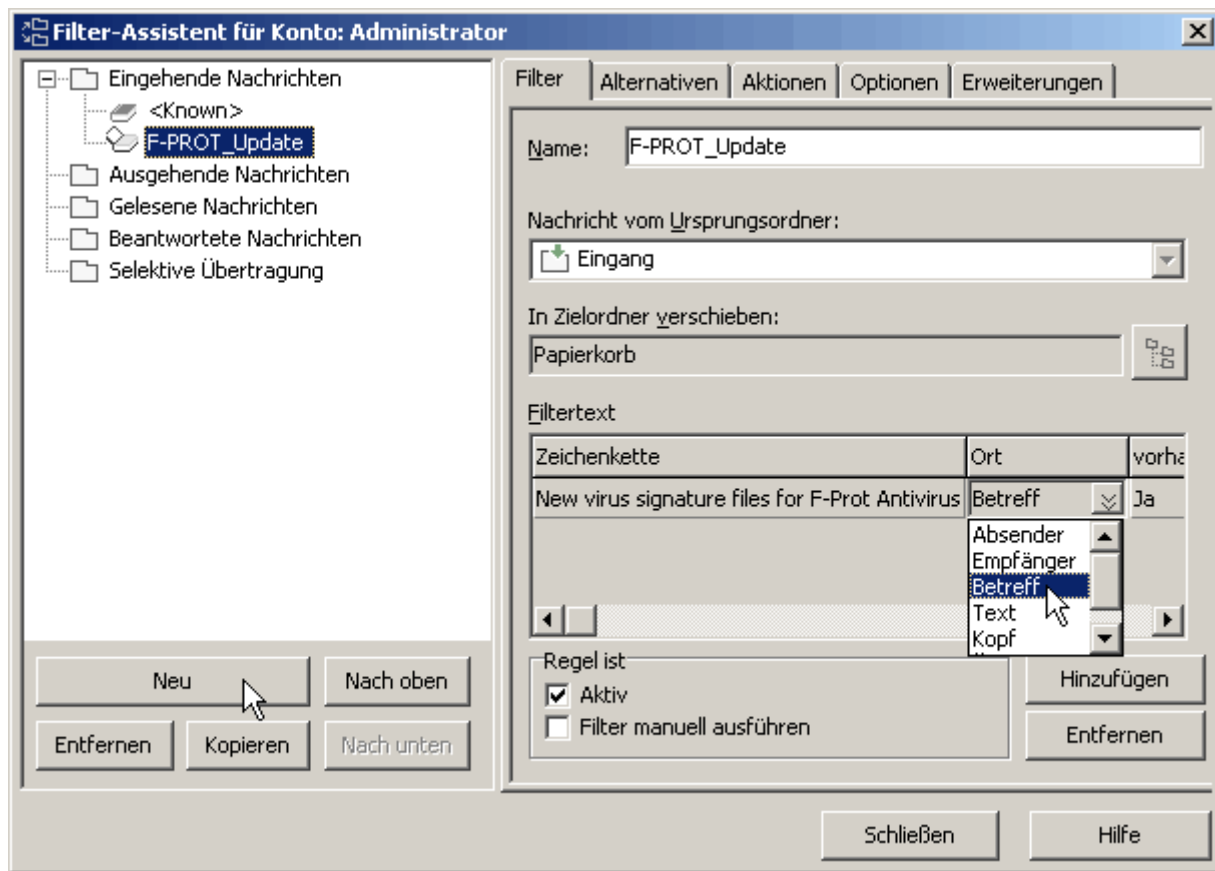
Filter für den Update in TheBat! erstellen

Zuvor muss allerdings ein Filter erstellt werden der bei Eintreffen der Benachrichtigungs-Mail automatisch das Update-Programm anstößt. Gehe hier wie folgt vor:

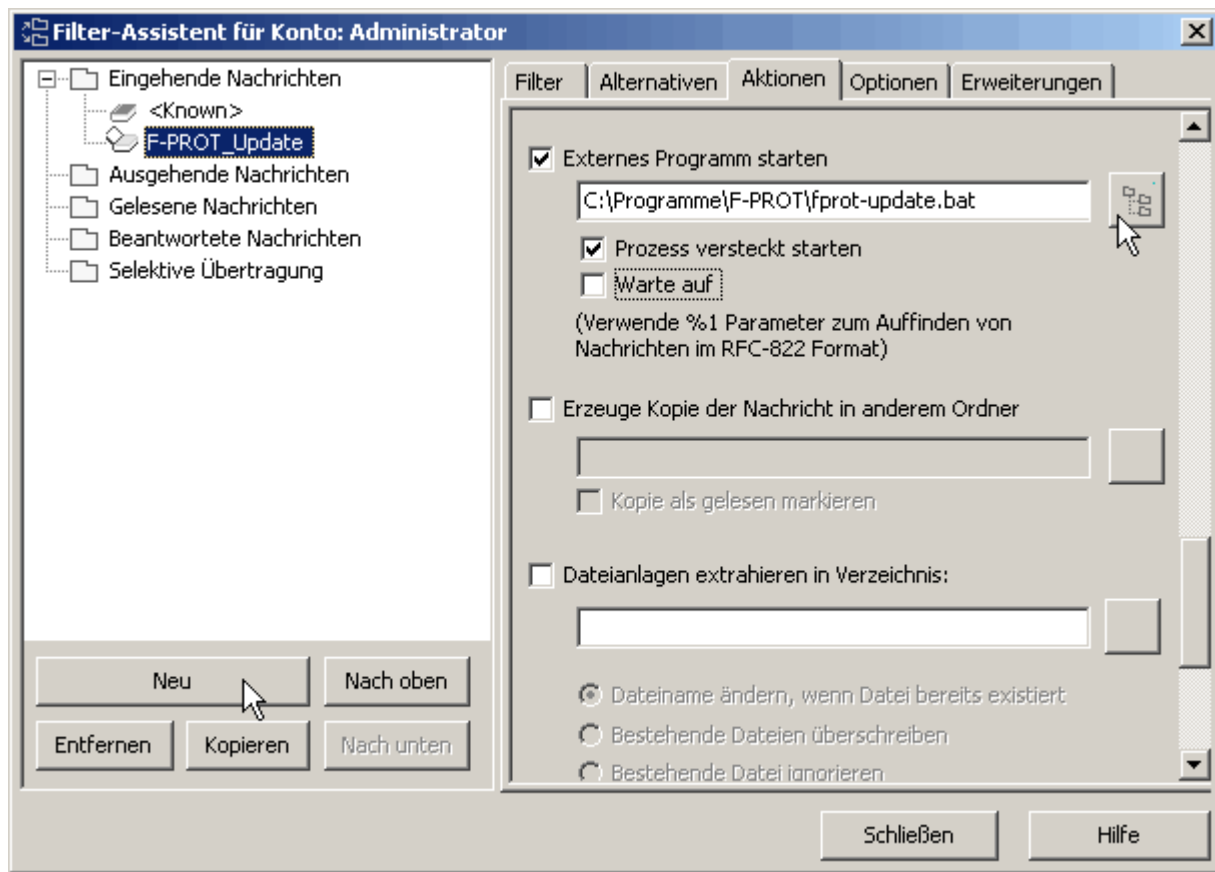
Rufe über die Menüleiste den Filter-Assistenten auf: Konto » Filter-Assistent



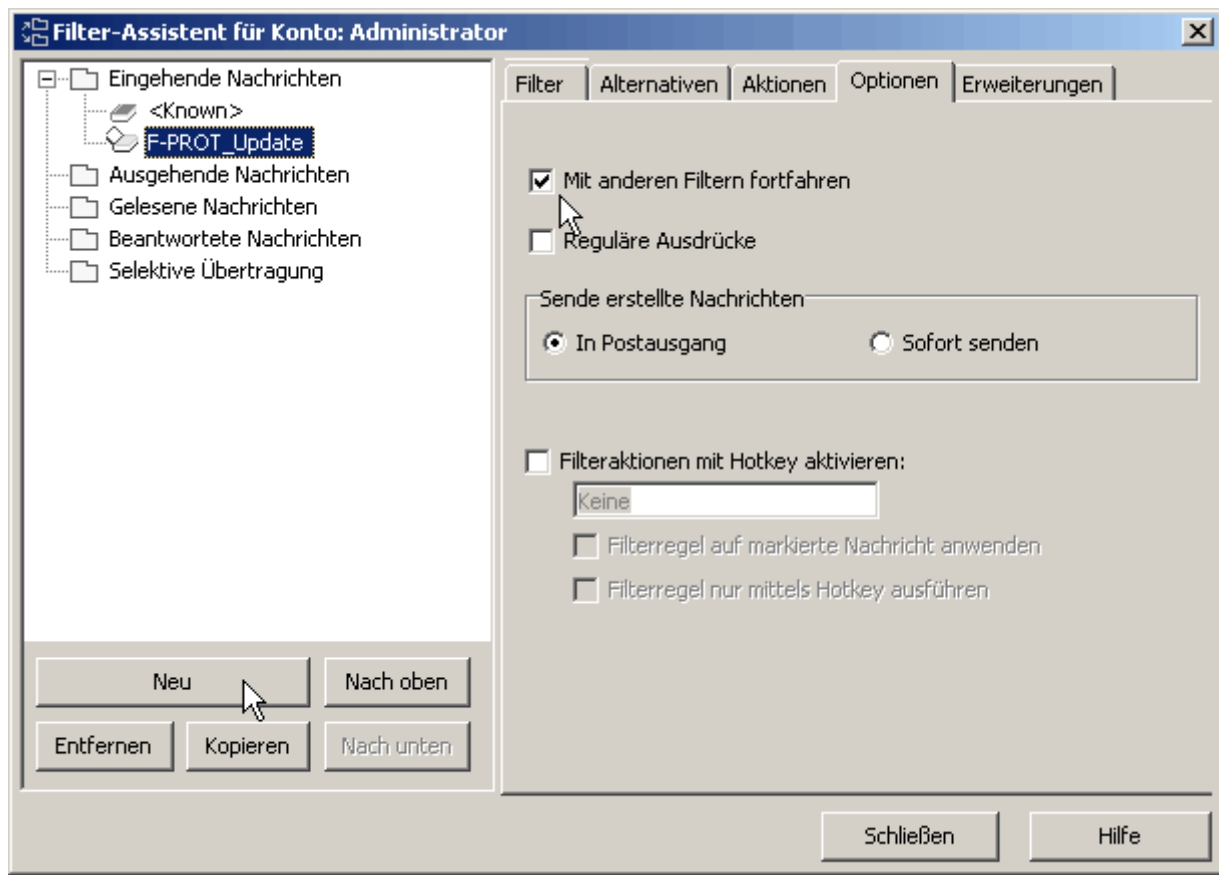
Jetzt erstellt man einen neuen Filter, benennt ihn beliebig und schreibt folgenden Betreff-Text unter das Feld Zeichenkette »New virus signature for F-Prot Antivirus« - unter »Ort« wählt man noch die Option »Betreff« aus.



Im Reiter »Aktionen« scrollt man so lange runter bis man zur Option »Externes Programm starten« kommt. Hier navigiert man zu der Datei »fprot-update.bat« - damit die Batch-Datei angezeigt wird, ändere den Dateityp nach dem du suchst auf 'Alle Dateien'.



Jetzt noch im Reiter »Optionen« den Punkt »Mit anderen Filtern fortfahren« aktivieren, somit ist der Filter fertiggestellt und der Filter-Assistent kann geschlossen werden.



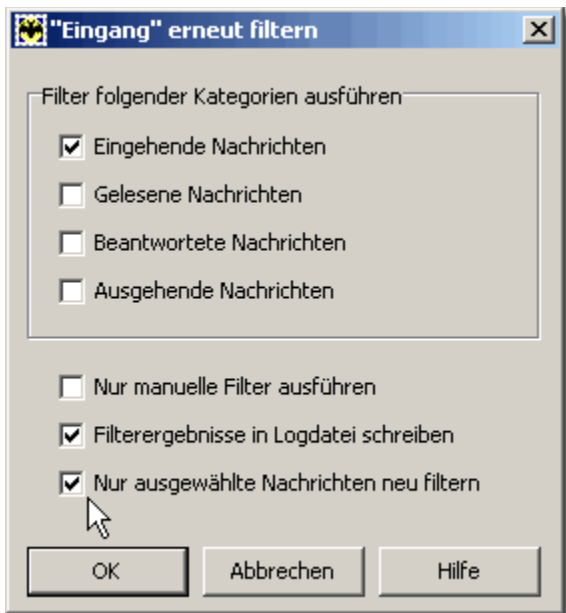
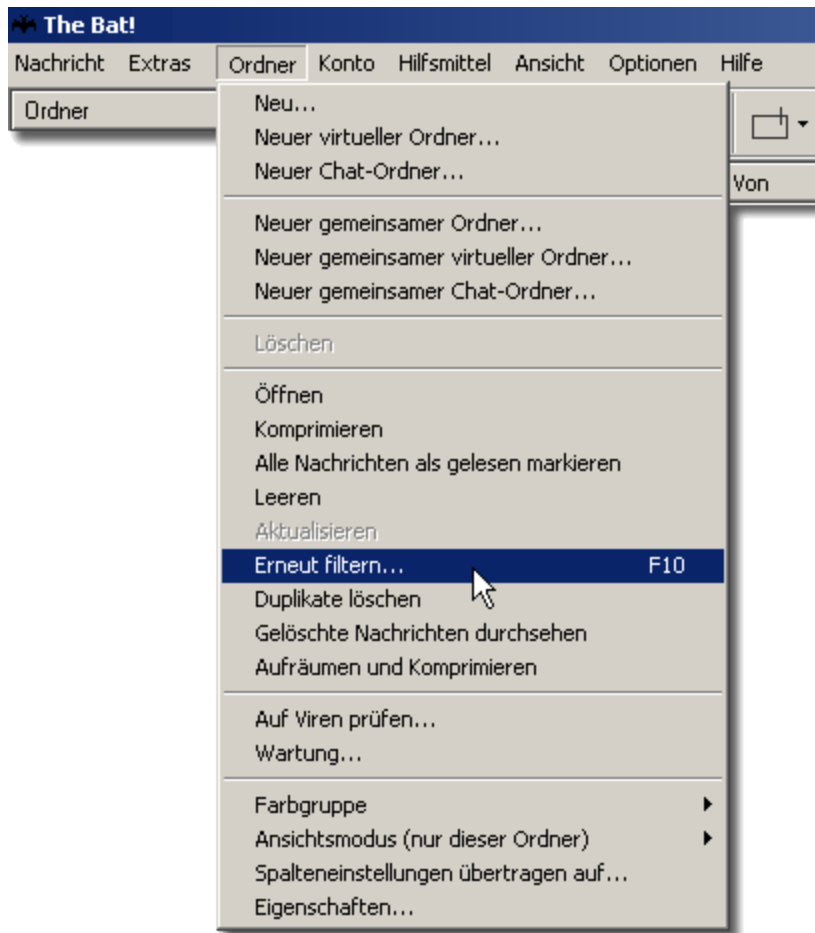
Sobald nun eine Benachrichtigungs-Mail im Eingangs-Ordner eintrifft, wird diese gefiltert, und bei Übereinstimmung des Betreffs wird die eingestellte Aktion ausgelöst. Da wir im Reiter »Aktionen« einen Haken bei »Prozess versteckt starten« gemacht haben, bekommt man von dem Update gar nichts mit. Diese Optionen kann nach persönlichen Bedürfnissen angepasst werden.

Filter für den F-PROT Update in TheBat! testen

Um den Filter zu testen erstellt ihr eine neue Dummy-Mail mit dem gleichen Betrefftext wie der vom Alert-Service »New virus signature for F-Prot Antivirus« und speichert sie im Postausgangs-Ordner.

Anschließend verschiebt ihr sie in den Eingangs-Ordner, markiert die Mail und ruft die Option »Erneut filtern« auf. Zusätzlich aktiviert ihr noch die Option »Nur ausgewählte Nachrichten neu filtern«, somit durchläuft nur die Testmail den Filter.



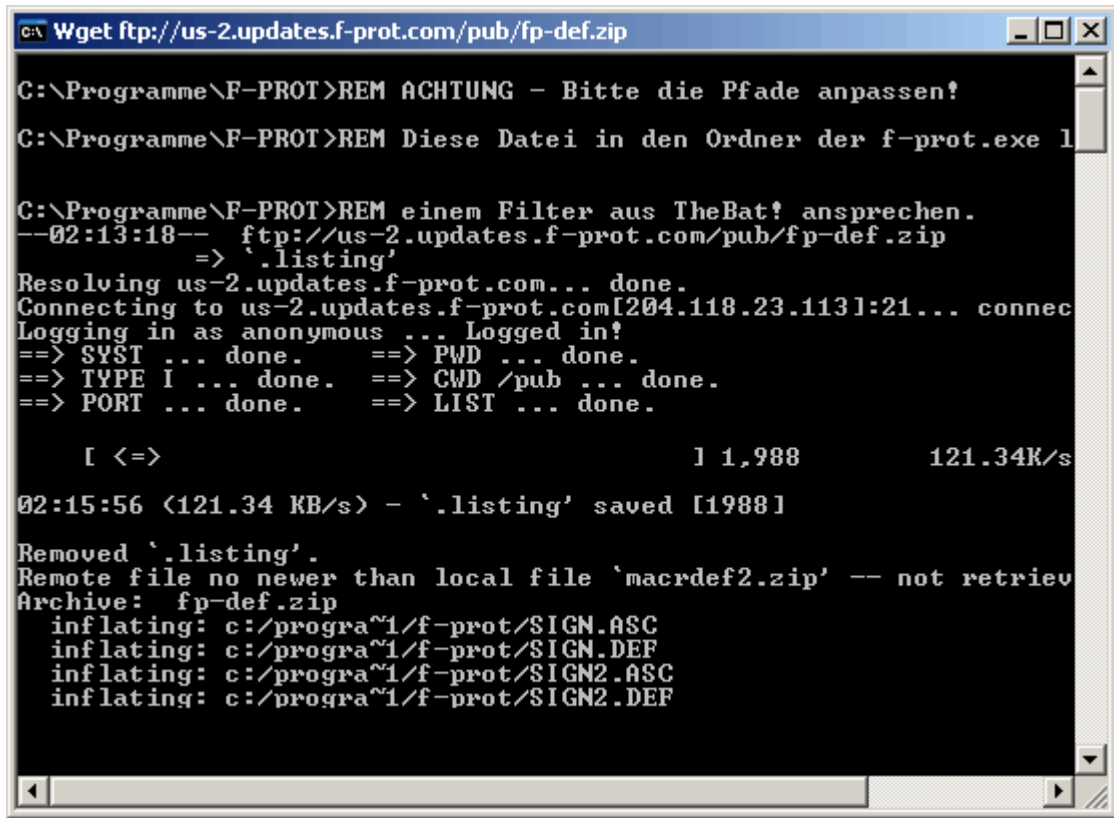


Um zu sehen ob der Update korrekt verläuft, sollte der Menüpunkt »Prozess versteckt starten« zum testen deaktiviert werde. (siehe voriger Abschnitt)

Update über die Batch-Datei »fprot-update.bat«

Jetzt sollte der Filter greifen und die Batch-Datei »fprot-update.bat« startet die Datei »WGET.exe«.

Es werden nun die beiden Signatur-Dateien »macrodef2.zip« und »fp-def.zip« auf ihr Datum geprüft. Sollten sie älter sein als die Dateien auf dem Server werden diese automatisch runter geladen, mit dem Programm »UNZIP.exe« entpackt, und die älteren Dateien ohne Nachfrage überschrieben.



```
c:\ Wget ftp://us-2.updates.f-prot.com/pub/fp-def.zip

C:\Programme\F-PROT>REM ACHTUNG - Bitte die Pfade anpassen!
C:\Programme\F-PROT>REM Diese Datei in den Ordner der f-prot.exe l

C:\Programme\F-PROT>REM einem Filter aus TheBat! ansprechen.
--02:13:18--  ftp://us-2.updates.f-prot.com/pub/fp-def.zip
=>  '.listing'
Resolving us-2.updates.f-prot.com... done.
Connecting to us-2.updates.f-prot.com[204.118.23.113]:21... connect
Logging in as anonymous ... Logged in!
==> SYST ... done.      ==> PWD ... done.
==> TYPE I ... done.   ==> CWD /pub ... done.
==> PORT ... done.    ==> LIST ... done.

[ <=>                               1 1,988           121.34K/s

02:15:56 (121.34 KB/s) - '.listing' saved [1988]

Removed '.listing'.
Remote file no newer than local file 'macrdef2.zip' -- not retriev
Archive:  fp-def.zip
  inflating: c:/progra~1/f-prot/SIGN.ASC
  inflating: c:/progra~1/f-prot/SIGN.DEF
  inflating: c:/progra~1/f-prot/SIGN2.ASC
  inflating: c:/progra~1/f-prot/SIGN2.DEF
```

Alternative kann der Update der Signatur-Dateien auch über das Tool »F-UPDATE« ausgeführt werden. Man erhält im Unterschied zu der Batch-Datei zusätzlich eine Log-Datei, in der jeder Update protokolliert wird.

Das Tool inklusive einer Anleitung findet ihr hier: <http://bat-mail.de.vu/zip/f-update.zip>

F-UPDATE.LOG

```
-----
06-01-2004 19:59:48 F-UPDATE program started.
06-01-2004 19:59:53 No new SIGN defs available.
06-01-2004 20:00:00 New MACRO def downloaded.
06-01-2004 20:00:00 Normal program exit. F-Prot version 314e
-----
```