

www.avira.de



Benutzerhandbuch

Avira AntiVir

Removal Tool für Windows

Warenzeichen

AntiVir ist ein registriertes Warenzeichen der Avira GmbH.

Windows ist ein registriertes Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern. Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer.

Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

Herausgeber

Avira GmbH
D-88069 Tett nang, Lindauer Str. 21
Telefon: +49 (0)7542 - 500 0
Telefax: +49 (0)7542 - 525 10
Email: info@avira.de
Internet: <http://www.avira.de>

Produktion

Avira GmbH
D-88069 Tett nang, Lindauer Str. 21

Copyright © 2006 Avira GmbH

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Alle Rechte vorbehalten. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira GmbH nicht gestattet. Irrtümer und technische Änderungen vorbehalten.

Ausgabe: September 2006

Inhaltsverzeichnis

1	Einleitung	4
2	Symbole und Hervorhebungen	5
3	Produktinformationen	6
	3.1 Leistungsumfang	7
	3.2 Systemvoraussetzungen	8
4	Bedienung	9
	4.1 Programm starten	9
	4.2 Programm beenden	10
	4.3 Suchlauf.....	10
	4.3.1 Suchlauf starten	10
	4.3.2 Suchlauf abbrechen	10
	4.4 Aufruf via Kommandozeile	11
	4.5 Kommandozeilenparameter.....	11
5	Berichte	12
	5.1 Suchergebnisse	12
	5.2 Meldungen	13
6	Goldene Regeln zur Virenvorsorge	14
7	Service	15
	7.1 Service-Hotline	15
	7.2 Online-Shop.....	15
	7.3 Kontaktadresse	15

1 Einleitung

Ein Antivirenprogramm steht und fällt mit der Aktualität der Virendefinitionen, auf die das Programm zugreifen kann. Avira bietet seinen Kunden deshalb mehrmals am Tag Aktualisierungen der Virendefinitionsdatei (VDF-Datei) an.


Es kommt jedoch immer wieder vor, dass Kunden diese Updates nicht oder nur in sehr unregelmäßigen Abständen durchführen. In solchen Fällen kann es dann zu ungewolltem Befall mit Viren und unerwünschten Programmen eines Computers kommen. Gehen Anwender ohne installiertes Antivirenprogramm ins Internet, dann ist diese Gefahr eines ungewollten Befalls mit Viren und unerwünschten Programmen noch sehr viel höher.

Ist es zu einem Befall gekommen, kann dieser in vielen Fällen nicht über die programminterne Entfernung- und Reparaturfunktionalität, sondern nur über ein separates Viren- und Malware Removal Tool wieder entfernt werden, das speziell auf ganz bestimmte Infizierungen zugeschnitten ist.

Ein solches spezifisches Viren- und Malware Removal Tool stellt AntiVir seinen Kunden und allen Betroffenen zur Verfügung.

Das AntiVir Removal Tool für Windows Version 3 ist in zwei Sprachversionen (Deutsch und Englisch) verfügbar:

 tool_de.com




 tool_en.com



Das AntiVir Removal Tool ist kein Ersatz für ein professionelles Antivirenprodukt. Um Ihr System zu schützen, sollten Sie unbedingt ein solches Sicherheitsprogramm installieren und in regelmäßigen Abständen - am besten täglich - aktualisieren.

2 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

Symbol	Erläuterung
	Steht vor einem Handlungsschritt, den Sie ausführen.
	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung des AntiVir Removal Tools erleichtert.

Folgende Hervorhebungen werden verwendet:

Hervorhebung	Erläuterung
<i>Kursiv</i>	Dateiname oder Pfadangabe.
Fett	Elemente der Software-Oberfläche, die angeklickt werden (z.B. Menüpunkt, Registerkarte oder Schaltfläche).

3 Produktinformationen

Das AntiVir Removal Tool behandelt eine Vielzahl von Viren und Malware. Eine aktuelle Übersicht, welche Malware mit Hilfe des AntiVir Removal Tools von Ihrem System entfernt werden kann, erhalten Sie auf der Avira Webseite unter <http://www.avira.de/removal-tool>.

Da das AntiVir Removal Tool in regelmäßigen Abständen aktualisiert wird, um Schutz vor aktuellen Bedrohungen zu liefern, empfehlen wir Ihnen, in regelmäßigen Abständen die Avira Webseite <http://www.avira.de> zu besuchen, um die aktuelle Version des AntiVir Removal Tools herunterzuladen.



Das AntiVir Removal Tool wird gefördert durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), <http://www.bsi.bund.de>.

3.1 Leistungsumfang

- **Reinigung des Systems**
Das AntiVir Removal Tool reinigt Ihr System von spezifischen Viren und Malware. Eine aktuelle Übersicht, welche Malware mit Hilfe des AntiVir Removal Tools von Ihrem System entfernt werden kann, erhalten Sie auf der Avira Webseite unter <http://www.avira.de/removal-tool>.
- **Reparatur von Dateien**
Das AntiVir Removal Tool repariert betroffene Dateien, sofern sie durch die Malware nicht irreparabel beschädigt wurden.
- **Beendigung von Malware-Prozessen**
Das AntiVir Removal Tool beendet alle aktiven von der Malware gestarteten Prozesse.
- **Malware-Hilfsdateien**
Das AntiVir Removal Tool identifiziert und entfernt Dateien, die von der Malware im Zuge der schädigenden Aktivitäten möglicherweise angelegt wurden.
- **Registerreinigung**
Das AntiVir Removal Tool entfernt die durch die Malware möglicherweise angelegten Registry Einträge und stellt die Standardwerte, sofern möglich, wieder her.

Zudem bietet das AntiVir Removal Tool folgende Eigenschaften:

- **Einfache Bedienung**
Sie laden das Programm herunter und starten es dann durch Doppelklick.
- **Ständige Transparenz**
Über die Benutzeroberfläche des AntiVir Removal Tools kann der Prüfvorgang verfolgt und der jeweilige Status der Überprüfung kontrolliert werden.
- **Anpassbare Durchführung**
Das Programm unterstützt Kommandozeilenparameter für zu prüfende Laufwerke, Protokolldateien und Hilfsinformationen.
- **Vollständige Berichte**
Die nach der Überprüfung ausgegebene Reportdatei gibt einen detaillierten Überblick über die erfolgte Überprüfung.

3.2 Systemvoraussetzungen

Das AntiVir Removal Tool unterstützt folgende Betriebssysteme:

- Microsoft Windows Server 2003
- Microsoft Windows XP Home oder Professional oder
- Microsoft Windows 2000 oder
- Microsoft Windows NT 4 oder
- Microsoft Windows Millennium Edition (kurz: Windows ME) oder
- Microsoft Windows 98 SE oder
- Microsoft Windows 98



Zur Benutzung des AntiVir Removal Tools müssen Sie über Administratorrechte verfügen, andernfalls gibt das Programm eine Fehlermeldung aus.



Nutzer der Betriebssysteme Windows 98, Windows 98 SE oder Windows ME benötigen zusätzlich "Microsoft Layer for Unicode". Die zusätzlich benötigte Datei ist im Microsoft Downloadcenter verfügbar.

4 Bedienung

Das AntiVir Removal Tool kann auf zwei verschiedene Arten gestartet werden:

- Standard
Start über Doppelklick. Alle Datenspeicher und Laufwerke werden gescannt. Es wird eine Protokolldatei erstellt.
- Kundenspezifisch
Start über Kommandozeile mit entsprechenden Parametern.

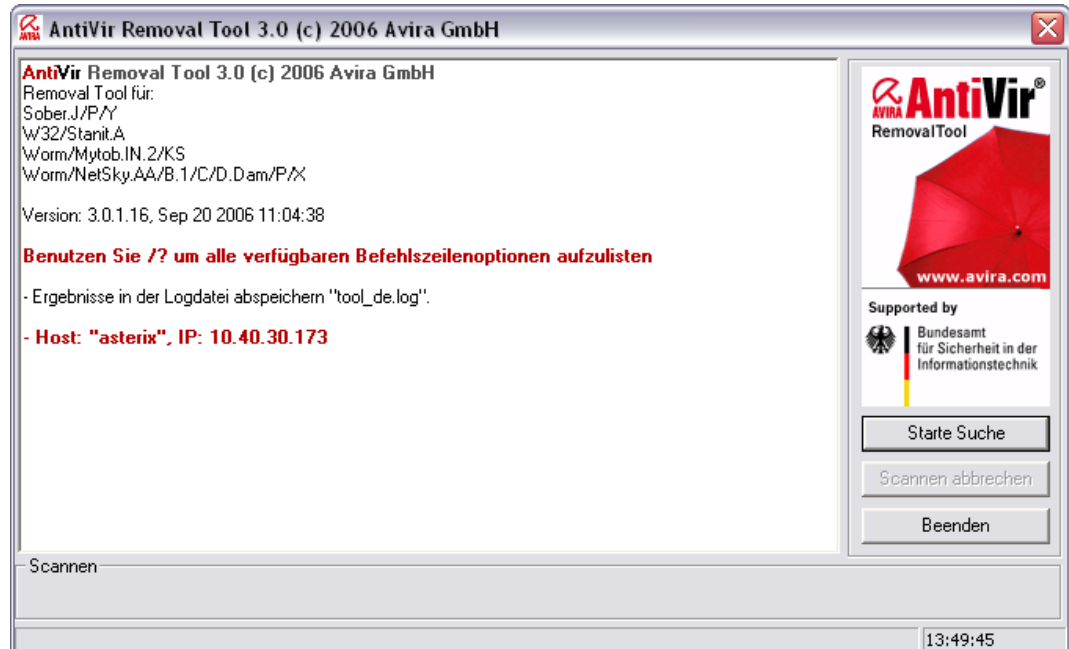
4.1 Programm starten

Das AntiVir Removal Tool muss nicht installiert werden. Nach dem Herunterladen können Sie es per Doppelklick starten und über die Benutzeroberfläche bedienen, um Ihr System von einem möglichen Befall zu reinigen.



Zur Benutzung des AntiVir Removal Tools müssen Sie über Administratorrechte verfügen, andernfalls gibt das Programm eine Fehlermeldung aus.

- ▶ Starten Sie das Programm mit einem Doppelklick auf *tool_de.com*.
↳ Der AntiVir Removal Tool Start-Bildschirm öffnet sich.



4.2 Programm beenden

- ▶ Wenn Sie das AntiVir Removal Tool beenden wollen, klicken Sie auf **Beenden**.
 - ↳ Das AntiVir Removal Tool wird beendet.



Die Datei *tool_de.log* ist die vorgegebene Logdatei in dem aktuellen Verzeichnis, in das die Suchergebnisse eingetragen werden.

4.3 Suchlauf

4.3.1 Suchlauf starten

- ▶ Um den Suchlauf zu starten, klicken Sie auf **Starte suche**.
 - ↳ Das Programm durchsucht alle Datenspeicher und Laufwerke.

Sie können den aktuellen Such-Status im Bereich am Bildschirm verfolgen.

```
Scannen des Speichers ... fertig  
Keine Malware im Speicher gefunden
```

```
Laufwerk scannen C: ...
```

4.3.2 Suchlauf abbrechen

- ▶ Wenn Sie den Suchlauf abbrechen wollen, klicken Sie auf **Scannen abbrechen**.
 - ↳ In die Protokolldatei (Logdatei) wird daraufhin die folgende Zeile eingetragen:

```
Scannen wurde vom Benutzer abgebrochen
```



Sie können den Suchlauf durch Klicken auf die Schaltfläche **Starte suche** jederzeit wieder aufnehmen. Aus Sicherheitsgründen wird der Suchlauf daraufhin erneut von Anfang an gestartet.

4.4 Aufruf via Kommandozeile

Wenn Sie das AntiVir Removal Tool mit anderen Einstellungen als den Standardeinstellungen starten wollen, können Sie das tun, indem Sie das Programm über die Kommandozeile starten.

Bitte verwenden Sie folgende Befehlssyntax:

```
TOOL_DE [pfad] /Optionen [Laufwerk: Laufwerk: ...]
```

Sie müssen den vollständigen Pfad zur Datei `tool_de.com` eingeben, wenn Sie das AntiVir Removal Tool aus einem anderen Verzeichnis heraus starten wollen.

Beispiel:

```
TOOL_DE /HELP
```

Das AntiVir Removal Tool wird gestartet und zeigt weitere Hilfsinformationen. Alternativ können Sie den Parameter `/?` benutzen.

4.5 Kommandozeilenparameter



Die Kommandozeilenparameter müssen für jeden Suchlauf neu eingegeben werden. Geschieht dies nicht, das durchsucht das AntiVir Removal Tool mit den Standardwerten.

```
/LOG <Dateiname>
```

Ändert den vorgegebenen Logdateinamen oder Pfad. Normalerweise trägt das AntiVir Removal Tool alle Prozessergebnisse in der Datei `tool_de.log` (die vorgegebene Protokolldatei im Toolverzeichnis) ein.

```
/NOLOG
```

Verhindert die Erstellung einer Logdatei.



Diesen Parameter können Sie nicht zusammen mit den Parametern `/LOG` oder `/APPEND` einsetzen.

```
/APPEND
```

Fügt Informationen einer bestehenden Logdatei hinzu, anstatt eine neue Logdatei zu erstellen.

```
/HELP (oder /?)
```

Zeigt Hilfsinformationen auf dem Bildschirm an.

5 Berichte

Das AntiVir Removal Tool ist in der Lage, eine Logdatei mit detaillierten Ergebnissen und Meldungen über den Scanprozess und die durchgeführten Reparatur- und Wiederherstellungsoperationen zu erstellen. Dieselben Informationen werden auch auf dem Bildschirm direkt angezeigt.

5.1 Suchergebnisse

Nach Beendigung oder Abbruch des Programms werden die Ergebnisse der Prüfung auf dem Bildschirm angezeigt. Diese Zusammenfassung enthält Angaben über die Anzahl der durchsuchten, betroffenen, reparierten oder beendeten Dateien und Prozesse, die abgelaufene Zeit und den Datendurchsatz des Scanners.

Beispiel:

Scanergebnisse:

Durchsuchte Verzeichnisse:	2533
Durchsuchte Dateien :	27110
Durchsuchte Datenströme:	1
Durchsuchte Prozesse:	38
Durchsuchte Module:	388
Infizierte Dateien:	6
Infizierte Prozesse:	0
Reparierte/entfernte Dateien:	6
Umbenennen der Dateien:	2
Beendete Prozesse:	0
Benötigte Zeit für Speicherscan:	1.41 Sekunden
Durchsatz des Speicherscanners:	94344.95 KB/s
Benötigte Zeit für Dateiscannen:	172.84 Sekunden
Durchsatz des Dateiscanners:	326.81 KB/s

5.2 Meldungen

Der Report gliedert sich in verschiedene Informationsblöcke. Zunächst werden Versionsdetails und die eingegebenen Parameter aufgelistet.

Dann folgen eventuelle Fehlermeldungen, z.B. über ungültige Parameter, die eingegeben wurden.

Zum Beispiel:

Fehler: Logdateiname enthält ungültige Zeichen.

Erkennt das AntiVir Removal Tool Malware auf Ihrem System, trägt es alle durchgeführten Aktionen zur Entfernung bzw. zur Reinigung und Wiederherstellung des Systems in die Logdatei ein:

```
Malware gefunden in der Datei ...;  
Ausführbares Programm entfernen ... fertig;  
Registry Keys reinigen ... fertig;  
Malware erfolgreich entfernt.
```



Fortgeschrittene Anwender können das Programmskript nach Prozessergebniscodes abfragen.

Rückgabewerte:

< 0 : Fehler beim Scannen.

= 0 : Keine Fehler aufgetreten und keine Malware gefunden.

> 0 : Malware gefunden.

6 Goldene Regeln zur Virenvorsorge

- Erstellen Sie Notfalldisketten/ Startdisketten für Ihre Windows-Version sowie Ihren Netzwerkserver und die einzelnen Workstations.
- Notfalldisketten sind auch bei anderen Betriebssystemen hilfreich.
- Nehmen Sie Disketten nach Beenden Ihrer Arbeit immer aus dem Laufwerk heraus. Auch Disketten ohne ausführbare Programme enthalten Programmcode im Bootsektor und können Träger eines Bootsektorvirus sein.
- Fertigen Sie regelmäßig vollständige Backups Ihrer Daten an.
- Begrenzen Sie den Programmaustausch: Das gilt besonders für Netzwerk, Mailboxen, Internet und gute Bekannte.
- Prüfen Sie neue Programme vor und nach einer Installation. Liegt das Programm auf einem Datenträger komprimiert vor, lässt sich ein Virus bzw. ein unerwünschtes Programm in der Regel erst nach dem Auspacken bei der Installation finden.

Haben andere Personen einen Zugang zu Ihrem Rechner, sollten Sie folgende Spielregeln zum Schutz vor Viren beachten:

- Stellen Sie einen Computer als Testrechner zur Eingangskontrolle neuer Software, Demoversionen oder evtl. virenverdächtiger Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerk-Medien) und von Downloads bereit. Trennen Sie diesen Rechner aber vom Netzwerk!
- Benennen Sie einen Datenschutzbeauftragten, der bei einem Befall mit Viren und unerwünschten Programmen für die Behandlung verantwortlich ist, und bestimmen Sie im Voraus alle zu einer Beseitigung eines Virus bzw. unerwünschten Programms notwendigen Schritte.
- Organisieren Sie vorsorglich einen durchführbaren Notfallplan: Dieser kann die Schäden durch mutwillige Zerstörung, Raub, Ausfall oder Zerstörungen/Veränderungen aufgrund von Inkompatibilitäten vermindern helfen. Programme und Massenspeicher lassen sich ersetzen; Daten, die für ein wirtschaftliches Überleben notwendig sind, nicht.
- Stellen Sie vorsorglich einen durchführbaren Schutz- und Wiederaufbauplan für Ihre Daten auf.
- Sorgen Sie für ein ordentlich installiertes Netzwerk, bei dem die Rechtevergabe vorbeugend eingesetzt wird.

7 Service

7.1 Service-Hotline

Auf unserer Webseite <http://www.avira.de/de/support> erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service. Die Experten beantworten Ihre Fragen und helfen bei technischen Problemen weiter.

7.2 Online-Shop

Sie wollen unsere Produkte bequem per Mausklick einkaufen?

Im Online-Shop der Avira GmbH können Sie unter <http://www.avira.de/de/onlineshop> schnell und sicher Lizenzen erwerben, verlängern oder erweitern. Der Online-Shop führt Sie Schritt für Schritt durch das Bestell-Menü. Ein multilinguales Customer Care Center informiert Sie über Bestellprozesse, Zahlungsabwicklungen und Auslieferung. Wiederverkäufer können auf Rechnung bestellen.

7.3 Kontaktadresse

Gerne helfen wir Ihnen weiter, wenn Sie Fragen und Anregungen zur Produktwelt von Avira haben. Falls Sie allgemeine Produktinformationen oder sonstige Auskünfte benötigen, können Sie sich an folgende Adresse wenden.

Allgemeine Informationen zu uns und unseren Produkten erhalten Sie auch auf unserer Webseite <http://www.avira.de>.

Avira GmbH

Lindauer Str. 21
D-88069 Tettnang

Telefon: +49 (0)7542 - 500 0
Telefax: +49 (0)7542 - 525 10

Email: info@avira.de
Internet: <http://www.avira.de>

www.avira.de



Avira GmbH

Lindauer Str. 21
D-88069 Tettnang
Telefon: +49 (0) 7542-500 0
Telefax: +49 (0) 7542-525 10
Email: info@avira.de
Internet: <http://www.avira.de>

Alle Rechte vorbehalten. Änderungen vorbehalten.
© Avira GmbH

MEHR ALS SICHERHEIT

