



Handbuch für Anwender



Avira AntiVir für KEN!

www.avira.de

Warenzeichen und Copyright

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.

Hinweise zum Copyright

Für Avira AntiVir für KEN! wurde Code von Drittanbietern verwendet. Wir bedanken uns bei den Copyright-Inhabern dafür, dass sie uns ihren Code zur Verfügung gestellt haben. Detaillierte Informationen zum Copyright finden Sie in der Hilfe von Avira AntiVir für KEN! unter Third Party Licenses.

Inhaltsverzeichnis

1	Einleitung	5
2	Symbole und Hervorhebungen	6
3	Produktinformationen	7
	3.1 Leistungsumfang	7
	3.2 Systemvoraussetzungen	8
	3.3 Lizenzierung	9
4	Installation und Deinstallation	10
	4.1 Installation	10
	4.2 Änderungsinstallation	13
	4.3 Installationsmodule	13
	4.4 Deinstallation	14
5	AntiVir für KEN! im Überblick	15
	5.1 Oberfläche und Bedienung	15
	5.1.1 Benutzeroberfläche und Bedienung	15
	5.1.2 Control Center	15
	5.1.3 Konfiguration	18
	5.1.4 Tray Icon	20
	5.2 So wird es gemacht	21
	5.2.1 Avira AntiVir für KEN! automatisiert aktualisieren	21
	5.2.2 Ein Update manuell starten	22
	5.2.3 Direktsuche: Mit einem Suchprofil nach Viren und Malware suchen	23
	5.2.4 Direktsuche: Per Drag&Drop nach Viren und Malware suchen	24
	5.2.5 Direktsuche: Über das Kontextmenü nach Viren und Malware suchen	24
	5.2.6 Direktsuche: Automatisiert nach Viren und Malware suchen	25
	5.2.7 Direktsuche: Gezielt nach aktiven Rootkits suchen	26
	5.2.8 Auf gefundene Viren und Malware reagieren	26
	5.2.9 Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen	28
	5.2.10 Quarantäne: Dateien in der Quarantäne wiederherstellen	29
	5.2.11 Quarantäne: Verdächtige Datei in die Quarantäne verschieben	30
	5.2.12 Suchprofil: Dateityp in einem Suchprofil ergänzen oder löschen	30
	5.2.13 Suchprofil: Desktop-Verknüpfung für Suchprofil erstellen	31
	5.2.14 Ereignisse: Ereignisse filtern	31
6	Scanner	33
7	Updates	34
8	FAQ, Tipps	35
	8.1 Hilfe im Problemfall	35
	8.2 Häufig gestellte Fragen (FAQ)	37
	8.3 Tastaturbefehle	40
	8.3.1 In Dialogfeldern	40
	8.3.2 In der Hilfe	41
	8.3.3 Im Control Center	41
	8.4 Windows Sicherheitscenter	43
	8.4.1 Allgemeines	43
	8.4.2 Das Windows Sicherheitscenter und Avira AntiVir für KEN!	43

9	Viren und mehr	46
9.1	Erweiterte Gefahrenkategorien	46
9.2	Viren sowie sonstige Malware.....	49
10	Info und Service	53
10.1	Kontaktadresse	53
10.2	Technischer Support.....	53
10.3	Verdächtige Datei.....	54
10.4	Fehlalarm melden	54
10.5	Ihr Feedback für mehr Sicherheit	54
11	Referenz: Konfigurationsoptionen.....	55
11.1	Scanner.....	55
11.1.1	Suche.....	55
11.1.1.1	Aktion bei Fund	57
11.1.1.2	Weitere Aktionen	60
11.1.1.3	Archiv-Liste	61
11.1.1.4	Ausnahmen	61
11.1.1.5	Heuristik.....	63
11.1.2	Report	64
11.2	Guard.....	65
11.2.1	Suche.....	65
11.2.1.1	Aktion bei Fund	67
11.2.1.2	Weitere Aktionen	70
11.2.1.3	Ausnahmen	70
11.2.1.4	Heuristik.....	73
11.2.2	Report	74
11.3	Allgemeines.....	75
11.3.1	Email.....	75
11.3.2	Erweiterte Gefahrenkategorien.....	76
11.3.3	Kennwort.....	77
11.3.4	Sicherheit.....	79
11.3.5	Verzeichnisse.....	80
11.3.6	Update	80
11.3.6.1	Webserver.....	81
11.3.7	Warnungen.....	83
11.3.7.1	Netzwerk	83
11.3.7.2	Email.....	86
11.3.8	Ereignisse	87
11.3.9	Berichte begrenzen	87

1 Einleitung

Die Avira AntiVir für KEN! der Avira GmbH schützt Ihren Computer vor Viren, Malware, Ad- und Spyware, unerwünschten Programmen und sonstigen Gefahren. Verkürzend wird in diesem Handbuch von Viren und Malware gesprochen.

Das Handbuch beschreibt die Installation und Bedienung des Programms.

Auf unserer Webseite <http://www.avira.de> können Sie das Handbuch zu Avira AntiVir für KEN! als PDF herunterladen, Avira AntiVir für KEN! aktualisieren oder Ihre Lizenz erneuern.



Zudem finden Sie auf unserer Webseite Informationen wie beispielsweise die Telefonnummer des Technischen Supports sowie unseren Newsletter, den Sie dort abonnieren können.

Avira AntiVir für KEN! wurde in enger Zusammenarbeit mit der AVM Computersysteme GmbH speziell für KEN! entwickelt. Auf der Webseite <http://www.avm.de> finden Sie weiterführende Informationen zur Softwarelösung KEN!.

Ihr Team von Avira GmbH

2 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

Symbol	Erläuterung
✓	Steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss.
▶	Steht vor einem Handlungsschritt, den Sie ausführen.
→	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
	Steht vor einer Warnung bei Gefahr von kritischem Datenverlust.
	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung von Avira AntiVir für KEN! erleichtert.

Folgende Hervorhebungen werden verwendet:

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

3 Produktinformationen

In diesem Kapitel erhalten Sie alle für den Erwerb und Einsatz von Avira AntiVir für KEN! relevanten Informationen:

- siehe Kapitel: Leistungsumfang
- siehe Kapitel: Systemvoraussetzungen
- siehe Kapitel: Lizenzierung

Avira AntiVir für KEN! ist ein umfassendes und flexibles Werkzeug, um Ihren Computer zuverlässig vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren zu schützen.

► Beachten Sie folgende Hinweise:

**Hinweis**

Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen. Fertigen Sie regelmäßig Sicherungskopien (Backups) Ihrer Daten an.

**Hinweis**

Ein Programm, das vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren schützt, ist nur dann zuverlässig und wirksam, wenn es aktuell ist. Stellen Sie die Aktualität von Avira AntiVir für KEN! über automatische Updates sicher. Konfigurieren Sie das Programm entsprechend.

3.1 Leistungsumfang

Avira AntiVir für KEN! bietet Ihnen folgende Funktionen:

- Integriert und verfügbar ab AVM KEN! 4
- Sicherer Schutz vor Viren, Würmern, Trojanern sowie Ad- und Spyware
- Residenter Virenwächter (On-Access-Scanner) zur permanenten Überwachung
- Konfigurierbare Suche nach unterschiedlichen „Malware“-Typen bzw. nach unerwünschten Programmen
- Überprüfung gebräuchlicher Archiv-Typen
- Definierbare Auspacktiefe bei verschachtelten Archiven
- Entfernung bzw. Reparatur vireninfizierter Programme und Dateien
- Umbenennen von betroffenen Dateien
- Heuristische Erkennung von Makroviren (Avira AntiVir AHeAD Technologie)
- Isolation infizierter/verdächtiger Dateien
- Integritätskontrolle der Dateien
- Einfache, halbautomatische Installation
- Vollautomatisches, tägliches Online-Update zentral über den KEN! Service-PC
- Unterstützung der Konfiguration durch kontextsensitive Hilfe bzw. Skripte
- Kennwortgeschützte Konfiguration

- Umfassende Protokoll-, Warn und Benachrichtigungsfunktionen
- Warnmeldungen über das Netzwerk

3.2 Systemvoraussetzungen

Damit Avira AntiVir für KEN! einwandfrei läuft, muss das Computersystem folgende Voraussetzungen erfüllen:

- Computer ab Pentium, mindestens 266 MHz
- Betriebssystem:
 - Microsoft Windows Vista (32 oder 64 Bit) oder
 - Microsoft Windows XP Home oder Professional, SP2 empfohlen oder
 - Microsoft Windows 2000, SP 4 empfohlen
 - Windows 2000 Server
 - Windows Server 2003



Hinweis

Avira AntiVir für KEN! unterstützt auch die Microsoft Windows XP x64 Edition und 64 Bit Microsoft Windows Vista.

- Mindestens 192 MB Arbeitsspeicher unter Windows 2000/XP
- Mindestens 512 MB Arbeitsspeicher unter Windows Vista, Windows 2000 Server oder Windows Server 2003
- 30 MB freier Speicherplatz auf der Festplatte (bei Verwendung der Quarantäne mehr)
- 100 MB temporärer Speicherplatz auf der Festplatte
- Für die Installation von Avira AntiVir für KEN!: Administrator-Rechte

Hinweise für die Benutzer von Windows Vista

Unter Windows 2000 und Windows XP arbeiten viele Benutzer mit Administratorrechten. Dies ist unter Sicherheitsaspekten jedoch nicht wünschenswert, denn so haben auch Viren und unerwünschte Programme leichtes Spiel, sich im Computer einzunisten.

Aus diesem Grund führt Microsoft mit Windows Vista die "Benutzerkontosteuerung" (User Account Control) ein. Diese bietet mehr Schutz für Anwender, die als Administrator angemeldet sind: So verfügt bei Windows Vista ein Administrator zunächst nur über die Privilegien eines normalen Benutzers. Aktionen, für die Administratorrechte erforderlich sind, markiert Windows Vista klar mit einem Hinweis-Icon. Zudem muss der Anwender die gewünschte Aktion explizit bestätigen. Erst, nachdem diese Zustimmung eingeholt ist, findet eine Erhöhung der Privilegien statt, und das Betriebssystem führt die jeweilige administrative Aufgabe aus.

Avira AntiVir für KEN! benötigt für einige Aktionen unter Windows Vista Administratorrechte. Diese Aktionen werden mit folgendem Zeichen gekennzeichnet:



. Erscheint dieses Zeichen zusätzlich auf einer Schaltfläche, so werden zum Ausführen dieser Aktion Administratorrechte benötigt. Besitzt Ihr aktuelles Benutzerkonto keine Administratorrechte, so fordert Sie der Windows Vista Dialog zur Benutzerkontensteuerung zur Eingabe des Administratorkennworts auf. Verfügen Sie über kein Administratorkennwort, so können Sie diese Aktion nicht ausführen.

3.3 Lizenzierung

Um Avira AntiVir für KEN! nutzen zu können, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen von Avira AntiVir für KEN! an.

Die Lizenz wird über einen digitalen Lizenzschlüssel in Form der Datei hbedv.key vergeben. Dieser digitale Lizenzschlüssel ist die Schaltzentrale Ihrer persönlichen Lizenz. Er enthält genaue Angaben, welche Programme Sie für welchen Zeitraum lizenziert haben. Ein digitaler Lizenzschlüssel kann also auch die Lizenz für mehrere Produkte enthalten.

Der digitale Lizenzschlüssel wird Ihnen in einer Email übermittelt, falls Sie AntiVir für KEN! im Internet erworben haben, oder befindet sich auf der Programm-CD/DVD von Avira AntiVir für KEN!.

Bei der Installation von KEN! wird Avira AntiVir für KEN! zusammen mit einer Testlizenz automatisch mitinstalliert. Innerhalb des KEN! Service-PC ist es jederzeit möglich, eine Lizenzdatei zu erwerben oder zu verlängern. Die Lizenzdatei wird auf dem Ken! Service PC geladen und automatisch an die verbundenen Clients verteilt.

4 Installation und Deinstallation

In diesem Kapitel erhalten Sie Informationen rund um die Installation und Deinstallation Ihrer Avira AntiVir für KEN!:

- siehe Kapitel Installation: Voraussetzungen, Installationsarten, Installation durchführen
- siehe Kapitel Installationsmodule
- siehe Kapitel Änderungsinstallation
- siehe Kapitel Deinstallation: Deinstallation durchführen

4.1 Installation

Überprüfen Sie vor der Installation von Avira AntiVir für KEN!, dass Ihr Computer die Mindestsystemanforderungen erfüllt. Falls Ihr Computer alle Voraussetzungen erfüllt, können Sie Avira AntiVir für KEN! installieren.



Hinweis

Ab Windows XP erzeugt Avira AntiVir für KEN! einen Wiederherstellungspunkt Ihres Computers vor der Installation von Avira AntiVir für KEN!. Dies ermöglicht Ihnen bei einer fehlgeschlagenen Installation Avira AntiVir für KEN! sicher zu entfernen. Beachten Sie, dass hierfür die Option **Systemwiederherstellung deaktivieren** unter: "Start | Einstellungen | Systemsteuerung | System | Registerkarte Systemwiederherstellung" nicht markiert sein darf. Möchten Sie Ihren Computer zu einem früheren Zeitpunkt wiederherstellen, können Sie dies über die Funktion "Start | Programme | Zubehör | Systemprogramme | Systemwiederherstellung" tun. Den von Avira AntiVir für KEN! erzeugten Wiederherstellungspunkt erkennen Sie am Eintrag AntiVir für KEN!.

Installationsarten

Während der Installation können Sie im Installationsassistenten einen Setup-Typ wählen:

Vollständig

AntiVir für KEN! wird vollständig mit allen Programmkomponenten installiert. Die Programmdateien werden in ein vorgegebenes Standardverzeichnis unter C:\Programme installiert.

Benutzerdefiniert

Sie haben die Möglichkeit, einzelne Programmkomponenten zur Installation auszuwählen (siehe Kapitel Installation und Deinstallation::Installationsmodule). Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden. Sie können das Erstellen eines Desktop-Icons und einer Programmgruppe im Startmenü deaktivieren und vorab eine Einstellung für die Win32 Dateiheuristik vornehmen.

Vor dem Start des Installationsvorgangs

- ▶ Schließen Sie Ihr Email-Programm. Es wird außerdem empfohlen, alle laufenden Anwendungen zu beenden.
- ▶ Vergewissern Sie sich, dass keine weiteren Virenschutzlösungen installiert sind. Die automatischen Schutzfunktionen verschiedener Sicherheitslösungen können sich gegenseitig behindern.

Installation durchführen

Das Installationsprogramm funktioniert im selbsterklärenden Dialogmodus. Jedes Fenster enthält eine bestimmte Auswahl von Schaltflächen zur Steuerung des Installationsprozesses.

Die wichtigsten Schaltflächen sind mit folgenden Funktionen belegt:

- **OK:** Aktion bestätigen.
- **Abbrechen:** Aktion abbrechen.
- **Weiter:** Zum nächsten Schritt übergehen.
- **Zurück:** Zum vorangegangenen Schritt übergehen.

So installieren Sie AntiVir für KEN!:



Hinweis

Avira AntiVir für KEN! ist eine speziell für KEN! entwickelte Virenschutz-Lösung. Bei der Installation von KEN! wird Avira AntiVir für KEN! zusammen mit einer Testlizenz automatisch mitinstalliert.

Auf den KEN! Klienten wird die Installation von Avira AntiVir für KEN! automatisch gestartet, sobald auf dem KEN! Service-PC die Option für den Avira AntiVir für KEN! Klienten aktiviert und eine Aktualisierung der Virendefinitionsdatei erfolgt ist.

Verfahren Sie nach dem automatischen Start der Installation weiter wie folgt:

- ▶ Klicken Sie auf **Annehmen**.
 - ↳ Das Setup-Programm für Avira AntiVir für KEN! startet.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Willkommen...* erscheint.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Erweiterte Gefahrenkategorien* mit Informationen zum Basis- und darüber hinausgehenden Schutz erscheint.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster mit der Lizenzvereinbarung erscheint.
- ▶ Bestätigen Sie, dass Sie die Lizenzvereinbarung akzeptieren und klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Installationsart wählen* erscheint.
- ▶ Entscheiden Sie sich, ob Sie eine vollständige oder eine benutzerdefinierte Installation durchführen wollen.
- ▶ Aktivieren Sie die Option **Vollständig** oder **Benutzerdefiniert** und bestätigen Sie mit **Weiter**.

Benutzerdefinierte Installation

- ↳ Das Dialogfenster *Zielverzeichnis wählen* erscheint.
- ▶ Bestätigen Sie das angegebene Zielverzeichnis mit **Weiter**.
 - ODER -
 - Wählen Sie mit **Durchsuchen** ein anderes Zielverzeichnis und bestätigen Sie mit **Weiter**.
- ↳ Das Dialogfenster *Komponenten installieren* erscheint:
- ▶ Aktivieren oder deaktivieren Sie die gewünschten Komponenten und bestätigen Sie mit **Weiter**.
 - ↳ Im folgenden Dialogfenster können Sie festlegen, ob die Win32 Dateiheuristik aktiviert werden soll.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Im folgenden Dialogfenster können Sie festlegen, ob eine Verknüpfung auf Ihrem Desktop und/oder eine Programmgruppe im Startmenü erstellt werden soll.
- ▶ Klicken Sie auf **Weiter**.

Fortsetzung für vollständige und benutzerdefinierte Installation

- ↳ Die Programmkomponenten werden installiert und gestartet.
- ↳ Das Setup-Programm fragt, ob die Datei *readme.txt* mit aktuellen Informationen zu Avira AntiVir für KEN! angezeigt werden soll.
- ▶ Stimmen Sie ggf. zu und klicken Sie auf **Fertig stellen**.
- ▶ Bestätigen Sie den Hinweis mit **OK**.

Weiterer Ablauf (je nach Betriebssystem mit geringfügigen Unterschieden):

- ↳ Das Setup-Programm schließt die Installation ab und legt ggf. eine Verknüpfung auf dem Desktop an.
- ↳ Die Datei *readme.txt* wird ggf. angezeigt.
- ↳ Sie werden gefragt, ob Sie ein Update durchführen wollen.



Hinweis

Nur die neueste Version von Avira AntiVir für KEN! kann Sie zuverlässig vor ständig neu in Umlauf gebrachten Viren und anderer Malware schützen. Führen Sie sofort nach der Installation ein Update durch. Nach diesem ersten Update meldet das Windows Sicherheitscenter (XP und Vista) Avira AntiVir für KEN! als AKTIV.

- ODER -

- ↳ Sie werden gefragt, ob der Computer neu gestartet werden soll.

Wenn Sie ein Update durchführen wollen:

- ▶ Bestätigen Sie mit **Ja**.
 - ↳ Über die bestehende Webserver Verbindung wird nach einem Update von Avira AntiVir für KEN! gesucht.
 - ↳ Avira AntiVir für KEN! startet dann automatisch mit einem Suchlauf über die Windows Systemverzeichnisse.

**Hinweis**

Der erste Suchlauf ist besonders wichtig, um sicherzustellen, dass Ihr System frei von Viren und Malware ist. Brechen Sie den ersten Suchlauf nicht ab.

Wenn Sie den Computer neu starten wollen:

- ▶ Bestätigen Sie mit **Ja**.
- ↳ Der Computer wird neu gestartet.

4.2 Änderungsinstallation

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Avira AntiVir für KEN! Installation hinzuzufügen oder zu entfernen (siehe Kapitel Installation und Deinstallation::Installationsmodule)

Wenn Sie Programmkomponenten der aktuellen Avira AntiVir für KEN! Installation hinzufügen oder entfernen möchten, können Sie die Option **Software** zum **Ändern/Entfernen** von Programmen in der **Windows-Systemsteuerung** verwenden.

Wählen Sie Avira AntiVir für KEN! und klicken Sie auf **Ändern**. Im Willkommen-Dialog der Avira AntiVir für KEN! wählen Sie die Option **Programm ändern**. Sie werden durch die Änderungsinstallation geführt.

4.3 Installationsmodule

Bei einer benutzerdefinierten Installation oder einer Änderungsinstallation können folgende Module zur Installation ausgewählt oder hinzugefügt bzw. entfernt werden:

- **AntiVir für KEN!**
Dieses Modul beinhaltet alle Komponenten, die für eine erfolgreiche Installation von Avira AntiVir für KEN! benötigt werden.
- **AntiVir Guard**
Der AntiVir Guard läuft im Hintergrund. Er überwacht und repariert, falls nötig, Dateien bei Operationen wie Öffnen, Schreiben und Kopieren in Echtzeit (On-Access = bei Zugriff). Führt ein Benutzer eine Dateioperation durch (Datei laden, ausführen, kopieren), durchsucht Avira AntiVir für KEN! automatisch die Datei. Bei der Dateioperation Umbenennen wird keine Suche des AntiVir Guard ausgeführt.
- **AntiVir Rootkit-Schutz**
Der AntiVir Rootkit-Schutz prüft, ob sich auf Ihrem Computer bereits Software installiert hat, die nach dem Einbruch in das Computersystem mit den herkömmlichen Methoden der Malware-Erkennung nicht gefunden werden kann.
- **Shell Extension**
Die Avira AntiVir für KEN! Shell Extension erzeugen im Kontextmenü des Windows Explorers (rechte Maustaste) einen Eintrag Ausgewählte Dateien mit AntiVir überprüfen. Mit diesem Eintrag können Sie einzelne Dateien oder Verzeichnisse direkt scannen.

4.4 Deinstallation

Wenn Sie Avira AntiVir für KEN! von Ihrem Computer entfernen möchten, können Sie die Option **Software** zum **Ändern/Entfernen** von Programmen in der Windows-Systemsteuerung verwenden.

So deinstallieren Sie Avira AntiVir für KEN! (beschrieben am Beispiel von Windows XP und Windows Vista):

- ▶ Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.
- ▶ Doppelklicken Sie auf **Software** (Windows Vista: **Programme**).
- ▶ Wählen Sie **Avira AntiVir für KEN!** und klicken Sie auf **Entfernen**.
 - ↳ Sie werden gefragt, ob Sie das Programm tatsächlich entfernen wollen.
- ▶ Bestätigen Sie mit **Ja**.
 - ↳ Alle Komponenten des Programms werden entfernt.
- ▶ Klicken Sie auf **Fertig stellen**, um die Deinstallation abzuschließen.
 - ↳ Ggf. erscheint ein Dialogfenster mit der Empfehlung, Ihren Computer neu zu starten.
- ▶ Bestätigen Sie mit **Ja**.
 - ↳ Avira AntiVir für KEN! ist deinstalliert, Ihr Computer wird bei Bedarf neu gestartet, dabei werden alle Verzeichnisse, Dateien und Registry-Einträge von Avira AntiVir für KEN! gelöscht.

5 AntiVir für KEN! im Überblick

In diesem Kapitel erhalten Sie einen Überblick über die Funktionalitäten und die Bedienung von AntiVir für KEN!.

- siehe Kapitel: Oberfläche und Bedienung
- siehe Kapitel: So wird es gemacht

5.1 Oberfläche und Bedienung

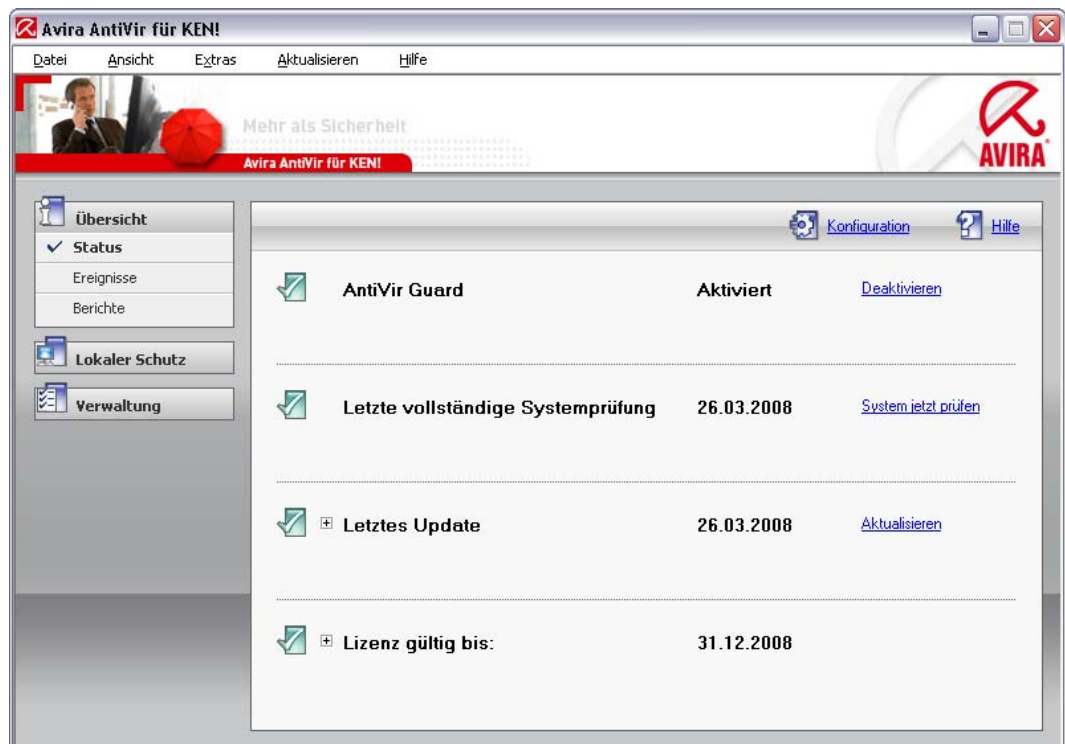
5.1.1 Benutzeroberfläche und Bedienung

Sie bedienen AntiVir für KEN! über drei Oberflächenelemente des Programms:

- Control Center: Überwachung und Steuerung von AntiVir für KEN!
- Avira AntiVir für KEN! Konfiguration: Konfiguration von AntiVir für KEN!
- Tray Icon im Systemtray der Taskleiste: Öffnen des Control Center und weitere Funktionen

5.1.2 Control Center

Das Control Center dient zur Überwachung des Schutzstatus Ihres Computersystems und zur Steuerung und Bedienung der Schutzkomponenten und Funktionen von AntiVir für KEN!.



Das Fenster von Control Center gliedert sich in drei Bereiche: Die **Menüleiste**, die **Navigationsleiste** und das Detailfenster **Ansicht**:

- **Menüleiste:** In den Menüs von Control Center können Sie allgemeine Programmfunktionen aufrufen und Informationen zu AntiVir für KEN! abrufen.

- **Navigationsbereich:** Im Navigationsbereich können Sie einfach zwischen den einzelnen Rubriken des Control Center wechseln. Die einzelnen Rubriken enthalten Informationen und Funktionen der Programmkomponenten von AntiVir für KEN! und sind in der Navigationsleiste nach Aufgabenbereichen angeordnet. Beispiel: Aufgabenbereich *Übersicht* - Rubrik **Status**.
- **Ansicht:** In diesem Fenster wird die Rubrik angezeigt, die im Navigationsbereich ausgewählt wurde. Je nach Rubrik finden Sie in der oberen Leiste des Detailfensters Schaltflächen zur Ausführung von Funktionen bzw. Aktionen. In einzelnen Rubriken werden Daten oder Datenobjekte in Listen angezeigt. Sie können die Listen sortieren, indem Sie auf das Feld klicken, nach dem Sie die Liste sortieren möchten.

Starten und beenden von Control Center

Sie haben folgende Möglichkeiten Control Center zu starten:

- Mit Doppelklick auf das Programm-Icon auf Ihrem Desktop
- Über den Programm-Eintrag von AntiVir für KEN! im Menü Start | Programme.
- Über das Avira AntiVir für KEN! Tray Icon.

Sie beenden Control Center über den Menübefehl **Beenden** im Menü **Datei** oder, indem Sie auf das Schließen-Kreuz im Control Center klicken.

Control Center bedienen

So navigieren Sie im Control Center

- ▶ Wählen Sie in der Navigationsleiste einen Aufgabenbereich an.
 - ↳ Der Aufgabenbereich öffnet sich und es erscheinen weitere Rubriken. Die erste Rubrik des Aufgabenbereichs ist ausgewählt und wird in der Ansicht angezeigt.
- ▶ Klicken Sie ggf. eine andere Rubrik an, um diese im Detailfenster anzuzeigen.
 - ODER -
- ▶ Wählen Sie eine Rubrik über das Menü *Ansicht* aus.



Hinweis

Die Tastaturnavigation in der Menüleiste aktivieren Sie mit Hilfe der [Alt]-Taste. Ist die Navigation aktiviert, können Sie sich mit den Pfeiltasten innerhalb des Menüs bewegen. Mit der Return-Taste aktivieren Sie den aktuell markierten Menüpunkt.

So bearbeiten Sie Daten oder Objekte, die im Detailfenster angezeigt werden:

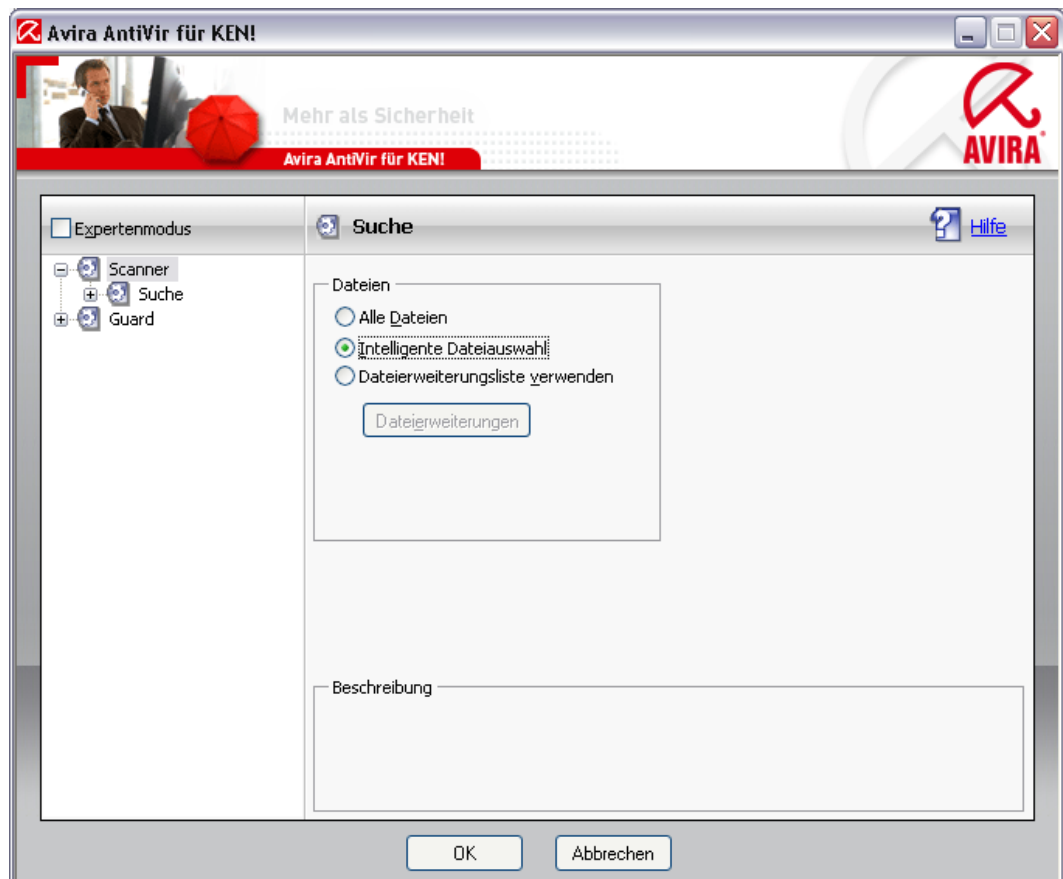
- ▶ Markieren Sie die Daten oder Objekte, die Sie bearbeiten möchten.
 - Um mehrere Elemente zu markieren, halten Sie die Strg-Taste oder die Shift-Taste (Auswahl untereinander stehender Elemente) gedrückt, während Sie die Elemente auswählen.
- ▶ Klicken Sie auf die gewünschte Schaltfläche in der oberen Leiste des Detailfensters, um das Objekt zu bearbeiten.

Control Center im Überblick

- **Übersicht:** Unter **Übersicht** finden Sie alle Rubriken, mit denen Sie die Funktionsfähigkeit von Avira AntiVir für KEN! überwachen können.
- Die Rubrik **Status** bietet die Möglichkeit auf einen Blick zu sehen, welche Avira AntiVir für KEN! Module aktiv sind und gibt Informationen über das letzte durchgeführte Update. Zudem ist ersichtlich ob Sie Inhaber einer gültigen Lizenz sind.
- Die Rubrik Ereignisse bietet Ihnen die Möglichkeit, sich über die Ereignisse zu informieren, die von den Modulen der Avira AntiVir für KEN! erzeugt werden.
- Die Rubrik Berichte bietet Ihnen die Möglichkeit, sich die Ergebnisse der von Avira AntiVir für KEN! durchgeführten Aktionen anzusehen.
- **Lokaler Schutz:** Unter **Lokaler Schutz** finden Sie die Komponenten, mit denen Sie Dateien auf Ihrem Computersystem auf Viren und Malware prüfen.
- Die Rubrik Prüfen bietet Ihnen die Möglichkeit, die Direktsuche auf einfache Art und Weise zu konfigurieren bzw. zu starten. Vordefinierte Profile ermöglichen einen Suchlauf mit bereits angepassten Standardoptionen. Genau so ist es möglich mit Hilfe der Manuellen Auswahl (wird nicht gespeichert) die Suche nach Viren und unerwünschten Programmen auf Ihre persönlichen Bedürfnisse anzupassen.
- Die Rubrik Guard zeigt Ihnen Informationen zu überprüften Dateien, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
- **Verwaltung:** Unter **Verwaltung** finden Sie Werkzeuge, mit denen Sie verdächtige oder von Viren betroffene Dateien isolieren und administrieren sowie wiederkehrende Aufgaben planen können.
- Hinter der Rubrik Quarantäne verbirgt sich der so genannte Quarantänenanager. Die zentrale Stelle für bereits in Quarantäne gestellte Dateien oder aber für verdächtige Dateien, die Sie in Quarantäne stellen möchten. Zudem besteht die Möglichkeit, eine ausgewählte Datei per Email an das Avira Malware Research Center zu senden.
- Die Rubrik Planer bietet Ihnen die Möglichkeit, zeitlich gesteuerte Prüf- und Update-Aufträge zu erstellen und bestehende Aufträge anzupassen bzw. zu löschen.

5.1.3 Konfiguration

In der Avira AntiVir für KEN! Konfiguration können Sie Einstellungen für AntiVir für KEN! vornehmen. Nach der Installation ist AntiVir für KEN! mit Standardeinstellungen konfiguriert, die gewährleisten, dass Ihr Computersystem optimal geschützt ist. Dennoch können Ihr Computersystem oder Ihre Anforderungen an AntiVir für KEN! Besonderheiten aufweisen, so dass Sie die Schutzkomponenten von AntiVir für KEN! anpassen möchten.



Die Avira AntiVir für KEN! Konfiguration hat den Aufbau eines Dialogfensters: Mit den Schaltflächen OK und Abbrechen bestätigen oder verwerfen Sie Ihre in der Konfiguration vorgenommenen Einstellungen. In der linken Navigationsleiste können Sie einzelne Konfigurationssrubriken anwählen.

Aufrufen von Avira AntiVir für KEN! Konfiguration

Sie haben mehrere Möglichkeiten die Konfiguration aufzurufen:

- Über die Windows Systemsteuerung.
- Über das Windows Sicherheitscenter - ab Windows XP Service Pack 2.
- Über das Avira AntiVir für KEN! Tray Icon.
- Im Avira AntiVir für KEN! Control Center über den Menüpunkt Extras | Konfiguration.
- Im Avira AntiVir für KEN! Control Center über die Schaltfläche Konfiguration.



Hinweis

Wenn Sie die Konfiguration über die Schaltfläche **Konfiguration** im Control Center aufrufen, gelangen Sie in das Konfigurationsregister der Rubrik, die im Control Center aktiv ist. Zum Anwählen einzelner Konfigurationsregister muss der Expertenmodus der Konfiguration aktiviert sein. In diesem Fall erscheint ein Dialog, in dem Sie aufgefordert werden, den Expertenmodus zu aktivieren.

Avira AntiVir für KEN! Konfiguration bedienen

Sie navigieren innerhalb des Konfigurationsfensters wie im Windows Explorer:

- ▶ Klicken Sie einen Eintrag in der Baumstruktur an, um diese Konfigurationsrubrik im Detailfenster anzuzeigen.
 - ▶ Klicken Sie auf das Plus-Zeichen vor einem Eintrag, um die Konfigurationsrubrik zu erweitern und untergeordnete Konfigurationsrubriken in der Baumstruktur anzuzeigen.
 - ▶ Um untergeordnete Konfigurationsrubriken zu verbergen, klicken Sie auf das Minus-Zeichen vor der erweiterten Konfigurationsrubrik.
-



Hinweis

Die gesamten Konfigurationsrubriken werden nur im Expertenmodus angezeigt. Aktivieren Sie den Expertenmodus, um alle Konfigurationsrubriken zu sehen. Der Expertenmodus kann mit einem Passwort versehen werden, das beim Aktivieren angegeben werden muss.

Wenn Sie Ihre Einstellungen in der Konfiguration übernehmen möchten:

- ▶ Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Das Konfigurationsfenster wird geschlossen und die Einstellungen werden übernommen.

Wenn Sie die Konfiguration beenden möchten ohne Ihre Einstellungen zu übernehmen:

- ▶ Klicken Sie auf die Schaltfläche **Abbrechen**.
 - ↳ Das Konfigurationsfenster wird geschlossen und die Einstellungen werden verworfen.

Konfigurationsoptionen im Überblick

Sie haben folgende Konfigurationsoptionen:

- **Scanner:** Konfiguration der Direktsuche
 - Suchoptionen
 - Aktionen bei Fund
 - Optionen bei Suche in Archiven
 - Ausnahmen der Direktsuche
 - Heuristik der Direktsuche
 - Einstellung der Reportfunktion
- **Guard:** Konfiguration der Echtzeitsuche
 - Suchoptionen

Aktionen bei Fund

Ausnahmen der Echtzeitsuche

Heuristik der Echtzeitsuche

Einstellung der Reportfunktion

– **Allgemeines:**

Konfiguration des Email-Versand per SMTP

Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche

Kennwortschutz für den Zugriff auf das Control Center und die Avira AntiVir für KEN! Konfiguration

Sicherheit: Warnung bei veraltetem AntiVir für KEN!, Schutz der Konfiguration, Prozessschutz,

Konfiguration der Ereignis-Protokollierung

Konfiguration der Bericht-Funktionen


Einstellung der verwendeten Verzeichnisse

Update: Konfiguration der Verbindung zum Downloadserver, Einstellung der Produktupdates

Warnungen: Konfiguration von Email-Warnungen der Komponente(n) Scanner, Guard, KEN! Updater und Konfiguration von Netzwerkwarnungen der Komponente(n) Scanner, Guard

5.1.4 Tray Icon

Nach der Installation sehen Sie das Tray Icon von AntiVir für KEN! im Systemtray der Taskleiste:

Symbol	Beschreibung
	AntiVir Guard ist aktiviert
	AntiVir Guard ist deaktiviert

Das Tray Icon zeigt den Status des AntiVir Guard Dienstes an.

Über das Kontextmenü des Tray Icons sind zentrale Funktionen von Avira AntiVir für KEN! schnell zugänglich. Um das Kontextmenü aufzurufen, klicken Sie mit der rechten Maustaste auf das Tray Icon.

Einträge im Kontextmenü

- **AntiVir Guard aktivieren:** Aktiviert bzw. deaktiviert den AntiVir für KEN! Guard.
- **AntiVir starten:** Öffnet das Avira AntiVir für KEN! Control Center.
- **AntiVir konfigurieren:** Öffnet die Avira AntiVir für KEN! Konfiguration.
- **Aktualisieren:** Startet ein Update.
- **Hilfe:** Öffnet diese Online-Hilfe.

- **Avira im Internet:** Öffnet das Webportal des Herstellers von AntiVir für KEN! im Internet. Voraussetzung ist, dass Sie einen aktiven Zugang zum Internet haben.

5.2 So wird es gemacht

5.2.1 Avira AntiVir für KEN! automatisiert aktualisieren


Durch die Integration von Avira AntiVir für KEN! in KEN! kann eine Aktualisierung von Avira AntiVir für KEN! automatisiert über den KEN! Service-PC durchgeführt werden. Alternativ haben Sie die Möglichkeit, ein automatisierte Aktualisierung auch innerhalb von Avira AntiVir für KEN! zu konfigurieren.



Hinweis

Vorinstalliert ist ein Update-Auftrag, der die Avira AntiVir für KEN! bei einer verfügbaren Internet-Verbindung alle 24 Stunden sowie zusätzlich beim Aufbau einer Internet-Verbindung aktualisiert.

So legen Sie mit dem AntiVir Planer einen Auftrag an, mit dem Avira AntiVir für KEN! automatisiert aktualisiert wird:

- ▶ Wählen Sie im Control Center die Rubrik **Verwaltung :: Planer**.
- ▶ Klicken Sie auf das Symbol  *Neuen Auftrag mit dem Wizard erstellen*.
 - ↳ Das Dialogfenster *Name und Beschreibung des Auftrags* erscheint.
- ▶ Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Art des Auftrags* wird angezeigt.
- ▶ Wählen Sie **Update-Auftrag** aus der Auswahlliste.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Zeitpunkt des Auftrags* erscheint.
- ▶ Wählen Sie, wann das Update ausgeführt werden soll:
 - **Sofort**
 - **Täglich**
 - **Wöchentlich**
 - **Intervall**
 - **Einmalig**
 - **Login**



Hinweis

Wir empfehlen, Avira AntiVir für KEN! regelmäßig und häufig zu aktualisieren, z.B. im Intervall alle 6 Stunden.

- ▶ Geben Sie je nach Auswahl ggf. den Termin an.
- ▶ Wählen Sie ggf. Zusatzoptionen (nur je nach Auftragsart verfügbar):
 - **Auftrag zusätzlich bei Internet-Verbindung starten**
Zusätzlich zur festgelegten Häufigkeit wird der Auftrag bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

- **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**

Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.

- ▶ Klicken Sie auf **Weiter**.

↳ Das Dialogfenster *Auswahl des Darstellungsmodus* erscheint.

- ▶ Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Auftragsfenster
- **Unsichtbar**: kein Auftragsfenster

- ▶ Klicken Sie auf **Fertig stellen**.

↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik **Verwaltung :: Prüfen** als aktiviert (Häkchen).

- ▶ Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:



Eigenschaften eines Auftrags ansehen



Auftrag ändern



Auftrag löschen

5.2.2 Ein Update manuell starten

Sie haben verschiedene Möglichkeiten ein Update von Avira AntiVir für KEN! manuell zu starten: Beim manuell gestarteten Update wird immer ein Update der Virendefinitionsdatei und der Suchengine durchgeführt. Ein Produktupdate erfolgt nur dann, wenn Sie in der Konfiguration unter Allgemeines :: Update die Option **Produktupdates herunterladen und automatisch installieren** aktiviert haben.

So starten Sie ein Update von Avira AntiVir für KEN! manuell:

- ▶ Klicken Sie mit der rechten Maustaste auf das Avira AntiVir für KEN! Tray Icon in der Taskleiste.

↳ Ein Kontextmenü erscheint.

- ▶ Wählen Sie **Aktualisieren**.

↳ Das Dialogfenster *Avira AntiVir für KEN! Updater* erscheint.

- ODER -

- ▶ Wählen Sie im Control Center die Rubrik **Übersicht :: Status**.

- ▶ Klicken Sie im Bereich *Letztes Update* auf den Link **Aktualisieren**.

↳ Das Dialogfenster Avira AntiVir für KEN! Updater erscheint.

- ODER -

- ▶ Wählen Sie im Control Center im Menü **Update** den Menübefehl *Update starten*.

↳ Das Dialogfenster Avira AntiVir für KEN! Updater erscheint.

**Hinweis**

Wir empfehlen dringend, die Avira AntiVir für KEN! regelmäßig automatisiert zu aktualisieren, z.B. alle 24 Stunden.

**Hinweis**

Sie können ein manuelles Update auch direkt über das Windows Sicherheitscenter ausführen.

5.2.3 Direktsuche: Mit einem Suchprofil nach Viren und Malware suchen

Ein Suchprofil ist eine Zusammenstellung von Laufwerken und Verzeichnissen, die durchsucht werden sollen.

Sie haben folgende Möglichkeit über ein Suchprofil zu suchen:

- Vordefiniertes Suchprofil verwenden

Wenn die vordefinierten Suchprofile Ihren Bedürfnissen entsprechen.

- Suchprofil anpassen und verwenden (manuelle Auswahl)

Wenn Sie mit einem individualisierten Suchprofil suchen möchten.

Je nach Betriebssystem stehen für das Starten eines Suchprofils verschiedene Symbole zur Verfügung:

- Unter Windows XP und 2000:



Mit diesem Symbol starten Sie die Suche über ein Suchprofil.

- Unter Windows Vista:

Unter Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.



Mit diesem Symbol starten Sie eine eingeschränkte Suche über ein Suchprofil. Es werden nur die Verzeichnisse und Dateien durchsucht, für die Windows Vista die Zugriffsrechte erteilt hat.



Mit diesem Symbol starten Sie die Suche mit erweiterten Administratorrechten. Nach einer Bestätigung werden alle Verzeichnisse und Dateien im gewählten Suchprofil durchsucht.

So suchen Sie mit einem Suchprofil nach Viren und Malware:

- ▶ Wählen Sie im Control Center die Rubrik **Lokaler Schutz :: Prüfen**.

↳ Vordefinierte Suchprofile erscheinen.

- ▶ Wählen Sie eines der vordefinierten Suchprofile aus.

-ODER-

- ▶ Passen Sie das Suchprofil *Manuelle Auswahl* an.

- ▶ Klicken auf das Symbol (Windows XP: oder Windows Vista:).

- ▶ Das Fenster *Luke Filewalker* erscheint und die Direktsuche startet.
 - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

Wenn Sie ein Suchprofil anpassen möchten:

- ▶ Klappen Sie im Suchprofil **Manuelle Auswahl** den Dateibaum so weit auf, dass alle Laufwerke und Verzeichnisse geöffnet sind, die geprüft werden sollen.
 - Klick auf das + Zeichen: Nächste Verzeichnisebene wird angezeigt.
 - Klick auf das - Zeichen: Nächste Verzeichnisebene wird verborgen.
- ▶ Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das jeweilige Kästchen der jeweiligen Verzeichnisebene.

Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:

- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)
- Verzeichnis ohne Unterverzeichnisse (grünes Häkchen)
- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Kein Verzeichnis (kein Häkchen)

5.2.4 Direktsuche: Per Drag&Drop nach Viren und Malware suchen

So suchen Sie per Drag&Drop gezielt nach Viren und Malware:

- ✓ Das Control Center von Avira AntiVir für KEN! ist geöffnet.
- ▶ Markieren Sie die Datei oder das Verzeichnis, die/das geprüft werden soll.
- ▶ Ziehen Sie mit der linken Maustaste die markierte Datei oder das markierte Verzeichnis in das *Control Center*.
 - ↳ Das Fenster *Luke Filewalker* erscheint und die Direktsuche startet.
 - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.


5.2.5 Direktsuche: Über das Kontextmenü nach Viren und Malware suchen

So suchen Sie über das Kontextmenü gezielt nach Viren und Malware:

- ▶ Klicken Sie (z.B. im Windows Explorer, auf dem Desktop oder in einem geöffneten Windows-Verzeichnis) mit der rechten Maustaste auf die Datei bzw. das Verzeichnis, die/das Sie prüfen wollen.
 - ↳ Das Kontextmenü des Windows Explorers erscheint.
- ▶ Wählen Sie im Kontextmenü **Ausgewählte Dateien mit AntiVir überprüfen**.
 - ↳ Das Fenster *Luke Filewalker* erscheint und die Direktsuche startet.
 - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

5.2.6 Direktsuche: Automatisiert nach Viren und Malware suchen

So legen Sie einen Auftrag an, nach dem automatisiert nach Viren und Malware gesucht wird:

- ▶ Wählen Sie im Control Center die Rubrik **Verwaltung :: Planer**.
- ▶ Klicken Sie auf das Symbol .
 - ↳ Das Dialogfenster *Name und Beschreibung des Auftrags* erscheint.
- ▶ Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Art des Auftrags* erscheint.
- ▶ Wählen Sie den **Prüfauftrag**.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Auswahl des Profils* erscheint.
- ▶ Wählen Sie, welches Profil durchsucht werden soll.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Zeitpunkt des Auftrags* erscheint.
- ▶ Wählen Sie aus, wann der Suchlauf ausgeführt werden soll:
 - **Sofort**
 - **Täglich**
 - **Wöchentlich**
 - **Intervall**
 - **Einmalig**
 - **Login**
- ▶ Geben Sie je nach Auswahl ggf. den Termin an.
- ▶ Wählen Sie ggf. folgende Zusatzoption (nur je nach Auftragsart verfügbar):
 - **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- ▶ Klicken Sie auf **Weiter**.
 - ↳ Das Dialogfenster *Auswahl des Darstellungsmodus* erscheint.
- ▶ Wählen Sie den Darstellungsmodus des Auftragsfensters:
 - **Minimiert**: nur Fortschrittsbalken
 - **Maximiert**: gesamtes Auftragsfenster
 - **Unsichtbar**: kein Auftragsfenster
- ▶ Klicken Sie auf **Fertig stellen**.
 - ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *Verwaltung :: Planer* als aktiviert (Häkchen).
- ▶ Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:



Eigenschaften zu einem Auftrag ansehen



Auftrag ändern





Auftrag löschen

5.2.7 Direktsuche: Gezielt nach aktiven Rootkits suchen

Um nach aktiven Rootkits zu suchen, nutzen Sie das vordefinierte Suchprofil *Suche nach Rootkits*.

So suchen Sie gezielt nach aktiven Rootkits:

- ▶ Wählen Sie im Control Center die Rubrik **Lokaler Schutz :: Prüfen**.
 - ↳ Vordefinierte Suchprofile erscheinen.
- ▶ Wählen Sie das vordefinierte Suchprofil **Suche nach Rootkits**.
- ▶ Markieren Sie ggf. weitere Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das Kästchen der Verzeichnisebene.
- ▶ Klicken Sie auf das Symbol (Windows XP:  oder Windows Vista: ).
 - ↳ Das Fenster *Luke Filewalker* erscheint und die Direktsuche startet.
 - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

5.2.8 Auf gefundene Viren und Malware reagieren

Für die einzelnen Schutzkomponenten von AntiVir für KEN! können Sie in der Konfiguration jeweils unter der Rubrik *Aktion bei Fund* einstellen, wie AntiVir für KEN! bei einem Fund eines Virus oder unerwünschten Programms reagiert:

– **Interaktiv**

Bei aktivierter Option erscheint bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit dem betroffenen Objekt weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

– **Automatisch**

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Die Komponente reagiert nach den von Ihnen vorgenommenen Einstellungen.

Wenn Sie für Schutzkomponenten die Option *Interaktiv* gewählt haben, bietet Ihnen Avira AntiVir für KEN! folgende Möglichkeiten an, darauf zu reagieren:



Hinweis

Welche Möglichkeiten angezeigt werden, ist abhängig vom Betriebssystem und von dem Modul (AntiVir Guard, AntiVir Scanner), das den Fund meldet.

– **Reparieren**

Die Datei wird repariert.

Diese Option ist nur aktivierbar, wenn eine Reparatur der gefundenen Datei möglich ist.

– **In Quarantäne verschieben**

Die Datei wird in ein spezielles Format (*.qua) gepackt und in das Quarantäne-Verzeichnis *INFECTED* auf Ihrer Festplatte verschoben, sodass kein direkter Zugriff mehr möglich ist. Dateien in diesem Verzeichnis können später in der Quarantäne repariert oder - falls nötig - an die Avira GmbH geschickt werden.

– **Löschen**

Die Datei wird gelöscht, kann aber mit entsprechenden Tools (z.B. *Avira UnErase*) wiederhergestellt werden. Damit kann die Virensignatur wiedergefunden werden. Dieser Vorgang ist bedeutend schneller als *Überschreiben und löschen*.

– **Überschreiben und löschen**

Die Datei wird mit einem Standardmuster überschrieben und anschließend gelöscht. Sie kann nicht wiederhergestellt werden.

– **Umbenennen**

Die Datei wird nach *.vir umbenannt. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurückbenannt werden.

– **Zugriff verweigern**

Der Fund wird nur in der Reportdatei eingetragen (wenn diese aktiviert ist).

– **Ignorieren**

Avira AntiVir für KEN! führt keine weiteren Aktionen aus. Die betroffene Datei bleibt auf Ihrem Computer aktiv.



Warnung

Gefahr von Datenverlust und Schäden am Betriebssystem! Nutzen Sie die Option Ignorieren nur in begründeten Ausnahmefällen.

– **Keine weitere Aktion durchführen**

Der Zugriff auf die Datei wird blockiert.

– **Datei vor Aktion in Quarantäne kopieren**

Diese Option ist nur wählbar, wenn eine der Optionen Reparieren, Löschen, Überschreiben und Löschen gewählt wird.

– **Auswahl auf alle folgenden Funde anwenden**

Die bei diesem Fund gewählte Aktion wird beim nächsten Fund wieder ausgeführt.



Hinweis

Wir empfehlen, eine verdächtige Datei, die nicht repariert werden kann, in die Quarantäne zu verschieben.

- ▶ Schicken Sie uns auch Dateien, die von der Heuristik gemeldet werden, zur Analyse zu.

Sie können diese Dateien z.B. über unsere Webseite hochladen:
<http://www.avira.de/datei-upload>

Dateien, die von der Heuristik gemeldet werden, erkennen Sie an der Bezeichnung *HEUR/* bzw. *HEURISTIC/*, die dem Dateinamen vorangestellt werden, z.B.: *HEUR/testdatei.**

Wenn Viren oder Malware in einer Archivdatei gefunden wurden, haben Sie folgende Möglichkeiten:

- Gesamtes Archiv löschen
- Archiv umbenennen
- Archiv in Quarantäne verschieben



Hinweis


Es ist nicht möglich, einzelne betroffene Dateien aus dem Archiv zu löschen.

5.2.9 Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen

So können Sie mit Dateien in der Quarantäne umgehen:


- ▶ Wählen Sie im Control Center die Rubrik **Verwaltung :: Quarantäne**.
- ▶ Prüfen Sie, um welche Dateien es sich handelt, sodass Sie deren Originale ggf. von anderer Stelle zurück auf Ihren Computer laden können.

Wenn Sie nähere Informationen zu einer Datei ansehen wollen:

- ▶ Markieren Sie die Datei und klicken Sie auf .
 - ↳ Das Dialogfenster *Eigenschaften* mit weiteren Informationen zur Datei erscheint.

Wenn Sie eine Datei erneut prüfen wollen:

Die Prüfung einer Datei empfiehlt sich, wenn die Virendefinitionsdatei von Avira AntiVir für KEN! aktualisiert wurde und ein Verdacht auf einen Fehlalarm vorliegt. So können Sie einen Fehlalarm beim erneuten Prüfen bestätigen und die Datei wiederherstellen.


- ▶ Markieren Sie die Datei und klicken Sie auf .
 - ↳ Die Datei wird mit den Einstellungen der Direktsuche auf Viren und Malware geprüft.
 - ↳ Nach der Prüfung erscheint der Dialog *Prüf-Statistik*, der eine Statistik zum Zustand der Datei vor und nach der erneuten Prüfung anzeigt.

Wenn Sie eine Datei löschen wollen:

- ▶ Markieren Sie die Datei und klicken Sie auf .

Wenn Sie unsicher sind, ob Sie die Dateien gefahrlos löschen können:

- ✓ Email-Einstellungen konfiguriert

- ▶ Schicken Sie die Dateien der Avira GmbH zur Analyse zu. Klicken Sie dazu auf .

Dateien in Quarantäne können Sie auch wiederherstellen:

- siehe Kapitel: Quarantäne: Dateien in der Quarantäne wiederherstellen

5.2.10 Quarantäne: Dateien in der Quarantäne wiederherstellen

Je nach Betriebssystem stehen für das Wiederherstellen verschiedene Symbole zur Verfügung:

- Unter Windows XP und 2000:



Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her.



Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.

- Unter Windows Vista:

Unter Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.



Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.



Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her. Wenn für den Zugriff auf dieses Verzeichnis erweiterte Administratorrechte nötig sind, erscheint eine entsprechende Abfrage.

So können Sie Dateien in der Quarantäne wiederherstellen:



Warnung


Gefahr von Datenverlust und Schäden am Betriebssystem des Computers! Verwenden Sie die Funktion *Ausgewähltes Objekt wiederherstellen* nur in Ausnahmefällen. Stellen Sie nur solche Dateien wieder her, die durch einen erneuten Suchlauf repariert werden konnten.

- ✓ Datei erneut mit Suchlauf geprüft und repariert.



- ▶ Wählen Sie im Control Center die Rubrik **Verwaltung :: Quarantäne**.



Hinweis


Emails und Anhänge von Emails können nur mit der Option  und mit der Endung **.eml* wiederhergestellt werden.

Wenn Sie eine Datei an ihrem Ursprungsort wiederherstellen wollen:

- ▶ Markieren Sie die Datei und klicken Sie auf das Symbol (Windows 2000/XP: , Windows Vista ).
- Diese Option ist für Emails nicht möglich.



Hinweis


Emails und Anhänge von Emails können nur mit der Option  und mit der Endung **.eml* wiederhergestellt werden.

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

▶ Klicken Sie auf **Ja**.

↳ Die Datei wird in dem Verzeichnis wiederhergestellt, aus dem sie in die Quarantäne verschoben wurde.

Wenn Sie eine Datei in einem bestimmten Verzeichnis wiederherstellen wollen:

▶ Markieren Sie die Datei und klicken Sie auf .

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

▶ Klicken Sie auf **Ja**.

↳ Das Windows-Standardfenster für die Auswahl des Verzeichnisses erscheint.

▶ Wählen Sie das Verzeichnis, in dem die Datei wiederhergestellt werden soll und bestätigen Sie.

↳ Die Datei wird in dem gewählten Verzeichnis wiederhergestellt.

5.2.11 Quarantäne: Verdächtige Datei in die Quarantäne verschieben

So können Sie manuell eine verdächtige Datei in die Quarantäne verschieben:

▶ Wählen Sie im Control Center die Rubrik **Verwaltung :: Quarantäne**.

▶ Klicken Sie auf .

↳ Das Windows-Standardfenster für die Auswahl einer Datei erscheint.

▶ Wählen Sie die Datei und bestätigen Sie.

↳ Die Datei wird in die Quarantäne verschoben.

Dateien in Quarantäne können Sie mit dem AntiVir Scanner prüfen:

- siehe Kapitel: Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen

5.2.12 Suchprofil: Dateityp in einem Suchprofil ergänzen oder löschen

So legen Sie für ein Suchprofil fest, dass zusätzliche Dateitypen durchsucht oder dass bestimmte Dateitypen von der Suche ausgeschlossen werden sollen (nur bei manueller Auswahlmöglich):

✓ Sie befinden sich im Control Center in der Rubrik **Lokaler Schutz :: Prüfen**.

▶ Klicken Sie mit der rechten Maustaste auf das Suchprofil, das Sie bearbeiten wollen.

↳ Ein Kontextmenü erscheint.

▶ Wählen Sie den Eintrag **Dateifilter**.

▶ Klappen Sie das Kontextmenü weiter auf, indem Sie auf das kleine Dreieck auf der rechten Seite des Kontextmenüs klicken.

↳ Die Einträge *Standard*, *Prüfe alle Dateien* und *Benutzerdefiniert* erscheinen.

- ▶ Wählen Sie den Eintrag **Benutzerdefiniert**.
 - ↳ Das Dialogfenster *Dateierweiterungen* erscheint mit einer Liste aller Dateitypen, die mit dem Suchprofil durchsucht werden.

Wenn Sie einen Dateityp aus der Suche ausschließen wollen:

- ▶ Markieren Sie den Dateityp und klicken Sie auf **Löschen**.

Wenn Sie einen Dateityp zur Suche hinzufügen wollen:

- ▶ Markieren Sie den Dateityp.
- ▶ Klicken Sie auf **Einfügen** und geben Sie die Dateierweiterung des Dateityps in das Eingabefeld ein.


Verwenden Sie dabei maximal 10 Zeichen und geben Sie den führenden Punkt nicht mit an. Wildcards (* und ?) als Stellvertreter sind erlaubt.

5.2.13 Suchprofil: Desktop-Verknüpfung für Suchprofil erstellen

Über eine Desktop-Verknüpfung zu einem Suchprofil können Sie eine Direktsuche direkt von Ihrem Desktop aus starten, ohne das Control Center von Avira AntiVir für KEN! aufzurufen.

So erstellen Sie eine Verknüpfung zu dem Suchprofil auf dem Desktop:

- ✓ Sie befinden sich im Control Center in der Rubrik **Lokaler Schutz :: Prüfen**.
- ▶ Wählen Sie das Suchprofil, zu dem Sie eine Verknüpfung erstellen möchten.

- ▶ Klicken Sie auf das Symbol .

↳ Die Desktop-Verknüpfung wird erstellt.

5.2.14 Ereignisse: Ereignisse filtern

Im Control Center werden unter **Übersicht :: Ereignisse** Ereignisse angezeigt, die von den Programmkomponenten von AntiVir für KEN! erzeugt wurden. (analog der Ereignisanzeige Ihres Windows Betriebssystems). Programmkomponenten sind:

- Updater
- Guard
- Scanner
- Planer

Es werden folgende Ereignistypen angezeigt:

- Information
- Warnung
- Fehler
- Fund

So filtern sie die angezeigten Ereignisse:

- ▶ Wählen Sie im Control Center die Rubrik **Übersicht :: Ereignisse**.
- ▶ Aktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der aktivierten Komponenten anzuzeigen.

- ODER -

Deaktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der deaktivierten Komponenten auszublenden.

- ▶ Aktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse anzuzeigen.
- ODER -
Deaktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse auszublenden.

6 Scanner

Mit Avira AntiVir für KEN! können Sie manuelle Suchläufe (Direktsuche) nach Viren und unerwünschten Programmen auf mehrere Arten durchführen.

– **Direktsuche über Kontextmenü**

Die Direktsuche über das Kontextmenü (rechte Maustaste - Eintrag **Ausgewählte Dateien mit AntiVir überprüfen**) empfiehlt sich, wenn Sie z.B. im Windows Explorer einzelne Dateien und Verzeichnisse prüfen wollen. Ein weiterer Vorteil ist, dass für die Direktsuche über Kontextmenü das Avira AntiVir für KEN! Control Center nicht erst gestartet werden muss.

– **Direktsuche über Drag & Drop**

Beim Ziehen einer Datei oder eines Verzeichnisses in das Programmfenster des Avira AntiVir für KEN! Control Center prüft der Scanner die Datei bzw. das Verzeichnis sowie alle enthaltenen Unterverzeichnisse. Dieses Vorgehen empfiehlt sich, wenn Sie einzelne Dateien und Verzeichnisse prüfen wollen, die Sie z.B. auf Ihrem Desktop abgelegt haben.

– Direktsuche über Profile

Dieses Vorgehen empfiehlt sich, wenn Sie regelmäßig bestimmte Verzeichnisse und Laufwerke (z.B. Ihr Arbeitsverzeichnis oder Laufwerke, auf denen Sie regelmäßig neue Dateien ablegen) prüfen wollen. Sie müssen diese Verzeichnisse und Laufwerke dann nicht für jede Prüfung neu wählen, sondern wählen eine Auswahl bequem mit dem entsprechenden Profil.

– **Direktsuche über den Planer**

Der Planer bietet die Möglichkeit, zeitlich gesteuerte Prüfaufträge durchführen zu lassen.

7 Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität des Programms, insbesondere der Virendefinitionsdatei und der Suchengine. Zur Ausführung von Updates ist die Komponente KEN! Updater in AntiVir für KEN! integriert. Der KEN! Updater sorgt dafür, dass Avira AntiVir für KEN! stets auf dem neuesten Niveau arbeitet und in der Lage ist, die täglich neu erscheinenden Viren zu erfassen. KEN! Updater aktualisiert die folgenden Komponenten:

- Virendefinitionsdatei:

Die Virendefinitionsdatei enthält die Erkennungsmuster der Schadprogramme, die AntiVir für KEN! bei der Suche nach Viren und Malware sowie bei der Reparatur von betroffenen Objekten verwendet.

- Suchengine:

Die Suchengine enthält die Methoden, mit denen AntiVir für KEN! nach Viren und Malware sucht.

- Programmdateien (Produktupdate):

Updatepakete für Produktupdates stellen weitere Funktionen für die einzelnen Programmkomponenten zur Verfügung.

Bei der Ausführung eines Updates werden die Virendefinitionsdatei und die Suchengine auf Aktualität geprüft und bei Bedarf aktualisiert. Je nach den Einstellungen in der Konfiguration führt KEN! Updater zusätzlich ein Produktupdate durch oder benachrichtigt Sie über verfügbare Produktupdates. Nach einem Update muss AntiVir für KEN! nicht neu gestartet werden.



Hinweis

Aus Sicherheitsgründen prüft der Avira AntiVir für KEN! Updater, ob die Windows host-Datei Ihres Computers dahingehend geändert wurde, das die Avira AntiVir für KEN! Update-URL beispielsweise durch Malware manipuliert wurde und den Avira AntiVir für KEN! Updater auf unerwünschte Download-Seiten umleitet. Wurde die Windows host-Datei manipuliert, so ist dies in der Avira AntiVir für KEN! Updater Reportdatei ersichtlich.

Im Control Center unter Planer können Sie Update-Aufträge einrichten, die in den angegebenen Intervallen von KEN! Updater ausgeführt werden. Standardmäßig ist nach einer Installation von AntiVir für KEN! ein Update-Auftrag angelegt. Sie haben auch die Möglichkeit, ein Update manuell zu starten:

- Im Control Center: Im Menü Update und in der Rubrik Status
- Über das Kontextmenü des Tray Icons

Sie beziehen Updates aus dem Internet über einen Webserver des Herstellers. Standardmäßig wird die existierende Netzwerkverbindung als Verbindung zu den Downloadservern der Avira GmbH genutzt. Sie können diese Standardeinstellung in der Avira AntiVir für KEN! Konfiguration unter Allgemeines :: Update anpassen.

8 FAQ, Tipps

In diesem Kapitel finden Sie eine Zusammenstellung häufig gestellter Fragen zu Avira AntiVir für KEN!, Hilfe bei Problemen sowie Tipps und Tricks im Umgang mit Avira AntiVir für KEN!.

siehe Kapitel: Häufig gestellte Fragen (FAQ)

siehe Kapitel: Hilfe im Problemfall

siehe Kapitel: Tastaturbefehle

siehe Kapitel: Windows XP Sicherheitscenter

8.1 Hilfe im Problemfall

Hier finden Sie Informationen zu Ursachen und Lösungen möglicher Probleme.

Die Fehlermeldung Der Verbindungsaufbau schlug fehl beim Downloaden der Datei ... erscheint beim Versuch, ein Update zu starten.

Ursache: Ihre Internetverbindung ist inaktiv. Deshalb findet Avira AntiVir für KEN! den Webserver im Internet nicht.

- ▶ Testen Sie, ob andere Internetdienste wie WWW oder Email funktionieren. Wenn nicht, stellen Sie die Internetverbindung wieder her.

Ursache: Der Proxyserver ist nicht erreichbar.

- ▶ Prüfen Sie, ob sich das Login für den Proxyserver geändert hat und passen Sie gegebenenfalls Ihre Konfiguration an.

Ursache: Die Datei update.exe ist bei Ihrer Personal Firewall nicht vollständig freigegeben.

- ▶ Stellen Sie sicher, dass die Datei update.exe bei Ihrer Personal Firewall vollständig freigegeben ist.

Ansonsten:

- ▶ Prüfen Sie in der Avira AntiVir für KEN! Konfiguration (Expertenmodus) unter Allgemeines :: Update Ihre Einstellungen.

Viren und Malware können nicht verschoben oder gelöscht werden.

Ursache: Die Datei wurde von Windows geladen und befindet sich in einem aktiven Zustand.

- ▶ Aktualisieren Sie Avira AntiVir für KEN!.
- ▶ Wenn Sie das Betriebssystem Windows XP verwenden, deaktivieren Sie die Systemwiederherstellung.
- ▶ Starten Sie den Computer im abgesicherten Modus.
- ▶ Starten Sie Avira AntiVir für KEN! und die Avira AntiVir für KEN! Konfiguration (Expertenmodus).
- ▶ Wählen Sie Scanner :: Suche :: Dateien :: Alle Dateien und bestätigen Sie das Fenster mit **OK**.

- ▶ Starten Sie einen Suchlauf über alle lokalen Laufwerke.
- ▶ Starten Sie den Computer im normalen Modus.
- ▶ Führen Sie einen Suchlauf im normalen Modus durch.
- ▶ Falls keine weiteren Viren und Malware gefunden werden, aktivieren Sie die Systemwiederherstellung, falls diese vorhanden ist und genutzt werden soll.

Das Tray Icon zeigt einen deaktivierten Zustand an.

Ursache: Der AntiVir Guard ist deaktiviert.

- ▶ Klicken Sie im Control Center in der Rubrik Übersicht :: Status im Bereich AntiVir Guard auf den Link **Aktivieren**.

Ursache: Der AntiVir Guard wird von einer Firewall blockiert.

- ▶ Definieren Sie in der Konfiguration Ihrer Firewall eine generelle Freigabe für den AntiVir Guard. Der AntiVir Guard arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut.

Ansonsten:

- ▶ Überprüfen Sie die Startart des AntiVir Guard Dienstes. Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste "Start | Einstellungen | Systemsteuerung". Starten Sie das Konfigurationspanel "Dienste" per Doppelklick (unter Windows 2000 und Windows XP finde Sie das Dienste-Applet im Unterordner "Verwaltung"). Suchen Sie nach dem Eintrag "AntiVir für KEN! Guard". Als Startart muss "Automatisch" eingetragen sein und als Status "Gestartet". Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche "Starten". Tritt eine Fehlermeldung auf, überprüfen Sie bitte die Ereignisanzeige.

Der Rechner wird extrem langsam, wenn ich eine Datensicherung durchführe.

Ursache: AntiVir Guard durchsucht während des Backup-Prozesses alle Dateien, mit denen die Datensicherung arbeitet.

- ▶ Wählen Sie in der Avira AntiVir für KEN! Konfiguration (Expertenmodus) Guard :: Suche :: Ausnahmen und tragen Sie den Prozessnamen der Backup-Software ein.

Meine Firewall meldet den AntiVir Guard, sobald diese aktiv sind.

Ursache: Die Kommunikation des AntiVir Guard erfolgt über das Internetprotokoll TCP/IP. Eine Firewall überwacht alle Verbindungen über dieses Protokoll.

- ▶ Definieren Sie eine generelle Freigabe für AntiVir Guard. Der AntiVir Guard arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut.



Hinweis

Wir empfehlen Ihnen, regelmäßig Microsoft Updates durchzuführen, um eventuelle Sicherheitslücken zu schließen.

8.2 Häufig gestellte Fragen (FAQ)

Hier finden Sie Antworten auf häufig gestellte Fragen.

Woher bekomme ich Avira AntiVir für KEN!?

Downloaden Sie das Programm von der Webseite <http://www.avira.de>.

Erhalte ich eine CD von Avira AntiVir für KEN!?

Das Programm steht ausschließlich auf unserer Webseite <http://www.avira.de> zum Download bereit.

Wo finde ich detaillierte Versionsinformationen?

Detaillierte Versionsinformationen finden Sie im Menüpunkt Hilfe :: Über AntiVir für KEN!... :: Versionsinformationen des Control Center.

Welche Einstellungen soll ich für Avira AntiVir für KEN! vornehmen?

Avira AntiVir für KEN! ist nach der Installation bereits mit sinnvollen Einstellungen vorkonfiguriert. Je nach gewünschter Sicherheitsstufe können Sie diese Einstellungen anpassen (z.B. Heuristikerkennung oder Ausweitung der Suche auf alle Datei- und Archivtypen).

Kann ich Einstellungen mit einem Kennwort schützen?

Ja, in der Avira AntiVir für KEN! Konfiguration (Expertenmodus) unter Allgemeines :: Kennwort.

Wie prüfe ich, ob Avira AntiVir für KEN! aktuell ist?

Die Avira AntiVir für KEN! ist aktuell, wenn Sie die aktuelle Virendefinitionsdatei besitzen. Diese Datei wird in der Regel mehrmals täglich aktualisiert.

So prüfen Sie, ob Sie die aktuelle Virendefinitionsdatei besitzen:

- ▶ Führen Sie ein Update durch.
- ODER -
- ▶ Besuchen Sie die Webseite <http://www.avira.de> und lesen Sie dort folgende Informationen nach:
 - Aktuelle VDF-Versionsnummer
 - Datum und Uhrzeit der Veröffentlichung der aktuellen VDF
- ▶ Wählen Sie im Control Center die Rubrik Übersicht :: Status.
- ▶ Vergleichen Sie diese Angaben mit den Angaben auf der Webseite.

Wenn die Angaben übereinstimmen: Die Avira AntiVir für KEN! ist aktuell.
Wenn die Angaben nicht übereinstimmen: Avira AntiVir für KEN! ist veraltet. Führen Sie ein Update durch.

Was ist ein inkrementelles VDF-Update (IVDF)?

Avira AntiVir für KEN! unterstützt das so genannte "inkrementelle Update" der Virendefinitionsdatei. Beim inkrementellen VDF-Update (IVDF-Update) werden täglichen Aktualisierungen der VDF-Datei nicht mehr in Form einer einzigen großen VDF-Datei heruntergeladen, sondern in Form einer kleinen, nur wenige Kilobyte großen VDF-Datei (Name: antivir3.vdf), die lediglich die neu hinzugekommenen Virenerkennungsmuster enthält.

Diese tägliche VDF-Datei ergänzt die wöchentliche VDF (Name: antivir2.vdf), die monatliche VDF (Name: antivir1.vdf) und die sogenannte Basis VDF (Name: antivir0.vdf), die bereits mit jedem Avira AntiVir für KEN! Programmpaket standardmäßig installiert werden.

Erreicht eine der genannten VDF-Dateien eine bestimmte Größe, so wird ihr Inhalt in die nächsthöhere VDF-Datei übertragen, die dann zusätzlich heruntergeladen werden muss.

Vorteil des inkrementellen VDF-Verfahrens ist, dass das Downloadvolumen extrem klein gehalten wird. Dies führt zu sehr kurzen Downloadzeiten und -kosten, auch wenn der Download über eine Internet-Modem-Verbindung erfolgt.

Was ist der Unterschied zwischen Echtzeitsuche und Direktsuche?

Die Echtzeitsuche wird vom AntiVir Guard automatisch durchgeführt. Es werden die Dateien nach Viren und Malware durchsucht, auf die gerade auf dem Computer zugegriffen wird (On-Access).

Die Direktsuche wird manuell gestartet. Es können gezielt bestimmte Laufwerke und Verzeichnisse nach Viren und Malware durchsucht werden (On-Demand).

Gibt es Probleme, wenn ich mehrere Virenschutzprogramme parallel installiere?

Für den Einsatz verschiedener Virenschutzprogramme nach dem Motto *Zwei Augen sehen mehr als eines* müssen folgende Regeln beachtet werden:

- ▶ Setzen Sie nur einen Echtzeitscanner (auch: On-Access-Scanner, Guard oder Wächter genannt) ein.
- ▶ Entscheiden Sie sich vor der Installation eines zweiten Softwarepakets, welchem Echtzeitscanner Sie Ihr Vertrauen schenken möchten. Wenn Sie sich für einen neuen Echtzeitscanner entscheiden, deaktivieren Sie den derzeit genutzten Echtzeitscanner. Ansonsten kann es zu schwer wiegenden Störungen kommen.

Die parallele Installation von Scannern, mit denen Suchläufe manuell gestartet werden, ist in der Regel möglich. Unter Umständen können Fehlermeldungen auftreten, wenn eine Antivirensoftware unverschlüsselte Suchstrings zur Erkennung verwendet oder sie eine Datei nur unvollständig repariert hat.

Ich will testen, ob mein Virenschutzprogramm wirklich funktioniert. Gibt es Testviren, die meinen Computer nicht schädigen?

Das European Institute for Computer Anti-Virus Research (eicar) stellt auf der Webseite http://www.eicar.org/anti_virus_test_file.htm Dateien mit Testviren zur Verfügung. Es handelt sich dabei nicht um echte Viren, sondern nur um sogenannte Erkennungsmuster. Diese Dateien können keinen Schaden auf Ihrem Rechner anrichten.

So sollte Avira AntiVir für KEN! auf das eicar-Testvirus reagieren, falls eine Standardinstallation mit den voreingestellten Dateitypen durchgeführt wurde:

– *eicar.com*

Der nackte Testvirus wird vom AntiVir Guard (sofern aktiviert) sofort erkannt. Natürlich auch bei der Direktsuche (Klicken Sie dazu mit der rechten Maustaste auf den Testvirus. Ein Kontextmenü öffnet sich. Wählen Sie **Ausgewählte Dateien mit AntiVir überprüfen**). Je nach Einstellungen in den Optionen wird eine Warnmeldung angezeigt, die nach der weiteren Vorgehensweise fragt.

– *eicar.com.txt*

Vorab: Um doppelte Datei-Endungen zu sehen, müssen Sie dies im Windows Explorer aktivieren. Diese Version wird vom AntiVir Guard zunächst nicht beanstandet, da *.txt Dateien keinen ausführbaren Programmcode beinhalten und daher ungefährlich sind. Wird die Datei in eicar.com umbenannt, wird AntiVir Guard wie oben beschrieben auf die Datei reagieren.

Bei der Direktsuche wird der Testvirus erkannt. Die Bearbeitung (s.o.) wird angeboten.

– *eicar_com.zip*

Hier ist der Testvirus in einem Zip-Archiv gepackt. Da ein Zip-Archiv an sich nicht gefährlich ist, reagiert der AntiVir Guard nicht. Er tritt erst beim Auspacken des Archivs in Aktion.

Bei der Direktsuche wird der Testvirus im Archiv gefunden. Ein Hinweisfenster erscheint, das darauf hinweist, dass ein Virus oder Malware gefunden wurde, aber im Zip-Archiv nicht bearbeitet werden kann, um die Integrität des Archivs nicht zu gefährden.

– *eicarcom2.zip*

Hier ist der Testvirus in einem Zip-Archiv gepackt, das wiederum in ein Zip-Archiv gepackt wurde. Also erschwerte Bedingungen für einen Virens Scanner. Die Reaktionen von AntiVir Guard und der Direktsuche entsprechen denen auf eicar_com.zip.

Bei der Direktsuche wird der Testvirus erkannt und das Hinweisfenster (s.o.) erscheint. Der AntiVir Guard reagiert erst beim zweiten, letzten Auspacken, wenn die Datei eicar.com vorliegt.

Ist ein manueller Suchlauf von Zeit zu Zeit notwendig?

AntiVir Guard überwacht Ihr System permanent (Echtzeitsuche). Um sicherzustellen, dass Sie ständig geschützt sind, prüfen Sie, ob der AntiVir Guard aktiv ist. Außerdem empfehlen wir Ihnen, für eine höhere Sicherheit in regelmäßigen Abständen einen manuellen Suchlauf (Direktsuche) durchzuführen.

8.3 Tastaturbefehle

Tastaturbefehle - auch Shortcuts genannt - bieten eine schnelle Möglichkeit durch Avira AntiVir für KEN! zu navigieren, einzelne Module aufzurufen und Aktionen zu starten.

Im Folgenden erhalten Sie eine Übersicht der in Avira AntiVir für KEN! verfügbaren Tastaturbefehle. Nähere Hinweise zur Funktionalität und Verfügbarkeit finden Sie im entsprechenden Kapitel der Hilfe.

8.3.1 In Dialogfeldern

Tastaturbefehl	Beschreibung
Strg + Tab Strg + Bild runter	Zur nächsten Rubrik wechseln.
Strg + Umsch + Tab Strg + Bild hoch	Zur vorherigen Rubrik wechseln.
Tab	Zur nächsten Option oder Optionsgruppe wechseln.
Umsch + Tab	Zur vorherigen Option oder Optionsgruppe wechseln.
← ↑ → ↓	Zwischen den Optionen in einem markierten Drop-Down-Listefeld oder zwischen mehreren Optionen in einer Optionsgruppe wechseln.
Leertaste	Aktivieren bzw. Deaktivieren eines Kontrollkästchens, wenn die aktive Option ein Kontrollkästchen ist.
Alt + unterstrichene Buchstabe	Option wählen bzw. Befehl ausführen.
Alt + ↓ F4	Ausgewähltes Drop-Down-Listefeld öffnen.
Esc	Ausgewähltes Drop-Down-Listefeld schließen. Befehl abbrechen und Dialogfeld schließen.
Eingabetaste	Befehl für die aktive Option oder Schaltfläche ausführen.

8.3.2 In der Hilfe

Tastaturbefehl	Beschreibung
Alt + Leertaste	Systemmenü anzeigen.
Alt + Tab	Umschalten zwischen der Hilfe und anderen geöffneten Fenstern.
Alt + F4	Hilfe schließen.
Umschalt + F10	Kontextmenüs der Hilfe anzeigen.
Strg + Tab	Zur nächsten Rubrik im Navigationsfenster wechseln.
Strg + Umsch + Tab	Zur vorherigen Rubrik im Navigationsfenster wechseln.
Bild hoch	Zum Thema wechseln, das oberhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
Bild runter	Zum Thema wechseln, das unterhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
F6	Zwischen dem Navigations- und dem Themenfenster umschalten.
Bild hoch Bild runter	Durch ein Thema blättern.

8.3.3 Im Control Center

Allgemein

Tastaturbefehl	Beschreibung
F1	Hilfe anzeigen
Alt + F4	Control Center schließen
F5	Ansicht aktualisieren
F8	Konfiguration öffnen
F9	Aktualisieren

Rubrik Prüfen

Tastaturbefehl	Beschreibung
F3	Suchlauf mit dem ausgewählten Profil starten
F4	Desktopverknüpfung für das ausgewählte Profil erstellen

Rubrik Quarantäne

Tastaturbefehl	Beschreibung
F2	Objekt erneut prüfen
F3	Objekt wiederherstellen
F4	Objekt senden
F6	Objekt wiederherstellen nach...
Enter	Eigenschaften
Einf	Datei hinzufügen
Entf	Objekt löschen

Rubrik Planer

Tastaturbefehl	Beschreibung
F2	Auftrag ändern
Enter	Eigenschaften
Einf	Neuen Auftrag einfügen
Entf	Auftrag löschen

Rubrik Berichte

Tastaturbefehl	Beschreibung
F3	Reportdatei anzeigen
F4	Reportdatei drucken
Enter	Bericht anzeigen
Entf	Bericht(e) löschen

Rubrik Ereignisse

Tastaturbefehl	Beschreibung
F3	Ereignis(se) exportieren
Enter	Ereignis anzeigen
Entf	Ereignis(se) löschen

8.4 Windows Sicherheitscenter

- ab Windows XP Service Pack 2 -

8.4.1 Allgemeines

Das Windows Sicherheitscenter überprüft den Status eines Computers im Hinblick auf wichtige Sicherheitsaspekte.

Wenn bei einem dieser wichtigen Punkte ein Problem festgestellt wird (z.B. ein veraltetes Antivirusprogramm), sendet das Sicherheitscenter eine Warnung und stellt Empfehlungen bereit, wie Sie den Computer besser schützen können.

8.4.2 Das Windows Sicherheitscenter und Avira AntiVir für KEN!

Virenschutzsoftware / Schutz vor schädlicher Software

Folgende Hinweise können Sie in Bezug auf Ihren Virenschutz vom Windows Sicherheitscenters erhalten.

Virenschutz NICHT GEFUNDEN

Virenschutz NICHT AKTUELL

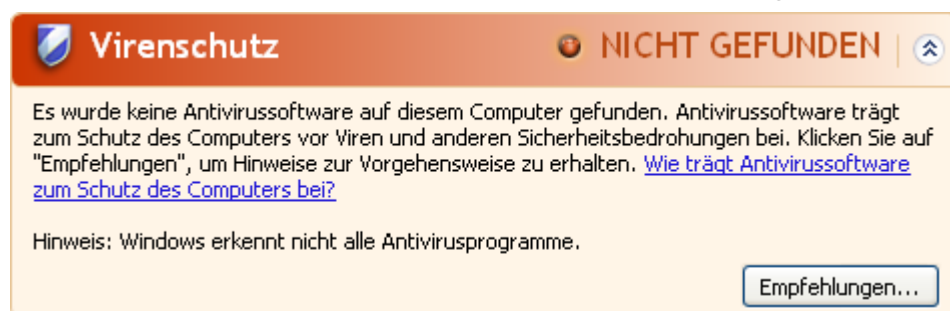
Virenschutz AKTIV

Virenschutz INAKTIV

Virenschutz NICHT ÜBERWACHT

Virenschutz NICHT GEFUNDEN

Dieser Hinweis des Windows Sicherheitscenters erscheint, wenn das Windows Sicherheitscenter keine Antivirussoftware auf Ihrem Computer gefunden hat.

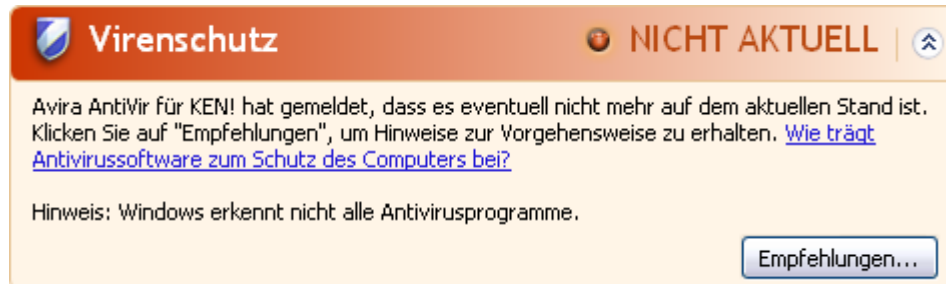


Hinweis

Installieren Sie Avira AntiVir für KEN! auf Ihrem Computer um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Virenschutz NICHT AKTUELL

Haben Sie den Windows XP Service Pack 2 bzw. Windows Vista bereits installiert und installieren danach Avira AntiVir für KEN! oder aber installieren Sie den Windows XP Service Pack 2 bzw. Windows Vista auf ein System, auf dem Avira AntiVir für KEN! bereits installiert war erhalten sie folgende Meldung:

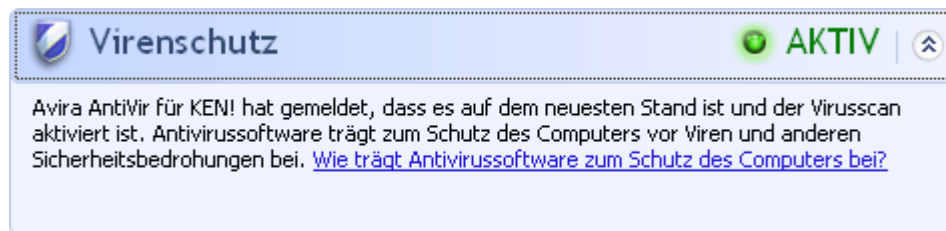


Hinweis

Damit das Windows Sicherheitscenter Avira AntiVir für KEN! als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Avira AntiVir für KEN! Update durchführen.

Virenschutz AKTIV

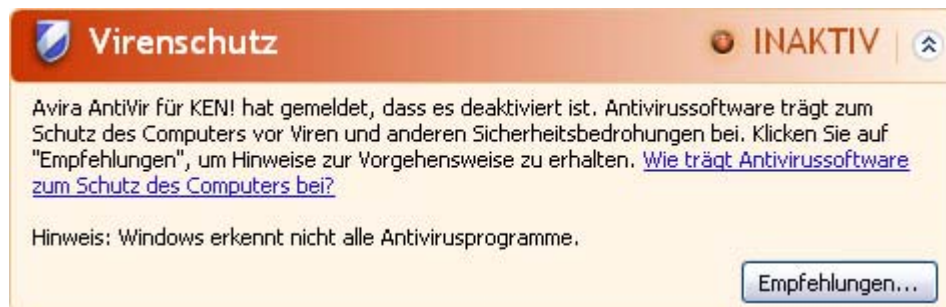
Nach der Installation von Avira AntiVir für KEN! und einem im Anschluss daran durchgeführten Update erhalten Sie folgenden Hinweis:



Avira AntiVir für KEN! ist nun auf aktuellem Stand und der AntiVir Guard ist aktiv.

Virenschutz INAKTIV

Nachfolgenden Hinweis erhalten Sie, wenn Sie den AntiVir Guard deaktivieren oder aber den Guard Dienst stoppen.

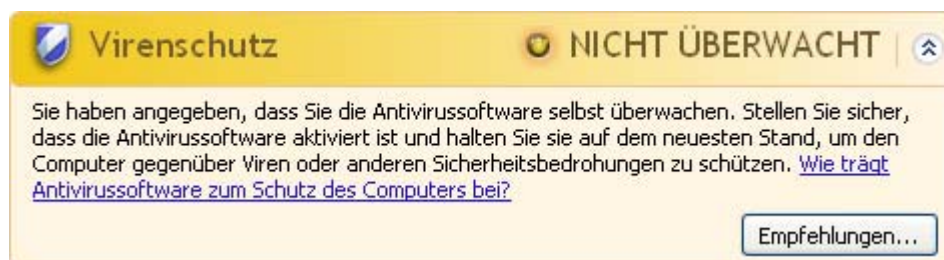


Hinweise

Den AntiVir Guard können Sie unter der Rubrik Übersicht :: Status des Avira AntiVir für KEN! Control Center aktivieren bzw. deaktivieren. Sie erkennen zudem, dass der AntiVir Guard aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist.

Virenschutz NICHT ÜBERWACHT

Erhalten Sie folgenden Hinweis vom Windows Sicherheitscenter, dann haben Sie sich dafür entschieden, dass Sie Ihre Antivirussoftware selbst überwachen.



Hinweis

Das Windows Sicherheitscenter wird von Avira AntiVir für KEN! unterstützt. Sie können diese Option jederzeit über die Schaltfläche "Empfehlungen..." aktivieren.



Hinweis

Auch wenn Sie den Windows XP Service Pack 2 bzw. Windows Vista installiert haben benötigen Sie weiterhin eine Virenschutzlösung, z.B. Avira AntiVir für KEN!. Obwohl Windows XP Service Pack 2 Ihre Antivirus-Software überwacht, enthält es selbst keinerlei Antivirus-Funktionen. Sie wären also ohne eine zusätzliche Virenschutzlösung nicht vor Viren und sonstiger Malware geschützt!

9 Viren und mehr

9.1 Erweiterte Gefahrenkategorien

Kostenverursachende Einwahlprogramme (DIALER)

Bestimmte im Internet angebotene Dienstleistungen sind kostenpflichtig. Die Abrechnung erfolgt in Deutschland über Einwahlprogramme mit 0190/0900-Nummern (in Österreich und der Schweiz über 09x0-Nummern; in Deutschland wird mittelfristig auf 09x0 umgestellt). Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Die Vermarktung von Online-Inhalten über den Weg der Telefonrechnung ist legal und kann für den Nutzer vorteilhaft sein. Seriöse Dialer lassen deshalb keinen Zweifel daran aufkommen, dass sie vom Kunden bewusst und mit Bedacht eingesetzt werden. Sie installieren sich nur dann auf dem Anwender-Rechner, wenn der Nutzer dazu seine Zustimmung abgibt, wobei diese Zustimmung aufgrund einer völlig eindeutigen und klar erkennbaren Etikettierung bzw. Aufforderung erfolgt sein muss. Der Verbindungsaufbau seriöser Dialer-Programme wird unmissverständlich angezeigt. Außerdem informieren seriöse Dialer exakt und augenfällig über die Höhe der dabei entstehenden Kosten.

Leider jedoch gibt es Dialer, die sich unauffällig, auf fragwürdige Weise oder gar in betrügerischer Absicht auf Rechnern installieren. Sie ersetzen z.B. die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine kostenverursachende, oft horrend überteuerte 0190/0900-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190/0900-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

Um sich generell vor unerwünschten kostenverursachenden Einwahlprogrammen (0190/0900-Dialern) zu schützen, empfehlen wir Ihnen, sich direkt bei Ihrem Telefon-Anbieter für diesen Nummernkreis sperren zu lassen.

Standardmäßig erkennt Avira AntiVir für KEN! die ihm bekannten kostenverursachende Einwahlprogramme.

Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Kostenverursachende Einwahlprogramme (DIALER)** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden eines kostenverursachenden Einwahlprogramms einen entsprechenden Warnhinweis. Sie haben nun die Möglichkeit, den eventuell unerwünschten 0190/0900-Dialer einfach zu löschen. Ist dies allerdings ein erwünschtes Einwahlprogramm, können Sie es als Ausnahmedatei deklarieren und diese Datei wird dann zukünftig nicht mehr untersucht.

Spiele (GAMES)

Computerspiele müssen sein - aber sie gehören nicht unbedingt an den Arbeitsplatz (die Mittagspause vielleicht einmal ausgenommen). Dennoch wird von Mitarbeitern in Unternehmen und Behörden so manches Moorhuhn erlegt und so mancher Karobube doppelgeklickt. Über das Internet kann eine Fülle von Spielen heruntergeladen werden. Auch Email-Games erfreuen sich wachsender Verbreitung: Vom simplen Schach bis zum "Flottenmanöver" (inklusive Torpedogefecht) sind zahlreiche Varianten in Umlauf: Die jeweiligen Spielzüge werden über Mailprogramme an Partner gesendet und von diesen beantwortet.

Untersuchungen haben ergeben, dass die zum Computerspielen verwendete Arbeitszeit längst wirtschaftlich relevante Größenordnungen erreicht hat. Umso verständlicher ist, dass immer mehr Unternehmen Möglichkeiten in Betracht ziehen, Computerspiele von Arbeitsplatzrechnern fern zu halten.

Avira AntiVir für KEN! erkennt Computerspiele. Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Spiele (GAMES)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist. Das Spiel ist nun im wahrsten Sinne des Wortes aus, denn Sie haben die Möglichkeit, es einfach zu löschen.

Witzprogramme (JOKES)

Die Witzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren. Meist fängt der Computer nach dem Aufruf eines Witzprogramms irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für Witzprogramme sind die Waschmaschine im Diskettenlaufwerk (DRAIN.COM) und der Bildschirmfresser (BUGSRES.COM).

Aber Vorsicht! Alle Symptome von Witzprogrammen könnten auch von einem Virus oder einem Trojaner stammen. Zumindest bekommt man aber einen gehörigen Schreck oder richtet in Panik hinterher sogar selbst tatsächlichen Schaden an.

Avira AntiVir für KEN! ist in der Lage, durch die Erweiterung seiner Such- und Identifikationsroutinen Witzprogramme zu erkennen und sie als unerwünschtes Programm ggf. zu eliminieren. Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Witzprogramme (JOKES)** mit einem Häkchen aktiviert, wird über entsprechende Funde informiert.

Security Privacy Risk (SPR)

Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann und daher möglicherweise unerwünscht ist.

Avira AntiVir für KEN! erkennt "Security Privacy Risk" Software. Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Security Privacy Risk (SPR)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist.

Backdoor-Steuersoftware (BDC)

Um Daten zu stehlen oder Rechner zu manipulieren, wird "durch die Hintertür" ein Backdoor-Server-Programm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor Steuersoftware (Client) von Dritten gesteuert werden.

Avira AntiVir für KEN! erkennt "Backdoor Steuersoftware". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Backdoor-Steuersoftware (BDC)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist.

Adware/Spyware (ADSPY)

Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.

Avira AntiVir für KEN! erkennt "Adware/Spyware". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Adware/Spyware (ADSPY)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist.

Ungewöhnliche Laufzeitpacker (PCK)

Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden und daher als möglicherweise verdächtig eingestuft werden können.

Avira AntiVir für KEN! erkennt "Ungewöhnliche Laufzeitpacker". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Ungewöhnliche Laufzeitpacker (PCK)** aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist.

Dateien mit verschleierte Dateieindungen (HEUR-DBLEXT)

Ausführbare Dateien, die ihre wahre Dateieindung in verdächtiger Weise verschleiern. Diese Methode der Verschleierung wird häufig von Malware benutzt.

Avira AntiVir für KEN! erkennt "Dateien mit verschleierte Dateieindungen". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Dateien mit verschleierte Dateieindungen (HEUR-DBLEXT)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! fündig geworden ist.

Phishing

Phishing, auch bekannt als *brand spoofing* ist eine raffinierte Form des Datendiebstahls, der auf Kunden bzw. potenzielle Kunden von Internet Service Providern, Banken, Online-Banking Diensten, Registrierungsbehörden abzielt.

Durch eine Weitergabe der eigenen Email-Adresse im Internet, das Ausfüllen von Online-Formularen, dem Beitritt von Newsgroups oder Webseiten ist es möglich, dass Ihre Daten von sog. "Internet crawling spiders" gestohlen und ohne Ihre Erlaubnis dazu verwendet werden einen Betrug oder andere Verbrechen zu begehen.

Avira AntiVir für KEN! erkennt "Phishing". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Phishing** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! ein solches Verhalten bemerkt.

Anwendung (APPL)

Bei der Bezeichnung APPL handelt es sich um eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.

Avira AntiVir für KEN! erkennt "Anwendung (APPL)". Ist in der Konfiguration unter Erweiterte Gefahrenkategorien die Option **Anwendung (APPL)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira AntiVir für KEN! ein solches Verhalten bemerkt.

9.2 Viren sowie sonstige Malware

Adware

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Backdoors

Einem Backdoor (deutsch: Hintertür) ist es möglich, unter Umgehung der Zugriffssicherung, Zugriff auf einen Computer zu erlangen.

Ein versteckt laufendes Programm ermöglicht einem Angreifer meist fast uneingeschränkte Rechte. Mit Hilfe des Backdoors können persönliche Daten des Anwenders ausspioniert werden. Aber Sie werden meist dazu benutzt, weitere Computerviren oder Würmer auf dem betroffenen System zu installieren.

Bootviren

Der Boot- bzw. Masterbootsektor von Festplatten wird mit Vorliebe von Bootsektorviren infiziert. Sie überschreiben wichtige Informationen zum Systemstart. Eine der unangenehmen Folgen: das Betriebssystem kann nicht mehr geladen werden...

Bot-Net

Unter einem Bot-Net versteht man ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojaner erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, DDoS Attacken, usw. verwendet werden, z.T. ohne dass die betroffenen PC-Nutzer etwas merken. Das Hauptpotenzial von Bot-Nets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt.

Exploit

Ein Exploit (Sicherheitslücke) ist ein Computerprogramm oder Script, welches spezifische Schwächen oder Fehlfunktionen eines Betriebssystems oder Programms ausnutzt. Eine Form des Exploits sind Angriffe aus dem Internet mit Hilfe von manipulierten Datenpaketen, die Schwachstellen in der Netzwerksoftware ausnutzen. Hier können Programme eingeschleust werden, mit denen ein größerer Zugriff erlangt werden kann.

Hoaxes (engl.: hoax - Scherz, Schabernack, Ulk)

Seit ein paar Jahren erhalten die User im Internet und in anderen Netzen Warnungen vor Viren, die sich angeblich per Email verbreiten sollen. Diese Warnungen werden über Email mit der Aufforderung verbreitet, sie an möglichst viele Kollegen und andere Benutzer weiter zu senden, um alle vor der "Gefahr" zu warnen.

Honeypot

Ein Honeypot (Honigtopf) ist ein in einem Netzwerk installierter Dienst (Programm oder Server). Dieser hat die Aufgabe, ein Netzwerk zu überwachen und Angriffe zu protokollieren. Dieser Dienst ist dem legitimen Nutzer unbekannt und wird daher niemals angesprochen. Wenn nun ein Angreifer ein Netzwerk auf Schwachstellen untersucht und dabei die von einem Honeypot angebotenen Dienste in Anspruch nimmt, wird er protokolliert und ein Alarm ausgelöst.

Makroviren

Makroviren sind kleine Programme, die in der Makrosprache einer Anwendung (z.B. WordBasic unter WinWord 6.0) geschrieben sind und sich normalerweise auch nur innerhalb von Dokumenten dieser Anwendung verbreiten können. Sie werden deshalb auch Dokumentviren genannt. Damit sie aktiv werden, sind sie immer darauf angewiesen, dass die entsprechende Applikation gestartet und eines der infizierten Makros ausgeführt wird. Im Unterschied zu "normalen" Viren befallen Makroviren also keine ausführbaren Dateien sondern die Dokumente der jeweiligen Wirts-Applikation.

Pharming

Pharming ist eine Manipulation der Hostdatei von Webbrowsern, um Anfragen auf gefälschte Webseiten umzuleiten. Es handelt sich um eine Weiterentwicklung des klassischen Phishings. Pharming-Betrüger unterhalten eigene große Server-Farmen, auf denen gefälschte Webseiten abgelegt sind. Pharming hat sich auch als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Bei einer Manipulation der Host-Datei wird unter Zuhilfenahme eines Trojaners oder eines Virus eine gezielte Manipulation des Systems vorgenommen. Die Folge davon ist, dass von diesem System nur noch gefälschte Websites abrufbar sind, selbst wenn die Web-Adresse korrekt eingegeben wurde.

Phishing

Phishing bedeutet ins Deutsche übersetzt das Fischen nach persönlichen Daten des Internetnutzers. Der Phisher schickt seinem Opfer in der Regel offiziell wirkende Schreiben, wie beispielsweise Emails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Klar ist: Banken und Versicherungen bitten niemals um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per Email, per SMS oder telefonisch.

Polymorphe Viren

Wahre Meister der Tarnung und Verkleidung sind polymorphe Viren. Sie verändern ihre eigenen Programmiercodes - und sind deshalb besonders schwer zu erkennen.

Programmviren

Ein Computervirus ist ein Programm, welches die Fähigkeit besitzt, sich nach seinem Aufruf selbsttätig an andere Programme auf irgendeine Weise anzuhängen und dadurch zu infizieren. Viren vervielfältigen sich also im Gegensatz zu logischen Bomben und Trojanern selber. Im Gegensatz zu einem Wurm benötigt der Virus immer ein fremdes Programm als Wirt, in dem er seinen virulenten Code ablegt. Im Normalfall wird aber der eigentliche Programmablauf des Wirtes selber nicht geändert.

Rootkit

Ein Rootkit ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem installiert werden, um Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden - generell gesagt: sich unsichtbar zu machen. Sie versuchen bereits installierte Spionageprogramme zu aktualisieren und gelöschte Spyware erneut zu installieren.

Skriptviren und Würmer

Diese Viren sind extrem einfach zu programmieren und verbreiten sich - entsprechende Techniken vorausgesetzt - innerhalb weniger Stunden per Email um den ganzen Erdball.

Skriptviren und -würmer benutzen eine der Script-Sprachen, wie beispielsweise Javascript, VBScript etc., um sich selbst in andere, neue Skripte einzufügen oder sich selber durch den Aufruf von Betriebssystemfunktionen zu verbreiten. Häufig geschieht dies per Email oder durch den Austausch von Dateien (Dokumenten).

Als Wurm wird ein Programm bezeichnet, das sich selber vervielfältigt jedoch keinen Wirt infiziert. Würmer können also nicht Bestandteil anderer Programmabläufe werden. Würmer sind auf Systemen mit restriktiveren Sicherheitsvorkehrungen oft die einzige Möglichkeit irgendwelche Schadensprogramme einzuschleusen.

Spyware

Spyware sind sogenannte Spionageprogramme, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet. Meist dienen Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren und gezielte Werbe-Banner oder Werbe-Popups einzublenden.

Trojanische Pferde (kurz Trojaner)

Trojaner sind in letzter Zeit recht häufig anzutreffen. So bezeichnet man Programme, die vorgeben, eine bestimmte Funktion zu haben, nach ihrem Start aber ihr wahres Gesicht zeigen und irgendeine andere Funktion ausführen, die zumeist zerstörerisch ist. Trojanische Pferde können sich nicht selber vermehren, was sie von Viren und Würmern unterscheidet. Die meisten haben einen interessanten Namen (SEX.EXE oder STARTME.EXE), der den Anwender zur Ausführung des Trojaners verleiten soll. Unmittelbar nach der Ausführung werden diese dann aktiv und formatieren z.B. die Festplatte. Eine spezielle Art eines Trojaners ist ein Dropper, der Viren 'droppt', d.h. in das Computersystem einpflanzt.

Zombie

Ein Zombie-PC ist ein Rechner, welcher mit Malwareprogrammen infiziert ist und es den Hackern erlaubt, Rechner per Fernsteuerung für ihre kriminellen Zwecke zu missbrauchen. Der betroffene PC startet auf Befehl beispielsweise Denial-of-Service-(DoS) Attacken oder versendet Spam und Phishing Emails.

10 Info und Service

In diesem Kapitel erhalten Sie Informationen, auf welchen Wegen Sie mit uns in Kontakt treten können.

siehe Kapitel: Kontaktadresse

siehe Kapitel: Technischer Support

siehe Kapitel: Verdächtige Datei

siehe Kapitel: Fehlalarm melden

siehe Kapitel: Ihr Feedback für mehr Sicherheit

10.1 Kontaktadresse

Gerne helfen wir Ihnen weiter, wenn Sie Fragen und Anregungen zur Produktwelt von Avira AntiVir für KEN! haben. Unsere Kontaktadressen finden Sie im Control Center unter Hilfe :: Über Avira AntiVir für KEN!.

10.2 Technischer Support

Der Avira AntiVir für KEN! Support steht Ihnen zuverlässig zur Seite, wenn es gilt, Ihre Fragen zu beantworten oder ein technisches Problem zu lösen.

Auf unserer Webseite <http://www.avira.de/ken-support> erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service.

Damit wir Ihnen schnell und zuverlässig helfen können, sollten Sie die folgenden Informationen bereithalten:

- **Lizenzdaten.** Diese finden Sie im Avira AntiVir für KEN! Control Center unter dem Menüpunkt Hilfe :: Über AntiVir für KEN! :: Lizenzinformationen.
- **Versionsinformationen.** Diese finden Sie im Avira AntiVir für KEN! Control Center unter dem Menüpunkt Hilfe :: Über AntiVir für KEN! :: Versionsinformationen.
- **Betriebssystemversion** und eventuell installierte Service-Packs.
- **Installierte Software-Pakete**, z.B. Antivirensoftware anderer Hersteller.
- **Genauere Meldungen** des Programms oder der Reportdatei.

10.3 Verdächtige Datei

Viren, die gegebenenfalls von unseren Produkten noch nicht erkannt bzw. entfernt werden können oder verdächtige Dateien können Sie an uns senden. Dafür stellen wir Ihnen mehrere Wege zur Verfügung.

- Wählen Sie die Datei im Quarantänemanager des Control Center aus und wählen Sie über das Kontextmenü oder die entsprechende Schaltfläche den Punkt Datei senden.
- Senden Sie die gewünschte Datei gepackt (WinZIP, PKZIP, Arj etc.) im Anhang einer Email an quarantine@avira.com. Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

Alternativ haben Sie die Möglichkeit, die verdächtige Datei über unsere Webseite an uns zu senden.

10.4 Fehlalarm melden

Sind Sie der Meinung Avira AntiVir für KEN! meldet einen Fund in einer Datei die jedoch mit hoher Wahrscheinlichkeit "sauber" ist, so senden Sie diese Datei, gepackt (WinZIP, PKZIP, Arj etc.) im Anhang einer Email, an quarantine@avira.com. Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

10.5 Ihr Feedback für mehr Sicherheit

Bei Avira steht die Sicherheit unserer Kunden an erster Stelle. Aus diesem Grund beschäftigen wir nicht nur ein eigenes Expertenteam, welches jede einzelne Avira-Lösung und jedes einzelne Update vor der Veröffentlichung aufwendigen Qualitäts- und Sicherheitstests unterzieht. Für uns gehört auch dazu, Hinweise auf eventuell auftretende, sicherheitsrelevante Schwachstellen ernst zu nehmen und mit diesen offen umzugehen.

Wenn Sie glauben, eine sicherheitsrelevante Schwachstellen in einem unserer Produkte gefunden zu haben, senden Sie bitte eine Email an vulnerabilities@avira.com.

11 Referenz: Konfigurationsoptionen

Die Referenz der Konfiguration dokumentiert alle Konfigurationsoptionen, die in Avira AntiVir für KEN! verfügbar sind.

11.1 Scanner

Die Rubrik Scanner der Avira AntiVir für KEN! Konfiguration ist für die Konfiguration der Direktsuche, d.h. für die Suche auf Verlangen, zuständig.

11.1.1 Suche

Hier legen Sie das grundlegende Verhalten der Suchroutine bei einer Direktsuche fest. Wenn Sie bei der Direktsuche bestimmte Verzeichnisse für die Prüfung wählen, prüft der Scanner je nach Konfiguration:

- mit einer bestimmten Suchleistung (Priorität),
- zusätzlich Bootsektoren und Hauptspeicher,
- bestimmte oder alle Bootsektoren und den Hauptspeicher,
- alle oder ausgewählte Dateien im Verzeichnis.

Dateien

Der Scanner kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von Ihrem Inhalt und Ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht. Der Filter wird nicht verwendet.



Hinweis

Ist Alle Dateien aktiv, lässt sich die Schaltfläche Dateierweiterungen nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch von Avira AntiVir für KEN! übernommen. D.h. Avira AntiVir für KEN! entscheidet anhand des Inhalts einer Datei, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als Dateierweiterungsliste verwenden, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.



Hinweis

Ist Intelligente Dateiauswahl aktiv, lässt sich die Schaltfläche Dateierweiterungen nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche Dateierweiterung manuell editieren.



Hinweis

Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "Keine Dateierweiterungen" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus **Dateierweiterungsliste verwenden** untersucht werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.



Hinweis

Beachten Sie bitte, dass sich die Standardliste von Version zu Version ändern kann.

Weitere Einstellungen

Bootsektor Suchlaufwerke

Bei aktivierter Option prüft der Scanner die Bootsektoren der bei der Direktsuche gewählten Laufwerke. Diese Einstellung ist standardmäßig aktiviert.

Masterbootsektoren durchsuchen

Bei aktivierter Option prüft der Scanner die Masterbootsektoren der im System verwendeten Festplatte(n).

Offline Dateien ignorieren

Bei aktivierter Option ignoriert die Direktsuche sog. Offline Dateien bei einem Suchlauf komplett. D.h., diese Dateien werden nicht auf Viren und unerwünschte Programme geprüft. Offline Dateien sind Dateien, die durch ein sog. Hierarchisches Speicher-Management-System (HSMS) physikalisch von der Festplatte auf z.B. ein Band ausgelagert wurden. Diese Einstellung ist standardmäßig aktiviert.

Symbolischen Verknüpfungen folgen

Bei aktivierter Option folgt der Scanner bei einer Suche allen symbolischen Verknüpfungen im Suchprofil oder ausgewählten Verzeichnis, um die verknüpften Dateien nach Viren und Malware zu durchsuchen. Diese Option wird nicht unter Windows 2000 unterstützt und ist standardmäßig deaktiviert.



Wichtig

Die Option schließt keine Dateiverknüpfungen (Shortcuts) ein, sondern bezieht sich ausschließlich auf symbolische Links (erzeugt mit mklink.exe) oder Junction Points (erzeugt mit junction.exe), die transparent im Dateisystem vorliegen.

Rootkit-Suche bei Suchstart

Bei aktivierter Option prüft der Scanner bei einem Suchstart in einem sog. Schnellverfahren das Windows-Systemverzeichnis auf aktive Rootkits. Dieses Verfahren prüft Ihren Rechner nicht so umfassend auf aktive Rootkits wie das Such-Profil **Suche nach Rootkits**, ist jedoch in der Ausführung bedeutend schneller.



Wichtig

Die Rootkit-Suche ist für 64-Bit-Systeme noch nicht verfügbar!

Suchvorgang

Stoppen zulassen

Bei aktivierter Option, lässt sich die Suche nach Viren oder unerwünschten Programmen jederzeit mit der Schaltfläche **Stopp** im Fenster des "Luke Filewalker" beenden. Haben Sie diese Einstellung deaktiviert, wird die Schaltfläche **Stopp** im Fenster "Luke Filewalker" grau unterlegt. Das vorzeitige Beenden eines Suchlaufs ist so nicht möglich! Diese Einstellung ist standardmäßig aktiviert.

Scanner-Priorität

Der Scanner unterscheidet bei der Direktsuche drei Prioritätsstufen. Dies ist nur wirksam, wenn auf dem Computer mehrere Prozesse gleichzeitig ablaufen. Die Wahl wirkt sich auf die Suchgeschwindigkeit aus.

Niedrig

Der Scanner erhält vom Betriebssystem nur dann Prozessorzeit zugewiesen, wenn kein anderer Prozess Rechenzeit benötigt, d.h. solange der Scanner alleine läuft, ist die Geschwindigkeit maximal. Insgesamt wird die Arbeit mit anderen Programmen dadurch sehr gut ermöglicht: Der Computer reagiert schneller, wenn andere Programme Rechenzeit benötigen, während dann der Scanner im Hintergrund weiterläuft. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Mittel

Der Scanner wird mit normaler Priorität ausgeführt. Alle Prozesse erhalten vom Betriebssystem gleich viel Prozessorzeit zugewiesen. Unter Umständen ist die Arbeit mit anderen Anwendungen beeinträchtigt.

Hoch

Der Scanner erhält höchste Priorität. Ein paralleles Arbeiten mit anderen Anwendungen ist kaum mehr möglich. Jedoch erledigt der Scanner seinen Suchlauf maximal schnell.

11.1.1.1. Aktion bei Fund

Aktion bei Fund

Sie können Aktionen festlegen, die der Scanner ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option erscheint während der Direktsuche bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Datei weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

Erlaubte Aktionen

In diesem Anzeigebereich können Sie diejenigen Aktionen auswählen, die beim Fund eines Virus bzw. unerwünschten Programms im Dialogfenster angezeigt werden. Sie müssen hierfür die entsprechenden Optionen aktivieren.

reparieren

Der Scanner repariert die betroffene Datei, falls dies möglich ist.

umbenennen

Der Scanner benennt die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und wieder um benannt werden.

Quarantäne

Der Scanner verschiebt die Datei in die Quarantäne. Die Datei kann vom Quarantänenanager aus wiederhergestellt werden kann, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden. Je nach Datei stehen im Quarantänenanager noch weitere Auswahlmöglichkeiten zur Verfügung.

löschen

Die Datei wird gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Die Virenerkennungsmuster kann wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

ignorieren

Die Datei wird belassen.

überschreiben und löschen

Der Scanner überschreibt die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Standard

Mit Hilfe dieser Schaltfläche können Sie die Aktion auswählen, die beim Fund eines Virus im Dialogfenster standardmäßig aktiviert ist. Markieren Sie die Aktion, die standardmäßig aktiviert sein soll, und klicken Sie auf die Schaltfläche **Standard**.



Hinweis

Die Aktion **reparieren** kann nicht als Standard-Aktion ausgewählt werden.

Weitere Informationen finden Sie hier.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Scanner reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der Scanner eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten primären bzw. sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt, wo die Datei wiederhergestellt werden kann, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie für weitere Untersuchungen an das Avira Malware Research Center senden.

Warnmeldungen anzeigen

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms eine Warnmeldung mit den Aktionen, die ausgeführt werden.

Primäre Aktion

Primäre Aktion, ist die Aktion die ausgeführt wird, wenn der Scanner einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option **reparieren** gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter **Sekundäre Aktion** gewählte Aktion ausgeführt.



Hinweis

Die Option Sekundäre Aktion ist nur dann auswählbar, wenn unter Primäre Aktion die Einstellung **reparieren** ausgewählt wurde.

reparieren

Bei aktivierter Option repariert der Scanner betroffene Dateien automatisch. Wenn der Scanner eine betroffene Datei nicht reparieren kann, führt es alternativ die unter Sekundäre Aktion gewählte Option aus.



Hinweis

Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der Scanner Dateien auf dem Computer verändert.

löschen

Bei aktivierter Option wird die Datei gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Damit kann die Virenerkennungsmuster wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

Bei aktivierter Option überschreibt der Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

umbenennen

Bei aktivierter Option benennt der Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.



Warnung

Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Quarantäne

Bei aktivierter Option verschiebt der Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Sekundäre Aktion

Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Einstellung reparieren ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.

löschen

Bei aktivierter Option wird die Datei gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Damit kann die Virenerkennungsmuster wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

Bei aktivierter Option überschreibt der Scanner die Datei mit einem Standardmuster und löscht sie anschließend (wipen). Sie kann nicht wiederhergestellt werden.

umbenennen

Bei aktivierter Option benennt der Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.



Warnung

Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Quarantäne

Bei aktivierter Option verschiebt der Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

11.1.1.2. Weitere Aktionen

Akustische Warnung

Akustische Warnung

Bei aktivierter Option spielt der Scanner bei einem Fund eine Tonfolge ab. Diese Einstellung ist standardmäßig aktiviert.

Wave Datei

In diesem Eingabefeld können Sie den Namen und den dazugehörigen Pfad einer Audiodatei Ihrer Wahl eintragen. Ist dieses Feld leer, wird der Standardwarnton verwendet.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei mit Hilfe des Datei-Explorers auszuwählen.

Test akustische Warnung

Diese Schaltfläche dient zum Testen der ausgewählten Wave Datei.

Bei der Suche in Archiven wendet der Scanner eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Die Dateien werden geprüft, dekomprimiert und noch einmal geprüft.

Archive durchsuchen

Bei aktivierter Option werden die in der Archiv-Liste markierten Archive geprüft. Diese Einstellung ist standardmäßig aktiviert.

Alle Archiv-Typen

Bei aktivierter Option werden alle Archivtypen in der Archiv-Liste markiert und geprüft.

Smart Extensions

Bei aktivierter Option erkennt der Scanner, ob es sich bei einer Datei um ein gepacktes Dateiformat (Archiv) handelt, auch wenn die Dateiendung von den gebräuchlichen Endungen abweicht, und prüft das Archiv. Dafür muss jedoch jede Datei geöffnet werden - was die Suchgeschwindigkeit verringert. Beispiel: Wenn ein *.zip-Archiv mit der Dateiendung *.xyz versehen ist, entpackt der Scanner auch dieses Archiv und prüft es. Diese Einstellung ist standardmäßig aktiviert.



Hinweis

Es werden nur diejenigen Archivtypen geprüft, die in der Archiv-Liste markiert sind.

Rekursionstiefe einschränken

Das Entpacken und Prüfen bei sehr tief geschachtelten Archiven kann sehr viel Rechnerzeit und -ressourcen benötigen. Bei aktivierter Option beschränken Sie die Tiefe der Suche in mehrfach gepackten Archiven auf eine bestimmte Zahl an Pack-Ebenen (Maximale Rekursionstiefe). So sparen Sie Zeit- und Rechnerressourcen.



Hinweis

Um einen Virus bzw. ein unerwünschtes Programm innerhalb eines Archivs zu ermitteln, muss der Scanner bis zu der Rekursions-Ebene scannen, in der sich der Virus bzw. das unerwünschte Programm befindet.

Maximale Rekursionstiefe

Um die maximale Rekursionstiefe eingeben zu können, muss die Option Rekursionstiefe einschränken aktiviert sein.

Sie können die gewünschte Rekursionstiefe entweder direkt eingeben oder aber mittels der Pfeiltasten rechts vom Eingabefeld ändern. Erlaubte Werte sind 1 bis 99. Der Standardwert ist 20 und wird empfohlen.

Standardwerte

Die Schaltfläche stellt die vordefinierten Werte für die Suche in Archiven wieder her.

11.1.1.3. Archiv-Liste

In diesem Anzeigebereich können Sie einstellen, welche Archive der Scanner durchsuchen soll. Sie müssen hierfür die entsprechenden Einträge markieren.

11.1.1.4. Ausnahmen

Vom Scanner auszulassende Dateiobjekte

Die Liste in diesem Fenster enthält Dateien und Pfade, die bei der Suche nach Viren bzw. unerwünschten Programmen vom Scanner nicht berücksichtigt werden sollen.

Bitte tragen Sie hier so wenige Ausnahmen wie möglich und wirklich nur Dateien ein, die aus welchen Gründen auch immer, bei einem normalen Suchlauf nicht geprüft werden sollen. Wir empfehlen, diese Dateien auf jeden Fall auf Viren bzw. unerwünschte Programme zu untersuchen, bevor sie in diese Liste aufgenommen werden!



Hinweis

Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.



Warnung

Diese Dateien werden bei einem Suchlauf nicht berücksichtigt!



Hinweis

Die in dieser Liste aufgenommenen Dateien werden in der Reportdatei vermerkt. Kontrollieren Sie bitte von Zeit zu Zeit die Reportdatei nach diesen nicht überprüften Dateien, denn vielleicht gibt es den Grund, aus dem Sie eine Datei hier ausgenommen haben gar nicht mehr. Dann sollten Sie den Namen dieser Datei aus der Liste wieder entfernen.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, der von der Direktsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei bzw. den gewünschten Pfad auszuwählen.

Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht auf Befehl überprüft. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht durchsucht.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.



Hinweis

Wenn Sie eine gesamte Partition zur Liste der auszunehmenden Dateiobjekte hinzufügen, werden nur die Dateien, die direkt unter der Partition gespeichert sind, von der Suche ausgenommen, jedoch nicht Dateien in Verzeichnissen auf der entsprechenden Partition:

Beispiel: Auszulassendes Dateiobjekt: `D:\ = D:\file.txt` wird von der Suche des Scanner ausgenommen, `D:\folder\file.txt` wird nicht von der Suche ausgenommen.

11.1.1.5. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Avira AntiVir für KEN! Suchengine.

Avira AntiVir für KEN! enthält sehr leistungsfähige Heuristiken, die auch unbekannte (neue) Viren, Würmer bzw. Trojaner entdecken kann. Dies geschieht durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Viren, Würmer oder Trojaner typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um einen Virus, einen Wurm oder um einen Trojaner handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Avira AntiVir für KEN! enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Win32 Dateiheuristik

Avira AntiVir für KEN! beinhaltet eine sehr leistungsfähige Heuristik für Windows Dateiviren, Würmer und Trojaner, die auch unbekannte Viren, Würmer und Trojaner erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option erkennt Avira AntiVir für KEN! etwas weniger Viren, Würmer bzw. Trojaner, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option erkennt Avira AntiVir für KEN! sehr viele unbekannte Viren, Würmer bzw. Trojaner, aber Sie müssen auch mit Fehlmeldungen rechnen.

11.1.2 Report

Der Scanner besitzt eine umfangreiche Protokollierfunktion. Damit erhalten Sie exakte Informationen über die Ergebnisse einer Direktsuche. Die Reportdatei enthält alle Einträge des Systems sowie Warnungen und Meldungen der Direktsuche.



Hinweis

Damit Sie bei einem Fund von Viren oder unerwünschten Programmen nachvollziehen können, welche Aktionen der Scanner ausgeführt hat, sollte immer eine Reportdatei erstellt werden.

Protokollierung

Aus

Bei aktivierter Option protokolliert der Scanner die Aktionen und Ergebnisse der Direktsuche nicht.

Standard

Bei aktivierter Option protokolliert der Scanner die Namen der betroffenen Dateien mit Pfadangabe. Zudem wird die Konfiguration für den aktuellen Suchlauf, Versionsinformationen und Informationen zum Lizenznehmer in die Reportdatei geschrieben.

Erweitert

Bei aktivierter Option protokolliert der Scanner zusätzlich zu den Standard-Informationen auch Warnungen und Hinweise.

Vollständig

Bei aktivierter Option protokolliert der Scanner zusätzlich alle durchsuchten Dateien. Zudem werden alle betroffenen Dateien sowie Warnungen und Hinweise mit in die Reportdatei aufgenommen.



Hinweis

Sollten Sie uns einmal eine Reportdatei zusenden müssen (zur Fehlersuche), bitten wir Sie, diese Reportdatei in diesem Modus zu erstellen.

11.2 Guard

Die Rubrik Guard der Avira AntiVir für KEN! Konfiguration ist für die Konfiguration der Echtzeitsuche zuständig.

11.2.1 Suche

Üblicherweise werden Sie Ihr System ständig überwachen wollen. Dafür nutzen Sie den Guard (Echtzeitsuche = On-Access-Scanner). Damit können Sie u.a. alle Dateien, die auf dem Computer kopiert oder geöffnet werden, "on the fly", nach Viren und unerwünschten Programmen durchsuchen lassen.

Suchmodus

Hier wird der Zeitpunkt für das Prüfen einer Datei festgelegt.

Beim Lesen durchsuchen

Bei aktivierter Option prüft der Guard die Dateien, bevor sie von einer Anwendung oder dem Betriebssystem gelesen oder ausgeführt werden.

Beim Schreiben durchsuchen

Bei aktivierter Option prüft der Guard eine Datei beim Schreiben. Erst nach diesem Vorgang können Sie wieder auf die Datei zugreifen.

Bei Lesen und Schreiben suchen

Bei aktivierter Option prüft der Guard Dateien vor dem Öffnen, Lesen und Ausführen und nach dem Schreiben. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Dateien

Der Guard kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von Ihrem Inhalt und Ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht.



Hinweis

Ist Alle Dateien aktiv, lässt sich die Schaltfläche Dateierweiterungen nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch von Avira AntiVir für KEN! übernommen. Dies bedeutet, dass Avira AntiVir für KEN! anhand des Inhalts einer Datei entscheidet, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als Dateierweiterungsliste verwenden, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird.



Hinweis

Ist Intelligente Dateiauswahl aktiv, lässt sich die Schaltfläche Dateierweiterungen nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche **Dateierweiterung** manuell editieren. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.



Hinweis

Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateierweiterungen gelöscht, wird dies durch den Text "Keine Dateierweiterungen" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateierweiterungen angezeigt werden, die bei einem Suchlauf im Modus **Dateierweiterungsliste verwenden** untersucht werden. Bei den Erweiterungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.



Hinweis

Beachten Sie bitte, dass sich die Dateierweiterungsliste von Version zu Version ändern kann.

Archive

Archive durchsuchen

Bei aktivierter Option werden Archive durchsucht. Die komprimierten Dateien werden durchsucht, dekomprimiert und noch einmal durchsucht. Standardmäßig ist die Option deaktiviert. Sie können mit weiteren Einstellungen die Suche in Archiven einschränken und die Rekursionstiefe der Suche festlegen. Dies wird empfohlen, wenn Sie die Archivsuche aktivieren.



Hinweis

Die Option ist standardmäßig deaktiviert, da der Prozess sehr viel Rechnerleistung in Anspruch nimmt. Generell wird empfohlen, Archive mit der Direktsuche zu prüfen.

Maximale Rekursionstiefe

Bei der Suche in Archiven kann der Guard eine rekursive Suche anwenden: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Sie können die Rekursionstiefe festlegen. Aktivieren Sie hierfür die Option. Erlaubte Werte sind 1 bis 20. Der Standardwert für die Rekursionstiefe ist 1 und wird empfohlen: Alle Archive, die direkt im Hauptarchiv liegen, werden entpackt und durchsucht.

Maximale Anzahl Dateien

Bei aktivierter Option können Sie die Suche auf eine maximale Anzahl von Dateien im Archiv beschränken. Erlaubte Werte sind 1 bis 99. Der Standardwert für die maximale Anzahl zu durchsuchender Dateien ist 10 und wird empfohlen.

Maximale Größe (KB)

Bei aktivierter Option können Sie die Suche auf eine maximale, zu entpackende Archivgröße beschränken. Erlaubte Werte sind 1 bis 9999 KB. Der Standardwert ist 1000 KB und wird empfohlen.

11.2.1.1. Aktion bei Fund

Aktion bei Fund

Sie können Aktionen festlegen, die der Guard ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option erscheint während der Echtzeitsuche bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Datei weiter geschehen soll. Diese Option ist standardmäßig aktiviert.

Erlaubte Aktionen

In diesem Anzeigebereich können Sie diejenigen Aktionen auswählen, die beim Fund eines Virus bzw. unerwünschten Programms im Dialogfenster angezeigt werden. Sie müssen hierfür die entsprechenden Optionen aktivieren.

reparieren

Der Guard repariert die betroffene Datei, falls dies möglich ist.

umbenennen

Der Guard benennt die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und wieder umbenannt werden.

Quarantäne

Der Guard verschiebt die Datei in die Quarantäne. Die Datei kann vom Quarantänenanager aus wiederhergestellt werden kann, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden. Je nach Datei stehen im Quarantänenanager noch weitere Auswahlmöglichkeiten zur Verfügung.

löschen

Die Datei wird gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Die Virenerkennungsmuster kann wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

ignorieren

Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

überschreiben und löschen

Der Guard überschreibt die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Zugriff verweigern

Der Zugriff auf die Datei wird verweigert. Der Guard trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.. Außerdem schreibt der Guard einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

Standard

Mit Hilfe dieser Schaltfläche können Sie die Aktion auswählen, die beim Fund eines Virus im Dialogfenster standardmäßig aktiviert ist. Markieren Sie die Aktion, die standardmäßig aktiviert sein soll, und klicken Sie auf die Schaltfläche **Standard**.



Hinweis

Die Aktion **reparieren** kann nicht als Standard-Aktion ausgewählt werden.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Guard reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der Guard eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten Primären bzw. Sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt. Sie kann vom Quarantänenanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie an das Avira Malware Research Center senden. Je nach Objekt stehen im Quarantänenanager noch weitere Auswahlmöglichkeiten zur Verfügung.

Warnmeldungen anzeigen

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms eine Warnmeldung mit den Aktionen, die ausgeführt werden.

Primäre Aktion

Primäre Aktion, ist die Aktion die ausgeführt wird, wenn der Guard einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option **reparieren** gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter **Sekundäre Aktion** gewählte Aktion ausgeführt.



Hinweis

Die Option Sekundäre Aktion ist nur dann auswählbar, wenn unter Primäre Aktion die Einstellung reparieren ausgewählt wurde.

reparieren

Bei aktivierter Option repariert der Guard betroffene Dateien automatisch. Wenn der Guard eine betroffene Datei nicht reparieren kann, führt es alternativ die unter Sekundäre Aktion gewählte Option aus.



Hinweis

Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der Guard Dateien auf dem Computer verändert.

löschen

Bei aktivierter Option wird die Datei gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Damit kann die Virenerkennungsmuster wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

Bei aktivierter Option überschreibt der Guard die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

umbenennen

Bei aktivierter Option benennt der Guard die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.



Warnung

Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Zugriff verweigern

Bei aktivierter Option trägt der Guard den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Guard einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

Quarantäne

Bei aktivierter Option verschiebt der Guard die Datei in ein Quarantäneverzeichnis. Die Dateien in diesem Verzeichnis können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Sekundäre Aktion

Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Option **reparieren** ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.

löschen

Bei aktivierter Option wird die Datei gelöscht, kann aber mit entsprechenden Tools (z.B. Avira UnErase) ggf. wiederhergestellt werden. Damit kann die Virenerkennungsmuster wieder gefunden werden. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

Bei aktivierter Option überschreibt der Guard die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

umbenennen

Bei aktivierter Option benennt der Guard die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.



Warnung

Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Zugriff verweigern

Bei aktivierter Option trägt der Guard den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Guard einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

Quarantäne

Bei aktivierter Option verschiebt der Guard die Datei in Quarantäne. Die Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

11.2.1.2. Weitere Aktionen

Benachrichtigungen

Ereignisprotokoll verwenden

Bei aktivierter Option wird bei jedem Fund ein Eintrag in das Ereignisprotokoll geschrieben. Der Administrator kann Funde erkennen und entsprechend reagieren. Diese Einstellung ist standardmäßig aktiviert.

Akustische Warnung

Bei aktivierter Option spielt der Guard bei einem Fund eine Tonfolge ab. Diese Einstellung ist standardmäßig aktiviert.

11.2.1.3. Ausnahmen

Mit diesen Optionen können Sie Ausnahme-Objekte für den Guard (Echtzeitsuche) konfigurieren. Die entsprechenden Objekte werden dann bei der Echtzeitsuche nicht beachtet. Der Guard kann über die Liste der auszulassenden Prozesse deren Dateizugriffe bei der Echtzeitsuche ignorieren. Dies ist zum Beispiel bei Datenbanken oder Backuplösungen sinnvoll.

Vom Guard auszulassende Prozesse

Alle Dateizugriffe von Prozessen in dieser Liste werden von der Überwachung durch den Guard ausgenommen.

Eingabefeld

In dieses Feld geben Sie den Namen des Prozesses ein, der von der Echtzeitsuche nicht berücksichtigt wird. Standardmäßig ist kein Prozess eingegeben. Die Namen des jeweiligen Prozesses erfahren Sie am einfachsten über den Taskmanager. Unter der Registerkarte "Prozesse" (englisch: "Processes") des Taskmanagers finden Sie die Namen aller aktuell aktiven Prozesse. Suchen Sie sich "Ihren" Prozess heraus und tragen Sie dessen Namen unter "Name" (englisch: "Image Name") ein.



Hinweis

Sie können bis zu 20 Prozesse eingeben.



Warnung:

Es werden nur die ersten 15 Zeichen des Prozessnamens (inklusive Dateierweiterung) berücksichtigt. Existieren 2 Prozesse, deren Namen in den ersten 15 Zeichen übereinstimmen, werden beide Prozesse von der Überwachung durch den Guard ausgenommen.



Warnung

Bitte beachten Sie, dass alle Dateizugriffe von Prozessen, die in der Liste vermerkt wurden, von der Suche nach Viren und unerwünschten Programmen ausgeschlossen sind! Der Windows Explorer und das Betriebssystem selbst können nicht ausgeschlossen werden. Ein entsprechender Eintrag in der Liste wird ignoriert.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen Prozess in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche entfernen Sie einen markierten Prozess aus dem Anzeigefenster.

Vom Guard auszulassende Dateiobjekte

Alle Dateizugriffe auf Objekte in dieser Liste werden von der Überwachung durch den Guard ausgenommen.



Hinweis

Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, welches von der Echtzeitsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, das gewünschte auszulassende Dateiobjekt auszuwählen.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche Löschen entfernen Sie ein markiertes Dateiobjekt aus dem Anzeigefenster.

Beachten Sie folgende Punkte:

- Die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) sind nur in Dateinamen erlaubt.
- Verzeichnisnamen müssen mit einem Backslash \ abgeschlossen sein, ansonsten wird ein Dateiname angenommen.
- Die Liste wird von oben nach unten abgearbeitet.
- Es können auch einzelne Dateierweiterungen ausgenommen werden (inklusive Platzhalter).
- Wenn ein Verzeichnis ausgenommen wird, werden automatisch auch alle darunter liegenden Verzeichnisse mit ausgenommen.
- Je länger die Liste ist, desto mehr Prozessorzeit braucht die Abarbeitung der Liste für jeden Zugriff. Halten Sie deshalb die Liste möglichst klein.
- Um Objekte auch dann auszunehmen, wenn darauf mit kurzen DOS-Dateinamen (DOS-Namenskonvention 8.3) zugegriffen wird, muss der entsprechende kurze Dateiname ebenfalls in die Liste eingetragen werden.



Hinweis

Ein Dateiname, der Platzhalter enthält, darf nicht mit einem Backslash abgeschlossen werden.

Beispielsweise:

C:\Programme\Anwendung\anwend* .exe\

Dieser Eintrag ist nicht gültig und wird nicht als Ausnahme behandelt!



Hinweis

Bei dynamischen Laufwerken, die als Verzeichnis auf einem anderen Laufwerk eingebunden (gemountet) werden, müssen Sie den Aliasnamen des Betriebssystems für das eingebundene Laufwerk in der Liste der Ausnahmen verwenden:

z.B. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\

Verwenden Sie den Bereitstellungspunkt (mount point) selbst, z.B.

,C:\DynDrive' wird das dynamische Laufwerk trotzdem durchsucht. Sie

können den zu verwendenden Aliasnamen des Betriebssystems aus der

Report-Datei des Guard ermitteln: Setzen Sie die Protokoll-Funktion des

Guard in der Konfiguration unter Guard :: Report auf **Vollständig**. Greifen

Sie nun mit dem aktivierten Guard auf das eingebundene Laufwerk zu. Sie

können nun den zu verwendenden Laufwerksnamen aus der Reportdatei des

Guard auslesen. Die Reportdatei rufen Sie im Control Center unter Lokaler

Schutz :: Guard ab.

Beispiele:

C:

C:\

C:*.*

C:*

*.exe

*.xl?

.

C:\Programme\Anwendung\anwendung.exe

C:\Programme\Anwendung\anwend*.exe

C:\Programme\Anwendung\anwend*

C:\Programme\Anwendung\anwend????.*

C:\Programme\

C:\Programme

C:\Programme\Anwendung*.mdb

11.2.1.4. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Avira AntiVir für KEN! Suchengine.

Avira AntiVir für KEN! enthält sehr leistungsfähige Heuristiken, die auch unbekannte (neue) Viren, Würmer bzw. Trojaner entdecken kann. Dies geschieht durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Viren, Würmer oder Trojaner typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um einen Virus, einen Wurm oder um einen Trojaner handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Avira AntiVir für KEN! enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Win32 Dateiheuristik

Avira AntiVir für KEN! beinhaltet eine sehr leistungsfähige Heuristik für Windows Dateiviren, Würmer und Trojaner, die auch unbekannte Viren, Würmer und Trojaner erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option erkennt Avira AntiVir für KEN! etwas weniger Viren, Würmer bzw. Trojaner, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option erkennt Avira AntiVir für KEN! sehr viele unbekannte Viren, Würmer bzw. Trojaner, aber Sie müssen auch mit Fehlmeldungen rechnen.

11.2.2 Report

Der Guard besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Guard kein Protokoll.

Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Guard wichtige Informationen (zu Fund, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Guard auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Guard sämtliche Informationen - auch solche zu Dateigröße, Dateityp, Datum etc. - in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Diese Einstellung ist standardmäßig aktiviert, mit einem Wert von 1 MB. Hierbei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe -50 Kilobytes erreicht worden ist.

Reportdatei vor dem Kürzen sichern

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration der Echtzeitsuche in die Reportdatei geschrieben.

11.3 Allgemeines

11.3.1 Email

Avira AntiVir für KEN! kann bei bestimmten Ereignissen, Warnungen und Nachrichten per Email an einen oder mehrere Empfänger senden. Dafür wird das Simple Message Transfer Protocol (SMTP) verwendet.

Die Nachrichten können hierbei durch unterschiedliche Ereignisse ausgelöst werden. Unterstützt wird die Versendung von Emails durch folgende Module:

- Email Warnungen vom Guard
- Email Warnungen vom Scanner
- Untersuchungsanfragen von verdächtigen Dateien an das Avira Malware Research Center



Hinweis

Bitte beachten Sie, dass kein ESMTP unterstützt wird. Zudem ist eine verschlüsselte Übertragung per TLS (Transport Layer Security) oder SSL (Secure Sockets Layer) derzeit noch nicht möglich.

Email-Nachrichten

SMTP-Server

Geben Sie hier den Namen des zu verwendenden Hosts an - entweder seine IP-Adresse oder den direkten Hostnamen.

Die maximal mögliche Länge des Hostnamens beträgt 127 Zeichen.

Beispielsweise:

192.168.1.100 oder mail.musterfirma.de.

Absenderadresse

Geben Sie in diesem Feld die Email-Adresse des Absenders an. Die Absenderadresse darf maximal 127 Zeichen lang sein.

Authentifizierung

Einige Mailserver erwarten, dass sich ein Programm vor dem Versenden einer Email gegenüber dem Server authentifiziert (anmeldet). Warnungen per Email kann Avira AntiVir für KEN! mit Authentifizierung an SMTP-Server übergeben.

Authentifizierung verwenden

Bei aktivierter Option kann für die Anmeldung (Authentifizierung) ein Benutzername und ein Kennwort in die entsprechenden Felder eingegeben werden.

- **Benutzername:** Geben Sie hier Ihren Benutzernamen ein.
- **Kennwort:** Geben Sie hier das entsprechende Kennwort ein. Das Kennwort wird verschlüsselt gespeichert. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Test Email senden

Mit Klick auf die Schaltfläche, versucht Avira AntiVir für KEN!, zur Überprüfung der eingegebenen Daten, eine Test-Email an die Absenderadresse zu senden.

11.3.2 Erweiterte Gefahrenkategorien

Auswahl erweiterter Gefahrenkategorien

Avira AntiVir für KEN! schützt Sie vor Computerviren.

Darüber hinaus haben Sie die Möglichkeit, differenziert nach folgenden erweiterten Gefahrenkategorien suchen zu lassen.

- Backdoor-Steuerungssoftware (BDC)
- Kostenverursachende Einwahlprogramme (DIALER)
- Spiele (GAMES)
- Witzprogramme (JOKES)
- Security Privacy Risk (SPR)
- Adware/Spyware (ADSPY)
- Ungewöhnliche Laufzeitpacker (PCK)
- Dateien mit verschleierte Dateieindungen (HEUR-DBLEXT)
- Phishing
- Anwendung (APPL)

Durch einen Klick auf das entsprechende Kästchen wird der gewählte Typ aktiviert (Häkchen gesetzt) bzw. deaktiviert (kein Häkchen).

Alle aktivieren

Bei aktivierter Option werden sämtliche Typen aktiviert.

Standardwerte

Diese Schaltfläche stellt die vordefinierten Standardwerte wieder her.



Hinweis

Wird ein Typ deaktiviert, werden Dateien, die als entsprechender Programmtyp erkannt werden, nicht mehr gemeldet. Es erfolgt auch kein Eintrag in die Reportdatei.

11.3.3 Kennwort

Sie können Avira AntiVir für KEN! in unterschiedlichen Bereichen durch ein Kennwort schützen. Wurde ein Kennwort vergeben, werden Sie jedes Mal nach diesem Kennwort gefragt, wenn Sie den jeweils geschützten Bereich öffnen wollen.

Kennwort

Kennwort eingeben

Geben Sie hier Ihr gewünschtes Kennwort ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt. Sie können maximal 19 Zeichen eingeben. Ist das Kennwort einmal angegeben, verweigert das Programm bei Angabe eines falschen Kennworts den Zugriff. Ein leeres Feld bedeutet "Kein Kennwort".

Kennwort bestätigen

Geben Sie hier das oben eingetragene Kennwort zur Bestätigung erneut ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.



Hinweis

Groß- und Kleinschreibung wird unterschieden!

Kennwort geschützte Bereiche

Avira AntiVir für KEN! kann einzelne Bereiche durch ein Kennwort schützen. Durch Klick auf das entsprechende Kästchen kann die Kennwortabfrage für einzelne Bereiche nach Wunsch deaktiviert bzw. wieder aktiviert werden.

Kennwortgeschützer Bereich	Funktion
Control Center	Bei aktivierter Option wird zum Start des Control Center ein Kennwort benötigt.
Guard aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung von AntiVir Guard das gesetzte Kennwort benötigt.
Hinzufügen und Ändern von Aufträgen	Bei aktivierter Option wird beim Hinzufügen und Ändern von Aufträgen im Planer ein Kennwort benötigt.
Produktupdates starten	Bei aktivierter Option wird beim Starten des Produktupdates im Menü Update ein Kennwort benötigt.
Rescue-CD aus Internet herunterladen	Bei aktivierter Option wird für den Start des Downloads der Avira Rescue-CD ein Kennwort benötigt.

Kennwortgeschützer Bereich	Funktion
Quarantäne	Bei aktivierter Option werden alle möglichen Bereiche des Quarantänenamangers, die durch ein Kennwort schützbar sind, aktiviert. Durch Klick auf das entsprechende Kästchen, kann die Kennwortabfrage nach Wunsch deaktiviert bzw. wieder aktiviert werden.
Wiederherstellen betroffener Objekte	Bei aktivierter Option wird zum Wiederherstellen eines Objekts ein Kennwort benötigt.
Reparieren betroffener Objekte	Bei aktivierter Option wird zur Reparatur eines Objekts ein Kennwort benötigt.
Eigenschaften betroffener Objekte	Bei aktivierter Option wird zur Anzeige der Eigenschaften eines Objekts ein Kennwort benötigt.
Löschen betroffener Objekte	Bei aktivierter Option wird für das Löschen eines Objekts ein Kennwort benötigt.
Email an AntiVir senden	Bei aktivierter Option wird für das Versenden eines Objekts zur Überprüfung an das Avira Malware Research Center ein Kennwort benötigt.
Konfiguration	Bei aktivierter Option ist die Konfiguration von Avira AntiVir für KEN! nur nach Eingabe des gesetzten Kennworts möglich.
Expertenmodus aktivieren	Bei aktivierter Option wird zur Aktivierung des Expertenmodus ein Kennwort benötigt.
Installation / Deinstallation	Bei aktivierter Option wird zur Installation bzw. Deinstallation von Avira AntiVir für KEN! ein Kennwort benötigt.

11.3.4 Sicherheit

Update**Warnung, falls letztes Update älter als n Tag(e)**

In diesem Feld können Sie die Anzahl an Tagen eingeben, die seit dem letzten Update von Avira AntiVir für KEN! maximal vergangen sein dürfen. Ist dieses Alter überschritten, wird ein Warnhinweis unter Planer angezeigt.

Hinweis anzeigen, falls Virendefinitionsdatei veraltet

Bei aktivierter Option erhalten Sie eine Warnmeldung, im Fall einer veralteten Virendefinitionsdatei. Mit Hilfe der Option Warnung, falls letztes Update älter als n Tag(e), können Sie den zeitlichen Abstand zur Warnmeldung konfigurieren.

Konfigurationsdatei vor unerwünschten Änderungen schützen**Konfiguration schützen**

Bei aktivierter Option kann die Avira AntiVir für KEN! Konfiguration nur mit Administrator-Rechten gespeichert werden.

**Warnung**

Diese Option ist nur wirksam, wenn Avira AntiVir für KEN! auf einer NTFS-Partition installiert ist.

Aufträge schützen

Bei aktivierter Option kann nur ein Benutzer mit Administratorrechten bereits bestehende Prüf- und Updateaufträge ändern sowie selbst erstellte Aufträge schützen.

Prozesse schützen**AntiVir Prozesse vor unerwünschtem Beenden schützen**

Bei aktivierter Option werden die AntiVir Prozesse vor unerwünschtem Beenden durch Viren und Malware oder vor einem 'unkontrollierten' Beenden durch einen Benutzer z.B. via Task-Manager geschützt. Diese Option ist standardmäßig aktiviert.

**Wichtig**

Der Prozess-Schutz ist für 64-Bit-Systeme noch nicht verfügbar!

11.3.5 Verzeichnisse

Temporärer Pfad

In diesem Eingabefeld tragen Sie den temporären Pfad ein, mit dem Avira AntiVir für KEN! arbeitet.

Systemeinstellung verwenden

Bei aktivierter Option werden für die Handhabung von temporären Dateien die Einstellungen des Systems verwendet.



Hinweis

Wo Ihr System temporäre Dateien speichert finden Sie - am Beispiel von Windows XP - unter: Start | Einstellungen | Systemsteuerung | System | Registerkarte "Erweitert" | Schaltfläche "Umgebungsvariablen". Die temporären Variablen (TEMP, TMP) für den jeweils angemeldeten Benutzer als auch für Systemvariablen (TEMP, TMP) sind hier mit ihren entsprechenden Werten ersichtlich.

Verwende folgendes Verzeichnis

Bei aktivierter Option wird der im Eingabefeld angezeigte Pfad verwendet.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, den gewünschten temporären Pfad auszuwählen.

Standard

Die Schaltfläche stellt das vordefinierte Verzeichnis für den temporären Pfad wieder her.

11.3.6 Update

Die Rubrik **Update** der Avira AntiVir für KEN! Konfiguration ist für die Konfiguration des Updaters zuständig.

Produktupdates

Produktupdates herunterladen und automatisch installieren

Bei aktivierter Option werden Produktupdates heruntergeladen und automatisch von KEN! Updater installiert, sobald Produktupdates verfügbar sind. Updates der Virendefinitionsdatei und der Suchengine erfolgen immer und unabhängig von dieser Einstellung. Voraussetzungen für diese Option sind: Die vollständige Konfiguration des Updates und eine bestehende Verbindung zu einem Download-Server.

Benachrichtigung, wenn neue Produktupdates verfügbar sind

Bei aktivierter Option werden Sie nur benachrichtigt, wenn neue Produktupdates verfügbar sind. Updates der Virendefinitionsdatei und der Suchengine erfolgen immer und unabhängig von dieser Einstellung. Voraussetzungen für diese Option sind: Die vollständige Konfiguration des Updates und eine bestehende Verbindung zu einem Download-Server. Die Benachrichtigung erfolgt über eine Desktopbenachrichtigung in Form eines Popup-Fensters und über eine Warnmeldung des KEN! Updater im Control Center unter Verwaltung ::Planer.

Keine Produktupdates herunterladen

Bei aktivierter Option erfolgen keine automatischen Produktupdates oder Benachrichtigungen zu verfügbaren Produktupdates durch KEN! Updater. Updates der Virendefinitionsdatei und der Suchengine erfolgen immer und unabhängig von dieser Einstellung.

**Wichtig**

Ein Update der Virendefinitionsdatei und der Suchengine erfolgt bei jedem ausgeführten Update unabhängig von den Einstellungen zum Produktupdate (siehe dazu Kap. Updates).

11.3.6.1. Webserver

Webserver

Das Update kann direkt über einen Webserver im Internet durchgeführt werden.

Verbindung zum Webserver**Vorhandene Verbindung (Netzwerk) verwenden**

Diese Einstellung wird angezeigt, wenn Ihre Verbindung über ein Netzwerk verwendet wird.

Die folgende Verbindung verwenden:

Diese Einstellung wird angezeigt, wenn Sie Ihre Verbindung individuell definieren.

Der Avira AntiVir für KEN! Updater erkennt automatisch, welche Verbindungsoptionen vorhanden sind. Nicht vorhandene Verbindungsoptionen sind grau hinterlegt und können nicht aktiviert werden. Eine DFÜ-Verbindung können Sie z.B. manuell über einen Telefonbucheintrag in Windows herstellen.

- **Benutzer:** Geben Sie den Benutzernamen Ihres ausgewählten Kontos ein.
 - **Kennwort:** Geben Sie das Kennwort für dieses Konto ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.
-

**Hinweis**

Wenden Sie sich an den Internetdienstanbieter, wenn Sie den Benutzernamen oder das Kennwort eines vorhandenen Internetkontos vergessen haben.

**Hinweis**

Die automatische Einwahl des Updaters über sogenannte Dial-Up Tools (z.B. SmartSurfer, Oleco, ...) steht momentan in Avira AntiVir für KEN! noch nicht zur Verfügung.

Eine für das Update geöffnete DFÜ-Verbindung wieder beenden

Bei aktivierter Option wird die für das Update geöffnete DFÜ-Verbindung automatisch wieder unterbrochen, sobald der Download erfolgreich durchgeführt wurde.

Proxy

Proxyserver

Keinen Proxyserver verwenden

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver nicht über einen Proxyserver.

Windows Systemeinstellungen verwenden

Bei aktivierter Option werden die aktuellen Windows Systemeinstellungen für die Verbindung zum Webserver über einen Proxyserver verwendet.

Verbindung über diesen Proxyserver

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver über einen Proxyserver, wobei die von Ihnen angegebenen Einstellungen verwendet werden.

Adresse

Geben Sie die URL oder IP-Adresse des Proxyservers ein, den Sie für das Verbinden mit dem Webserver verwenden möchten.

Port

Geben Sie die Port-Nummer des Proxyservers ein, den Sie für das Verbinden mit dem Webserver verwenden möchten.

Login Name

Geben Sie Ihren Login Anmelde-Name am Proxyserver ein.

Login Kennwort

Geben Sie das entsprechende Kennwort für die Anmeldung am Proxyserver ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Beispiele:

Adresse: prox.domain.de Port: 8080

Adresse: 192.168.1.100 Port: 3128

11.3.7 Warnungen

11.3.7.1. Netzwerk

Netzwerk

Sie können individuell konfigurierbare Warnungen vom Scanner bzw. vom Guard an beliebige Computer in Ihrem Netzwerk senden.

**Hinweis**

Prüfen Sie, ob der "Nachrichtendienst" gestartet ist. Den Dienst finden Sie (am Beispiel von Windows XP) unter "Start | Einstellungen | Systemsteuerung | Verwaltung | Dienste".

**Hinweis**

Eine Warnung wird immer an Computer versendet, NICHT an einen bestimmten Nutzer.

Nachricht senden an

Die Liste in diesem Fenster zeigt Namen von Computern, die bei einem Fund eine Nachricht erhalten.

**Hinweis**

Ein Computer kann immer nur einmal in dieser Liste eingetragen werden.

Einfügen

Mit dieser Schaltfläche können Sie einen weiteren Computer hinzufügen. Es öffnet sich ein Fenster, in das Sie den Namen neuen Computers eingeben können. Ein Computernamen kann maximal 15 Zeichen lang sein.



Die Schaltfläche öffnet ein Fenster, in dem Sie alternativ die Möglichkeit haben, direkt einen Computer aus Ihrer Netzwerkumgebung auszuwählen.

Löschen

Mit dieser Schaltfläche können Sie den aktuell markierten Eintrag aus der Liste löschen.

Guard

Netzwerkwarnungen

Bei aktivierter Option werden Netzwerkwarnungen gesendet. Standardmäßig ist diese Option deaktiviert.



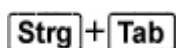
Hinweis

Um diese Option aktivieren zu können, muss unter Allgemeines :: Warnungen :: Netzwerk mindestens ein Empfänger eingetragen sein.

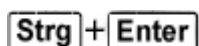
Zu sendende Nachricht

Das Fenster zeigt die Nachricht, die bei einem Fund an den gewählten Computer gesendet wird. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombinationen können Sie zum Formatieren der Nachricht verwenden:



fügt einen Tabulator ein. Die aktuelle Zeile wird um einige Zeichen nach rechts eingerückt.



fügt einen Zeilenumbruch ein.

Die Nachricht kann außerdem Platzhalter für die während der Suche ermittelten Informationen enthalten. Diese Platzhalter werden beim Versenden durch den eigentlichen Text ersetzt.

Folgende Platzhalter sind verwendbar:

%VIRUS%	enthält den Namen des gefundenen Virus bzw. des unerwünschten Programms
%FILE%	enthält den Pfad und Dateinamen der betroffenen Datei
%COMPUTER%	enthält den Namen des Computers, auf dem der Guard läuft
%NAME%	enthält den Namen des Benutzers, der auf die betroffene Datei zugegriffen hat
%ACTION%	enthält die Aktion, die nach dem Fund des Virus ausgeführt wurde
%MACADDR%	enthält die MAC-Adresse des Computers, auf dem der Guard läuft

Standard

Die Schaltfläche stellt den vordefinierten Standardtext für einen Warnhinweis wieder her.

Scanner

Netzwerkwarnungen aktivieren

Bei aktivierter Option werden Netzwerkwarnungen gesendet. Standardmäßig ist diese Option deaktiviert.



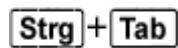
Hinweis

Um diese Option aktivieren zu können, muss unter Allgemeines :: Warnungen :: Netzwerk mindestens ein Empfänger eingetragen sein.

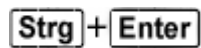
Zu sendende Nachricht

Das Fenster zeigt die Nachricht, die bei einem Fund an den gewählten Computer gesendet wird. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombinationen können Sie zum Formatieren der Nachricht verwenden:



fügt einen Tabulator ein. Die aktuelle Zeile wird um einige Zeichen nach rechts eingerückt.



fügt einen Zeilenumbruch ein.

Die Nachricht kann außerdem Platzhalter für die während der Suche ermittelten Informationen enthalten. Diese Platzhalter werden beim Versenden durch den eigentlichen Text ersetzt.

Folgende Platzhalter sind verwendbar:

- | | |
|---------|---|
| %VIRUS% | enthält den Namen des gefundenen Virus bzw. des unerwünschten Programms |
| %NAME% | enthält den Namen des eingeloggten Benutzers, der den Scanner ausführt |

Standard

Die Schaltfläche stellt den vordefinierten Standardtext für einen Warnhinweis wieder her.

11.3.7.2. Email

Guard

AntiVir Guard kann bei bestimmten Ereignissen Warnungen per Email an einen oder mehrere Empfänger senden.

Guard

Email Warnungen

Bei aktivierter Option sendet AntiVir Guard Email-Nachrichten mit den wichtigsten Daten, wenn ein bestimmtes Ereignis eintritt. Standardmäßig ist diese Option deaktiviert.

Benachrichtigung per Email bei folgenden Ereignissen

- **Bei der Echtzeitsuche wurde ein Fund gemeldet**
Bei aktivierter Option erhalten Sie eine Email mit dem Namen des Virus oder unerwünschten Programms und der betroffenen Datei immer dann, wenn die Echtzeitsuche einen Virus bzw. ein unerwünschtes Programm findet.
- **Innerhalb des Guard ist ein kritischer Fehler aufgetreten**
Bei aktivierter Option erhalten Sie eine Email, wenn Avira AntiVir für KEN! einen internen kritischen Fehler feststellt.



Hinweis

Bitte informieren Sie in diesem Fall unseren Technischen Support und senden Sie die in der Email angegebenen Daten mit. Die angegebene Datei sollte ebenfalls zur Prüfung mit gesendet werden.

Empfänger

In diesem Feld geben Sie die Email-Adresse(n) des oder der Empfänger an. Die einzelnen Adressen werden durch Kommas getrennt. Die maximale Länge aller Adressen zusammen (also der gesamten Zeichenkette) beträgt 260 Zeichen.

Scanner

Die Direktsuche, d.h. die Suche auf Verlangen, kann bei bestimmten Ereignissen Warnungen per Email an einen oder mehrere Empfänger senden.

Scanner

Email Warnungen aktivieren

Bei aktivierter Option sendet Avira AntiVir für KEN! Email-Nachrichten mit den wichtigsten Daten, wenn ein bestimmtes Ereignis eintritt. Standardmäßig ist diese Option deaktiviert.

Benachrichtigung per Email bei folgenden Ereignissen

- **Bei der Suche wurde ein Fund gemeldet**
Bei aktivierter Option erhalten Sie eine Email mit dem Namen des Virus oder unerwünschten Programms und der betroffenen Datei immer dann, wenn die Direktsuche einen Virus bzw. ein unerwünschtes Programm findet.

– **Ende eines geplanten Suchlaufs**

Bei aktivierter Option wird eine Email versendet, wenn ein Prüfauftrag ausgeführt wurde. Die Email enthält Daten zum Zeitpunkt und zur Dauer des Suchlaufs, zu den durchsuchten Verzeichnissen und Dateien sowie zu Virenfunden und Warnungen.

Empfängeradresse(n)

In diesem Feld geben Sie die Email-Adresse(n) des oder der Empfänger an. Die einzelnen Adressen werden durch Kommas getrennt. Die maximale Länge aller Adressen zusammen (also der gesamten Zeichenkette) beträgt 260 Zeichen.

11.3.8 Ereignisse

Größe der Ereignisdatenbank begrenzen

Größe begrenzen auf maximal n Einträge

Bei aktivierter Option kann die maximale Anzahl der Einträge in der Ereignisdatenbank auf eine bestimmte Größe begrenzt werden; erlaubte Werte sind: 100 bis 10 000 Einträge. Wird die Anzahl der eingegebenen Einträge überschritten, werden die jeweils ältesten Einträge gelöscht.

Alle Ereignisse löschen älter als n Tag(e)

Bei aktivierter Option werden Ereignisse nach einer gewissen Anzahl von Tagen aus der Ereignisdatenbank gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Datenbankgröße nicht begrenzen (Ereignisse manuell löschen)

Bei aktivierter Option ist die Größe der Ereignisdatenbank nicht begrenzt. Im Control Center unter Ereignisse werden jedoch maximal 20 000 Einträge angezeigt.

11.3.9 Berichte begrenzen

Anzahl der Berichte begrenzen

Anzahl begrenzen auf n Stück

Bei aktivierter Option kann die maximale Anzahl von Berichten auf eine bestimmte Menge begrenzt werden; erlaubte Werte sind: 1 bis 300. Wird die angegebene Anzahl überschritten, werden die jeweils ältesten Berichte gelöscht.

Alle Berichte löschen älter als n Tag(e)

Bei aktivierter Option werden Berichte nach einer gewissen Anzahl von Tagen automatisch gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Anzahl der Berichte nicht begrenzen (Berichte manuell löschen)

Bei aktivierter Option ist die Anzahl der Berichte nicht begrenzt.



Avira GmbH

Lindauer Str. 21
88069 Tettnang
Germany
Telefon: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: <http://www.avira.de>

© Avira GmbH. Alle Rechte vorbehalten.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. 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 Q3-2008

AntiVir[®] ist ein registriertes Warenzeichen der Avira GmbH. Alle anderen Marken- und Produkt-namen 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.