

# Avira AntiVir Professional

Handbuch für Anwender

---

## 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 Professional 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 Professional unter Third Party Licenses.

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung .....</b>	<b>1</b>
<b>2</b>	<b>Symbole und Hervorhebungen.....</b>	<b>2</b>
<b>3</b>	<b>Produktinformationen .....</b>	<b>3</b>
3.1	Leistungsumfang.....	3
3.2	Systemvoraussetzungen.....	4
3.3	Lizenzierung und Upgrade .....	4
3.3.1	Lizenzverwaltung.....	5
<b>4</b>	<b>Installation und Deinstallation .....</b>	<b>7</b>
4.1	Installation .....	7
4.2	Änderungsinstallation.....	11
4.3	Installationsmodule .....	12
4.4	Deinstallation .....	13
4.5	Installation und Deinstallation im Netzwerk.....	13
4.5.1	Installation im Netzwerk.....	14
4.5.2	Deinstallation im Netzwerk.....	15
4.5.3	Kommandozeilenparameter für das Setup-Programm .....	15
4.5.4	Parameter der Datei setup.inf.....	16
<b>5</b>	<b>Überblick .....</b>	<b>20</b>
5.1	Oberfläche und Bedienung .....	20
5.1.1	Control Center .....	20
5.1.2	Konfiguration.....	23
5.1.3	Tray Icon .....	27
5.2	So wird es gemacht.....	28
5.2.1	Lizenz aktivieren.....	28
5.2.2	Automatisierte Updates durchführen .....	28
5.2.3	Ein Update manuell starten .....	30
5.2.4	Direktsuche: Mit einem Suchprofil nach Viren und Malware suchen .....	30
5.2.5	Direktsuche: Per Drag & Drop nach Viren und Malware suchen.....	32
5.2.6	Direktsuche: Über das Kontextmenü nach Viren und Malware suchen .....	32
5.2.7	Direktsuche: Automatisiert nach Viren und Malware suchen .....	33
5.2.8	Direktsuche: Gezielt nach aktiven Rootkits suchen.....	34
5.2.9	Auf gefundene Viren und Malware reagieren.....	34
5.2.10	Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen .....	39
5.2.11	Quarantäne: Dateien in der Quarantäne wiederherstellen.....	40
5.2.12	Quarantäne: Verdächtige Datei in die Quarantäne verschieben.....	42
5.2.13	Suchprofil: Dateityp in einem Suchprofil ergänzen oder löschen.....	42
5.2.14	Suchprofil: Desktop-Verknüpfung für Suchprofil erstellen .....	43
5.2.15	Ereignisse: Ereignisse filtern.....	43
5.2.16	MailGuard: Email-Adressen von der Prüfung ausschließen.....	44
5.2.17	FireWall: Sicherheitsstufe für die FireWall wählen .....	44

<b>6</b>	<b>Scanner .....</b>	<b>47</b>
<b>7</b>	<b>Updates.....</b>	<b>49</b>
<b>8</b>	<b>Avira FireWall :: Überblick.....</b>	<b>52</b>
<b>9</b>	<b>Problembhebung, Tipps .....</b>	<b>54</b>
9.1	Hilfe im Problemfall .....	54
9.2	Tastaturbefehle.....	58
9.2.1	In Dialogfeldern .....	58
9.2.2	In der Hilfe .....	59
9.2.3	Im Control Center .....	59
9.3	Windows Sicherheitscenter.....	61
9.3.1	Allgemeines .....	61
9.3.2	Das Windows Sicherheitscenter und Ihr AntiVir Programm.....	61
<b>10</b>	<b>Viren und mehr .....</b>	<b>65</b>
10.1	Gefahrenkategorien.....	65
10.2	Viren sowie sonstige Malware.....	68
<b>11</b>	<b>Info und Service .....</b>	<b>72</b>
11.1	Kontaktadresse.....	72
11.2	Technischer Support.....	72
11.3	Verdächtige Datei .....	72
11.4	Fehlalarm melden.....	73
11.5	Ihr Feedback für mehr Sicherheit.....	73
<b>12</b>	<b>Referenz: Konfigurationsoptionen .....</b>	<b>74</b>
12.1	Scanner .....	74
12.1.1	Suche .....	74
12.1.1.1.	Aktion bei Fund.....	77
12.1.1.2.	Weitere Aktionen .....	80
12.1.1.3.	Ausnahmen .....	81
12.1.1.4.	Heuristik .....	82
12.1.2	Report.....	83
12.2	Guard .....	84
12.2.1	Suche .....	84
12.2.1.1.	Aktion bei Fund.....	86
12.2.1.2.	Weitere Aktionen .....	89
12.2.1.3.	Ausnahmen .....	90
12.2.1.4.	Heuristik .....	94
12.2.2	ProActiv.....	95
12.2.2.1.	Anwendungsfilter: Zu blockierende Anwendungen .....	96
12.2.2.2.	Anwendungsfilter: Erlaubte Anwendungen .....	97
12.2.3	Report.....	98
12.3	MailGuard.....	99
12.3.1	Suche .....	99
12.3.1.1.	Aktion bei Fund.....	101
12.3.1.2.	Andere Aktionen .....	103
12.3.1.3.	Heuristik .....	103
12.3.2	Allgemeines .....	104
12.3.2.1.	Ausnahmen .....	104
12.3.2.2.	Zwischenspeicher.....	105
12.3.2.3.	Fußzeile.....	105
12.3.3	Report.....	106

12.4	Firewall .....	107
12.4.1	Adapterregeln.....	107
12.4.1.1.	Eingehende Regeln.....	110
12.4.1.2.	Ausgehende Regeln .....	117
12.4.2	Anwendungsregeln.....	118
12.4.3	Vertrauenswürdige Anbieter.....	121
12.4.4	Einstellungen .....	122
12.4.5	Popup-Einstellungen.....	123
12.5	FireWall unter SMC.....	125
12.5.1	Allgemeine Einstellungen .....	125
12.5.2	Allgemeine Adapterregeln.....	126
12.5.2.1.	Eingehende Regeln.....	129
12.5.2.2.	Ausgehende Regeln .....	136
12.5.3	Anwendungsliste.....	137
12.5.4	Vertrauenswürdige Anbieter.....	138
12.5.5	Weitere Einstellungen.....	139
12.5.6	Anzeigeinstellungen.....	140
12.6	WebGuard.....	141
12.6.1	Suche .....	141
12.6.1.1.	Aktion bei Fund.....	142
12.6.1.2.	Gespernte Zugriffe.....	144
12.6.1.3.	Ausnahmen .....	145
12.6.1.4.	Heuristik .....	148
12.6.2	Report.....	149
12.7	Update .....	150
12.7.1	Produktupdate .....	151
12.7.2	Neustart-Einstellungen.....	152
12.7.3	Dateiserver .....	153
12.7.4	Webserver.....	154
12.7.4.1.	Proxy .....	155
12.8	Allgemeines .....	156
12.8.1	Email.....	156
12.8.2	Gefahrenkategorien .....	157
12.8.3	Kennwort .....	157
12.8.4	Sicherheit .....	159
12.8.5	WMI.....	160
12.8.6	Verzeichnisse .....	161
12.8.7	Warnungen.....	162
12.8.7.1.	Netzwerk .....	162
12.8.7.2.	Email.....	164
12.8.7.3.	Akustische Warnungen .....	171
12.8.7.4.	Warnungen.....	172
12.8.8	Ereignisse .....	172
12.8.9	Berichte begrenzen .....	173

# 1 Einleitung

Mit Ihrem AntiVir Programm schützen Sie Ihren Computer vor Viren, Würmern, Trojanern, Ad- und Spyware sowie weiteren Gefahren. Verkürzend wird in diesem Handbuch von Viren oder Malware (Schadsoftware) und unerwünschten Programmen gesprochen.

Das Handbuch beschreibt die Installation und Bedienung des Programms.

Auf unserer Webseite können Sie vielfältige Optionen und weitere Informationsmöglichkeiten nutzen:

<http://www.avira.de>

Sie können auf der Avira Webseite...

- Informationen zu weiteren AntiVir Desktop-Programmen abrufen
- die aktuellsten AntiVir Desktop-Programme herunterladen
- die aktuellsten Produkthandbücher im Format PDF herunterladen
- kostenfreie Support- und Reparatur-Werkzeuge herunterladen
- die umfassenden Wissensdatenbank und FAQ-Artikel bei der Behebung von Problemen nutzen
- die landesspezifischen Supportadressen abrufen.

Ihr Avira Team

## 2 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

<b>Symbol / Bezeichnung</b>	<b>Erläuterung</b>
✓	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.
<b>Warnung</b>	Steht vor einer Warnung bei Gefahr von kritischem Datenverlust.
<b>Hinweis</b>	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung Ihres AntiVir Programms erleichtert.

Folgende Hervorhebungen werden verwendet:

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

## 3 Produktinformationen

In diesem Kapitel erhalten Sie alle Informationen, die für den Erwerb und Einsatz Ihres AntiVir Produkts relevant sind:

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

AntiVir Programme bieten umfassende und flexible Werkzeuge, 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 Ihres AntiVir Programms über automatische Updates sicher. Konfigurieren Sie das Programm entsprechend.

### 3.1 Leistungsumfang

Ihr AntiVir Programm verfügt über folgende Funktionen:

- Control Center zur Überwachung, Administration und Steuerung des gesamten Programms
- Zentrale Konfiguration mit benutzerfreundlicher Standard- und Expertenkonfiguration und kontextsensitiver Hilfe
- Scanner (On-Demand Scan) mit profilgesteuerter und konfigurierbarer Suche nach allen bekannten Typen von Viren und Malware
- Integration in die Windows Vista Benutzerkontensteuerung (User Account Control), um Aufgaben durchführen zu können, für die administrative Rechte erforderlich sind.
- Guard (On-Access Scan) zur ständigen Überwachung sämtlicher Dateizugriffe
- ProActiv-Komponente zur permanenten Überwachung von Programmaktionen (Nur für 32-Bit-Systeme, nicht verfügbar unter Windows 2000)
- MailGuard (POP3-Scanner, IMAP-Scanner und SMTP-Scanner) zur permanenten Kontrolle Ihrer Emails auf Viren und Malware. Inklusiv Überprüfung der Email-Anhänge
- WebGuard zur Überwachung der aus dem Internet per HTTP-Protokoll übertragenen Daten und Dateien (Überwachung der Ports 80, 8080, 3128)



- Integriertes Quarantäne-Management zur Isolation und Behandlung verdächtiger Dateien
- Rootkit-Schutz zum Auffinden von Malware, die versteckt im System des Rechners installiert wurde (sog. Rootkits)  
(Nicht verfügbar unter Windows XP 64 Bit)
- Direkter Zugriff auf detaillierte Informationen zu gefundenen Viren und Malware über das Internet
- Einfaches und schnelles Update des Programms, der Virendefinitionen (VDF) sowie der Suchengine durch Single File Update und inkrementelles VDF-Update über einen Webserver im Internet oder Intranet
- Benutzerfreundliche Lizenzierung in der Lizenzverwaltung
- Integrierter Planer zur Planung von einmaligen oder wiederkehrenden Aufgaben wie Updates oder Prüfläufen
- Extrem hohe Viren- und Malware-Erkennung durch innovative Suchtechnologien (Suchengine) inklusive heuristischer Suchverfahren
- Erkennung aller gebräuchlichen Archivtypen inklusive Erkennung verschachtelter Archive und Smart-Extension-Erkennung
- Hohe Performanz durch Multithreading-Fähigkeit (gleichzeitiges Scannen vieler Dateien mit hoher Geschwindigkeit)
- Avira FireWall zum Schutz Ihres Computers vor unerlaubten Zugriffen aus dem Internet bzw. aus einem Netzwerk sowie vor unerlaubten Zugriffen auf das Internet/Netzwerk durch nicht autorisierte Benutzer.

## 3.2 Systemvoraussetzungen

Es bestehen folgende Systemvoraussetzungen::

- Computer ab Pentium, mindestens 266 MHz
- Betriebssystem
- Windows XP, SP2 (32 oder 64 Bit) oder
- Windows Vista (32 oder 64 Bit, SP 1)
- Windows 7 (32 oder 64 Bit)
- Mindestens 150 MB freier Speicherplatz auf der Festplatte (bei Verwendung der Quarantäne und für temporären Speicher mehr)
- Mindestens 256 MB Arbeitsspeicher unter Windows XP
- Mindestens 1024 MB Arbeitsspeicher unter Windows Vista, Windows 7
- Für die Programminstallation: Administrator-Rechte
- Für alle Installationen: Windows Internet Explorer 6.0 oder höher
- Ggf. Internetverbindung (siehe Installation)

## 3.3 Lizenzierung und Upgrade

Um Ihr AntiVir Produkt nutzen zu können, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen 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 Ihr AntiVir Programm im Internet erworben haben, oder befindet sich auf der Programm-CD/DVD. Sie können den Lizenzschlüssel bei der Installation des Programms laden oder nachträglich in der Lizenzverwaltung installieren.

### 3.3.1 Lizenzverwaltung

Die Avira AntiVir Professional Lizenzverwaltung ermöglicht eine sehr einfache Installation der Avira AntiVir Professional Lizenz.

#### Avira AntiVir Professional Lizenzverwaltung



Sie können eine Installation der Lizenz vornehmen, in dem Sie in ihrem Dateimanager oder der Aktivierungs-Email mit Doppelklick die Lizenzdatei auswählen und den entsprechenden Bildschirmanweisungen folgen.

**Hinweis**

Die Avira AntiVir Professional Lizenzverwaltung kopiert die entsprechende Lizenz automatisch in den entsprechenden Produktordner. Ist bereits eine Lizenz vorhanden, erscheint ein Hinweis, ob die bestehende Lizenzdatei ersetzt werden soll. Die bereits bestehende Datei wird in diesem Fall mit der aktuellen Lizenzdatei überschrieben.

## 4 Installation und Deinstallation

In diesem Kapitel erhalten Sie Informationen rund um die Installation und Deinstallation Ihres AntiVir Programms:

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

### 4.1 Installation

Überprüfen Sie vor der Installation, ob Ihr Computer die Mindestsystemanforderungen erfüllt. Falls Ihr Computer alle Voraussetzungen erfüllt, können Sie das AntiVir Programm installieren.

#### **Hinweis**

Sie haben die Möglichkeit, während des Installationsprozesses einen Wiederherstellungspunkt zu erstellen. Ein Wiederherstellungspunkt dient zum Zurücksetzen des Betriebssystems auf einen Zustand vor der Installation. Wenn Sie diese Option nutzen möchten, stellen Sie sicher, dass das Betriebssystem eine Erstellung von Wiederherstellungspunkten erlaubt:

Windows XP: Systemeigenschaften -> Systemwiederherstellung: Deaktivieren Sie die Option **Systemwiederherstellung deaktivieren**.

Windows Vista / Windows 7: Systemeigenschaften -> Computerschutz: Markieren Sie im Bereich **Schutz Einstellungen** das Laufwerk, auf dem das System installiert ist und drücken Sie die Schaltfläche **Konfigurieren**. Aktivieren Sie im Fenster **Systemschutz** die Option **Systemeinstellungen und vorherige Dateiversionen wiederherstellen**.

#### **Installationsarten**

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

##### Express

- Es werden nicht alle verfügbaren Programmkomponenten installiert. Folgende Komponenten werden nicht installiert:

Avira AntiVir ProActiv

Avira FireWall

- Die Programmdateien werden in ein vorgegebenes Standardverzeichnis unter C:\Programme installiert.
- Ihr AntiVir Programm wird mit Standardeinstellungen installiert. Sie haben keine Möglichkeit, Voreinstellungen im Konfigurationsassistenten vorzunehmen.

##### 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.
- Im Konfigurationsassistenten können Sie Voreinstellungen Ihres AntiVir Programms vornehmen und eine kurze Systemprüfung, die automatisch nach der Installation ausgeführt wird, anstoßen.

### 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.
- ▶ Stellen Sie eine Internetverbindung her. Die Internetverbindung wird zur Ausführung folgender Installationsschritte benötigt:
- ▶ Herunterladen der aktuellen Programmdateien und der Suchengine sowie der tagesaktuellen Virendefinitionsdateien durch das Installationsprogramm (bei internetbasierter Installation)
- ▶ Ggf. Ausführung eines Updates nach beendeter Installation
- ▶ Speichern Sie die Lizenzdatei hbedv.key auf Ihrem Computersystem, wenn Sie Ihr AntiVir Programm aktivieren möchten.

#### **Hinweis**

Internetbasierte Installation:

Zur internetbasierten Installation des Programms steht ein Installationsprogramm zur Verfügung, welches die aktuellen Programmdateien vor der Ausführung der Installation von den Webservern der Avira GmbH lädt. Durch dieses Verfahren wird gewährleistet, dass Ihr AntiVir Programm mit einer tagesaktuellen Virendefinitionsdatei installiert wird.

Installation mit einem Installationspaket:

Das Installationspaket enthält sowohl das Installationsprogramm als auch alle benötigten Programmdateien. Es besteht bei der Installation mit einem Installationspaket jedoch keine Sprachauswahl für Ihr AntiVir Programm. Es wird empfohlen im Anschluss an die Installation, ein Update auszuführen, um die Virendefinitionsdatei zu aktualisieren.

### 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 Ihr AntiVir Programm:

### **Hinweis**

Die nachfolgend beschriebenen Handlungen zum Deaktivieren der Windows Firewall betreffen nur das Betriebssystem Windows XP.

- ▶ Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.

### Internetbasierte Installation

Das Dialogfenster *Willkommen...* erscheint.

- ▶ Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

Das Dialogfenster *Sprachauswahl* erscheint.

- ▶ Wählen Sie die Sprache aus, in der Sie Ihr AntiVir Programm installieren möchten und bestätigen Sie Ihre Sprachauswahl mit **Weiter**.

Das Dialogfenster *Download* erscheint. Alle zur Installation benötigten Dateien werden von den Webservern der Avira GmbH heruntergeladen. Nach Abschluss des Downloads schließt sich das Fenster *Download*.

### Installation mit einem Installationspaket

Der Installationsassistent öffnet sich mit dem Dialogfenster *Avira AntiVir Professional*.

- ▶ Klicken Sie auf *Annehmen*, um die Installation zu starten.

Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.

Das Dialogfenster *Willkommen...* erscheint.

- ▶ Klicken Sie auf **Weiter**.

### Fortsetzung internetbasierte Installation und Installation mit einem Installationspaket

Das Dialogfenster mit der Lizenzvereinbarung erscheint.

- ▶ Bestätigen Sie, dass Sie die Lizenzvereinbarung akzeptieren und klicken Sie auf **Weiter**.

Das Dialogfenster *Seriennummer erzeugen* erscheint.

- ▶ Bestätigen Sie ggf., dass eine zufällige Seriennummer generiert und beim Update übertragen wird und klicken Sie auf **Weiter**.

Das Dialogfenster *Installationsart wählen* erscheint.

- ▶ Aktivieren Sie die Option **Express** oder **Benutzerdefiniert**. Wenn Sie einen Wiederherstellungspunkt erstellen möchten, aktivieren Sie die Option **Systemwiederherstellungspunkt erstellen**. Bestätigen Sie Ihre Angaben 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**.

Wenn Sie die Komponente ProActiv zur Installation ausgewählt haben, erscheint das Fenster *AntiVir ProActiv Community*. Sie haben die Möglichkeit, eine Teilnahme an der AntiVir ProActiv Community zu bestätigen: Bei aktivierter Option sendet Avira AntiVir ProActiv Daten zu verdächtigen Programmen, die von der ProActiv-Komponente gemeldet wurden, an das Avira Malware Research Center. Die Daten werden allein zu einer erweiterten Online-Prüfung und zur Erweiterung und Verfeinerung der Erkennungstechnologie genutzt. Über den Link **weitere Informationen** können Sie Details zur erweiterten Online-Prüfung abrufen.

- ▶ Aktivieren oder deaktivieren Sie die Teilnahme an der AntiVir ProActiv Community und bestätigen Sie mit **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: Expressinstallation und benutzerdefinierte Installation

Das Dialogfenster *Lizenz installieren* erscheint:

- ▶ Wählen Sie das Verzeichnis, in dem Sie die Lizenzdatei gespeichert haben, beachten Sie die Hinweise im Dialogfenster und bestätigen Sie mit **Weiter**.

Die Lizenzdatei wird kopiert, die Komponenten werden installiert und gestartet.

Im folgenden Dialogfenster können Sie wählen, ob nach dem Abschluss der Installation die Readme-Datei geöffnet werden soll und ein Neustart des Rechners erfolgen soll.

- ▶ Stimmen Sie ggf. zu und schließen Sie die Installation mit *Fertig stellen* ab.

Der Installationsassistent wird geschlossen.

### Fortsetzung: Benutzerdefinierte Installation Konfigurationsassistent

Bei einer benutzerdefinierten Installation wird im folgenden Schritt der Konfigurationsassistent geöffnet. Sie können im Konfigurationsassistenten wichtige Voreinstellungen für Ihr AntiVir Programm vornehmen.

- ▶ Klicken Sie im Willkommensfenster des Konfigurationsassistenten auf **Weiter**, um mit der Konfiguration des Programms zu beginnen.

Im Dialogfenster *AHeAD konfigurieren*, können Sie eine Erkennungsstufe für die AHead-Technologie wählen. Die gewählte Erkennungsstufe wird für die Einstellung der AHead-Technologie des Scanner (Direktsuche) und des Guard (Echtzeitsuche) übernommen.

- ▶ Wählen Sie eine Erkennungsstufe und setzen Sie die Konfiguration mit **Weiter** fort.

Im folgenden Dialogfenster *Erweiterte Gefahrenkategorien wählen*, können Sie mit der Auswahl von Gefahrenkategorien die Schutzfunktionen Ihres AntiVir Programms anpassen.

- ▶ Aktivieren Sie ggf. weitere Gefahrenkategorien und setzen Sie die Konfiguration mit *Weiter* fort.

Falls Sie das Installationsmodul Avira FireWall zur Installation ausgewählt haben, erscheint das Dialogfenster *FireWall-Sicherheitsniveau*. Sie können festlegen, ob Avira FireWall externe Zugriffe auf freigegebene Ressourcen sowie Netzzugriffe von Anwendungen vertrauenswürdiger Unternehmen erlaubt.

- ▶ Aktivieren Sie die gewünschten Optionen und setzen Sie die Konfiguration mit *Weiter fort*.

Falls Sie das Installationsmodul AntiVir Guard zur Installation ausgewählt haben, erscheint das Dialogfenster *Startmodus des Guard*. Sie können den Startzeitpunkt des Guard festlegen. Der Guard wird bei jedem Neustart des Computers im angegebenen Startmodus gestartet.

### **Hinweis**

Der angegebene Startmodus des Guard wird in der Registry hinterlegt und kann nicht über die Konfiguration geändert werden.

- ▶ Aktivieren Sie die gewünschte Option und setzen Sie die Konfiguration mit *Weiter fort*.

Im folgenden Dialogfenster *Email-Einstellungen wählen*, können Sie die Servereinstellungen für den Email-Versand vornehmen. Ihr AntiVir Programm nutzt Email-Versand per SMTP beim Versenden von Email-Warnungen.

- ▶ Machen Sie ggf. die notwendigen Angaben zu den Servereinstellungen und setzen Sie die Konfiguration mit *Weiter fort*.

Im folgenden Dialogfenster *Systemprüfung* kann die Durchführung einer kurzen Systemprüfung aktiviert oder deaktiviert werden. Die kurze Systemprüfung wird nach abgeschlossener Konfiguration und vor dem Neustart des Computers ausgeführt und durchsucht gestartete Programme und die wichtigsten Systemdateien nach Viren und Malware.

- ▶ Aktivieren oder deaktivieren Sie die Option *Kurze Systemprüfung* und setzen Sie die Konfiguration mit *Weiter fort*.

Im folgenden Dialogfenster können Sie die Konfiguration mit *Fertig stellen* abschließen.

- ▶ Klicken Sie auf *Fertig stellen*, um die Konfiguration zu beenden.

Die angegebenen und ausgewählten Einstellungen werden übernommen.

Wenn Sie die Option *Kurze Systemprüfung* aktiviert haben, öffnet sich das Fenster Luke Filewalker. Der Scanner führt eine kurze Systemprüfung durch.

### **Fortsetzung: Expressinstallation und benutzerdefinierte Installation**

Wenn Sie im letzten Installationsassistenten die Option **Computer neu starten** ausgewählt haben, erfolgt ein Neustart des Rechners.

Nach dem Neustart des Rechners wird die Readme-Datei angezeigt, wenn Sie im Installationsassistenten die Option **Readme.txt anzeigen** ausgewählt haben.

Nach der erfolgreichen Installation wird empfohlen im Control Center unter *Übersicht :: Status* die Aktualität des Programms zu prüfen.

- ▶ Führen Sie ggf. ein Update aus, um die Virendefinitionsdatei zu aktualisieren.
- ▶ Führen Sie im Anschluss eine vollständige Systemprüfung durch.

## 4.2 Änderungsinstallation

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Installation des AntiVir Programms hinzuzufügen oder zu entfernen (siehe Kapitel Installation und Deinstallation::Installationsmodule)



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

Wählen Sie Ihr AntiVir Programm aus und klicken Sie auf **Ändern**. Im Willkommen-Dialog des Programms 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 Professional**  
Dieses Modul beinhaltet alle Komponenten, die für eine erfolgreiche Installation Ihres AntiVir Programms benötigt werden.
- **AntiVir Guard**  
Der AntiVir Guard läuft im Hintergrund. Er überwacht und repariert, falls möglich, 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 das AntiVir Programm automatisch die Datei. Bei der Dateioperation Umbenennen wird keine Suche des AntiVir Guard ausgeführt.
- **AntiVir ProActiv**  
Die ProActiv-Komponente überwacht Aktionen von Anwendungen und meldet ein verdächtiges Verhalten von Anwendungen. Mit dieser verhaltensbasierten Erkennung können Sie sich vor unbekannter Malware schützen. Die ProActiv-Komponente ist in den AntiVir Guard integriert.
- **AntiVir MailGuard**  
MailGuard ist die Schnittstelle zwischen Ihrem Computer und dem Email-Server, von dem Ihr Email-Programm (Email-Client) die Emails herunterlädt. MailGuard hängt sich als sogenannter Proxy zwischen das Email-Programm und den Email-Server. Alle eingehenden Emails werden durch diesen Proxy geleitet, dabei auf Viren bzw. unerwünschte Programme geprüft und an Ihr Email-Programm weitergeleitet. Je nach Konfiguration behandelt das Programm die betroffenen Emails automatisch oder fragt den Benutzer nach einer bestimmten Aktion.
- **AntiVir WebGuard**  
Beim 'Surfen' im Internet fordern Sie über Ihren Webbrowser Daten von einem Webserver an. Die vom Webserver übertragenen Daten (HTML- Dateien, Skript- und Bilddateien, Flash-Dateien, Video- und Musik-Streams etc.) gelangen normalerweise vom Browser-Cache direkt zur Ausführung in den Webbrowser, sodass eine Prüfung durch eine Echtzeitsuche, wie sie der AntiVir Guard zur Verfügung stellt, nicht möglich ist. Auf diesem Weg können Viren und unerwünschte Programme in Ihr Computersystem gelangen. Der WebGuard ist ein sogenannter HTTP-Proxy, der die zur Datenübertragung genutzten Ports (80, 8080, 3128) überwacht und die übertragenen Daten auf Viren und unerwünschte Programme prüft. Je nach Konfiguration behandelt das Programm die betroffenen Dateien automatisch oder fragt den Benutzer nach einer bestimmten Aktion.

- **Avira FireWall**  
Die Avira FireWall kontrolliert die Kommunikationswege von und zu Ihrem Computer. Sie erlaubt oder verweigert die Kommunikation auf der Basis von Sicherheitsrichtlinien.
- *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 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 das AntiVir Programm von Ihrem Computer entfernen möchten, können Sie die Option **Software** zum **Ändern/Entfernen** von Programmen in der Windows-Systemsteuerung verwenden.

So deinstallieren Sie Ihr AntiVir Programm (beschrieben am Beispiel von Windows XP und Windows Vista):

- ▶ Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.
  - ▶ Doppelklicken Sie auf **Programme** (Windows XP: **Software**).
  - ▶ Wählen Sie Ihr AntiVir Programm in der Liste aus und klicken Sie auf **Entfernen**.
- Sie werden gefragt, ob Sie das Programm tatsächlich entfernen wollen.

- ▶ Bestätigen Sie mit **Ja**.

Sie werden gefragt, ob die Windows Firewall wieder aktiviert werden soll (da die Avira FireWall deaktiviert wird).

- ▶ 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**.

Das AntiVir Programm ist deinstalliert, Ihr Computer wird bei Bedarf neu gestartet, dabei werden alle Verzeichnisse, Dateien und Registry-Einträge des Programms gelöscht.

## 4.5 Installation und Deinstallation im Netzwerk

Um die Installation von AntiVir Programmen in einem Netzwerk mit mehreren Clientrechnern für den Systemadministrator zu vereinfachen, bietet Ihr AntiVir Programm ein spezielles Verfahren für die Erstinstallation und die Änderungsinstallation.

Für die automatische Installation arbeitet das Setup-Programm mit der Steuerdatei `setup.inf`. Das Setup-Programm (`presetup.exe`) ist im Installationspaket des Programms enthalten. Die Installation wird mit einem Script oder einer Batch-Datei gestartet und erhält alle notwendigen Informationen aus der Steuerdatei. Die Kommandos im Script ersetzen dabei die üblichen manuellen Eingaben während einer Installation.

---

**Hinweis**

Bitte beachten Sie, dass für die Erstinstallation im Netzwerk eine Lizenzdatei zwingend erforderlich ist.

**Hinweis**

Bitte beachten Sie, dass Sie zur Installation über das Netzwerk ein Installationspaket für das AntiVir Programm benötigen. Eine Installationsdatei für die internetbasierte Installation kann nicht genutzt werden.

Mit einem Login-Skript des Servers oder über SMS können AntiVir Programme komfortabel im Netzwerk verteilt werden.

Hier finden Sie Informationen zur Installation und Deinstallation im Netzwerk:

- siehe Kapitel: Kommandozeilenparameter für das Setup-Programm
- siehe Kapitel: Parameter der Datei `setup.inf`
- siehe Kapitel: Installation im Netzwerk
- siehe Kapitel: Deinstallation im Netzwerk

---

**Hinweis**

Eine weitere, komfortable Möglichkeit der Installation und Deinstallation von AntiVir Programmen im Netzwerk bietet das AntiVir Security Management Center. Das AntiVir Security Management Center dient der Ferninstallation und -wartung der AntiVir-Produkte im Netzwerk. Weitere Informationen finden Sie auf unserer Webseite: <http://www.avira.de>

---

### 4.5.1 Installation im Netzwerk

Die Installation kann skriptgesteuert im Batch-Modus ausgeführt werden.

Das Setup ist für folgende Installationen geeignet:

- Erstinstallation über das Netzwerk (unattended setup)
- Installation von Einzelplatz-Computern
- ▶ Änderungsinstallation bzw. Update

---

**Hinweis**

Wir empfehlen, die automatische Installation zu testen, bevor die Installationsroutine im Netzwerk durchgeführt wird.

So installieren Sie AntiVir Programme automatisch im Netzwerk:

Administrator-Rechte vorhanden (auch im Batch-Modus notwendig)

- ▶ Konfigurieren Sie die Parameter der Datei `setup.inf` und speichern Sie die Datei.

- ▶ Starten Sie die Installation mit dem Parameter `/inf` oder binden Sie den Parameter in das Login-Skript des Servers ein.
  - Beispiele: `presetup.exe /inf="c:\temp\setup.inf"`  
Die Installation läuft automatisch ab.

### 4.5.2 Deinstallation im Netzwerk

So deinstallieren Sie AntiVir Programme automatisch im Netzwerk:

Administrator-Rechte vorhanden (auch im Batch-Modus notwendig)

- ▶ Starten Sie die Deinstallation mit dem Parameter `/remsilent` oder `/remsilentaskreboot` oder binden Sie den Parameter in das Login-Skript des Servers ein.

Zusätzlich können Sie den Parameter für die Protokollierung der Deinstallation angeben.

- Beispiele: `presetup.exe /remsilent /unsetuplog="c:\logfiles\unsetup.log"`

Die Deinstallation läuft automatisch ab.

#### **Hinweis**

Starten Sie das Setup-Programm zur Deinstallation nicht auf einem freigegebenen Netzlaufwerk, sondern lokal auf dem Rechner, auf dem das AntiVir Programm deinstalliert werden soll.

### 4.5.3 Kommandozeilenparameter für das Setup-Programm

Alle Angaben zu Pfaden oder Dateien müssen in `"..."` gesetzt werden.

Für die Installation ist folgender Parameter möglich:

– `/inf`

Das Setup-Programm startet mit dem angegebenen Script und entnimmt ihm alle benötigten Parameter.

Beispiel: `presetup.exe /inf="c:\temp\setup.inf"`

Für die Deinstallation sind folgende Parameter möglich:

– `/remove`

Das Setup-Programm deinstalliert das AntiVir Programm.

Beispiel: `presetup.exe /remove`

– `/remsilent`

Das Setup-Programm deinstalliert das AntiVir Programm, ohne Dialoge anzuzeigen. Der Computer wird nach der Deinstallation neu gestartet.

Beispiel: `presetup.exe /remsilent`

- /remsilentaskreboot

Das Setup-Programm deinstalliert das AntiVir Programm, ohne Dialoge anzuzeigen, und fragt nach der Deinstallation, ob der Computer neu gestartet werden soll.

Beispiel: `presetup.exe /remsilentaskreboot`

Für die Protokollierung der Deinstallation ist optional folgender Parameter möglich:

- /unsetuplog

Alle Aktionen bei der Deinstallation werden aufgezeichnet.

Beispiel: `presetup.exe /remsilent  
/unsetuplog="c:\logfile\unsetup.log"`

### 4.5.4 Parameter der Datei setup.inf

In der Steuerdatei setup.inf können Sie für die automatische Installation des AntiVir Programms folgende Parameter im Bereich [DATA] einstellen. Die Reihenfolge der Parameter spielt keine Rolle. Wenn ein Parameter fehlt oder falsch eingestellt ist, bricht die Setup-Routine mit einer Fehlermeldung ab.

- DestinationPath

Zielpfad, in dem das Programm installiert wird. Er muss im Script angegeben werden. Bitte beachten Sie, dass das Setup automatisch Firmennamen und Produktnamen anhängt. Es können Umgebungsvariablen verwendet werden.

Beispiel: `DestinationPath=%PROGRAMFILES%`  
ergibt z.B. den Installationspfad `C:\Programme\Avira\AntiVir Desktop`

- ProgramGroup

Legt eine Programm-Gruppe für alle Nutzer des Computers im Windows Startmenü an.

1: Programm-Gruppe anlegen

0: Programm-Gruppe nicht anlegen

Beispiel: `ProgramGroup=1`

- DesktopIcon

Legt ein verknüpftes Desktop-Icon für alle Nutzer des Computers auf dem Desktop an.

1: Desktop-Icon anlegen

0: Desktop-Icon nicht anlegen

Beispiel: `DesktopIcon=1`

- ShellExtension

Meldet die Shell-Extension in der Registry an. Mit der Shell-Extension können Dateien oder Verzeichnisse mit dem Kontextmenü der rechten Maustaste auf Viren und Malware geprüft werden.

1: Shell-Extension anmelden

0: Shell-Extension nicht anmelden

Beispiel: ShellExtension=1

– Guard

Installiert den AntiVir Guard (On-Access-Scanner).

1: AntiVir Guard installieren

0: AntiVir Guard nicht installieren

Beispiel: Guard=1

– MailScanner

Installiert den AntiVir MailGuard.

1: AntiVir MailGuard installieren

0: AntiVir MailGuard nicht installieren

Beispiel: MailScanner=1

– KeyFile

Gibt den Pfad zur Lizenzdatei an, die bei der Installation kopiert wird. Bei Erstinstallation: zwingend erforderlich. Der Dateiname muss vollständig (vollqualifiziert) angegeben werden. (Bei Änderungsinstallation: optional.)

Beispiel: KeyFile=D:\inst\license\hbedv.key

– ShowReadMe

Zeigt die Datei readme.txt nach der Installation an.

1: Datei anzeigen

0: Datei nicht anzeigen

Beispiel: ShowReadMe=1

– RestartWindows

Startet den Computer nach der Installation neu. Dieser Eintrag hat höhere Priorität als ShowRestartMessage.

1: Computer neu starten

0: Computer nicht neu starten

Beispiel: RestartWindows=1

- ShowRestartMessage

Zeigt während des Setups vor einem automatischen Neustart eine Information an

0: Information nicht anzeigen

1: Information anzeigen

Beispiel: ShowRestartMessage=1

- SetupMode

Bei Erstinstallation nicht erforderlich. Das Setup-Programm erkennt, ob eine Erstinstallation ausgeführt wird. Legt die Art der Installation fest. Bei einer bereits vorhandenen Installation muss mit SetupMode angegeben werden, ob zu dieser Installation lediglich ein Update oder eine Modifikation (Rekonfiguration) oder eine Deinstallation ausgeführt wird.

Update: Führt ein Update einer vorhandenen Installation aus. Dabei werden Konfigurations-Parameter, wie z.B. Guard, ignoriert.

Modify: Führt eine Modifikation (Rekonfiguration) einer vorhandenen Installation aus. Dabei werden keine Dateien in den Zielpfad kopiert.

Remove: Deinstalliert Ihr AntiVir Programm vom System.

Beispiel: SetupMode=Update

- AVWinIni (optional)

Gibt den Zielpfad zur Konfigurationsdatei an, die bei der Installation kopiert werden kann. Der Dateiname muss vollständig (vollqualifiziert) angegeben werden.

Beispiel: AVWinIni=d:\inst\config\avwin.ini

- Password

Diese Option übergibt der Setup-Routine das Passwort, das für die (Änderungs-)Installation und Deinstallation gesetzt wurde. Der Eintrag wird von der Setup-Routine nur dann geprüft, wenn ein Passwort gesetzt wurde. Falls ein Passwort gesetzt wurde und der Password-Parameter fehlt oder falsch ist, wird die Setup-Routine abgebrochen.

Beispiel: Password=Password123

- WebGuard

Installiert den AntiVir WebGuard .

1: AntiVir WebGuard installieren

0: AntiVir WebGuard nicht installieren

Beispiel: WebGuard=1

- RootKit

Installiert das Modul AntiVir Rootkit-Schutz. Ohne AntiVir Rootkit-Schutz kann der Scanner nicht nach Rootkits auf dem System suchen!

1: AntiVir Rootkit-Schutz installieren

0: AntiVir Rootkit-Schutz nicht installieren

Beispiel: RootKit=1

– HIPS

Installiert die Komponente AntiVir ProActiv. AntiVir ProActiv ist eine verhaltensbasierte Erkennungstechnologie, mit der noch unbekannte Malware erkannt werden kann.

1: ProActiv installieren

0: ProActiv nicht installieren

Beispiel: HIPS=1

– Firewall

Installiert die Komponente Avira Firewall. Avira Firewall überwacht und regelt ein- und ausgehenden Datenverkehr auf Ihrem Computersystem und schützt Ihren Rechner so vor Bedrohungen aus dem Internet oder anderen Netzwerkimgebungen.

1: Firewall installieren

0: Firewall nicht installieren

Beispiel: Firewall=1



# 5 Überblick

In diesem Kapitel erhalten Sie einen Überblick über die Funktionalitäten und die Bedienung Ihres AntiVir Programms.

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

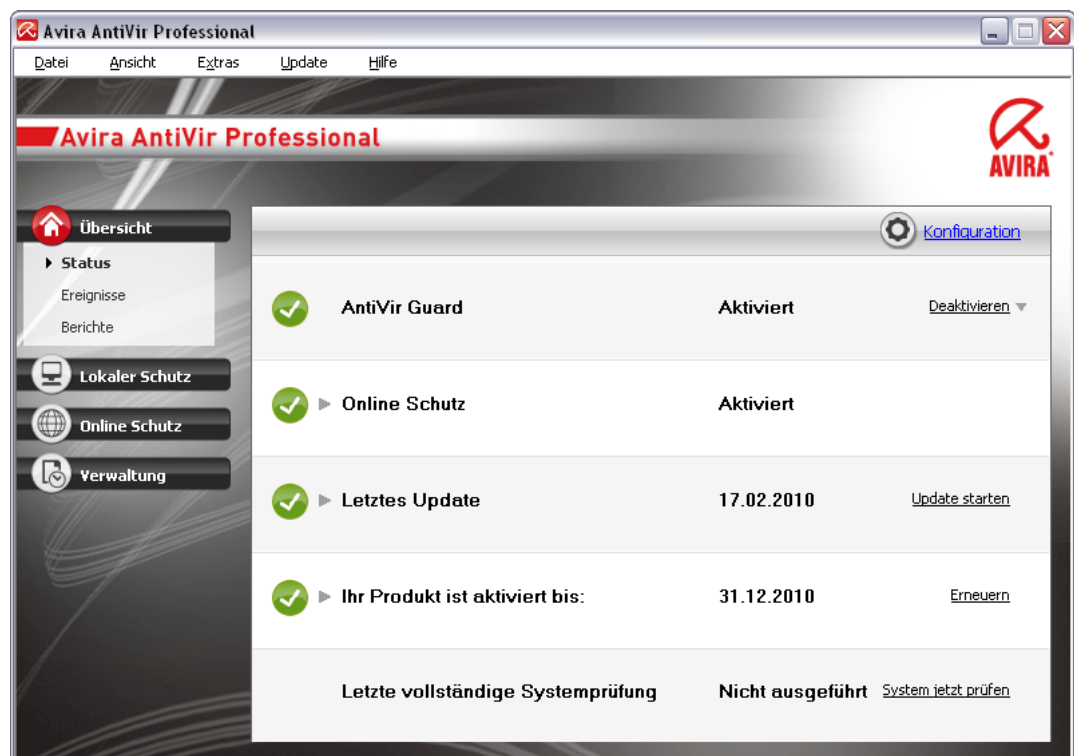
## 5.1 Oberfläche und Bedienung

Sie bedienen Ihr AntiVir Programm über drei Oberflächenelemente des Programms:

- Control Center: Überwachung und Steuerung des AntiVir Programms
- Konfiguration: Konfiguration des AntiVir Programms
- Tray Icon im Systemtray der Taskleiste: Öffnen des Control Center und weitere Funktionen

### 5.1.1 Control Center

Das Control Center dient zur Überwachung des Schutzstatus Ihres Computersystems und zur Steuerung und Bedienung der Schutzkomponenten und Funktionen Ihres AntiVir Programms .



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 zum Programm abrufen.

- **Navigationsbereich:** Im Navigationsbereich können Sie einfach zwischen den einzelnen Rubriken des Control Center wechseln. Die einzelnen Rubriken enthalten Informationen und Funktionen der Programmkomponenten 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 das Control Center zu starten:

- Mit Doppelklick auf das Programm-Icon auf Ihrem Desktop
- Über den Programm-Eintrag im Menü Start | Programme.
- Über das Tray Icon Ihres AntiVir Programms.

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.

Um Menüs im Control Center zu öffnen, zu schließen oder in den Menüs zu navigieren können Sie auch die Tastenkombinationen verwenden: [Alt]-Taste + unterstrichener Buchstabe im Menü oder Menübefehl. Halten Sie die [Alt]-Taste gedrückt, wenn Sie aus einem Menü einen Menübefehl oder ein Untermenü aufrufen möchten.

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.

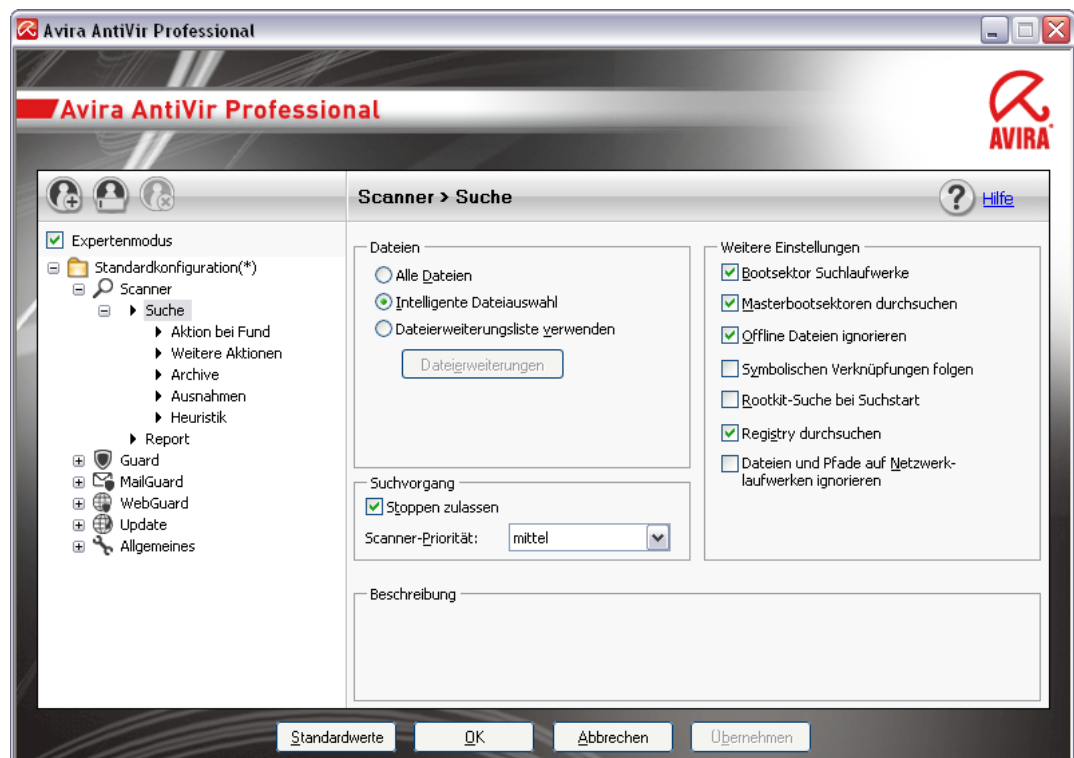
- ▶ Klicken Sie auf die gewünschte Schaltfläche in der oberen Leiste des Detailfensters, um das Objekt zu bearbeiten.

### Control Center im Überblick

- **Übersicht:** Unter **Übersicht** finden Sie alle Rubriken, mit denen Sie die Funktionsfähigkeit Ihres AntiVir Programms überwachen können.
- Die Rubrik **Status** bietet die Möglichkeit auf einen Blick zu sehen, welche Programmmodule 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 Programmmodulen erzeugt werden.
- Die Rubrik Berichte bietet Ihnen die Möglichkeit, sich die Ergebnisse der 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) bzw. durch die Erstellung benutzerdefinierter Profile, 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".
- **Online Schutz:** Unter **Online Schutz** finden Sie die Komponenten, mit denen Sie Ihr Computersystem vor Viren und Malware aus dem Internet sowie vor unerwünschten Netzzugriffen schützen.
- Die Rubrik MailGuard zeigt Ihnen die vom MailGuard überprüften Emails, deren Eigenschaften sowie weitere statistische Daten.
- Die Rubrik WebGuard zeigt Ihnen Informationen zu überprüften URLs und gefundenen Viren, 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".
- Die Rubrik FireWall bietet Ihnen die Möglichkeit, die Grundeinstellungen der Avira FireWall zu konfigurieren. Es werden Ihnen außerdem die aktuelle Datenübertragungsrate und alle aktiven Anwendungen angezeigt, die eine Netzwerkverbindung verwenden.
- **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.

## 5.1.2 Konfiguration

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



Die Konfiguration hat den Aufbau eines Dialogfensters: Mit den Schaltflächen OK oder Übernehmen speichern Sie Ihre in der Konfiguration vorgenommenen Einstellungen, mit Abbrechen verwerfen Sie Ihre Einstellungen, mit der Schaltfläche Standardwerte können Sie die Einstellungen in der Konfiguration auf die Standardwerte zurücksetzen. In der linken Navigationsleiste können Sie einzelne Konfigurationsrubriken anwählen.

### Aufrufen der Konfiguration

Sie haben mehrere Möglichkeiten die Konfiguration aufzurufen:

- Über die Windows Systemsteuerung.
- Über das Windows Sicherheitscenter - ab Windows XP Service Pack 2.
- Über das Tray Icon Ihres AntiVir Programms.
- Im Control Center über den Menüpunkt Extras | Konfiguration.
- Im 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.

## **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**

Um in der Konfiguration Optionen zu aktivieren oder deaktivieren und Schaltflächen zu drücken, können Sie auch die Tastenkombinationen verwenden: [Alt]-Taste + unterstrichener Buchstabe im Optionsnamen oder der Schaltflächenbezeichnung.

### **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.

- ODER -

- ▶ Klicken Sie auf die Schaltfläche **Übernehmen**.

Die Einstellungen werden übernommen. Das Konfigurationsfenster bleibt geöffnet.

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.

Wenn Sie alle Einstellungen in der Konfiguration auf Standardwerte zurücksetzen möchten:

- ▶ Klicken Sie auf **Standardwerte**.

Alle Einstellungen in der Konfiguration werden auf Standardwerte zurückgesetzt. Alle Änderungen und alle eigenen Einträge gehen beim Zurücksetzen auf die Standardwerte verloren.

## **Konfigurationsprofile**

Sie haben die Möglichkeit, Ihre Einstellungen in der Konfiguration als Konfigurationsprofile abzuspeichern. Im Konfigurationsprofil, d.h. einer Konfiguration sind alle Konfigurationsoptionen zu einer Gruppe zusammengefasst. Die Konfiguration wird in der Navigationsleiste als ein Knoten abgebildet. Sie können weitere Konfigurationen zur Standardkonfiguration hinzufügen. Es besteht auch die Möglichkeit, Regeln für das Umschalten auf eine bestimmte Konfiguration zu definieren: Beim regelbasierten Umschalten der Konfiguration können Konfigurationen an die Nutzung einer LAN- bzw. Internetverbindung gekoppelt werden (Identifizierung über Standardgateway): So können Sie beispielsweise Konfigurationsprofile für die verschiedenen Nutzungsszenarien eines Laptops erstellen:

- Nutzung im Firmennetz: Update über Intranet Server, WebGuard deaktiviert
- Nutzung zuhause: Update über die Standard Webserver der Avira GmbH, WebGuard aktiviert

Wenn keine Umschaltregeln definiert worden sind, können Sie im Kontextmenü des Tray Icons manuell auf eine Konfiguration umschalten. Mit den Schaltflächen über der Navigationsleiste oder mit Befehlen aus dem Kontextmenü der Konfigurationsrubriken können Sie Konfigurationen hinzufügen, umbenennen, löschen, kopieren, zurücksetzen und Regeln für das Umschalten auf eine Konfiguration definieren.

#### **Hinweis**

Unter Windows 2000 wird das automatische Umschalten auf eine Konfiguration nicht unterstützt. Unter Windows 2000 können keine Regeln zum Umschalten auf eine Konfiguration definiert werden.

### **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

- **MailGuard:** Konfiguration des MailGuard

Suchoptionen: Aktivierung der Überwachung von POP3-Konten, IMAP-Konten, ausgehenden Emails (SMTP)

Aktionen bei Malware

Heuristik der Suche des MailGuard

Ausnahmen der Suche des MailGuard

Konfiguration des Zwischenspeichers, Zwischenspeicher leeren

Konfiguration einer Fußzeile in gesendeten Emails

Einstellung der Reportfunktion

- **WebGuard:** Konfiguration des WebGuard

Suchoptionen, Aktivierung und Deaktivierung des WebGuard

Aktionen bei Fund

Gesperrte Zugriffe: Unerwünschte Dateitypen und MIME-Typen, Web-Filter für bekannte unerwünschte URLs (Malware, Phishing etc.)

Ausnahmen der Suche des WebGuard: URLs, Dateitypen, MIME-Typen

Heuristik des WebGuard

Einstellung der Reportfunktion

- **FireWall:** Konfiguration der FireWall

Einstellung von Adapterregeln

Benutzerdefinierte Einstellung von Anwendungsregeln

Liste vertrauenswürdiger Hersteller (Ausnahmen beim Netzzugriff von Anwendungen)

Erweiterte Einstellungen: Timeout für Regeln, Windows Host-Datei sperren, Windows FireWall stoppen, Benachrichtigungen

Popup-Einstellungen (Warnmeldungen beim Netzzugriff von Anwendungen)

- **Allgemeines:**

Konfiguration des Email-Versand per SMTP

Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche

Kennwortschutz für den Zugriff auf das Control Center und die Konfiguration

Sicherheit: Statusanzeige Update, Statusanzeige Vollständige Systemprüfung, Produktschutz

WMI: WMI-Unterstützung aktivieren

Konfiguration der Ereignis-Protokollierung

Konfiguration der Bericht-Funktionen

Einstellung der verwendeten Verzeichnisse

Update: Konfiguration der Verbindung zum Downloadserver, Download über Webserver oder Dateiserver, Einstellung der Produktupdates

Warnungen: Konfiguration von Email-Warnungen der Komponente(n):

Scanner

Guard



Updater

Konfiguration von Netzwerkwarnungen der Komponente(n) Scanner, Guard

Konfiguration von akustischen Warnungen bei Malware-Fund

### 5.1.3 Tray Icon

Nach der Installation sehen Sie das Tray Icon Ihres AntiVir Programms im Systemtray der Taskleiste:

Symbol	Beschreibung
	AntiVir Guard ist aktiviert und die FireWall ist aktiviert
	AntiVir Guard ist deaktiviert oder die FireWall ist deaktiviert

Das Tray Icon zeigt den Status des Guard und des FireWall Dienstes an.

Über das Kontextmenü des Tray Icons sind zentrale Funktionen Ihres AntiVir Programms 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 AntiVir Guard.
- **AntiVir MailGuard aktivieren:** Aktiviert bzw. deaktiviert den AntiVir MailGuard.
- **AntiVir WebGuard aktivieren:** Aktiviert bzw. deaktiviert den AntiVir WebGuard.
- **FireWall:**
  - FireWall aktivieren: Aktiviert bzw. deaktiviert die FireWall
  - Gesamten Verkehr blockieren: Aktiviert: Blockiert jede Datenübertragung mit Ausnahme von Übertragungen zum eigenen Computersystem (Local Host / IP 127.0.0.1).
  - Spielmodus aktivieren: Aktiviert bzw. deaktiviert den Modus:  
Aktiviert: Alle definierten Adapter- und Anwendungsregeln werden angewendet. Anwendungen, für die keine Regel definiert ist, wird der Netzwerkzugriff erlaubt und kein Popup-Fenster geöffnet.
- **AntiVir starten:** Öffnet das Control Center.
- **AntiVir konfigurieren:** Öffnet die Konfiguration.
- **Update starten:** Startet ein Update.
- **Konfiguration wählen:** Öffnet ein Untermenü mit den verfügbaren Konfigurationsprofilen. Klicken Sie eine Konfiguration an, um die Konfiguration zu aktivieren. Der Menübefehl ist deaktiviert, wenn Sie bereits Regeln zum automatischen Umschalten auf eine Konfiguration definiert haben.
- **Hilfe:** Öffnet die Online-Hilfe.
- **Über AntiVir Professional:** Öffnet ein Dialogfenster mit Informationen zu Ihrem AntiVir Programm: Produktinformationen, Versionsinformationen, Lizenzinformationen.
- **Avira im Internet:** Öffnet das Avira Webportal im Internet. Voraussetzung ist, dass Sie einen aktiven Zugang zum Internet haben.



## 5.2 So wird es gemacht

### 5.2.1 Lizenz aktivieren

#### So aktivieren Sie die Lizenz Ihres AntiVir Programms:

Mit der Lizenzdatei hbedv.key aktivieren Sie Ihre Lizenz für Ihr AntiVir Produkt. Die Lizenzdatei erhalten Sie von der Avira GmbH per Email. Die Lizenzdatei enthält die Lizenz für alle Produkte, die Sie bei einem Bestellvorgang bestellt haben.

Wenn Sie Ihr AntiVir Programm noch nicht installiert haben:

- ▶ Speichern Sie die Lizenzdatei in einem lokalen Verzeichnis auf Ihrem Computer.
- ▶ Installieren Sie Ihr AntiVir Programm.
- ▶ Geben Sie bei der Installation an, wo Sie die Lizenzdatei gespeichert haben.

Wenn Sie Ihr AntiVir Programm bereits installiert haben:

- ▶ Doppelklicken Sie in Ihrem Dateimanager oder in der Aktivierungs-Email auf die Lizenzdatei und folgen Sie den Bildschirmanweisungen der sich öffnenden Lizenzverwaltung.  
- ODER -
- ▶ Wählen Sie im Control Center Ihres AntiVir Programms den Menüpunkt Hilfe / Lizenzdatei laden....


#### **Hinweis**

Unter Windows Vista erscheint das Dialogfenster Benutzerkontensteuerung. Melden Sie sich ggf. als Administrator an. Klicken Sie auf **Fortsetzen**.

- ▶ Markieren Sie die Lizenzdatei und klicken Sie auf **Öffnen**.  
Eine Meldung erscheint.
- ▶ Bestätigen Sie mit **OK**.  
Die Lizenz ist aktiviert.
- ▶ Starten Sie Ihr System ggf. neu.

### 5.2.2 Automatisierte Updates durchführen

So legen Sie mit dem AntiVir Planer einen Auftrag an, mit dem Ihr AntiVir Programm 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, regelmäßig und häufig Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 60 Minuten.

- ▶ 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
-  Auftrag starten
-  Auftrag stoppen

### 5.2.3 Ein Update manuell starten

Sie haben verschiedene Möglichkeiten ein Update 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 manuell ein Update von Ihres AntiVir Programms:

- ▶ Klicken Sie mit der rechten Maustaste auf das AntiVir Tray Icon in der Taskleiste.  
Ein Kontextmenü erscheint.
- ▶ Wählen Sie **Update starten**.  
Das Dialogfenster *Updater* erscheint.  
- ODER -
- ▶ Wählen Sie im Control Center die Rubrik **Übersicht :: Status**.
- ▶ Klicken Sie im Bereich *Letztes Update* auf den Link **Update starten**.  
Das Dialogfenster *Updater* erscheint.  
- ODER -
- ▶ Wählen Sie im Control Center im Menü **Update** den Menübefehl *Update starten*.  
Das Dialogfenster *Updater* erscheint.

#### **Hinweis**

Wir empfehlen, regelmäßige automatische Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 60 Minuten.

#### **Hinweis**

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

### 5.2.4 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.

- Neues Suchprofil erstellen und verwenden

Wenn Sie ein eigenes Suchprofil anlegen 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.  
-ODER-
- ▶ Erstellen Sie ein neues Suchprofil
- ▶ 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)

Wenn Sie ein neues Suchprofil erstellen möchten:

- ▶ Klicken Sie auf das Symbol  **Neues Profil erstellen.**  
Das Profil *Neues Profil* erscheint unter den bisher vorhandenen Profilen.
- ▶ Benennen Sie das Suchprofil ggf. um, indem Sie auf das Symbol  klicken.
- ▶ Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das 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)
  - Keine Verzeichnisse (kein Häkchen)

### 5.2.5 Direktsuche: Per Drag & Drop nach Viren und Malware suchen

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

Das Control Center Ihres AntiVir Programms 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.

### 5.2.6 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.

## 5.2.7 Direktsuche: Automatisiert nach Viren und Malware suchen

### Hinweis

Nach der Installation ist der Prüfauftrag *Vollständige Systemprüfung* im Planer angelegt: In einem empfohlenen Intervall wird automatisch eine vollständige Systemprüfung ausgeführt.

So legen Sie einen Auftrag an, der automatisiert nach Viren und Malware sucht:

- ▶ 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
- ▶ Wählen Sie die Option *Computer herunterfahren*, wenn Sie möchten, dass der Rechner automatisch heruntergefahren wird, sobald der Auftrag ausgeführt und beendet

wurde. Die Option ist nur im minimierten oder maximierten Darstellungsmodus verfügbar.

- ▶ 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



Auftrag starten





Auftrag stoppen

## 5.2.8 Direktsuche: Gezielt nach aktiven Rootkits suchen

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

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 und aktiver Malware**.
- ▶ 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.

## 5.2.9 Auf gefundene Viren und Malware reagieren

Für die einzelnen Schutzkomponenten Ihres AntiVir Programms können Sie in der Konfiguration jeweils unter der Rubrik *Aktion bei Fund* einstellen, wie Ihr AntiVir Programm bei einem Fund eines Virus oder unerwünschten Programms reagiert.

Bei der ProActiv-Komponente des Guard bestehen keine konfigurierbaren Aktionsoptionen: Ein Fund wird immer im Fenster *Guard: Verdächtiges Verhalten einer Anwendung* gemeldet.

Aktionsoptionen beim Scanner:

– **Interaktiv**

Im interaktiven Aktionsmodus werden Funde der Suche des Scanner in einem Dialogfenster gemeldet. Diese Einstellung ist standardmäßig aktiviert.

Bei der **Suche des Scanner** erhalten Sie beim Abschluss der Suche eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den Scanner beenden.

– **Automatisch**

Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben. Wenn Sie die Option *Warnmeldung anzeigen* aktivieren, erhalten Sie beim Virenfund eine Warnmeldung, in der die ausgeführte Aktion angezeigt wird.

Aktionsoptionen beim Guard:

– **Interaktiv**

Im interaktiven Aktionsmodus wird der Datenzugriff verweigert und eine Desktop-Benachrichtigung angezeigt. In der Desktop-Benachrichtigung können Sie die gefundene Malware entfernen oder über die Schaltfläche Details zur weiteren Virenbehandlung an die Komponente Scanner übergeben. Der Scanner meldet den Fund in einem Fenster, in dem Sie über ein Kontextmenü verschiedene Optionen zur Behandlung der betroffenen Datei haben (siehe Fund::Scanner).

– **Automatisch**

Im automatischen Aktionsmodus wird beim Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben. Wenn Sie die Option *Warnmeldung anzeigen* aktivieren, erhalten Sie beim Virenfund eine Desktop-Benachrichtigung.

Aktionsoptionen beim MailGuard, WebGuard:

– **Interaktiv**

Im interaktiven Aktionsmodus 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**

Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben. Wenn Sie die Option *Warnmeldung anzeigen* aktivieren, erhalten Sie beim Virenfund eine Warnmeldung, in der Sie die auszuführende Aktion bestätigen können.

Im interaktiven Aktionsmodus reagieren Sie auf gefundene Viren und unerwünschte Programme, indem Sie in der Warnmeldung eine Aktion für die betroffenen Objekte auswählen und die gewählte Aktion durch Bestätigen ausführen.

Folgende Aktionen zur Behandlung betroffener Objekte stehen zur Auswahl:



### Hinweis

Welche Aktionen zur Auswahl stehen, ist abhängig vom Betriebssystem, von der Schutzkomponente (AntiVir Guard, AntiVir Scanner, AntiVir MailGuard, AntiVir WebGuard), die den Fund meldet und von der gefundenen Malware.

### Aktionen des Scanner und des Guard (ohne Funde von ProActiv):

- **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. Dieser Vorgang ist bedeutend schneller als *Überschreiben und löschen*. Handelt es sich bei dem Fund um einen Bootsektorvirus, wird beim Löschen der Bootsektor gelöscht. Es wird ein neuer Bootsektor geschrieben.

- **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.

- **Ignorieren**

Es werden keine weiteren Aktionen ausgeführt. 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.

- **Immer ignorieren**

Aktionsoption bei Funden des Guard: Es werden keine weiteren Aktionen vom Guard ausgeführt. Ein Zugriff auf die Datei wird zugelassen. Alle weiteren Zugriffe auf diese Datei werden zugelassen und nicht mehr gemeldet bis ein Neustart des Rechners oder ein Update der Virendefinitionsdatei erfolgt.

- **In Quarantäne kopieren**

Aktionsoption beim Fund eines Rootkit: Der Fund wird in die Quarantäne kopiert.

- **Bootsektor reparieren | Repairtool herunterladen**

Aktionsoptionen beim Fund von infizierten Bootsektoren: Für infizierte Diskettenlaufwerke stehen Optionen zur Reparatur zur Verfügung. Ist keine Reparatur mit Ihrem AntiVir Programm möglich, können Sie ein Spezialtool zum Erkennen und Entfernen von Bootsektorviren herunterladen.

**Hinweis**

Wenn Sie Aktionen auf laufende Prozesse anwenden, werden die betroffenen Prozesse vor der Ausführung der Aktion beendet.

**Aktionen des Guard bei Funden der ProActiv-Komponente (Meldung von verdächtigen Aktionen einer Anwendung):****– Vertrauenswürdige Programm**

Die Ausführung der Anwendung wird fortgesetzt. Das Programm wird zur Liste der erlaubten Anwendungen hinzugefügt und von der Überwachung durch die ProActiv-Komponente ausgenommen. Beim Hinzufügen zur Liste der erlaubten Anwendungen wird der Überwachungstyp *Inhalt* gesetzt. Dies bedeutet, dass die Anwendung nur bei unverändertem Inhalt von einer Überwachung durch die ProActiv-Komponente ausgenommen wird (siehe Konfiguration::Guard::ProActiv::Anwendungsfilter: Erlaubte Anwendungen).

**– Programm einmal blockieren**

Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

**– Dieses Programm immer blockieren**

Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Das Programm wird zur Liste der zu blockierenden Anwendungen hinzugefügt und kann nicht mehr ausgeführt werden (siehe Konfiguration::Guard::ProActiv::Anwendungsfilter: Zu blockierende Anwendungen).

**– Ignorieren**

Die Ausführung der Anwendung wird fortgesetzt. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

**Aktionen des MailGuard: Eingehende Emails****– In Quarantäne verschieben**

Die Email wird inklusive aller Anhänge in Quarantäne verschoben. Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge der Email werden durch einen Standardtext ersetzt.

**– Löschen**

Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

**– Anhang löschen**

Der betroffene Anhang wird durch einen Standardtext ersetzt. Sollte der Textkörper der Email betroffen sein, wird dieser gelöscht und ebenfalls durch einen Standardtext ersetzt. Die Email selbst wird zugestellt.

**– Anhang in Quarantäne verschieben**

Der betroffene Anhang wird in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der Textkörper der Email wird zugestellt. Die betroffene Anlage kann später über den Quarantänenanager zugestellt werden.

**– Ignorieren**

Die betroffene Email wird zugestellt.

### **Warnung**

Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen. Deaktivieren Sie die Vorschau in Microsoft Outlook, starten Sie Anlagen auf keinen Fall per Doppelklick!

### **Aktionen des MailGuard: Ausgehende Emails**

#### – **Mail in Quarantäne verschieben (nicht senden)**

Die Email wird inklusive aller Anhänge in die Quarantäne kopiert und nicht gesendet. Die Email verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

#### – **Mailversand blockieren (nicht senden)**

Die Email wird nicht versandt und verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

#### – **Ignorieren**

Die betroffene Email wird versendet.

### **Warnung**

Hierdurch können Viren sowie unerwünschte Programme auf das Computersystem des Email-Empfängers gelangen.

### **Aktionen des WebGuard:**

#### – **Zugriff verweigern**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt.

#### – **In Quarantäne verschieben**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänenanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

#### – **Ignorieren**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom WebGuard an Ihren Webbrowser weitergeleitet.

### **Warnung**

Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

### **Hinweis**

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

**Hinweis**

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/sample-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.\**.

### 5.2.10 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 Ihres AntiVir Programms 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 die Datei zur Analyse auf einen Webserver des Avira Malware Research Center hochladen möchten:

- ▶ Markieren Sie die Datei, die Sie hochladen möchten.

- ▶ Klicken Sie auf .

Es öffnet sich ein Dialog mit einem Formular zur Eingabe Ihrer Kontaktdaten.

- ▶ Geben Sie die Daten vollständig an.
- ▶ Wählen Sie einen Typ aus: **Verdächtige Datei** oder **Fehlalarm**.
- ▶ Drücken Sie auf **OK**.

Die Datei wird gepackt auf einen Webserver des Avira Malware Research Center hochgeladen.

**Hinweis**

In folgenden Fällen wird eine Analyse durch das Avira Malware Research Center empfohlen:

**Heuristischer Treffer (Verdächtige Datei):** Bei einem Suchlauf wurde eine Datei von Ihrem AntiVir Programm als verdächtig eingestuft und in die Quarantäne verschoben: Im Dialogfenster zum Virenfund oder in der Reportdatei des Suchlaufs wurde die Analyse der Datei durch das Avira Malware Research Center empfohlen.

**Verdächtige Datei:** Sie halten eine Datei für verdächtig und haben diese deshalb zur Quarantäne hinzugefügt, die Prüfung der Datei auf Viren und Malware ist jedoch negativ.

**Fehlalarm:** Sie gehen davon aus, dass es sich bei einem Virenfund um einen Fehlalarm handelt: Ihr AntiVir Programm meldet einen Fund in einer Datei die jedoch mit hoher Wahrscheinlichkeit nicht von Malware betroffen ist.


**Hinweis**

Die Größe der Dateien, die Sie hochladen, ist begrenzt auf 20 MB ungepackt oder 8 MB gepackt.

**Hinweis**

Sie können mehrere Dateien gleichzeitig hochladen, indem Sie alle Dateien, die sie hochladen möchten, markieren und dann auf die Schaltfläche **Objekt senden** klicken.

Wenn Sie ein Quarantäneobjekt aus der Quarantäne in ein anderes Verzeichnis kopieren möchten:

- ▶ Markieren Sie das Quarantäneobjekt und klicken Sie auf .

Es öffnet sich ein Durchsuchen-Dialog, in dem Sie ein Verzeichnis auswählen können.

- ▶ Wählen Sie ein Verzeichnis aus, in dem eine Kopie des Quarantäneobjekts abgelegt werden soll und bestätigen Sie Ihre Auswahl.

Das ausgewählte Quarantäneobjekt wird im ausgewählten Verzeichnis abgelegt.

**Hinweis**

Das Quarantäneobjekt ist nicht identisch mit der wiederhergestellten Datei. Das Quarantäneobjekt ist verschlüsselt und kann nicht ausgeführt oder im Ursprungsformat gelesen werden.

Wenn Sie die Eigenschaften eines Quarantäneobjekts in eine Textdatei exportieren möchten:

- ▶ Markieren Sie das Quarantäneobjekt und klicken Sie auf .

Es öffnet sich eine Textdatei mit den Daten zum ausgewählten Quarantäneobjekt.

- ▶ Speichern Sie die Textdatei ab.

Dateien in Quarantäne können Sie auch wiederherstellen:

- siehe Kapitel: Quarantäne: Dateien in der Quarantäne wiederherstellen

## 5.2.11 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.

### 5.2.12 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

### 5.2.13 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 Auswahl und selbstdefinierten Suchprofilen möglich):

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.


### 5.2.14 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 Ihres AntiVir Programms 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.

### 5.2.15 Ereignisse: Ereignisse filtern

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

- Updater
- Guard
- MailGuard
- Scanner
- Planer
- FireWall
- WebGuard
- Hilfsdienst
- ProActiv

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.

### 5.2.16 MailGuard: Email-Adressen von der Prüfung ausschließen

So stellen Sie ein, welche Email-Adressen (Absender) von der Prüfung durch den MailGuard ausgeschlossen werden (sogenanntes Whitelisting):

- ▶ Wählen Sie im Control Center die Rubrik **Online Schutz :: MailGuard**.
  - In der Liste sehen Sie die eingegangenen Emails.
- ▶ Markieren Sie die Email, die Sie von der Prüfung des MailGuard ausschließen möchten.
- ▶ Klicken Sie auf das gewünschte Symbol, um die Email von der Prüfung des MailGuard auszuschließen:



Die ausgewählte Email-Adresse wird in Zukunft nicht mehr auf Viren und unerwünschte Programme geprüft.

Die Email-Absender-Adresse wird in die Ausschlussliste übernommen und nicht mehr auf Viren und Malware geprüft.

#### **Warnung**

Schließen Sie nur Email-Adressen von absolut vertrauenswürdigen Absendern von der Prüfung des MailGuard aus.

#### **Hinweis**

In der Konfiguration unter MailGuard :: Allgemeines :: Ausnahmen können Sie weitere Email-Adressen in die Ausschlussliste einpflegen oder Email-Adressen aus der Ausschlussliste entfernen.

### 5.2.17 FireWall: Sicherheitsstufe für die FireWall wählen

Sie können zwischen verschiedenen Sicherheitsstufen wählen. Abhängig davon haben Sie unterschiedliche Konfigurationsmöglichkeiten für die Adapterregeln.

Folgende Sicherheitsniveaus stehen zur Verfügung:

- **Niedrig**
  - Flooding und Port-Scan werden erkannt.
- **Mittel**
  - Verdächtige TCP- und UDP-Pakete werden verworfen.
  - Flooding und Port-Scan werden verhindert.

- **Hoch**
  - Der Computer ist im Netzwerk unsichtbar.
  - Verbindungen von außen werden blockiert.
  - Flooding und Port-Scan werden verhindert.
- **Benutzer**
  - Benutzerdefinierte Regeln: Auf dieses Sicherheitsniveau stellt das Programm automatisch um, wenn Sie Adapterregeln geändert haben.

---

**Hinweis**

Die Standardeinstellung des Sicherheitsniveaus für alle vordefinierten Regeln der Avira FireWall ist **Hoch**.

---

So stellen Sie das Sicherheitsniveau für die FireWall ein:

- ▶ Wählen Sie im Control Center die Rubrik Online **Schutz :: FireWall**.
- ▶ Stellen Sie den Schieberegler auf das gewünschte Sicherheitsniveau.

Das gewählte Sicherheitsniveau ist sofort aktiv.



## 6 Scanner

Mit der Komponente Scanner können Sie gezielte Suchläufe nach Viren und unerwünschten Programmen (Direktsuche) ausführen. Sie haben folgende Möglichkeiten nach betroffenen Dateien zu suchen:

- **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 Control Center nicht erst gestartet werden muss.
- **Direktsuche über Drag & Drop**  
Beim Ziehen einer Datei oder eines Verzeichnisses in das Programmfenster des 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.

Bei der Suche nach Rootkits, Bootsekturviren und beim Durchsuchen von aktiven Prozessen sind besondere Verfahren erforderlich. Sie haben folgende Optionen:

- Suche nach Rootkits über das Suchprofil *Suche nach Aktiver Malware*
- Durchsuchen von aktiven Prozessen über das Suchprofil **Aktive Prozesse**
- Suche nach Bootsekturviren über den Menübefehl **Bootsekturviren prüfen** im Menü **Extras**



## 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 Updater in Ihr AntiVir integriert. Der Updater sorgt dafür, dass Ihr AntiVir Programm stets auf dem neuesten Niveau arbeitet und in der Lage ist, die täglich neu erscheinenden Viren zu erfassen. Updater aktualisiert die folgenden Komponenten:

- Virendefinitionsdatei:

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

- Suchengine:

Die Suchengine enthält die Methoden, mit denen Ihr AntiVir Programm 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 der Updater zusätzlich ein Produktupdate durch oder benachrichtigt Sie über verfügbare Produktupdates. Nach einem Produktupdate kann ein Neustart Ihres Computersystems erforderlich sein. Erfolgt nur ein Update der Virendefinitionsdatei und der Suchengine, muss der Rechner nicht neu gestartet werden.

---

### **Hinweis**

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

---

Ein Update wird in folgendem Intervall automatisch ausgeführt: 60 Minuten. Sie können das automatische Update über die Konfiguration (Konfiguration::Update) ändern oder deaktivieren.

Im Control Center unter Planer können Sie weitere Update-Aufträge einrichten, die in den angegebenen Intervallen vom Updater ausgeführt werden. 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 oder über einen Web- oder Dateiserver im Intranet, der die Update-Dateien aus dem Internet herunterlädt und sie anderen Rechnern im Netzwerk zur Verfügung stellt. Dies ist sinnvoll, wenn Sie AntiVir Programme auf mehreren Computern in einem Netzwerk aktualisieren wollen. Durch die Einrichtung eines Downloadservers im Intranet kann die Aktualität von AntiVir Programmen auf den zu schützenden Rechnern ressourcenschonend gewährleistet werden. Um einen funktionierenden Downloadserver im Intranet einzurichten, benötigen Sie einen Server, der die Update-Struktur Ihres AntiVir Programms anbietet.

---

**Hinweis**

Als Web- oder Dateiserver im Intranet können Sie AntiVir Internet Update Manager (Datei- oder Webserver unter Windows) nutzen. AntiVir Internet Update Manager spiegelt Downloadserver von Avira AntiVir Produkten und ist im Internet auf der Avira Webseite beziehbar:

<http://www.avira.de>

---

Bei der Nutzung eines Webservers erfolgt der Download per HTTP-Protokoll. Bei der Nutzung eines Dateiservers erfolgt ein Zugriff auf die Update-Dateien über das Netzwerk. Sie konfigurieren die Verbindung zum Web- oder Dateiserver in der Konfiguration unter Allgemeines :: Update. Für die Standardkonfiguration wird die existierende Internetverbindung als Verbindung zu den Webservern der Avira GmbH genutzt.





## 8 Avira FireWall :: Überblick

Avira FireWall überwacht und regelt den ein- und ausgehenden Datenverkehr auf Ihrem Computersystem und schützt Sie so vor einer Vielzahl von Angriffen und Bedrohungen aus dem Internet: Auf der Basis von Sicherheitsrichtlinien wird ein- und ausgehender Datenverkehr oder das Abhören von Ports zugelassen oder zurückgewiesen. Sie erhalten eine Desktopbenachrichtigung, wenn Avira FireWall Netzwerkaktivitäten zurückweist und so Netzwerkverbindungen blockiert. Sie haben folgende Möglichkeiten Avira FireWall einzustellen:

- über die Einstellung eines Sicherheitsniveaus im Control Center

Im Control Center können Sie eine Sicherheitsstufe einstellen. Die Sicherheitsstufen *Niedrig*, *Mittel* und *Hoch* beinhalten jeweils mehrere, sich ergänzende Sicherheitsregeln, die auf Paketfiltern basieren. Diese Sicherheitsregeln sind als vordefinierte Adapterregeln in der Konfiguration unter FireWall::Adapterregeln hinterlegt.

- über das Speichern von Aktionen im Fenster Netzwerkereignis

Versucht eine Anwendung erstmalig eine Netzwerk- oder Internetverbindung herzustellen, öffnet sich das Popup-Fenster *Netzwerkereignis*. Im Fenster *Netzwerkereignis* kann der Benutzer wählen, ob die Netzwerkaktivität der Anwendung zugelassen oder zurückgewiesen wird. Wenn die Option **Aktion für diese Anwendung speichern** aktiviert ist, wird die Aktion als Anwendungsregel erstellt und in der Konfiguration unter FireWall::Anwendungsregeln hinterlegt. Über das Speichern der Aktionen im Fenster Netzwerkereignis erhalten Sie ein Regelset für die Netzwerkaktivitäten von Anwendungen.

### Hinweis

Bei Anwendungen vertrauenswürdiger Anbieter wird der Netzwerkzugang standardmäßig erlaubt, es sei denn eine Adapterregel verbietet den Netzzugriff. Sie haben die Möglichkeit, Anbieter aus der Liste vertrauenswürdiger Anbieter zu entfernen.

- über die Erstellung von Adapter- und Anwendungsregeln in der Konfiguration

In der Konfiguration können Sie vordefinierte Adapterregeln ändern oder neue Adapterregeln erstellen. Das Sicherheitsniveau der FireWall wird automatisch auf den Wert *Benutzer* gesetzt, wenn Sie Adapterregeln hinzufügen oder ändern. Mit Anwendungsregeln können Sie Überwachungsregeln definieren, die auf Anwendungen spezifiziert sind:

Mit einfachen Anwendungsregeln können Sie einstellen, ob alle Netzwerkaktivitäten einer Software-Anwendung zurückgewiesen oder zugelassen werden sollen oder interaktiv über das Popup-Fenster *Netzwerkereignis* behandelt werden sollen.

In der erweiterten Konfiguration der Rubrik *Anwendungsregeln* können Sie für eine Anwendung unterschiedliche Paketfilter definieren, die als spezifizierte Anwendungsregeln ausgeführt werden.

**Hinweis**

Bei Anwendungsregeln werden zwei Modi unterschieden: *Privilegiert* und *gefiltert*. Bei Anwendungsregeln im Modus *gefiltert* werden zutreffende Adapterregeln priorisiert, d.h. die zutreffende Adapterregel wird nach der Anwendungsregel ausgeführt. So kann der Fall eintreten, dass der Netzzugriff von zugelassenen Anwendungen aufgrund eines hohen Sicherheitsniveaus oder entsprechenden Adapterregeln zurückgewiesen wird. Bei Anwendungsregeln im Modus *privilegiert* werden die Adapterregeln ignoriert. Wenn Anwendungen im Modus *privilegiert* zugelassen sind, wird der Netzzugriff der Anwendung in jedem Fall zugelassen.

## 9 Problembehebung, Tipps

In diesem Kapitel finden Sie wichtige Hinweise zur Behebung von Problemen und weitere Tipps zum Umgang mit Ihrem AntiVir Programm.

siehe Kapitel Hilfe im Problemfall

siehe Kapitel Tastaturbefehle

siehe Kapitel Windows Sicherheitscenter

### 9.1 Hilfe im Problemfall

Hier finden Sie Informationen zu Ursachen und Lösungen möglicher Probleme.

- Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.
- AntiVir MailGuard funktioniert nicht.
- Es ist keine Netzwerkverbindung in virtuellen Maschinen verfügbar, wenn Avira FireWall auf dem Host-Betriebssystem installiert ist und das Sicherheitsniveau der Avira FireWall auf Mittel bzw. Hoch eingestellt wurde.
- Virtual Private Network (VPN) Verbindung wird blockiert, wenn das Sicherheitsniveau der Avira FireWall auf Mittel bzw. Hoch eingestellt ist.
- Eine Email, die über eine TSL-Verbindung versendet wurde, wurde vom MailGuard blockiert.
- Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt

#### **Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.**

Ursache: Die Datei ist verschlüsselt.

- ▶ Zur Aktivierung der Lizenz müssen Sie die Datei nicht öffnen, sondern im Programmverzeichnis speichern. Siehe auch Lizenzverwaltung.

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

Ursache: Ihre Internetverbindung ist inaktiv. Deshalb kann keine Verbindung zum Webserver im Internet erstellt werden.

- ▶ 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 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 Ihr AntiVir Produkt.
- ▶ Wenn Sie das Betriebssystem Windows XP verwenden, deaktivieren Sie die Systemwiederherstellung.
- ▶ Starten Sie den Computer im abgesicherten Modus.
- ▶ Starten Sie das AntiVir Programm und die 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. Gleiches gilt für den AntiVir MailGuard.

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 *Avira AntiVir 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 Konfiguration (Expertenmodus) Guard :: Suche :: Ausnahmen und tragen Sie den Prozessnamen der Backup-Software ein.

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

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

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

### AntiVir MailGuard funktioniert nicht.

Bitte prüfen Sie die Funktionsfähigkeit des AntiVir MailGuard anhand der folgenden Checklisten, falls in Zusammenhang mit AntiVir MailGuard Probleme auftreten.

#### Checkliste

- ▶ Prüfen Sie, ob Ihr Mail Client sich per Kerberos, APOP oder RPA beim Server anmeldet. Diese Authentifizierungsmethoden werden derzeit nicht unterstützt.
- ▶ Prüfen Sie, ob sich Ihr Mail Client per SSL (auch häufig TSL - Transport Layer Security - genannt) am Server anmeldet. AntiVir MailGuard unterstützt kein SSL und beendet daher die SSL verschlüsselte Verbindungen. Falls Sie SSL verschlüsselte Verbindungen ohne Schutz des MailGuard verwenden möchten, müssen Sie für die Verbindung einen anderen Port nutzen als die vom MailGuard überwachten Ports. Die vom MailGuard überwachten Ports können in der Konfiguration unter MailGuard::Suche konfiguriert werden.
- ▶ Ist der AntiVir MailGuard Dienst (Service) aktiv? 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 *Avira AntiVir MailGuard*. 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. Ist dies nicht von Erfolg gekrönt, sollten Sie ggf. das AntiVir Programm über "Start | Einstellungen | Systemsteuerung | Software" komplett deinstallieren, den Rechner neu starten und Ihr AntiVir Programm anschließend neu installieren.

#### Allgemeines

- ▶ Über SSL (Secure Sockets Layer) verschlüsselte POP3 Verbindungen (auch häufig als TLS (Transport Layer Security) bezeichnet) können derzeit nicht geschützt werden und werden ignoriert.
- ▶ Authentifizierung zum Mail Server wird derzeit nur über "Passwords" unterstützt. "Kerberos" und "RPA" werden derzeit nicht unterstützt.
- ▶ Ihr AntiVir Programm prüft beim Versenden von Emails diese nicht auf Viren sowie unerwünschte Programme.

#### Hinweis

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

**Es ist keine Netzwerkverbindung in virtuellen Maschinen verfügbar, wenn Avira FireWall auf dem Host-Betriebssystem installiert ist und das Sicherheitsniveau der Avira FireWall auf Mittel bzw. Hoch eingestellt wurde.**

Wenn Avira FireWall auf einem Computer installiert ist, auf dem zusätzlich eine virtuelle Maschine (beispielsweise VMWare, Virtual PC, u.a.) betrieben wird, blockiert diese alle Netzwerkverbindungen der virtuellen Maschine, wenn das Sicherheitsniveau der Avira FireWall auf Mittel bzw. Hoch eingestellt wurde. Beim Sicherheitsniveau Niedrig reagiert die FireWall wie erwartet.

Ursache: Die virtuelle Maschine emuliert per Software eine Netzwerkkarte. Durch diese Emulation werden die Datenpakete des Gastsystems in spezielle (sog. UDP) Pakete gekapselt und über das externe Gateway zurück zum Host-System geroutet. In der Avira FireWall werden ab dem Sicherheitsniveau Mittel diese von außen kommenden Pakete blockiert.

Um dieses Verhalten zu umgehen gehen Sie wie folgt vor:

- ▶ Wählen Sie im Control Center die Rubrik **Online Schutz :: FireWall**.
- ▶ Klicken Sie auf den Link **Konfiguration**.
- ▶ Das Dialogfenster *Konfiguration* erscheint. Sie befinden sich in der Konfigurationsrubrik *Anwendungsregeln*.
- ▶ Aktivieren Sie den **Expertenmodus**.
- ▶ Wählen Sie die Konfigurationsrubrik **Adapterregeln**.
- ▶ Klicken Sie auf **Hinzufügen**.
- ▶ Wählen Sie unter *Eingehende Regel* **UDP**.
- ▶ Geben Sie der Regel im Bereich Name der Regel einen **Namen**.
- ▶ Klicken Sie **OK**.
- ▶ Prüfen Sie, ob die Regel eine Prioritätsstufe über der Regel **Alle IP-Pakete zurückweisen** liegt.

#### **Warnung**

Diese Regel birgt potentielle Gefahren in sich, da sie grundsätzlich UDP-Pakete erlaubt! Wechseln Sie nach dem Betrieb Ihrer virtuellen Maschine wieder in Ihr vorheriges Sicherheitsniveau.

**Virtual Private Network (VPN) Verbindung wird blockiert, wenn das Sicherheitsniveau der Avira FireWall auf Mittel bzw. Hoch eingestellt ist.**

Ursache: Das Problem ist die letzte Regel der Kette **Alle IP-Pakete zurückweisen** die immer dann in Kraft tritt, wenn ein Paket keiner der darüber liegenden Regeln entspricht. Die durch die VPN-Software versendeten Pakete werden durch diese Regel gefiltert, da Sie aufgrund Ihres Typs (sog. GRE-Pakete) in keine der anderen Kategorien fallen.

Ersetzen Sie die Regel **Alle IP-Pakete zurückweisen** durch zwei neue Regeln die TCP- und UDP-Pakete zurückweisen. Auf diese Weise besteht die Möglichkeit, dass Pakete anderer Protokolle zugelassen werden.

**Eine Email, die über eine TSL-Verbindung versendet wurde, wurde vom MailGuard blockiert.**

Ursache: Transport Layer Security (TLS: Verschlüsselungsprotokoll für Datenübertragungen im Internet) wird derzeit nicht vom MailGuard unterstützt. Sie haben folgende Möglichkeiten die Email zu senden:

- ▶ Nutzen Sie einen anderen Port als den von SMTP genutzten Port 25. Sie umgehen damit die Überwachung durch den MailGuard
- ▶ Verzichten Sie auf die TSL verschlüsselte Verbindung und deaktivieren Sie die TSL-Unterstützung in Ihrem Email-Client.
- ▶ Deaktivieren Sie (vorübergehend) die Überwachung der ausgehenden Emails durch den MailGuard in der Konfiguration unter MailGuard::Suche.

### Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt, im Browser werden Daten geladen.

Dieses Phänomen kann bei Chats auftreten, die auf dem HTTP-Protokoll mit 'transfer-encoding= chunked' basieren.

Ursache: WebGuard prüft gesendete Daten zunächst vollständig auf Viren und unerwünschte Programme, bevor die Daten im Webbrowser geladen werden. Bei einem Datentransfer mit 'r;r;transfer-encoding= chunked' kann der WebGuard die Nachrichtenlänge bzw. die Datenmenge nicht ermitteln.

- ▶ Geben Sie in der Konfiguration die URL des Webchats als Ausnahme an (siehe Konfiguration: WebGuard::Ausnahmen).

## 9.2 Tastaturbefehle

Tastaturbefehle - auch Shortcuts genannt - bieten eine schnelle Möglichkeit durch das Programm zu navigieren, einzelne Module aufzurufen und Aktionen zu starten.

Im Folgenden erhalten Sie eine Übersicht über die verfügbaren Tastaturbefehle. Nähere Hinweise zur Funktionalität und Verfügbarkeit finden Sie im entsprechenden Kapitel der Hilfe.

### 9.2.1 In Dialogfeldern

Tastaturbefehl	Beschreibung
Strg + Tab Strg + Bild runter	Navigation im Control Center Zur nächsten Rubrik wechseln.
Strg + Umsch + Tab Strg + Bild hoch	Navigation im Control Center Zur vorherigen Rubrik wechseln.
← ↑ → ↓	Navigation in den Konfigurationsrubriken Setzen Sie zunächst den Fokus mit der Maus auf eine Konfigurationsrubrik.
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.

### 9.2.2 In der Hilfe

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
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.
Bild hoch Bild runter	Durch ein Thema blättern.

### 9.2.3 Im Control Center

#### Allgemein

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
F1	Hilfe anzeigen
Alt + F4	Control Center schließen



F5	Ansicht aktualisieren
F8	Konfiguration öffnen
F9	Update starten

#### Rubrik Prüfen

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
F2	Ausgewähltes Profil umbenennen
F3	Suchlauf mit dem ausgewählten Profil starten
F4	Desktopverknüpfung für das ausgewählte Profil erstellen
Einf	Neues Profil erstellen
Entf	Ausgewähltes Profil löschen

#### Rubrik FireWall

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
Enter	Eigenschaften

#### Rubrik Quarantäne

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

#### Rubrik Planer

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
F2	Auftrag ändern
Enter	Eigenschaften
Einf	Neuen Auftrag einfügen
Entf	Auftrag löschen

#### Rubrik Berichte

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
F3	Reportdatei anzeigen
F4	Reportdatei drucken
Enter	Bericht anzeigen
Entf	Bericht(e) löschen

#### Rubrik Ereignisse

<b>Tastaturbefehl</b>	<b>Beschreibung</b>
F3	Ereignis(se) exportieren
Enter	Ereignis anzeigen
Entf	Ereignis(se) löschen

## 9.3 Windows Sicherheitscenter

- ab Windows XP Service Pack 2 -

### 9.3.1 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.

### 9.3.2 Das Windows Sicherheitscenter und Ihr AntiVir Programm

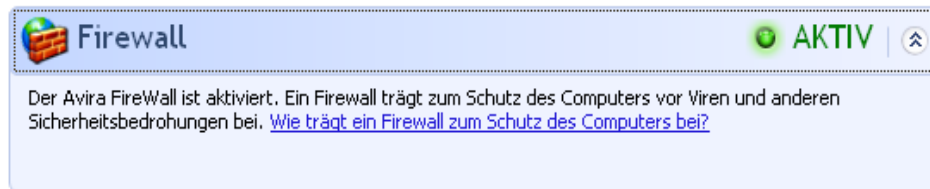
#### Firewall

Es ist möglich, dass Sie vom Sicherheitscenter die folgende firewallbezogene Information erhalten:

- Firewall AKTIV / Firewall ein
- Firewall INAKTIV / Firewall aus

#### Firewall AKTIV / Firewall aus

Nach der Installation Ihres AntiVir Programms und dem Abschalten der Windows Firewall erhalten Sie die folgende Meldung:

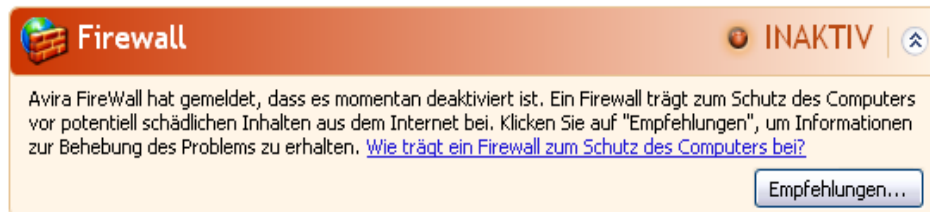


**Firewall** AKTIV

Der Avira FireWall ist aktiviert. Ein Firewall trägt zum Schutz des Computers vor Viren und anderen Sicherheitsbedrohungen bei. [Wie trägt ein Firewall zum Schutz des Computers bei?](#)

**Firewall INAKTIV / Firewall aus**

Sie erhalten die folgende Meldung, sobald Sie die Avira FireWall deaktivieren:



**Firewall** INAKTIV

Avira FireWall hat gemeldet, dass es momentan deaktiviert ist. Ein Firewall trägt zum Schutz des Computers vor potentiell schädlichen Inhalten aus dem Internet bei. Klicken Sie auf "Empfehlungen", um Informationen zur Behebung des Problems zu erhalten. [Wie trägt ein Firewall zum Schutz des Computers bei?](#)

Empfehlungen...

**Hinweis**

Sie können die Avira FireWall über Status im Control Center aktivieren bzw. deaktivieren.

**Warnung**

Wenn Sie die Avira FireWall deaktivieren, ist Ihr Computer nicht länger vor dem unautorisierten Zugriff über das Netzwerk oder das Internet geschützt.

**Virenschutzsoftware / Schutz vor schädlicher Software**

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

Virenschutz NICHT GEFUNDEN

Virenschutz NICHT AKTUELL

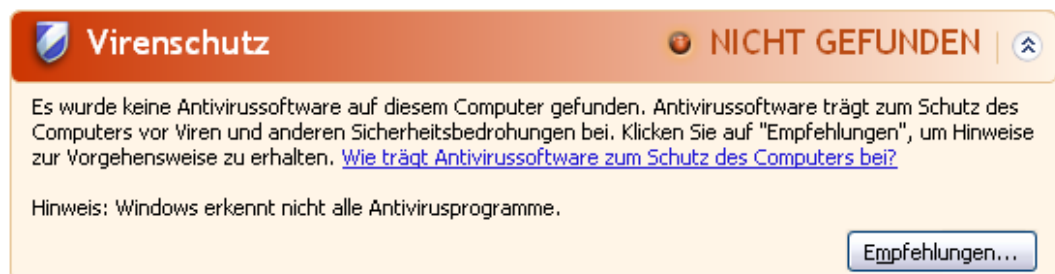
Virenschutz AKTIV

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.



**Virenschutz** NICHT GEFUNDEN

Es wurde keine Antivirussoftware auf diesem Computer gefunden. Antivirussoftware trägt zum Schutz des Computers vor Viren und anderen Sicherheitsbedrohungen bei. Klicken Sie auf "Empfehlungen", um Hinweise zur Vorgehensweise zu erhalten. [Wie trägt Antivirussoftware zum Schutz des Computers bei?](#)

Hinweis: Windows erkennt nicht alle Antivirusprogramme.

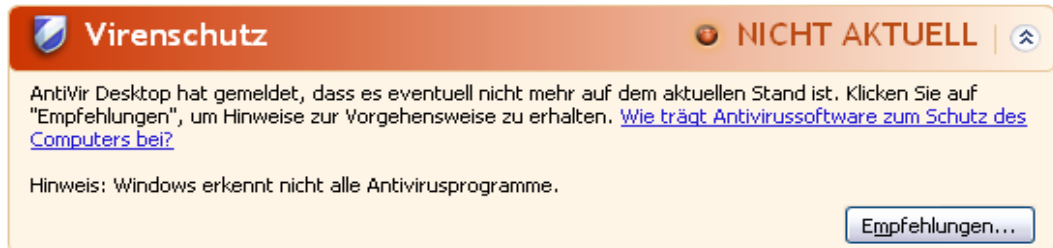
Empfehlungen...

**Hinweis**

Installieren Sie Ihr AntiVir Programm 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 Ihr AntiVir Programm oder aber installieren Sie den Windows XP Service Pack 2 bzw. Windows Vista auf ein System, auf dem Ihr AntiVir Programm bereits installiert war erhalten sie folgende Meldung:

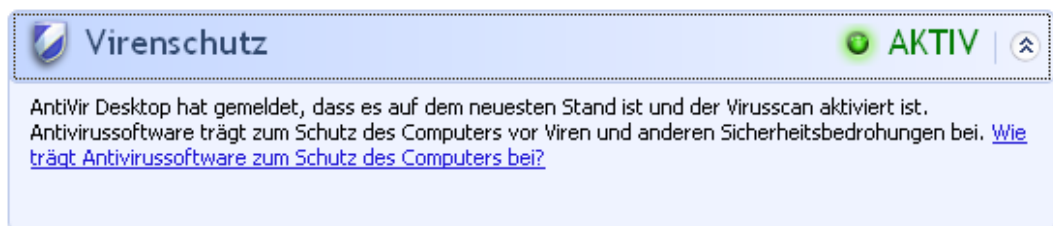


**Hinweis**

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

**Virenschutz AKTIV**

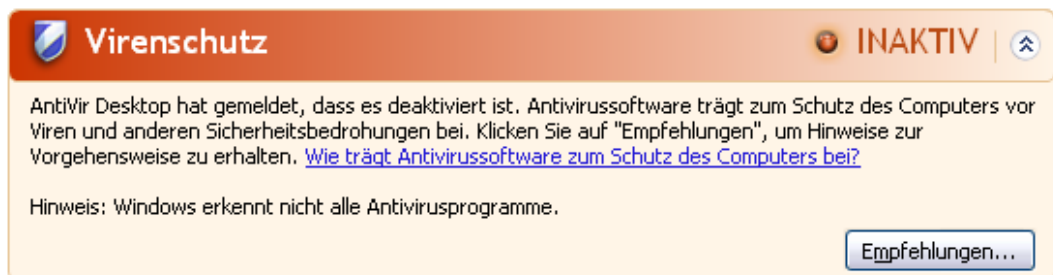
Nach der Installation Ihres AntiVir Programms und einem im Anschluss daran durchgeführten Update erhalten Sie folgenden Hinweis:



Ihr AntiVir Programm 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 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**

Die Funktion wird von Windows Vista nicht unterstützt.

 **Virenschutz**  **NICHT ÜBERWACHT** 

Sie haben angegeben, dass Sie die Antivirussoftware selbst überwachen. Stellen Sie sicher, dass die Antivirussoftware aktiviert ist und halten Sie sie auf dem neuesten Stand, um den Computer gegenüber Viren oder anderen Sicherheitsbedrohungen zu schützen. [Wie trägt Antivirussoftware zum Schutz des Computers bei?](#)

---

**Hinweis**

Das Windows Sicherheitscenter wird von Ihrem AntiVir Programm 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. 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!

---

# 10 Viren und mehr

## 10.1 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 überbewertete 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 Ihr AntiVir Programm die ihm bekannten kostenverursachende Einwahlprogramme.

Ist in der Konfiguration unter Gefahrenkategorien die Option **Kostenverursachende Einwahlprogramme (DIALER)** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden eines kostenverursachenden Einwahlprogramms eine 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.

Ihr AntiVir Programm erkennt Computerspiele. Ist in der Konfiguration unter Gefahrenkategorien die Option **Spiele (GAMES)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.

Ihr AntiVir Programm 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 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.

Ihr AntiVir Programm erkennt "Security Privacy Risk" Software. Ist in der Konfiguration unter Gefahrenkategorien die Option **Security Privacy Risk (SPR)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.

Ihr AntiVir Programm erkennt "Backdoor Steuersoftware". Ist in der Konfiguration unter Gefahrenkategorien die Option **Backdoor-Steuersoftware (BDC)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.

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

### Ungewöhnliche Laufzeitpacker (PCK)

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

Ihr AntiVir Programm erkennt "Ungewöhnliche Laufzeitpacker". Ist in der Konfiguration unter Gefahrenkategorien die Option **Ungewöhnliche Laufzeitpacker (PCK)** aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.

Ihr AntiVir Programm erkennt "Dateien mit verschleierte Dateieindungen". Ist in der Konfiguration unter Gefahrenkategorien die Option **Dateien mit verschleierte Dateieindungen (HEUR-DBLEXT)** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.

Ihr AntiVir Programm erkennt "Phishing". Ist in der Konfiguration unter Gefahrenkategorien die Option **Phishing** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr AntiVir Programm 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.



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

## 10.2 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.

# 11 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

## 11.1 Kontaktadresse

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

## 11.2 Technischer Support

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

Auf unserer Webseite erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service:

<http://www.avira.de/professional-support>

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

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

## 11.3 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 Quarantänenmanager 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 folgende Adresse:  
virus-professional@avira.de  
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: <http://www.avira.de/sample-upload>

## 11.4 Fehlalarm melden

Sind Sie der Meinung, dass Ihr AntiVir Programm einen Fund in einer Datei meldet, die jedoch mit hoher Wahrscheinlichkeit "sauber" ist, so senden Sie diese Datei, gepackt (WinZIP, PKZIP, Arj etc.) im Anhang einer Email, an folgende Adresse:

- virus-professional@avira.de

Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

## 11.5 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 Lösung der Avira GmbH 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 folgende Adresse:

vulnerabilities-professional@avira.de

## 12 Referenz: Konfigurationsoptionen

Die Referenz der Konfiguration dokumentiert alle verfügbaren Konfigurationsoptionen.

### 12.1 Scanner

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

#### 12.1.1 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 vom Programm übernommen. D.h. Ihr AntiVir Programm 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 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 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.

### **Integritätsprüfung von Systemdateien**

Bei aktivierter Option werden bei jeder Direktsuche die wichtigsten Windows Systemdateien einer besonders sicheren Prüfung auf Veränderungen durch Malware unterzogen. Wird eine veränderte Datei gefunden, wird diese als verdächtiger Fund gemeldet. Die Funktion nimmt viel Rechnerleistung in Anspruch. Daher ist die Option standardmäßig deaktiviert.

### **Wichtig**

Die Option ist nur ab Windows Vista verfügbar. Falls Sie AntiVir Programm unter SMC administrieren ist die Option nicht verfügbar.

### **Hinweis**

Falls Sie Drittanbieter Tools einsetzen, die Systemdateien verändern und den Boot- oder Startbildschirm auf eigene Bedürfnisse anpassen, sollten Sie diese Option nicht verwenden. Beispiele für diese Tools sind sogenannte Skinpacks, TuneUp Utilities oder Vista Customization.

### **Optimierter Suchlauf**

Bei aktivierter Option wird die Prozessor-Kapazität bei einem Suchlauf des Scanner optimal ausgelastet. Aus Gründen der Performance erfolgt die Protokollierung beim optimierten Suchlauf höchstens auf einem Standard-Level.



### **Hinweis**

Die Option ist nur bei Multi-Prozessor-Rechnern verfügbar. Wird Ihr AntiVir Programm über SMC administriert, wird die Option in jedem Fall angezeigt und kann aktiviert werden: Falls der administrierte Rechner nicht über mehrere Prozessoren verfügt, wird die Option vom Scanner nicht genutzt.

### **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 unter Windows XP 64 Bit nicht verfügbar!

### **Registry durchsuchen**

Bei aktivierter Option wird bei einem Suchlauf die Registry nach Verweisen auf Schadsoftware durchsucht.

### **Keine Dateien und Pfade auf Netzlaufwerken durchsuchen**

Bei aktivierter Option sind mit dem Computer verbundene Netzlaufwerke von der Direktsuche ausgenommen. Diese Option empfiehlt sich, wenn die Server oder andere Workstations selbst durch eine Antiviren-Software geschützt werden. Diese Option ist standardmäßig deaktiviert.

## **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.

## 12.1.1.1. 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 werden Funde der Suche des Scanners in einem Dialogfenster gemeldet. Bei der Suche des Scanners erhalten Sie beim Abschluss des Suchlaufs eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den Scanner beenden.

### **Hinweis**

Im Scanner-Dialog wird die Aktion 'In Quarantäne verschieben' als Standardaktion angezeigt.

### **Erlaubte Aktionen**

In diesem Anzeigebereich können Sie Aktionen auswählen, die beim Virenfund im individuellen oder im Experten-Benachrichtigungsmodus im Dialogfenster ausgewählt werden können. 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 umbenannt werden.

### **Quarantäne**

Der Scanner verschiebt die Datei in die Quarantäne. Die Datei kann vom Quarantänenanager aus wiederhergestellt werden, 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. 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 der Schaltfläche legen Sie eine Standardaktion des Scanners zur Behandlung von betroffenen Dateien fest. Markieren Sie eine Aktion und klicken Sie auf die Schaltfläche "**Standard**". Im kombinierten Benachrichtigungsmodus kann nur die ausgewählte Standardaktion für die betroffenen Dateien ausgeführt werden. Im individuellen und Experten-Benachrichtigungsmodus ist die ausgewählte Standardaktion für die betroffenen Dateien vorausgewählt.

### **Hinweis**

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

### **Hinweis**

Wenn Sie als Standardaktion *löschen* oder *überschreiben und löschen* ausgewählt haben und den Benachrichtigungsmodus auf kombiniert setzen möchten, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

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 er 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. 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. 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.

### **Hinweis**

Wenn Sie als primäre oder sekundäre Aktion **löschen** oder **überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

## 12.1.1.2. Weitere Aktionen

### **Programm nach Fund starten**

Nach der Direktsuche kann der Scanner eine Datei Ihrer Wahl (beispielsweise ein Programm) öffnen, wenn mindestens ein Virus oder unerwünschtes Programm gefunden wurde, z.B. ein Email-Programm, damit Sie andere Nutzer oder den Administrator benachrichtigen können.

### **Hinweis**

Aus Sicherheitsgründen ist es nur möglich ein Programm nach einem Fund zu starten, wenn ein Benutzer am Computer angemeldet ist. Die Datei wird dann mit den Rechten gestartet, die für den angemeldeten Benutzer gelten. Ist kein Benutzer angemeldet, wird diese Option nicht ausgeführt.

### **Programmname**

In diesem Eingabefeld können Sie den Namen sowie den dazugehörigen Pfad des Programms eingeben, welches der Scanner nach einem Fund starten soll.



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

### **Argumente**

In diesem Eingabefeld können Sie ggf. Kommandozeilenparameter des zu startenden Programms eintragen.

## **Ereignisprotokoll**

### **Ereignisprotokoll verwenden**

Bei aktivierter Option wird nach einem erfolgten Suchlauf des Scanner eine Ereignismeldung mit den Ergebnissen der Suche an die Windows Ereignisprotokollierung übergeben. Die Ereignisse können in der Windows Ereignisanzeige abgerufen werden. Die Option ist standardmäßig deaktiviert.

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 Dateierweiterung 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 Dateierweiterung \*.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.

### **Archiv-Liste**

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

## 12.1.1.3. 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 Dateiojekt 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 Dateiojekt 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 Dateiojekt: `D:\ = D:\file.txt` wird von der Suche des Scanner ausgenommen, `D:\folder\file.txt` wird nicht von der Suche ausgenommen.

**Hinweis**

Wenn Sie das AntiVir Programm unter SMC administrieren, können Sie Variablen in Pfadangaben bei Dateiausnahmen verwenden. Eine Liste der Variablen, die Sie verwenden können, finden Sie unter Variablen: Guard- und Scanner-Ausnahmen.

#### 12.1.1.4. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

AntiVir Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware 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 Malware 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**

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

### **Advanced Heuristic Analysis and Detection (AHeAD)**

#### **AHeAD aktivieren**

Ihr AntiVir Programm beinhaltet mit der AntiVir AHeAD Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware 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 wird weniger unbekannte Malware erkannt, 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 wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

## 12.1.2 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.

## 12.2 Guard

Die Rubrik Guard der Konfiguration ist für die Konfiguration der Echtzeitsuche zuständig.

### 12.2.1 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 vom Programm übernommen. Dies bedeutet, dass das Programm 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. Die Archivsuche wird über die Rekursionstiefe, die Anzahl der zu durchsuchenden Dateien und die Archivgröße eingeschränkt. Sie können die maximale Rekursionstiefe, die Anzahl der zu durchsuchenden Dateien und die maximale Archivgröße einstellen.

**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 wendet der Guard eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Sie können die Rekursionstiefe festlegen. Der Standardwert für die Rekursionstiefe ist 1 und wird empfohlen: Alle Archive, die direkt im Hauptarchiv liegen, werden durchsucht.

**Maximale Anzahl Dateien**

Bei der Suche in Archiven wird die Suche auf eine maximale Anzahl von Dateien im Archiv beschränkt. Der Standardwert für die maximale Anzahl zu durchsuchender Dateien ist 10 und wird empfohlen.

**Maximale Größe (KB)**

Bei der Suche in Archiven wird die Suche auf eine maximale, zu entpackende Archivgröße beschränkt. Der Standardwert ist 1000 KB und wird empfohlen.

**Laufwerke**

**Netzlaufwerke**

Bei aktivierter Option werden Dateien auf Netzlaufwerken (gemappte Laufwerke) wie z.B. Server-Volumes, Peer-Laufwerke, etc. überwacht.

**Hinweis**

Um die Leistungsfähigkeit Ihres Rechners nicht zu stark zu beeinträchtigen, sollte die Option **Netzlaufwerke** nur im Ausnahmefall aktiviert werden.

**Warnung**

Bei deaktivierter Option werden die Netzlaufwerke **nicht** überwacht. Sie sind nicht mehr vor Viren bzw. unerwünschten Programmen geschützt!

**Hinweis**

Wenn Dateien auf Netzlaufwerken ausgeführt werden, werden diese vom Guard durchsucht - unabhängig von der Einstellung der Option *Netzlaufwerke*. In einigen Fällen werden Dateien auf Netzlaufwerken beim Öffnen durchsucht, obwohl die Option *Netzlaufwerke* deaktiviert ist. Der Grund: Auf diese Dateien wird mit der Berechtigung 'Datei ausführen' zugegriffen. Wenn Sie diese Dateien oder auch ausgeführte Dateien auf Netzlaufwerken von einer Überwachung des Guard ausnehmen wollen, tragen Sie die Dateien in die Liste der auszulassenden Dateiobjekte ein (siehe: Guard::Suche::Ausnahmen).

**Caching aktivieren**

Bei aktivierter Option werden überwachte Dateien auf Netzlaufwerken im Cache des Guard zur Verfügung gestellt. Die Überwachung von Netzlaufwerken ohne Caching-Funktion bietet mehr Sicherheit, ist jedoch weniger performant als die Überwachung von Netzlaufwerken mit Caching-Funktion.

## 12.2.1.1. 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 bei einem Fund des Guard eine Desktop-Benachrichtigung. Sie haben die Möglichkeit, die gefundene Malware zu entfernen oder weitere mögliche Aktionen zur Virenbehandlung über die Schaltfläche 'Details' abzurufen. Die Aktionen werden in einem Dialogfenster angezeigt. Diese Option ist standardmäßig aktiviert.

### Erlaubte Aktionen

In diesem Anzeigebereich können Sie diejenigen Aktionen auswählen, die als weitere Aktionen im Dialogfenster zur Virenbehandlung zur Verfügung stehen sollen. 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. 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.

### 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 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.

### **Primäre Aktion**

Die 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. 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. 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.

#### **Hinweis**

Wenn Sie als primäre oder sekundäre Aktion **löschen** oder **überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

## 12.2.1.2. Weitere Aktionen

### **Benachrichtigungen**

#### **Ereignisprotokoll**

##### **Ereignisprotokoll verwenden**

Bei aktivierter Option wird bei jedem Fund ein Eintrag in das Windows Ereignisprotokoll geschrieben. Die Ereignisse können in der Windows Ereignisanzeige abgerufen werden. Diese Einstellung ist standardmäßig aktiviert.

### **Autostart**

#### **Autostart-Funktion blockieren**

Bei aktivierter Option wird die Ausführung der Windows Autostart-Funktion auf allen eingebundenen Laufwerken wie USB-Sticks, CD- und DVD-Laufwerken, Netzlaufwerken blockiert. Mit der Windows Autostart-Funktion werden Dateien auf Datenträgern oder Netzlaufwerken beim Einlegen oder beim Verbinden sofort gelesen, Dateien können so automatisch gestartet und wiedergegeben werden. Diese Funktionalität birgt jedoch ein hohes Sicherheitsrisiko, da mit dem automatischen Start von Dateien Malware und unerwünschte Programme installiert werden können. Besonders kritisch ist die Autostart-Funktion für USB-Sticks, da sich Daten auf einem Stick ständig ändern können.

#### **CD's und DVD's ausnehmen**

Bei aktivierter Option wird die Autostart-Funktion auf CD- und DVD-Laufwerken zugelassen.

#### **Warnung**

Deaktivieren Sie die Autostart-Funktion für CD- und DVD-Laufwerke nur dann, wenn Sie sicher sind, dass Sie ausschließlich vertrauenswürdige Datenträger verwenden.

### 12.2.1.3. 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.

Beachten Sie bei der Angabe von auszulassenden Prozessen und Dateiobjekten folgendes: Die Liste wird von oben nach unten abgearbeitet. Je länger die Liste ist, desto mehr Prozessorzeit braucht die Abarbeitung der Liste für jeden Zugriff. Halten Sie deshalb die Listen möglichst klein.

#### **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 werden soll. Standardmäßig ist kein Prozess eingegeben.

#### **Hinweis**

Sie können bis zu 128 Prozesse eingeben.

#### **Hinweis**

Bei der Angabe des Prozesses werden Unicode-Zeichen akzeptiert. Sie können daher Prozess- oder Verzeichnisnamen angeben, die Sonderzeichen enthalten.

### **Hinweis**

Sie haben die Möglichkeit, Prozesse ohne vollständige Pfadangabe von der Überwachung des Guard auszunehmen:

anwendung.exe

Dies gilt jedoch ausschließlich für Prozesse, deren ausführbare Dateien auf Laufwerken der Festplatte liegen.

Eine vollständige Pfadangabe ist bei Prozessen erforderlich, deren ausführbare Dateien auf verbundenen Laufwerken, z.B. Netzlaufwerken liegen. Beachten Sie hierzu die allgemeinen Hinweise zur Notation von Ausnahmen auf verbundenen Netzlaufwerken. Geben Sie keine Ausnahmen für Prozesse an, deren ausführbare Dateien auf dynamischen Laufwerken liegen. Dynamische Laufwerke werden für Wechseldatenträger wie CD, DVD oder USB-Stick verwendet.

### **Hinweis**

Laufwerke müssen wie folgt angegeben werden: [Laufwerksbuchstabe]:\

Das Zeichen Doppelpunkt (:) darf nur zur Angabe von Laufwerken verwendet werden.

### **Hinweis**

Bei der Angabe des Prozesses können Sie die Platzhalter \* (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden:

C:\Programme\Anwendung\anwendung.exe

C:\Programme\Anwendung\anwendun?.exe

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

C:\Programme\Anwendung\\*.exe

Um zu vermeiden, dass Prozesse global von der Überwachung des Guard ausgenommen werden, sind Angaben ungültig, die ausschließlich aus folgenden Zeichen bestehen: \* (Stern), ? (Fragezeichen), / (Slash), \ (Backslash), . (Punkt), : (Doppelpunkt).

### **Hinweis**

Der angegebene Pfad und der Dateiname des Prozesses dürfen maximal 255 Zeichen enthalten. Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

### **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.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, eine ausführbare Datei auszuwählen.

### **Prozesse**

Die Schaltfläche "**Prozesse**" öffnet das Fenster "*Prozessauswahl*", in dem die laufenden Prozesse angezeigt werden.

### **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.

### **Eingabefeld**

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

### **Hinweis**

Bei der Angabe von auszulassenden Dateiobjekten können Sie die Platzhalter \* (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden. Es können auch einzelne Dateierweiterungen ausgenommen werden (inklusive Platzhalter):

C:\Verzeichnis\\*.mdb

\*.mdb

\*.md?

\*.xls\*

C:\Verzeichnis\\*.log

### **Hinweis**

Verzeichnisnamen müssen mit einem Backslash \ abgeschlossen sein, ansonsten wird ein Dateiname angenommen.

### **Hinweis**

Die Einträge der Liste dürfen zusammen nicht mehr als 6000 Zeichen ergeben.

### **Hinweis**

Wenn ein Verzeichnis ausgenommen wird, werden automatisch auch alle darunter liegende Verzeichnisse mit ausgenommen.

### **Hinweis**

Pro Laufwerk können Sie maximal 20 Ausnahmen mit vollständigem Pfad (beginnend mit dem Laufwerksbuchstaben) angeben.

Bsp.: C:\Programme\Anwendung\Name.log

Die maximale Anzahl von Ausnahmen ohne vollständigen Pfad beträgt 64.

Bsp: \*.log

\Rechner1\C\Verzeichnis1

### **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.



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 bei der Angabe von Ausnahmen die weiteren Hinweise:

**Hinweis**

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**

Beachten Sie bei Ausnahmen auf verbundenen Netzlaufwerken folgendes: Wenn Sie den Laufwerksbuchstaben des verbundenen Netzlaufwerks verwenden, werden die angegebenen Dateien und Verzeichnisse NICHT von der Suche des Guard ausgenommen. Wenn der UNC-Pfad in der Liste der Ausnahmen vom UNC-Pfad, der zur Verbindung mit dem Netzlaufwerk genutzt wird, abweicht (Angabe von IP-Adresse in Liste der Ausnahmen - Angabe vom Computernamen zur Verbindung mit Netzlaufwerk) werden die angegebenen Verzeichnisse und Dateien NICHT von der Suche des Guard ausgenommen. Ermitteln Sie den zu verwendenden UNC-Pfad anhand der Report-Datei des Guard:

```
\\<Computernamen>\<Freigabe>\ - ODER- \\<IP-Adresse>\<Freigabe>\
```

**Hinweis**

Anhand der Report-Datei des Guard können Sie die Pfade ermitteln, die der Guard bei der Suche nach betroffenen Dateien verwendet. Verwenden Sie grundsätzlich in der Liste der Ausnahmen dieselben Pfade. Gehen Sie wie folgt vor: Setzen Sie die Protokoll-Funktion des Guard in der Konfiguration unter Guard :: Report auf **Vollständig**. Greifen Sie nun mit dem aktivierten Guard auf die Dateien, Verzeichnisse, eingebundenen Laufwerke oder verbundenen Netzlaufwerke zu. Sie können nun den zu verwendenden Pfad aus der Reportdatei des Guard auslesen. Die Reportdatei rufen Sie im Control Center unter Lokaler Schutz :: Guard ab.

**Hinweis**

Wenn Sie das AntiVir Programm unter SMC administrieren, können Sie Variablen in Pfadangaben bei Prozess- und Dateiausnahmen verwenden. Eine Liste der Variablen, die Sie verwenden können, finden Sie unter Variablen: Guard- und Scanner-Ausnahmen.

Beispiele für auszunehmende Prozesse:

- anwendung.exe

Der Prozess von anwendung.exe wird von der Suche des Guard ausgenommen, unabhängig davon auf welchem Festplattenlaufwerk und in welchem Verzeichnis anwendung.exe liegt.

- C:\Programme1\anwendung.exe

Der Prozess von der Datei anwendung.exe, die unter dem Pfad C:\Programme1 liegt, wird von der Suche des Guard ausgenommen.

- C:\Programme1\\*.exe

Alle Prozesse von ausführbaren Dateien, die unter dem Pfad C:\Programme1 liegen, werden von der Suche des Guard ausgenommen.

Beispiele für auszunehmende Dateien:

- \*.mdb

Alle Dateien mit der Dateierweiterung 'mdb' werden von einer Suche des Guard ausgenommen.

- \*.xls\*

Alle Dateien, deren Dateierweiterung mit 'xls' beginnt, werden von der Suche des Guard ausgenommen, z.B. Dateien mit den Dateierweiterungen .xls und xlsx.

- C:\Verzeichnis\\*.log

Alle Log-Dateien mit der Dateierweiterung 'log', die unter dem Pfad C:\Verzeichnis liegen, werden von der Suche des Guard ausgenommen.

- \\Computername1\Freigabe1\

Alle Dateien werden von der Suche des Guard ausgenommen, auf die mit einer Verbindung '\\Compuername1\Freigabe1' zugegriffen wird. Dies ist meist ein verbundenes Netzlaufwerk, welches mit dem Computernamen 'Computername1' und dem Freigabenamen 'Freigabe1' auf einen anderen Rechner mit freigegebenem Verzeichnis zugreift.

- \\1.0.0.0\Freigabe1\\*.mdb

Alle Dateien mit der Dateierweiterung 'mdb' werden von der Suche des Guard ausgenommen, auf die mit einer Verbindung '\\1.0.0.0\Freigabe1' zugegriffen wird. Dies ist meist ein verbundenes Netzlaufwerk, welches mit der IP-Adresse '1.0.0.0' und dem Freigabenamen 'Freigabe1' auf einen anderen Rechner mit freigegebenem Verzeichnis zugreift.

-

#### 12.2.1.4. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

AntiVir Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware 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 Malware 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

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

### Advanced Heuristic Analysis and Detection (AHeAD)

#### AHeAD aktivieren

Ihr AntiVir Programm beinhaltet mit der AntiVir AHeAD Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware 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 wird weniger unbekannte Malware erkannt, 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 wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

## 12.2.2 ProActiv

Mit dem Einsatz von Avira AntiVir ProActiv schützen Sie sich vor neuen und unbekanntem Bedrohungen, für die noch keine Virendefinitionen und Heuristiken vorliegen. Die ProActiv-Technologie ist in die Komponente Guard integriert und beobachtet und analysiert die ausgeführten Aktionen von Programmen. Das Verhalten von Programmen wird auf typische Aktionsmuster von Malware untersucht: Art der Aktion und Aktionsabfolgen. Falls ein Programm ein für Malware typisches Verhalten zeigt, wird dies wie ein Virenfund behandelt und gemeldet : Sie haben die Möglichkeit, die Ausführung des Programms zu blockieren oder die Meldung zu ignorieren und die Ausführung des Programms fortzusetzen. Sie können das Programm als vertrauenswürdig einstufen und so zum Anwendungsfilter der erlaubten Programme hinzufügen. Sie haben auch die Möglichkeit, das Programm über die Anweisung *Immer blockieren* zum Anwendungsfilter der zu blockierenden Programme hinzuzufügen.

Zur Ermittlung des verdächtigen Verhaltens verwendet die ProActiv-Komponente Regelsets, die vom Avira Malware Research Center entwickelt wurden. Die Regelsets werden von den Datenbanken der Avira GmbH gespeist. Zur Informationserfassung in den Avira Datenbanken sendet Avira AntiVir ProActiv Informationen über gemeldete, verdächtige Programme. Sie haben die Möglichkeit, die Datenübermittlung an die Avira Datenbanken zu deaktivieren.

#### **Hinweis**

Die ProActiv-Technologie ist für 64-Bit-Systeme noch nicht verfügbar! Unter Windows 2000 besteht keine Unterstützung für die ProActiv-Komponente.

## Allgemein

### Avira AntiVir ProActiv aktivieren

Bei aktivierter Option werden Programme auf Ihrem Computersystem überwacht und auf verdächtige Aktionen überprüft. Tritt ein Verhalten auf, das für Malware typisch ist, erhalten Sie eine Meldung. Sie können das Programm blockieren oder mit "Ignorieren" die Ausführung des Programms fortsetzen. Von der Überwachung ausgenommen sind: Als vertrauenswürdig eingestufte Programme, vertrauenswürdige und signierte Programme, die standardmäßig im Anwendungsfiler der erlaubten Anwendungen enthalten sind, alle Programme, die Sie zum Anwendungsfiler der erlaubten Programme hinzugefügt haben.

### Die Sicherheit ihres Computers durch Ihre Teilnahme an der AntiVir ProActiv Community verbessern

Bei aktivierter Option sendet Avira AntiVir ProActiv Daten zu verdächtigen Programmen und in einigen Fällen verdächtige Programmdateien (ausführbare Dateien) an das Avira Malware Research Center zur erweiterten Online-Prüfung. Die Daten gehen nach ihrer Auswertung in die Regelsets der ProActiv-Verhaltensanalyse ein. So nehmen Sie an der Avira ProActiv-Community teil und leisten einen Beitrag zur kontinuierlichen Verbesserung und Verfeinerung der ProActiv-Sicherheitstechnologie. Bei deaktivierter Option werden keine Daten gesendet. Dies hat keine Auswirkungen auf die Funktionalität von ProActiv.

### Klicken Sie hier für weitere Informationen

Über den Link gelangen Sie auf eine Internetseite, auf der Sie detaillierte Informationen über die erweiterte Online-Prüfung erhalten. Die Daten, die bei einer erweiterten Online-Prüfung übertragen werden, werden auf der Internetseite vollständig angegeben.

## 12.2.2.1. Anwendungsfiler: Zu blockierende Anwendungen

Unter *Anwendungsfiler: Zu blockierende Anwendungen* können Sie Anwendungen einpflegen, die Sie als schädlich einstufen und die von Avira AntiVir ProActiv standardmäßig geblockt werden sollen. Die eingepflegten Anwendungen können auf Ihrem Computersystem nicht ausgeführt werden. Sie können Programme dem Anwendungsfiler für zu blockierende Anwendungen auch über die Meldungen des Guard zu einem verdächtigen Programmverhalten hinzufügen, indem Sie die Option *Dieses Programm immer blockieren* nutzen.

### **Zu blockierende Anwendungen**

#### **Anwendungen**

In der Liste sind alle Anwendungen aufgeführt, die Sie als schädlich eingestuft und über die Konfiguration oder über die Meldungen der ProActiv-Komponente eingefügt haben. Die Anwendungen der Liste werden von Avira AntiVir ProActiv blockiert und können auf Ihrem Computersystem nicht ausgeführt werden. Beim Start eines zu blockierenden Programms erscheint eine Meldung des Betriebssystems. Die zu blockierenden Anwendungen werden von Avira AntiVir ProActiv anhand des angegebenen Pfads und des Dateinamens identifiziert und unabhängig von ihrem Inhalt blockiert.

#### **Eingabefeld**

In diesem Feld geben Sie die Anwendung an, die blockiert werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiergung angegeben werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die zu blockierende Anwendung auszuwählen.

### Hinzufügen

Mit der Schaltfläche "**Hinzufügen**" können Sie die im Eingabefeld angegebene Anwendung in die Liste der zu blockierenden Anwendungen übernehmen.

### Hinweis

Anwendungen, die für die Funktionsfähigkeit des Betriebssystems erforderlich sind, können nicht hinzugefügt werden.

### Löschen

Mit der Schaltfläche "**Löschen**" entfernen Sie eine markierte Anwendung aus der Liste der zu blockierenden Anwendungen.

## 12.2.2.2. Anwendungsfiler: Erlaubte Anwendungen

Unter *Anwendungsfiler: Erlaubte Anwendungen* sind Anwendungen gelistet, die von der Überwachung der ProActiv-Komponente ausgenommen sind: Signierte Programme, die als vertrauenswürdig eingestuft wurden und standardmäßig in der Liste enthalten sind, alle Anwendungen, die Sie als vertrauenswürdig eingestuft und in den Anwendungsfiler eingepflegt haben: Sie können in der Konfiguration Anwendungen zur Liste der erlaubten Anwendungen hinzufügen. Sie haben auch die Möglichkeit, über die Meldungen des Guard zu einem verdächtigen Programmverhalten Anwendungen hinzuzufügen, indem Sie in der Guard-Meldung die Option **Vertrauenswürdiges Programm** nutzen.

### Auszulassende Anwendungen

### Anwendungen

Die Liste enthält Anwendungen, die von der Überwachung der ProActiv Komponente ausgenommen sind. In den Standardeinstellungen nach der Installation enthält die Liste signierte Anwendungen von vertrauenswürdigen Herstellern. Sie haben die Möglichkeit, Anwendungen, die Sie als vertrauenswürdig einstufen, über die Konfiguration oder über Meldungen des Guard einzupflegen. Die ProActiv-Komponente identifiziert Anwendungen anhand des Pfades, des Dateinamens und des Inhalts. Eine Inhaltsprüfung ist sinnvoll, da einem Programm über Veränderungen wie Updates nachträglich Schadcode hinzugefügt werden kann. Sie können über den angegebenen Typ festlegen, ob eine Inhaltsprüfung erfolgen soll: Beim Typ "*Inhalt*" werden die mit Pfad und Dateinamen angegebenen Anwendungen auf Veränderungen des Dateiinhalts geprüft, bevor Sie von der Überwachung durch die ProActiv-Komponente ausgenommen werden. Bei einem veränderten Dateiinhalt wird die Anwendung von der ProActiv-Komponente wieder überwacht. Beim Typ "*Pfad*" erfolgt keine Inhaltsüberprüfung, bevor die Anwendung von der Überwachung durch den Guard ausgenommen wird. Um den Ausschlusstyp zu wechseln, klicken Sie den angezeigten Typ an.

### **Warnung**

Verwenden Sie den Typ *Pfad* nur in Ausnahmefällen. Durch ein Update kann einer Anwendung Schadcode hinzugefügt werden. Die ursprünglich harmlose Anwendung ist nun Malware.

### **Hinweis**

Einige vertrauenswürdige Anwendungen, wie z.B. alle Anwendungskomponenten Ihres AntiVir Programms, sind standardmäßig von einer Überwachung durch die ProActiv-Komponente ausgenommen, sind aber in der Liste nicht aufgeführt.

### **Eingabefeld**

In diesem Feld geben Sie die Anwendung an, die von der Überwachung durch die ProActiv-Komponente ausgenommen werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiendung angegeben werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die auszulassende Anwendung auszuwählen.

### **Hinzufügen**

Mit der Schaltfläche "**Hinzufügen**" können Sie die im Eingabefeld angegebene Anwendung in die Liste der auszulassenden Anwendungen übernehmen.

### **Löschen**

Mit der Schaltfläche "**Löschen**" entfernen Sie eine markierte Anwendung aus der Liste der auszulassenden Anwendungen.

## 12.2.3 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. Bei der Beschränkung der Reportdatei 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 weniger 50 Kilobytes erreicht worden ist.

### **Reportdatei vor dem Kürzen sichern**

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert. Sicherungsort siehe Konfiguration :: Allgemeines :: Verzeichnisse :: Reportverzeichnis.

### **Konfiguration in Reportdatei schreiben**

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

### **Hinweis**

Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.

## 12.3 MailGuard

Die Rubrik MailGuard der Konfiguration ist für die Konfiguration des MailGuard zuständig.

### 12.3.1 Suche



Sie nutzen den MailGuard, um eingehende Emails auf Viren und Malware zu prüfen. Ausgehende Emails können vom MailGuard auf Viren und Malware geprüft werden.

### Suche

#### MailGuard einschalten

Bei aktivierter Option wird der Email-Verkehr durch den MailGuard überwacht. Der MailGuard ist ein Proxy-Server, der den Datenverkehr zwischen dem Email-Server, den Sie verwenden, und dem Email-Client-Programm auf Ihrem Computersystem prüft: In den Standardeinstellungen werden eingehende Emails nach Malware durchsucht. Bei deaktivierter Option bleibt der MailGuard-Dienst gestartet, die Überwachung durch den MailGuard ist jedoch deaktiviert.

#### Eingehende Emails durchsuchen

Bei aktivierter Option werden eingehende Emails auf Viren und Malware geprüft. MailGuard unterstützt die Protokolle POP3 und IMAP. Aktivieren Sie das Posteingangskonto, welches von Ihrem Email-Client zum Empfang von Emails genutzt wird, zur Überwachung durch den MailGuard.

#### POP3-Konten überwachen

Bei aktivierter Option werden die POP3-Konten an den angegebenen Ports überwacht.

#### Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Posteingang vom Protokoll POP3 genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

#### Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von POP3 zurück.

#### IMAP-Konten überwachen

Bei aktivierter Option werden die IMAP-Konten an den angegebenen Ports überwacht.

#### Überwachte Ports

In diesem Feld geben Sie den Port ein, der vom Protokoll IMAP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

#### Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von IMAP zurück.

#### Ausgehende Emails durchsuchen (SMTP)

Bei aktivierter Option werden ausgehende Emails auf Viren und Malware geprüft.

#### Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Postausgang vom Protokoll SMTP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

#### Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von SMTP zurück.

#### **Hinweis**

Um die genutzten Protokolle und Ports zu verifizieren, rufen Sie in Ihrem Email-Client-Programm die Eigenschaften Ihrer Email-Konten ab. Meist werden Standard-Ports genutzt.

### 12.3.1.1. Aktion bei Fund

Diese Konfigurationsrubrik enthält Einstellungen, welche Aktionen durchgeführt werden, wenn MailGuard einen Virus bzw. unerwünschtes Programm in einer Email oder in einer Anlage findet.

#### **Hinweis**

Die hier eingestellten Aktionen erfolgen sowohl bei einem Virenfund in eingehenden Emails als auch bei einem Virenfund in ausgehenden Emails.

#### **Aktion bei Fund**

##### Interaktiv

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms in einer Email oder einem Anhang ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Email bzw. der Anlage 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.

##### *In Quarantäne verschieben*

Bei aktivierter Option wird die Email inklusive aller Anhänge in die Quarantäne verschoben. Sie kann später über den Quarantänenanager zugestellt werden. Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge der Email werden durch einen Standardtext ersetzt.

##### *Löschen*

Bei aktivierter Option wird die betroffene Email beim Fund eines Virus bzw. unerwünschten Programms gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

##### *Anhang löschen*

Bei aktivierter Option wird der betroffene Anhang durch einen Standardtext ersetzt. Sollte der Textkörper der Email betroffen sein, wird dieser gelöscht und ebenfalls durch einen Standardtext ersetzt. Die Email selbst wird zugestellt.

##### *Anhang in Quarantäne verschieben*

Bei aktivierter Option wird der betroffene Anhang in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der Textkörper der Email wird zugestellt. Die betroffene Anlage kann später über den Quarantänenanager zugestellt werden.

##### *Ignorieren*

Bei aktivierter Option wird eine betroffene Email trotz des Funds eines Virus oder unerwünschten Programms zugestellt.

##### 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**.

##### Fortschrittsanzeige einblenden

Bei aktivierter Option blendet der MailGuard während des Downloads von Emails eine Fortschrittsanzeige ein. Eine Aktivierung dieser Option ist nur möglich, wenn die Option **Interaktiv** ausgewählt wurde.

### Automatisch

Bei aktivierter Option werden bei dem Fund eines Virus bzw. unerwünschten Programms nicht mehr benachrichtigt. Der MailGuard reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

### Primäre Aktion

Die primäre Aktion, ist die Aktion die ausgeführt wird, wenn der MailGuard einen Virus bzw. ein unerwünschtes Programm in einer Email findet. Ist die Option "**Email ignorieren**" gewählt, kann unter "**Betroffene Anlagen**" zusätzlich ausgewählt werden, was im Falle eines Funds in einer Anlage geschehen soll.

### Email löschen

Bei aktivierter Option wird die betroffene Email beim Fund eines Virus bzw. unerwünschten Programms automatisch gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

### Email isolieren

Bei aktivierter Option wird die komplette Email inkl. aller Anlagen beim Fund eines Virus bzw. unerwünschten Programms in Quarantäne gestellt. Sie kann später - falls gewünscht - wieder hergestellt werden. Die betroffene Email selbst wird gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

### Email ignorieren

Bei aktivierter Option wird die betroffene Email trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert. Sie haben jedoch noch die Möglichkeit zu entscheiden, was mit einer betroffenen Anlage geschehen soll:

### Betroffene Anlagen

Die Option "**Betroffene Anlagen**" ist nur dann auswählbar, wenn unter "**Primäre Aktion**" die Einstellung "**Email ignorieren**" ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was im Fall eines Funds in einer Anlage geschehen soll.

### löschen

Bei aktivierter Option wird die betroffene Anlage beim Fund eines Virus bzw. unerwünschten Programms gelöscht und durch einen Standardtext ersetzt.

### isolieren

Bei aktivierter Option wird die betroffene Anlage in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Die betroffene Anlage (Anlagen) kann später - falls gewünscht - wieder hergestellt werden.

### ignorieren

Bei aktivierter Option wird die Anlage trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert und zugestellt.

---

### **Warnung**

Wenn Sie diese Option wählen, haben Sie keinerlei Schutz vor Viren und unerwünschten Programmen durch den MailGuard. Wählen Sie diesen Punkt nur dann, wenn Sie genau wissen, was Sie tun. Deaktivieren Sie die Vorschau in Ihrem Email-Programm, starten Sie Anlagen auf keinen Fall per Doppelklick!

---

### 12.3.1.2. Andere Aktionen

Diese Konfigurationsrubrik enthält weitere Einstellungen, welche Aktionen durchgeführt werden, wenn MailGuard einen Virus bzw. unerwünschtes Programm in einer Email oder in einer Anlage findet.

#### **Hinweis**

Die hier eingestellten Aktionen erfolgen ausschließlich bei einem Virenfund in eingehenden Emails.

#### **Standardtext für gelöschte und verschobene Emails**

Der Text in diesem Feld wird anstelle der betroffenen Email als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

**Strg** + **Enter** fügt einen Zeilenumbruch ein.

#### **Standard**

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

#### **Standardtext für gelöschte und verschobene Anlagen**

Der Text in diesem Feld wird anstelle der betroffenen Anlage als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

**Strg** + **Enter** fügt einen Zeilenumbruch ein.

#### **Standard**

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

### 12.3.1.3. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

AntiVir Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekanntes Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware 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 Malware 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 aktivieren**

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

## **Advanced Heuristic Analysis and Detection (AHeAD)**

### **AHeAD aktivieren**

Ihr AntiVir Programm beinhaltet mit der AntiVir AHeAD Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware 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 wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

### **Erkennungsstufe mittel**

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

### **Erkennungsstufe hoch**

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

## 12.3.2 Allgemeines

### 12.3.2.1. Ausnahmen


#### **Email-Adressen, die nicht überprüft werden**

Diese Tabelle zeigt Ihnen die Liste der Email-Adressen, die von der Überprüfung durch den AntiVir MailGuard ausgeschlossen wurden (Whitelist).

#### **Hinweis**

Die Liste der Ausnahmen wird ausschließlich bei eingehenden Emails vom MailGuard verwendet.

#### **Status**

<b>Symbol</b>	<b>Beschreibung</b>
	Diese Email-Adresse wird nicht mehr auf Malware überprüft.

#### **Email-Adresse**

Email-Adresse, die nicht mehr durchsucht werden soll.

#### **Malware**

Bei aktivierter Option wird die Email-Adresse nicht mehr auf Malware überprüft.

#### nach oben

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach oben. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der ersten Position in der Liste steht.

#### nach unten

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach unten. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der letzten Position in der Liste steht.

#### Eingabefeld

In diesem Feld geben Sie die Email-Adresse ein, die Sie in die Liste der nicht zu prüfenden Email-Adressen hinzufügen wollen. Die Email-Adresse wird in Zukunft - abhängig von Ihren Einstellungen - nicht mehr vom MailGuard überprüft.

#### Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene Email-Adresse der Liste der nicht zu prüfenden Email-Adressen hinzufügen.

#### Löschen

Die Schaltfläche löscht eine markierte Email-Adresse in der Liste.

### 12.3.2.2. Zwischenspeicher

#### **Zwischenspeicher**

Der MailGuard Zwischenspeicher enthält die Daten zu den durchsuchten Emails, die in der Statistik im Control Center unter MailGuard angezeigt werden.

#### **Maximale Anzahl der im Zwischenspeicher zu speichernden Emails**

In diesem Feld wird die maximale Anzahl der Emails eingegeben, die der MailGuard im Zwischenspeicher aufbewahrt. Es werden jeweils die ältesten Emails gelöscht.

#### **Maximale Speicherdauer einer Email in Tagen**

In diesem Feld ist die maximale Speicherdauer einer Email in Tagen eingegeben. Nach dieser Zeit wird die Email aus dem Zwischenspeicher entfernt.

#### **Zwischenspeicher leeren**

Bei Klick auf die Schaltfläche werden die Emails, die im Zwischenspeicher aufbewahrt werden, gelöscht.

### 12.3.2.3. Fußzeile

Unter *Fußzeile* können Sie eine Email-Fußzeile konfigurieren, die in den Emails, die Sie senden, angezeigt wird. Voraussetzung für die Funktion ist die Aktivierung der MailGuard-Prüfung für ausgehende Emails (siehe Option *Ausgehende Emails durchsuchen (SMTP)* unter Konfiguration::MailGuard::Suche) . Sie können die definierte AntiVir MailGuard Fußzeile nutzen, mit der Sie bestätigen, dass die gesendete Email von einem Virenschutzprogramm geprüft wurde. Sie haben auch die Möglichkeit, selbst einen Text für eine benutzerdefinierte Fußzeile einzugeben. Wenn Sie beide Optionen zur Fußzeile nutzen, wird der benutzerdefinierte Text der AntiVir MailGuard Fußzeile vorangestellt.

### **Fußzeile bei zu versendenden Emails**

#### **AntiVir MailGuard Fußzeile anhängen**

Bei aktivierter Option wird unter dem Nachrichtentext von gesendeten Emails die AntiVir MailGuard Fußzeile angezeigt. Mit der AntiVir MailGuard Fußzeile bestätigen Sie, dass die gesendete Email vom AntiVir MailGuard auf Viren und unerwünschte Programme geprüft wurde. Die AntiVir MailGuard Fußzeile enthält folgenden Text: "Durchsucht mit AntiVir MailGuard [Produktversion] [Namenskürzel und Versionsnummer der Suchengine] [Namenskürzel und Versionsnummer der Virendefinitionsdatei]".

#### **Diese Fußzeile anhängen**

Bei aktivierter Option wird der Text, den Sie im Eingabefeld angeben, als Fußzeile in gesendeten Emails angezeigt.

#### **Eingabefeld**

In diesem Eingabefeld können Sie einen Text eingeben, der als Fußzeile in gesendeten Emails angezeigt wird.

## 12.3.3 Report

Der MailGuard 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 MailGuard 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 MailGuard 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 MailGuard auch weniger wichtige Informationen in die Reportdatei mit auf.

#### **Vollständig**

Bei aktivierter Option nimmt der MailGuard sämtliche Informationen 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. Bei der Beschränkung der Reportdatei 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 weniger 50 Kilobytes erreicht worden ist.

#### **Reportdatei vor dem Kürzen sichern**

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert. Sicherungsort siehe Konfiguration :: Allgemeines :: Verzeichnisse :: Reportverzeichnis.

#### **Konfiguration in Reportdatei schreiben**

Bei aktivierter Option wird die verwendete Konfiguration des MailGuard in die Reportdatei geschrieben.

---

#### **Hinweis**

Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.

---

## 12.4 Firewall

Die Rubrik FireWall der Konfiguration ist für die Konfiguration der Avira FireWall zuständig.

### 12.4.1 Adapterregeln

Als Adapter wird in der Avira FireWall jede von einer Software simulierte Hardwareeinheit (z.B. Miniport, Bridge Connection, usw.) oder jede Hardwareeinheit (z.B. eine Netzwerkkarte) betrachtet.

Die Avira FireWall zeigt die Adapterregeln für alle auf Ihrem Computer existierenden Adapter an, für die ein Treiber installiert ist.

Eine vordefinierte Adapterregel ist abhängig vom Sicherheitsniveau. Sie können das Sicherheitsniveau über die Rubrik Online Schutz :: FireWall des Control Center ändern oder die Adapterregeln auf Ihre Bedürfnisse anpassen. Haben Sie die Adapterregeln auf Ihre Bedürfnisse angepasst, wird unter der Rubrik FireWall des Control Center im Bereich Sicherheitsniveau der Regler auf Benutzer platziert.

---

#### **Hinweis**

Die Standardeinstellung des Sicherheitsniveaus für alle vordefinierten Regeln der Avira FireWall ist **Mittel**.

---

### ICMP-Protokoll



Das Internet Control Message Protocol (ICMP) dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen. Das Protokoll wird auch für Statusmeldungen mittels Ping oder Tracert verwendet.

Mit dieser Regel können Sie ein- und ausgehende ICMP-Typen definieren, die blockiert werden sollen, die Parameter für Flooding festlegen und das Verhalten bei Vorliegen von fragmentierten ICMP-Paketen definieren. Diese Regel dient dazu sogenannte ICMP Flood-Attacken zu verhindern, die zu einer Belastung bzw. Überlastung des Prozessors des attackierten Rechners führen können, da auf jedes Paket geantwortet wird.

**Vordefinierte Regeln für das ICMP-Protokoll**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
Blockiert eingehende Typen: <b>kein Typ</b> . Blockiert ausgehende Typen: <b>kein Typ</b> . Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als <b>50</b> Millisekunden beträgt. Fragmentierte ICMP-Pakete <b>ablehnen</b> .	Dieselbe Regel wie bei der Einstellung Niedrig.	Blockiert eingehende Typen: <b>verschiedene Typen</b> . Blockiert ausgehende Typen: <b>verschiedene Typen</b> . Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als <b>50</b> Millisekunden beträgt. Fragmentierte ICMP-Pakete <b>ablehnen</b> .

**Blockierte eingehende Typen: keine Typen/verschiedene Typen**

Durch Mausklick auf den Link öffnet sich eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten eingehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

**Blockierte ausgehende Typen: keine Typen/verschiedene Typen**

Durch Mausklick auf den Link öffnet sich eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten ausgehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

**Flooding**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Maximalwert für die erlaubte ICMP-Verzögerung eintragen können.

**Fragmentierte ICMP-Pakete**

Durch Mausklick auf den Link haben Sie die Möglichkeit zwischen dem Annehmen und dem Ablehnen von fragmentierten ICMP Paketen zu wählen.

**TCP Port-Scan**

Mit dieser Regel können Sie definieren, wann die FireWall von einem TCP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu, sogenannte TCP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

Vordefinierte Regeln für den TCP Port-Scan

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
TCP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>nicht hinzufügen</b> , um den Angriff zu blockieren.	TCP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>hinzufügen</b> , um den Angriff zu blockieren.	Dieselbe Regel wie bei der Einstellung Mittel.

Ports

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

Port-Scan Zeitfenster

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

Reportdatei

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Reportdatei geschrieben werden soll oder nicht.

Regel

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des TCP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

**UDP Port-Scan**

Mit dieser Regel definieren Sie, wann die FireWall von einem UDP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu sogenannte UDP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

Vordefinierte Regeln für den UDP Port-Scan

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
UDP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines UDP Port-Scan, IP-	UDP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scan, IP-	Dieselbe Regel wie bei der Einstellung Mittel.

Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>nicht hinzufügen</b> , um den Angriff zu blockieren.	Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>hinzufügen</b> , um den Angriff zu blockieren.
---	---

**Ports**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

**Port-Scan Zeitfenster**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

**Reportdatei**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Reportdatei geschrieben werden soll oder nicht.

**Regel**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des UDP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

12.4.1.1. Eingehende Regeln

Eingehende Regeln dienen zur Kontrolle des eingehenden Datenverkehrs durch die Avira FireWall.

**Hinweis**

Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

Vordefinierte Regeln zur Überwachung des TCP-Datenverkehrs

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
Eingehender Datenverkehr wird von der Avira FireWall nicht blockiert.	<ul style="list-style-type: none"> <li>Bestehende TCP-Verbindung auf Port 135 zulassen</li> </ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{135}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>Pakete von</b></p>	<ul style="list-style-type: none"> <li>Zugelassenen TCP-Datenverkehr überwachen</li> </ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b></p>

	<p><b>vorhandenen Verbindungen. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <ul style="list-style-type: none"> <li>– TCP-Pakete auf Port 135 zurückweisen</li> </ul> <p>TCP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{135}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Pakete. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <ul style="list-style-type: none"> <li>– Überwachen des TCP konformen Datenverkehrs</li> </ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>Beginn des</b></p>	<p>liegen. Anwenden auf <b>Pakete von vorhandenen Verbindungen. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>
--	---	---

	<p><b>Verbindungsaufbau und auf Pakete von vorhandenen Verbindungen.</b> <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <p>– Alle TCP-Pakete zurückweisen</p> <p>TCP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Pakete</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>	
--	--	--

**TCP-Pakete zulassen / verweigern**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte TCP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

### Lokale Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

### Remote Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte remote Ports und auch ganze Portbereiche eintragen können.

### Anwendungsmethode

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf Pakete von vorhandenen Verbindungen anwenden möchten, auf den Beginn des Verbindungsaufbaus und Pakete von vorhandenen Verbindungen oder auf alle Verbindungen.

### Reportdatei

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

### Filterung nach Inhalt: Daten

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

### Filterung nach Inhalt: Maske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

### Filterung nach Inhalt: Offset

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des TCP-Headers an berechnet.

## Vordefinierte Regeln zur Überwachung des UDP-Datenverkehrs

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	<ul style="list-style-type: none"> <li>Überwachen des UDP konformen Datenverkehrs</li> </ul> <p>UDP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Regel anwenden auf <b>geöffnete Ports</b>.</p>	<p>Zugelassenen UDP-Datenverkehr überwachen</p> <p>UDP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{53, 67, 68, 123}</b> liegen. Regel anwenden auf <b>geöffnete Ports</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel</p>

	<p><b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <p>– Alle UDP-Pakete zurückweisen</p> <p>UDP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Ports</b>.</p> <p><b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>	<p>entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>
--	--	---

**UDP-Pakete zulassen / verweigern**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte UDP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Lokale Ports**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

**Remote Ports**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte remote Ports und auch ganze Portbereiche eintragen können.

**Anwendungsmethode**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf alle Ports oder nur auf alle geöffnete Ports anwenden möchten.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

**Filterung nach Inhalt: Daten**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

**Filterung nach Inhalt: Maske**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

**Filterung nach Inhalt: Offset**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des UDP-Headers an berechnet.

**Vordefinierte Regeln zur Überwachung des ICMP-Datenverkehrs**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	<ul style="list-style-type: none"> <li>- Keine ICMP-Pakete auf der Basis der IP-Adresse verwerfen</li>   <li>ICMP-Pakete <b>zulassen</b> von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen</li> </ul>	Dieselbe Regel wie bei der Einstellung Mittel.



	<p>&lt;leer&gt; mit Maske &lt;leer&gt; am Offset <b>0.</b></p>	
--	--	--

**ICMP-Pakete zulassen / verweigern**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte ICMP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

**Filterung nach Inhalt: Daten**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

**Filterung nach Inhalt: Maske**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

**Filterung nach Inhalt: Offset**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des ICMP-Headers an berechnet.

**Vordefinierte Regel für IP-Pakete**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	-	<p>Alle IP-Pakete zurückweisen</p> <p>IP-Pakete <b>zurückweisen</b> von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht.</p>

**IP-Pakete zulassen / verweigern**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte IP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

**Mögliche Regel zur Überwachung von IP-Paketen anhand von IP-Protokollen**

**IP-Pakete**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte IP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Protokoll**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie das gewünschte IP-Protokoll auswählen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

12.4.1.2. Ausgehende Regeln

Ausgehende Regeln dienen zur Kontrolle des ausgehenden Datenverkehrs durch die Avira FireWall. Sie können eine ausgehende Regel für die folgenden Protokolle definieren: IP, ICMP, UDP und TCP.

**Hinweis**

Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

**Schaltflächen**

Schaltfläche	Beschreibung
Hinzufügen	Ermöglicht Ihnen das Erstellen einer neuen Regel. Wenn Sie auf diese Schaltfläche klicken, erscheint das Dialogfenster " <b>Neue Regel hinzufügen</b> ". In diesem Dialogfenster können Sie neue

	Regeln auswählen.
Entfernen	Entfernen einer ausgewählten Regel.
Nach unten	Verschieben einer ausgewählten Regel um eine Position nach unten, wodurch die Priorität dieser Regel reduziert wird.
Nach oben	Verschieben einer ausgewählten Regel um eine Position nach oben, wodurch die Priorität dieser Regel erhöht wird.
Umbenennen	Umbenennen einer ausgewählten Regel.

**Hinweis**

Sie können neue Regeln für einzelne Adapter oder aber für alle vorhandenen Adapter des Computers hinzufügen. Um eine Adapterregel für alle Adapter hinzuzufügen, wählen Sie **Computer** in der angezeigten Adapterstruktur und klicken Sie auf die Schaltfläche **Hinzufügen**.

**Hinweis**

Um die Position einer Regel zu ändern, können Sie die Regel auch mit der Maus an die gewünschte Position ziehen.

## 12.4.2 Anwendungsregeln

### Anwendungsbezogene Regeln für den Benutzer

Diese Liste enthält alle Anwender im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, für den Sie Regeln erstellen möchten. Falls Sie kein Anwender mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.

### Liste der Anwendungen

Diese Tabelle zeigt Ihnen die Liste der Anwendungen, für die Regeln definiert sind. Die Liste zeigt die Einstellungen für jede Anwendung, die seit der Installation der Avira FireWall ausgeführt wurde und für die eine Regel gespeichert wurde.

Standardansicht

	<b>Beschreibung</b>
Anwendung	Name der Anwendung.
Modus	Zeigt den eingestellten Modus der Anwendungsregel an: Im Modus <b>gefiltert</b> werden nach der Ausführung der Anwendungsregel Adapterregeln geprüft und ausgeführt. Im Modus <i>privilegiert</i> werden Adapterregeln ignoriert. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf einen anderen Modus zu wechseln.
Aktion	Zeigt die Aktion an, die die Avira FireWall automatisch

durchführen wird, falls die Anwendung das Netzwerk nutzt, gleich welcher Art diese Nutzung ist. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf eine andere Aktionsart zu wechseln. Die Aktionsarten **Fragen, Zulassen** oder **Zurückweisen** stehen zur Auswahl. Die Standardeinstellung ist **Fragen**.

### Erweiterte Konfiguration

Wenn Sie die Netzwerkzugänge einer Anwendung individuell regeln möchten, können Sie vergleichbar den Adapterregeln spezifizierte Anwendungsregeln, die auf Paketfiltern basieren, erstellen. Um zur erweiterten Konfiguration der Anwendungsregeln zu wechseln, aktivieren Sie zunächst den Expertenmodus. Ändern Sie nun in der Rubrik FireWall:: Einstellungen die Einstellung für Anwendungsregeln: Aktivieren Sie die Option **Erweiterte Einstellungen** und speichern Sie die Einstellung mit **Übernehmen** oder **OK**. Wechseln Sie in der FireWall Konfiguration zur Rubrik

**FireWall::Anwendungsregeln**: Es wird in der Liste der Anwendungsregeln eine weitere Spalte *Filterung* mit dem Eintrag *Einfach* angezeigt. Sie haben nun die Zusatzoption **Filterung: Fortgeschritten - Aktion: Regeln**, mit der Sie in die erweiterte Konfiguration wechseln können.

	<b>Beschreibung</b>
Anwendung	Name der Anwendung.
Modus	Zeigt den eingestellten Modus der Anwendungsregel an: Im Modus <b>gefiltert</b> werden nach der Ausführung der Anwendungsregel Adapterregeln geprüft und ausgeführt. Im Modus <i>privilegiert</i> werden Adapterregeln ignoriert. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf einen anderen Modus zu wechseln.
Aktion	Zeigt die Aktion an, die die Avira FireWall automatisch durchführen wird, falls die Anwendung das Netzwerk nutzt, gleich welcher Art diese Nutzung ist. Bei der Einstellung <i>Filterung - Einfach</i> können Sie durch einen Mausklick auf den Link auf eine andere Aktionsart zu wechseln. Die Aktionsarten <b>Fragen, Zulassen, Zurückweisen</b> oder <i>Erweitert</i> stehen zur Auswahl. Bei der Einstellung <i>Filterung - Fortgeschritten</i> wird die Aktionsart <i>Regeln</i> angezeigt. Der Link <b>Regeln</b> öffnet das Fenster <b>Anwendungsregeln</b> , in dem Sie spezifizierte Regeln für die Anwendung hinterlegen können.
Filterung	Zeigt die Art der Filterung an. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf eine andere Filterung zu wechseln. <i>Einfach</i> : Bei einfacher Filterung wird die angegebene Aktion bei allen Netzwerkaktivitäten der Software-Anwendung ausgeführt. <i>Fortgeschritten</i> : Bei der Filterung werden die Regeln ausgeführt, die in der erweiterten Konfiguration hinterlegt wurden.

Wenn Sie für eine Anwendung spezifizierte Anwendungsregeln erstellen möchten, wechseln Sie unter *Filterung* auf den Eintrag **Fortgeschritten**. In der Spalte **Aktion** wird nun der Eintrag *Regeln* angezeigt. Klicken Sie auf **Regeln**, um in das Fenster zur Erstellung von spezifizierten Anwendungsregeln zu gelangen.

**Spezifizierte Anwendungsregeln in der erweiterten Konfiguration**

Mit spezifizierten Anwendungsregeln können Sie spezifizierten Datenverkehr der Anwendung zulassen oder zurückweisen sowie das passive Abhören von einzelnen Ports zulassen oder zurückweisen. Sie haben folgende Optionen:

- Code-Injektion zulassen oder zurückweisen

Code-Injektion ist eine Technik, mit der man Code im Adressraum eines anderen Prozesses zur Ausführung bringt, indem man diesen Prozess zwingt, eine Dynamic Link Library (DLL) zu laden. Die Technik der Code-Injektion wird u.a. von Malware eingesetzt, um Code unter dem Deckmantel eines anderen Programms auszuführen. Dadurch können z.B. Zugriffe auf das Internet vor der FireWall verschleiert werden. Standardmäßig wird Code-Injektion für alle signierten Anwendungen erlaubt.

- Passives Abhören der Anwendung von Ports zulassen oder zurückweisen
- Datenverkehr zulassen oder zurückweisen:

Eingehende und / oder ausgehende IP-Pakete zulassen oder zurückweisen

Eingehende und / oder ausgehende TCP-Pakete zulassen oder zurückweisen

Eingehende und / oder ausgehende UDP-Pakete zulassen oder zurückweisen

Sie können zu jeder Anwendung beliebig viele Anwendungsregeln erstellen. Die Anwendungsregeln werden in der angezeigten Reihenfolge ausgeführt .

**Hinweis**

Wenn Sie die Filterung *Fortgeschritten* bei einer Anwendungsregel ändern, werden die bereits angelegten Anwendungsregeln in der erweiterten Konfiguration nicht endgültig gelöscht, sondern nur deaktiviert. Wechseln Sie wieder zur Filterung *Fortgeschritten*, werden die bereits angelegten Anwendungsregeln wieder aktiviert und im Fenster der erweiterten Konfiguration für Anwendungsregeln angezeigt.

**Anwendungsdetails**

In dieser Rubrik werden Detailinformationen zu der Anwendung angezeigt, die sie in der Liste der Anwendungen ausgewählt haben.

	<b>Beschreibung</b>
Name	Name der Anwendung.
Pfad	Vollständiger Pfad zu der ausführbaren Datei.

**Schaltflächen**

<b>Schaltfläche</b>	<b>Beschreibung</b>
Anwendung hinzufügen	Ermöglicht Ihnen das Erstellen einer neuen Anwendungsregel. Wenn Sie auf diese Schaltfläche klicken, erscheint ein Dialogfenster. Nun können Sie eine Anwendung auswählen, für die Sie eine Regel erstellen möchten.

Regel entfernen	Entfernen der ausgewählten Anwendungsregel.
Neu laden	Erneutes Laden der Liste der Anwendungen mit gleichzeitigem Verwerfen aller gerade gemachten Änderungen an den Anwendungsregeln.

### 12.4.3 Vertrauenswürdige Anbieter

Unter *Vertrauenswürdige Anbieter* wird eine Liste von vertrauenswürdigen Software-Herstellern angezeigt. Sie können Hersteller aus der Liste entfernen oder hinzufügen, indem Sie die Option *Diesem Anbieter immer vertrauen* im Popup-Fenster *Netzwerkereignis* nutzen. Sie können den Netzzugriff von Anwendungen, die von den aufgelisteten Anbietern signiert sind, standardmäßig erlauben, indem Sie die Option **Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen** aktivieren.

#### Vertrauenswürdige Anbieter für Benutzer

Diese Liste enthält alle Benutzer im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, dessen Liste vertrauenswürdiger Anbieter Sie einsehen oder pflegen möchten. Falls Sie kein Benutzer mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.

#### Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen

Bei aktivierter Option wird Anwendungen mit einer Signatur von bekannten und vertrauenswürdigen Anbietern automatisch der Zugang zum Netzwerk erlaubt. Die Option ist standardmäßig aktiviert.

#### Anbieter

Die Liste zeigt alle Anbieter, die als vertrauenswürdige eingestuft werden.

#### Schaltflächen

Schaltfläche	Beschreibung
Entfernen	Der markierte Eintrag wird aus der Liste der vertrauenswürdigen Anbieter entfernt. Um den ausgewählten Anbieter endgültig aus der Liste zu entfernen, drücken Sie auf <b>Übernehmen</b> oder <b>OK</b> im Fenster der Konfiguration.
Neu laden	Die vorgenommenen Änderungen werden rückgängig gemacht: Die letzte gespeicherte Liste wird geladen.

#### Hinweis

Wenn Sie Anbieter aus der Liste entfernen und anschließend die Schaltfläche **Anwenden** drücken, werden die Anbieter endgültig aus der Liste gelöscht. Die Änderung kann nicht mit *Neu laden* rückgängig gemacht werden. Sie haben jedoch die Möglichkeit, über die Option *Diesem Anbieter immer vertrauen* im Popup-Fenster *Netzwerkereignis* einen Anbieter wieder zur Liste der vertrauenswürdigen Anbieter hinzuzufügen.

### **Hinweis**

Die FireWall priorisiert Anwendungsregeln vor den Einträgen in der Liste der vertrauenswürdigen Anbieter: Wenn Sie eine Anwendungsregel erstellt haben und der Anbieter der Anwendung ist in der Liste der vertrauenswürdigen Anbieter aufgeführt, wird die Anwendungsregel ausgeführt.

## 12.4.4 Einstellungen

### **Erweiterte Einstellungen**

#### **FireWall aktivieren**

Bei aktivierter Option ist die Avira FireWall aktiv und schützt Ihren Rechner vor Gefahren aus dem Internet und anderen Netzwerken.

#### **Windows Firewall beim Hochfahren deaktivieren**

Bei aktivierter Option ist die Windows Firewall beim Hochfahren des Rechners deaktiviert. Diese Option ist standardmäßig aktiviert.

#### **Windows hosts-Datei ist NICHT GESPERRT/GESPERRT**

Steht diese Option auf GESPERRT, ist die Windows hosts-Datei schreibgeschützt. Eine Manipulation der Datei ist dann nicht länger möglich. Malware ist dann beispielsweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten. Standardmäßig ist diese Option auf NICHT GESPERRT eingestellt.

### **Zeitüberschreitung der Regel**

#### **Immer blockieren**

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Port-Scan automatisch erstellt wurde, beibehalten.

#### **Regel entfernen nach n Sekunden**

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan automatisch erstellt wurde, nach der von Ihnen angegebenen Zeit wieder entfernt. Diese Option ist standardmäßig aktiviert.

### **Benachrichtigungen**

Unter Benachrichtigungen legen Sie fest, bei welchen Ereignissen Sie eine Desktopbenachrichtigung der FireWall erhalten möchten.

#### **Port Scan**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der FireWall ein Port Scan erkannt wurde.

#### **Flooding**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der FireWall eine Flooding-Attacke erkannt wurde.

#### **Anwendungen wurden blockiert**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die FireWall eine Netzwerkaktivität einer Anwendung zurückgewiesen, d.h. blockiert hat.

### **IP blockiert**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die FireWall den Datenverkehr von einer IP-Adresse zurückgewiesen hat.

## **Anwendungsregeln**

Mit den Optionen im Bereich Anwendungsregeln stellen Sie die Konfigurationsmöglichkeiten für Anwendungsregeln unter der Rubrik FireWall::Anwendungsregeln ein.

### **Erweiterte Einstellungen**

Bei aktivierter Option haben Sie die Möglichkeit, verschiedene Netzwerkzugänge einer Anwendung individuell zu regeln.

### **Grundeinstellungen**

Bei aktivierter Option kann nur eine einzige Aktion für verschiedene Netzwerkzugänge der Anwendung eingestellt werden.

## 12.4.5 Popup-Einstellungen

### **Popup-Einstellungen**

#### **Startblock des Prozesses überprüfen**

Bei aktivierter Option erfolgt eine präzisere Überprüfung des Prozess Stapels. Die FireWall geht dann davon aus, dass jeder Prozess im Stapel, der nicht vertrauenswürdig ist, derjenige ist, über dessen Kindprozess auf das Netzwerk zugegriffen wird. Deshalb wird in diesem Fall für jeden nicht vertrauenswürdigen Prozess im Stapel ein eigenes Popup-Fenster geöffnet. Diese Option ist standardmäßig deaktiviert.

#### **Mehrere Dialogfenster pro Prozess anzeigen**

Bei aktivierter Option wird jedes Mal, wenn eine Anwendung versucht eine Netzwerkverbindung herzustellen, ein Popup-Fenster geöffnet. Alternativ erfolgt die Information nur beim ersten Verbindungsversuch. Diese Option ist standardmäßig deaktiviert.

#### **Popup-Benachrichtigung im Spielmodus automatisch unterdrücken**

Bei aktivierter Option schaltet Avira FireWall automatisch in den Spielmodus um, wenn auf Ihrem Computersystem eine Anwendung im Vollbildmodus ausgeführt wird. Im Spielmodus werden alle definierten Adapter- und Anwendungsregeln angewendet. Anwendungen, für die keine Regeln mit den Aktionen "Zulassen" oder "Zurückweisen" definiert sind, wird der Netzwerkzugriff temporär erlaubt, so dass keine Popup-Fenster mit Abfragen zum Netzwerkereignis geöffnet werden.

### **Aktion für diese Anwendung speichern**

#### **Immer aktiviert**



Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig aktiviert. Diese Option ist standardmäßig aktiviert.

#### Immer deaktiviert

Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig deaktiviert.

#### Signierte Anwendung erlauben

Bei aktivierter Option ist beim Netzzugriff signierter Anwendungen bestimmter Hersteller die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" automatisch aktiviert. Die Hersteller sind: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

#### Letzten Stand merken

Bei aktivierter Option wird die Aktivierung der Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" gehandhabt wie beim letzten Netzwerkereignis. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern**" aktiviert, ist die Option beim folgenden Netzwerkereignis aktiv. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern**" deaktiviert, ist die Option beim folgenden Netzwerkereignis deaktiviert.

### Details anzeigen

In dieser Gruppe von Konfigurationsoptionen können Sie die Anzeige von Detailinformationen im Fenster **Netzwerkereignis** einstellen.

#### Details auf Anfrage anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "*Netzwerkereignis*" nur auf Anfrage angezeigt, d.h. eine Anzeige der Detailinformationen erfolgt mit Klick auf die Schaltfläche "**Details einblenden**" im Fenster "*Netzwerkereignis*".

#### Details immer anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "*Netzwerkereignis*" immer angezeigt.

#### Letzten Stand merken

Bei aktivierter Option wird die Anzeige von Detailinformationen gehandhabt wie beim vorangegangenen Netzwerkereignis. Wurden beim letzten Netzwerkereignis Detailinformationen angezeigt oder abgerufen, werden beim folgenden Netzwerkereignis Detailinformationen angezeigt. Wurden beim letzten Netzwerkereignis die Detailinformationen nicht angezeigt oder ausgeblendet, werden beim folgenden Netzwerkereignis die Detailinformationen nicht angezeigt.

### Privilegierte zulassen

In dieser Gruppe von Konfigurationsoptionen können Sie den Status der Option *Privilegiert zulassen* im Fenster **Netzwerkereignis** einstellen.

#### Immer aktiviert

Bei aktivierter Option ist die Option "*Privilegierte zulassen*" im Fenster "*Netzwerkereignis*" standardmäßig aktiviert.

#### Immer deaktiviert

Bei aktivierter Option ist die Option "*Privilegierte zulassen*" im Fenster "*Netzwerkereignis*" standardmäßig deaktiviert.

### **Letzten Stand merken**

Bei aktivierter Option wird der Status der Option "*Privilegiert zulassen*" im Fenster "*Netzwerkereignis*" gehandhabt wie beim vorangegangenen Netzwerkereignis: War bei der Ausführung des letzten Netzwerkereignisses die Option "*Privilegiert zulassen*" aktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig aktiviert. War bei der Ausführung des letzten Netzwerkereignisses die Option "*Privilegiert zulassen*" deaktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig deaktiviert.

## 12.5 FireWall unter SMC

Die FireWall-Konfiguration ist auf die speziellen Anforderungen einer Administration über das Avira Security Management Center angepasst. Es bestehen erweiterte Optionen und Einschränkungen von einzelnen Konfigurationsoptionen:

- Die Einstellungen der FireWall gelten für alle Benutzer der Client-Rechner
- Adapterregeln: Für einzelne Adapter können Sicherheitsstufen über Kontextmenüs eingestellt werden
- Anwendungsregeln: Der Netzzugriff von Anwendungen kann freigegeben oder blockiert werden. Es besteht keine Möglichkeit, spezifische Anwendungsregeln zu erstellen.

Wenn Ihr AntiVir Programm über das Avira Security Management Center administriert wird, sind die folgenden Einstellungsmöglichkeiten der FireWall im Control Center auf den Client-Rechnern deaktiviert:

- Einstellung der Sicherheitsstufen der FireWall
- Einstellung von Adapterregeln und Anwendungsregeln

### 12.5.1 Allgemeine Einstellungen

#### **Erweiterte Einstellungen**

##### **Windows hosts-Datei sperren**

Bei aktivierter Option ist die Windows hosts-Datei schreibgeschützt. Eine Manipulation der Datei ist dann nicht länger möglich. Malware ist dann beispielsweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten.

##### **Spielmodus aktivieren**

Bei aktivierter Option schaltet Avira FireWall automatisch in den Spielmodus um, wenn auf Ihrem Computersystem eine Anwendung im Vollbildmodus ausgeführt wird. Im Spielmodus werden alle definierten Adapter- und Anwendungsregeln angewendet. Anwendungen, für die keine Regeln mit den Aktionen "*Zulassen*" oder "*Zurückweisen*" definiert sind, wird der Netzzugriff temporär erlaubt, so dass keine Popup-Fenster mit Abfragen zum Netzwerkereignis geöffnet werden.

##### **Windows Firewall beim Hochfahren deaktivieren**

Bei aktivierter Option ist die Windows Firewall beim Hochfahren des Rechners deaktiviert. Diese Option ist standardmäßig aktiviert.

### FireWall aktivieren

Bei aktivierter Option ist die Avira FireWall aktiv und schützt Ihren Rechner vor Gefahren aus dem Internet und anderen Netzwerken.

### **Zeitüberschreitung der Regel**

#### Immer blockieren

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Port-Scan automatisch erstellt wurde, beibehalten.

#### Regel entfernen nach n Sekunden

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan automatisch erstellt wurde, nach der von Ihnen angegebenen Zeit wieder entfernt. Diese Option ist standardmäßig aktiviert.

## 12.5.2 Allgemeine Adapterregeln

Als Adapter werden eingerichtete Netzwerkverbindungen bezeichnet. Für die folgenden Client-Netzwerkverbindungen können Adapterregeln erstellt werden:

- Default-Adapter: LAN oder Hochgeschwindigkeitsinternet
- Wireless
- DFÜ Verbindung

Sie können für jeden verfügbaren Adapter vordefinierte Adapterregeln über das Kontextmenü zum Adapter einstellen:

- Sicherheitsstufe Hoch
- Sicherheitsstufe Mittel
- Sicherheitsstufe Niedrig

Sie haben auch die Möglichkeit, einzelne Adapterregeln anzupassen und individuell einzustellen.

### **Hinweis**

Die Standardeinstellung des Sicherheitsniveaus für alle vordefinierten Regeln der Avira FireWall ist **Mittel**.

### **ICMP-Protokoll**

Das Internet Control Message Protocol (ICMP) dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen. Das Protokoll wird auch für Statusmeldungen mittels Ping oder Tracert verwendet.

Mit dieser Regel können Sie ein- und ausgehende ICMP-Typen definieren, die blockiert werden sollen, die Parameter für Flooding festlegen und das Verhalten bei Vorliegen von fragmentierten ICMP-Paketen definieren. Diese Regel dient dazu sogenannte ICPM Flood-Attacken zu verhindern, die zu einer Belastung bzw. Überlastung des Prozessors des attackierten Rechners führen können, da auf jedes Paket geantwortet wird.

#### Vordefinierte Regeln für das ICMP-Protokoll

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
Blockiert eingehende Typen: <b>kein Typ</b> . Blockiert ausgehende Typen: <b>kein Typ</b> . Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als <b>50</b> Millisekunden beträgt. Fragmentierte ICMP-Pakete <b>ablehnen</b> .	Dieselbe Regel wie bei der Einstellung Niedrig.	Blockiert eingehende Typen: <b>verschiedene Typen</b> . Blockiert ausgehende Typen: <b>verschiedene Typen</b> . Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als <b>50</b> Millisekunden beträgt. Fragmentierte ICMP-Pakete <b>ablehnen</b> .

**Blockierte eingehende Typen: keine Typen/verschiedene Typen**

Durch Mausklick auf den Link öffnet sich eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten eingehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

**Blockierte ausgehende Typen: keine Typen/verschiedene Typen**

Durch Mausklick auf den Link öffnet sich eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten ausgehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

**Flooding**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Maximalwert für die erlaubte ICMP-Verzögerung eintragen können.

**Fragmentierte ICMP-Pakete**

Durch Mausklick auf den Link haben Sie die Möglichkeit zwischen dem Annehmen und dem Ablehnen von fragmentierten ICMP Paketen zu wählen.

**TCP Port-Scan**

Mit dieser Regel können Sie definieren, wann die FireWall von einem TCP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu, sogenannte TCP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

**Vordefinierte Regeln für den TCP Port-Scan**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
TCP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind.	TCP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind.	Dieselbe Regel wie bei der Einstellung Mittel.

Bei Feststellung eines TCP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>nicht hinzufügen</b> , um den Angriff zu blockieren.	Bei Feststellung eines TCP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>hinzufügen</b> , um den Angriff zu blockieren.
--	--

**Ports**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

**Port-Scan Zeitfenster**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

**Reportdatei**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Reportdatei geschrieben werden soll oder nicht.

**Regel**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des TCP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

**UDP Port-Scan**

Mit dieser Regel definieren Sie, wann die FireWall von einem UDP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu sogenannte UDP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

**Vordefinierte Regeln für den UDP Port-Scan**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
UDP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines UDP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>nicht hinzufügen</b> , um den Angriff zu blockieren.	UDP Port-Scan vermuten, wenn <b>50</b> oder mehr Ports in <b>5000</b> Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scan, IP-Adresse des Angreifers <b>in Reportdatei schreiben</b> und den Regeln <b>hinzufügen</b> , um den Angriff zu blockieren.	Dieselbe Regel wie bei der Einstellung Mittel.

**Ports**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

**Port-Scan Zeitfenster**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

**Reportdatei**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Reportdatei geschrieben werden soll oder nicht.

**Regel**

Durch Mausklick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des UDP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

### 12.5.2.1. Eingehende Regeln

Eingehende Regeln dienen zur Kontrolle des eingehenden Datenverkehrs durch die Avira FireWall.

**Hinweis**

Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

#### Vordefinierte Regeln zur Überwachung des TCP-Datenverkehrs

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
Eingehender Datenverkehr wird von der Avira FireWall nicht blockiert.	<ul style="list-style-type: none"> <li>– Bestehende TCP-Verbindung auf Port 135 zulassen</li> </ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{135}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>Pakete von vorhandenen Verbindungen. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete</p>	<ul style="list-style-type: none"> <li>– Zugelassenen TCP-Datenverkehr überwachen</li> </ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>Pakete von vorhandenen Verbindungen. Nicht in Reportdatei schreiben</b>, wenn</p>

	<p>mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <ul style="list-style-type: none"><li>– TCP-Pakete auf Port 135 zurückweisen</li></ul> <p>TCP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{135}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Pakete. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <ul style="list-style-type: none"><li>– Überwachen des TCP konformen Datenverkehrs</li></ul> <p>TCP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>Beginn des Verbindungsaufbaus und auf Pakete von vorhandenen Verbindungen. Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel</p>	<p>das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>
--	--	---

	<p>entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p> <p>– Alle TCP-Pakete zurückweisen</p> <p>TCP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Pakete</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>	
--	--	--

#### TCP-Pakete zulassen / verweigern

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte TCP-Pakete zulassen oder zurückweisen wollen.

#### IP-Adresse

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

#### IP-Maske

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

#### Lokale Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

#### Remote Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte remote Ports und auch ganze Portbereiche eintragen können.

#### Anwendungsmethode



Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf Pakete von vorhandenen Verbindungen anwenden möchten, auf den Beginn des Verbindungsaufbaus und Pakete von vorhandenen Verbindungen oder auf alle Verbindungen.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

**Filterung nach Inhalt: Daten**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

**Filterung nach Inhalt: Maske**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

**Filterung nach Inhalt: Offset**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des TCP-Headers an berechnet.

**Vordefinierte Regeln zur Überwachung des UDP-Datenverkehrs**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	<ul style="list-style-type: none"> <li>- Überwachen des UDP konformen Datenverkehrs</li>   <li>UDP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Regel anwenden auf <b>geöffnete Ports</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen</li> </ul>	<p>Zugelassenen UDP-Datenverkehr überwachen</p> <p>UDP-Pakete <b>zulassen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{53, 67, 68, 123}</b> liegen. Regel anwenden auf <b>geöffnete Ports</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</p>

	<p><b>&lt;leer&gt;</b> mit Maske  <b>&lt;leer&gt;</b> am Offset  <b>0.</b></p> <p>– Alle UDP-Pakete zurückweisen</p> <p>UDP-Pakete <b>zurückweisen</b>, von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>, wenn der lokale Port in <b>{0-65535}</b> und der remote Port in <b>{0-65535}</b> liegen. Anwenden auf <b>alle Ports</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0.</b></p>	
--	--	--

#### UDP-Pakete zulassen / verweigern

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte UDP-Pakete zulassen oder zurückweisen wollen.

#### IP-Adresse

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

#### IP-Maske

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

#### Lokale Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

#### Remote Ports

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte remote Ports und auch ganze Portbereiche eintragen können.

#### Anwendungsmethode

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf alle Ports oder nur auf alle geöffnete Ports anwenden möchten.

### Reportdatei

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

### Filterung nach Inhalt: Daten

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

### Filterung nach Inhalt: Maske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

### Filterung nach Inhalt: Offset

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des UDP-Headers an berechnet.

## Vordefinierte Regeln zur Überwachung des ICMP-Datenverkehrs

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	<ul style="list-style-type: none"> <li>- Keine ICMP-Pakete auf der Basis der IP-Adresse verwerfen</li>   <li>ICMP-Pakete <b>zulassen</b> von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht. Erweitert: Pakete mit folgenden Bytes ablehnen <b>&lt;leer&gt;</b> mit Maske <b>&lt;leer&gt;</b> am Offset <b>0</b>.</li> </ul>	Dieselbe Regel wie bei der Einstellung Mittel.

### ICMP-Pakete zulassen / verweigern

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte ICMP-Pakete zulassen oder zurückweisen wollen.

### IP-Adresse

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

**Filterung nach Inhalt: Daten**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

**Filterung nach Inhalt: Maske**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

**Filterung nach Inhalt: Offset**

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des ICMP-Headers an berechnet.

**Vordefinierte Regel für IP-Pakete**

<b>Einstellung: Niedrig</b>	<b>Einstellung: Mittel</b>	<b>Einstellung: Hoch</b>
-	-	<p>Alle IP-Pakete zurückweisen</p> <p>IP-Pakete <b>zurückweisen</b> von Adresse <b>0.0.0.0</b> mit Maske <b>0.0.0.0</b>. <b>Nicht in Reportdatei schreiben</b>, wenn das Paket der Regel entspricht.</p>

**IP-Pakete zulassen / verweigern**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte IP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

**Mögliche Regel zur Überwachung von IP-Paketen anhand von IP-Protokollen**

**IP-Pakete**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte IP-Pakete zulassen oder zurückweisen wollen.

**IP-Adresse**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eintragen können.

**IP-Maske**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eintragen können.

**Protokoll**

Durch Mausklick auf diesen Link öffnet sich ein Dialogfenster, in dem Sie das gewünschte IP-Protokoll auswählen können.

**Reportdatei**

Durch Mausklick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Reportdatei zu schreiben oder nicht, wenn das Paket der Regel entspricht.

12.5.2.2. Ausgehende Regeln

Ausgehende Regeln dienen zur Kontrolle des ausgehenden Datenverkehrs durch die Avira FireWall. Sie können eine ausgehende Regel für die folgenden Protokolle definieren: IP, ICMP, UDP und TCP.

**Hinweis**

Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

**Schaltflächen**

Schaltfläche	Beschreibung
Hinzufügen	Ermöglicht Ihnen das Erstellen einer neuen Regel. Wenn Sie auf diese Schaltfläche klicken, erscheint das Dialogfenster " <b>Neue Regel hinzufügen</b> ". In diesem Dialogfenster können Sie neue Regeln auswählen.
Entfernen	Entfernen einer ausgewählten Regel.
Nach unten	Verschieben einer ausgewählten Regel um eine Position nach unten, wodurch die Priorität dieser Regel reduziert wird.
Nach oben	Verschieben einer ausgewählten Regel um eine Position nach oben, wodurch die Priorität dieser Regel erhöht wird.
Umbenennen	Umbenennen einer ausgewählten Regel.

**Hinweis**

Sie können neue Regeln für einzelne Adapter oder aber für alle vorhandenen Adapter des Computers hinzufügen. Um eine Adapterregel für alle Adapter hinzuzufügen, wählen Sie **Computer** in der angezeigten Adapterstruktur und klicken Sie auf die Schaltfläche **Hinzufügen**.

**Hinweis**

Um die Position einer Regel zu ändern, können Sie die Regel auch mit der Maus an die gewünschte Position ziehen.

### 12.5.3 Anwendungsliste

Unter Anwendungsliste haben Sie die Möglichkeit, für die Netzzugriffe von Anwendungen Regeln zu erstellen. Sie können Anwendungen zur Liste hinzufügen und über ein Kontextmenü die Regeln *Erlauben* und **Blockieren** für die ausgewählte Anwendung setzen:

- Netzzugriffe von Anwendungen mit der Regel *Erlauben* werden zugelassen.
- Netzzugriffe von Anwendungen mit der Regel *Blockieren* werden zurückgewiesen.

Beim Hinzufügen von Anwendungen wird die Regel *Erlauben* gesetzt.

#### Liste der Anwendungen

Diese Tabelle zeigt Ihnen die Liste der Anwendungen, für die Regeln definiert sind. Die Symbole zeigen an, ob die Netzzugriffe der Anwendungen erlaubt oder blockiert werden. Sie können die Regeln zu den Anwendungen über ein Kontextmenü ändern.

#### Schaltflächen

Schaltfläche	Beschreibung
Durch Pfad hinzufügen	Die Schaltfläche öffnet einen Dialog, in dem Sie Anwendungen auswählen können. Die Anwendung wird mit der Regel <b>"Netzzugriff erlauben"</b> zur Anwendungsliste hinzugefügt. Wenn Sie die Option <b>"Durch Pfad hinzufügen"</b> nutzen, wird die hinzugefügte Anwendung von der FireWall anhand des Pfades und des Dateinamens identifiziert. Regeln für eine Anwendung bleiben gültig und werden von der FireWall angewendet, selbst wenn der Inhalt einer eingepflegten ausführbaren Datei beispielsweise durch ein Update verändert wurde.
Durch md5 hinzufügen	Die Schaltfläche öffnet einen Dialog, in dem Sie Anwendungen auswählen können. Die Anwendung wird mit der Regel <b>"Netzzugriff erlauben"</b> zur Anwendungsliste hinzugefügt. Wenn Sie die Option <b>"Durch md5 hinzufügen"</b> nutzen, werden alle hinzugefügten Anwendungen anhand der MD5-Prüfsumme eindeutig identifiziert. Dies erlaubt es der FireWall Änderungen an Dateiinhalten zu erkennen. Ändert sich eine Anwendung, beispielsweise aufgrund eines Updates, wird die

	Anwendung mit der gesetzten Regel automatisch aus der Anwendungsliste entfernt. Die Anwendung muss nach der Änderung erneut zur Liste hinzugefügt werden, die gewünschte Regel muss neu gesetzt werden.
Gruppe hinzufügen	Die Schaltfläche öffnet einen Dialog, in dem Sie ein Verzeichnis auswählen können. Alle Anwendungen unter dem ausgewählten Pfad werden zur Anwendungsliste mit der Regel " <b>Netzzugriff erlauben</b> " hinzugefügt.
Entfernen	Die ausgewählte Anwendungsregel wird entfernt.
Alle entfernen	Alle Anwendungsregeln werden entfernt.

## 12.5.4 Vertrauenswürdige Anbieter

Unter *Vertrauenswürdige Anbieter* wird eine Liste von vertrauenswürdigen Software-Herstellern angezeigt. Die Netzzugriffe der Anwendungen von den gelisteten Software-Herstellern werden zugelassen. Sie können Hersteller aus der Liste entfernen oder hinzufügen.

### Anbieter

Die Liste zeigt alle Anbieter, die als vertrauenswürdige eingestuft werden.

### Schaltflächen

Schaltfläche	Beschreibung
Hinzufügen	Die Schaltfläche öffnet einen Dialog, in dem Sie Anwendungen auswählen können. Der Hersteller der Anwendung wird ermittelt und zur Liste der vertrauenswürdigen Anbieter hinzugefügt.
Gruppe hinzufügen	Die Schaltfläche öffnet einen Dialog, in dem Sie ein Verzeichnis auswählen können. Die Hersteller aller Anwendungen unter dem ausgewählten Pfad werden ermittelt und zur Liste der vertrauenswürdigen Anbieter hinzugefügt.
Entfernen	Der markierte Eintrag wird aus der Liste der vertrauenswürdigen Anbieter entfernt. Um den ausgewählten Anbieter endgültig aus der Liste zu entfernen, drücken Sie auf " <b>Übernehmen</b> " oder " <b>OK</b> " im Fenster der Konfiguration.
Alle entfernen	Alle Einträge werden aus der Liste der vertrauenswürdigen Anbieter entfernt.
Neu laden	Die vorgenommenen Änderungen werden rückgängig gemacht: Die letzte gespeicherte Liste wird geladen.

### Hinweis

Wenn Sie Anbieter aus der Liste entfernen und anschließend die Schaltfläche **Anwenden** drücken, werden die Anbieter endgültig aus der Liste gelöscht. Die Änderung kann nicht mit *Neu laden* rückgängig gemacht werden.

### **Hinweis**

Die FireWall priorisiert Anwendungsregeln vor den Einträgen in der Liste der vertrauenswürdigen Anbieter: Wenn Sie eine Anwendungsregel erstellt haben und der Anbieter der Anwendung ist in der Liste der vertrauenswürdigen Anbieter aufgeführt, wird die Anwendungsregel ausgeführt.

## 12.5.5 Weitere Einstellungen

### **Benachrichtigungen**

Unter Benachrichtigungen legen Sie fest, bei welchen Ereignissen Sie eine Desktopbenachrichtigung der FireWall erhalten möchten.

#### **Port Scan**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der FireWall ein Port Scan erkannt wurde.

#### **Flooding**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der FireWall eine Flooding-Attacke erkannt wurde.

#### **Anwendungen wurden blockiert**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die FireWall eine Netzwerkaktivität einer Anwendung zurückgewiesen, d.h. blockiert hat.

#### **IP blockiert**

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die FireWall den Datenverkehr von einer IP-Adresse zurückgewiesen hat.

### **Popup-Einstellungen**

#### **Startblock des Prozesses überprüfen**

Bei aktivierter Option erfolgt eine präzisere Überprüfung des Prozess Stapels. Die FireWall geht dann davon aus, dass jeder Prozess im Stapel, der nicht vertrauenswürdig ist, derjenige ist, über dessen Kindprozess auf das Netzwerk zugegriffen wird. Deshalb wird in diesem Fall für jeden nicht vertrauenswürdigen Prozess im Stapel ein eigenes Popup-Fenster geöffnet. Diese Option ist standardmäßig deaktiviert.

#### **Mehrere Dialogfenster pro Prozess anzeigen**

Bei aktivierter Option wird jedes Mal, wenn eine Anwendung versucht eine Netzwerkverbindung herzustellen, ein Popup-Fenster geöffnet. Alternativ erfolgt die Information nur beim ersten Verbindungsversuch. Diese Option ist standardmäßig deaktiviert.

#### **Popup-Benachrichtigung im Spielmodus automatisch unterdrücken**

Bei aktivierter Option schaltet Avira FireWall automatisch in den Spielmodus um, wenn auf Ihrem Computersystem eine Anwendung im Vollbildmodus ausgeführt wird. Im Spielmodus werden alle definierten Adapter- und Anwendungsregeln angewendet. Anwendungen, für die keine Regeln mit den Aktionen "Zulassen" oder "Zurückweisen" definiert sind, wird der Netzwerkzugriff temporär erlaubt, so dass keine Popup-Fenster mit Abfragen zum Netzwerkereignis geöffnet werden.



## 12.5.6 Anzeigeeinstellungen

### **Aktion für diese Anwendung speichern**

#### Immer aktiviert

Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig aktiviert. Diese Option ist standardmäßig aktiviert.

#### Immer deaktiviert

Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig deaktiviert.

#### Signierte Anwendung erlauben

Bei aktivierter Option ist beim Netzzugriff signierter Anwendungen bestimmter Hersteller die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" automatisch aktiviert. Die Hersteller sind: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

#### Letzten Stand merken

Bei aktivierter Option wird die Aktivierung der Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" gehandhabt wie beim letzten Netzwerkereignis. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern**" aktiviert, ist die Option beim folgenden Netzwerkereignis aktiv. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern**" deaktiviert, ist die Option beim folgenden Netzwerkereignis deaktiviert.

### **Details anzeigen**

In dieser Gruppe von Konfigurationsoptionen können Sie die Anzeige von Detailinformationen im Fenster **Netzwerkereignis** einstellen.

#### Details auf Anfrage anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "*Netzwerkereignis*" nur auf Anfrage angezeigt, d.h. eine Anzeige der Detailinformationen erfolgt mit Klick auf die Schaltfläche "**Details einblenden**" im Fenster "*Netzwerkereignis*".

#### Details immer anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "*Netzwerkereignis*" immer angezeigt.

#### Letzten Stand merken

Bei aktivierter Option wird die Anzeige von Detailinformationen gehandhabt wie beim vorangegangenen Netzwerkereignis. Wurden beim letzten Netzwerkereignis Detailinformationen angezeigt oder abgerufen, werden beim folgenden Netzwerkereignis Detailinformationen angezeigt. Wurden beim letzten Netzwerkereignis die Detailinformationen nicht angezeigt oder ausgeblendet, werden beim folgenden Netzwerkereignis die Detailinformationen nicht angezeigt.

### Privilegierte zulassen

In dieser Gruppe von Konfigurationsoptionen können Sie den Status der Option *Privilegiert zulassen* im Fenster **Netzwerkereignis** einstellen.

#### Immer aktiviert

Bei aktivierter Option ist die Option "*Privilegierte zulassen*" im Fenster "*Netzwerkereignis*" standardmäßig aktiviert.

#### Immer deaktiviert

Bei aktivierter Option ist die Option "*Privilegierte zulassen*" im Fenster "*Netzwerkereignis*" standardmäßig deaktiviert.

#### Letzten Stand merken

Bei aktivierter Option wird der Status der Option "*Privilegiert zulassen*" im Fenster "*Netzwerkereignis*" gehandhabt wie beim vorangegangenen Netzwerkereignis: War bei der Ausführung des letzten Netzwerkereignisses die Option *Privilegiert zulassen* aktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig aktiviert. War bei der Ausführung des letzten Netzwerkereignisses die Option *Privilegiert zulassen* deaktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig deaktiviert.

## 12.6 WebGuard

Die Rubrik WebGuard der Konfiguration ist für die Konfiguration des WebGuard zuständig.

### 12.6.1 Suche

Mit dem WebGuard schützen Sie sich vor Viren und Malware, die über Webseiten auf Ihren Computer gelangen, die Sie aus dem Internet in Ihren Webbrowser laden. In der Rubrik *Suche* können Sie das Verhalten des WebGuard einstellen.

#### Suche

##### WebGuard aktivieren

Bei aktivierter Option werden Webseiten, die Sie über einen Internetbrowser anfordern, auf Viren und Malware geprüft: Der WebGuard überwacht die aus dem Internet per HTTP-Protokoll übertragenen Daten an den Ports 80, 8080 und 3128. Bei betroffenen Webseiten wird das Laden der Webseite blockiert. Bei deaktivierter Option bleibt der WebGuard-Dienst gestartet, die Suche nach Viren und Malware wird jedoch deaktiviert.

#### Drive-By Schutz

Unter Drive-By-Schutz haben Sie die Möglichkeit, Einstellungen zum Blockieren von I-Frames, auch Inlineframes genannt, vorzunehmen. I-Frames sind HTML-Elemente, d.h. Elemente von Internetseiten, die einen Bereich einer Webseite abgrenzen. Mit I-Frames können andere Webinhalte - meist anderer URLs - als selbständige Dokumente in einem Unterfenster des Browsers geladen und angezeigt werden. Meist werden I-Frames für Banner-Werbung genutzt. In einigen Fällen werden I-Frames zum Verstecken von Malware verwendet. In diesen Fällen ist der Bereich des I-Frame im Browser meist kaum oder nicht sichtbar. Mit der Option *Verdächtige I-Frames blockieren* haben Sie die Möglichkeit, das Laden von I-Frames zu kontrollieren und zu blockieren.

### **Verdächtige I-Frames blockieren**

Bei aktivierter Option werden I-Frames auf angeforderten Webseiten nach bestimmten Kriterien geprüft. Sind auf einer angeforderten Webseite verdächtige I-Frames vorhanden, wird das I-Frame blockiert. Im Fenster des I-Frames wird eine Fehlermeldung angezeigt.

### **Standard**

Bei aktivierter Option werden I-Frames mit verdächtigen Inhalten blockiert.

### **Erweitert**

Bei aktivierter Option werden I-Frames mit verdächtigen Inhalten und I-Frames, die in einer verdächtigen Art und Weise verwendet werden, blockiert. Eine verdächtige Verwendung von I-Frames besteht, wenn das I-Frame sehr klein ist und so im Browser nicht oder kaum sichtbar ist oder wenn das I-Frame auf einer ungewöhnlichen Position auf der Webseite platziert ist.

## 12.6.1.1. Aktion bei Fund

### **Aktion bei Fund**

Sie können Aktionen festlegen, die der WebGuard 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.

### **Zugriff verweigern**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt. Der WebGuard trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.

### **Quarantäne**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden beim Fund eines Virus bzw. einer Malware in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

### ***ignorieren***

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom WebGuard an Ihren Webbrowser weitergeleitet.

### **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".

Weitere Informationen finden Sie hier.

### **Fortschrittsbalken anzeigen**

Bei aktivierter Option erscheint eine Desktopbenachrichtigung mit einem Download-Fortschrittsbalken, wenn ein Download oder das Herunterladen von Webseiten-Inhalten ein Timeout von 20 Sek. überschreitet. Diese Desktopbenachrichtigung dient insbesondere zur Kontrolle beim Herunterladen von Webseiten mit größerem Datenvolumen: Beim Surfen mit WebGuard werden die Webseiteninhalte im Internet-Browser nicht sukzessive geladen, da sie vor der Anzeige im Internet-Browser nach Viren und Malware durchsucht werden. Diese Option ist standardmäßig deaktiviert.

### **Automatisch**

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

### **Warnmeldungen anzeigen**

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

### **Primäre Aktion**

Die primäre Aktion ist die Aktion, die ausgeführt wird, wenn der WebGuard einen Virus bzw. ein unerwünschtes Programm findet.

### **Zugriff verweigern**

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt. Der WebGuard trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.

### ***isolieren***

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden beim Fund eines Virus bzw. einer Malware in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

### ***ignorieren***

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom WebGuard an Ihren Webbrowser weitergeleitet. Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

**Warnung**

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

### 12.6.1.2. Gesperrte Zugriffe

Unter **Gesperrte Zugriffe** können Sie Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) angeben, die vom WebGuard blockiert werden sollen. Mit dem Web-Filter können Sie bekannte, unerwünschte URLs, wie z.B. Phishing- und Malware-URLs, blockieren. Der WebGuard verhindert die Übertragung der Daten vom Internet auf Ihr Computersystem.

#### Vom WebGuard zu blockierende Dateitypen / MIME-Typen (benutzerdefiniert)

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden vom WebGuard blockiert.

##### Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die vom WebGuard blockiert werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. **.htm**. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. **video/mpeg** oder **audio/x-wav**.

##### **Hinweis**

Dateien, die bereits auf Ihrem Computersystem als temporäre Internetdateien gespeichert worden sind, werden zwar vom WebGuard blockiert, können jedoch vom Internet-Browser lokal von Ihrem Computer geladen werden. Temporäre Internetdateien sind Dateien, die vom Internet-Browser auf Ihrem Computer gesichert werden, um Webseiten schneller anzeigen zu können.

##### **Hinweis**

Die Liste der zu blockierenden Datei- und MIME-Typen wird bei Einträgen in der Liste der auszulassenden Datei- und MIME-Typen unter WebGuard::Suche::Ausnahmen ignoriert.

##### **Hinweis**

Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards (Platzhalter \* für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

##### MIME-Typen: Beispiele für Medientypen:

- text = für Textdateien
- image = für Grafikdateien
- video = für Videodateien
- audio = für Sound-Dateien
- application = für Dateien, die an ein bestimmtes Programm gebunden sind

##### Beispiele: Auszulassende Datei- und MIME-Typen

- application/octet-stream = Dateien des MIME-Typs application/octet-stream (ausführbare Dateien \*.bin, \*.exe, \*.com, \*.dll, \*.class) werden vom WebGuard blockiert.
- application/olescript = Dateien des MIME-Typs application/olescript (ActiveX Skript-Dateien \*.axs) werden vom WebGuard blockiert.

- `.exe` = Alle Dateien mit der Dateierweiterung `.exe` (ausführbare Dateien) werden WebGuard blockiert.
- `.msi` = Alle Dateien mit der Dateierweiterung `.msi` (Windows Installer Dateien) werden vom WebGuard blockiert.

### Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.

### Löschen

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

### **Web-Filter**

Der Web-Filter verfügt über eine interne und täglich aktualisierte Datenbank, in der URLs nach Inhaltskriterien klassifiziert sind.

### Web-Filter aktivieren

Bei aktivierter Option werden alle URLs, die zu den ausgewählten Kategorien in der Web-Filter-Liste zählen, blockiert.

### Web-Filter-Liste

In der Web-Filter-Liste können Sie die Inhaltskategorien wählen, deren URLs vom WebGuard blockiert werden sollen.

### **Hinweis**

Der Web-Filter wird bei Einträgen in der Liste der auszulassenden URLs unter WebGuard::Suche::Ausnahmen ignoriert.

### **Hinweis**

Unter Spam-URLs werden URLs kategorisiert, die mit Spam-E-mails verbreitet werden. Die Kategorie Betrug und Täuschung umfasst Webseiten mit 'Abonnement-Fallen' und anderen Angeboten von Dienstleistungen, deren Kosten vom Anbieter verschleiert werden.

## 12.6.1.3. Ausnahmen

Mit diesen Optionen können Sie MIME-Typen (Inhaltstypen der übertragenen Daten) und Dateitypen für URLs (Internetadressen) von der Suche des WebGuard ausschließen. Die angegebenen MIME-Typen und URLs werden vom WebGuard ignoriert, d.h. diese Daten werden beim Übertragen auf Ihr Computersystem nicht auf Viren und Malware durchsucht.

### **Vom WebGuard auszulassende MIME-Typen**

In diesem Feld können Sie die MIME-Typen (Inhaltstypen der übertragenen Daten) auswählen, die von der Suche des WebGuard ausgenommen werden sollen.

### **Vom WebGuard auszulassende Dateitypen / MIME-Typen (benutzerdefiniert)**

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden von der Suche des WebGuard ausgenommen.

### Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die von der Suche des WebGuard ausgenommen werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. **.htm**. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. **video/mpeg** oder **audio/x-wav**.

### **Hinweis**

Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards (Platzhalter \* für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

### **Warnung**

Alle Dateitypen und Inhaltstypen auf der Ausschlussliste werden ohne weitere Prüfung der gesperrten Zugriffe (Liste der zu blockierenden Datei- und MIME-Typen unter WebGuard::Suche::Gesperrte Zugriffe) oder des WebGuard im Internet-Browser geladen: Bei allen Einträgen auf der Ausschlussliste werden die Einträge der Liste der zu blockierenden Datei- und MIME-Typen ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt.

### MIME-Typen: Beispiele für Medientypen:

- text = für Textdateien
- image = für Grafikdateien
- video = für Videodateien
- audio = für Sound-Dateien
- application = für Dateien, die an ein bestimmtes Programm gebunden sind

### Beispiele: Auszulassende Datei- und MIME-Typen

- audio/ = Alle Dateien vom Medientyp Audio werden von der Suche des WebGuard ausgenommen
- video/quicktime = Alle Videodateien vom Subtyp Quicktime (\*.qt, \*.mov) werden von der Suche des WebGuard ausgenommen
- .pdf = Alle Adobe-PDF-Dateien sind von der Suche des WebGuard ausgenommen.

### Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.

### Löschen

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

### **Vom WebGuard auszulassende URLs**

Alle URLs in dieser Liste werden von der Suche des WebGuard ausgenommen.

### Eingabefeld

In diesem Feld geben Sie URLs (Internetadressen) an, die von der Suche des WebGuard ausgenommen werden sollen, z.B. **www.domainname.com**. Sie können Teile der URL angeben, wobei Sie mit abschließenden oder führenden Punkten den Domain-Level kennzeichnen: `.domainname.de` für alle Seiten und alle Subdomains der Domain. Eine Webseite mit beliebiger Top-Level-Domain (`.com` oder `.net`) notieren Sie mit einem abschließendem Punkt: **domainname.**. Wenn Sie eine Zeichenfolge ohne führenden oder abschließenden Punkt notieren, wird die Zeichenfolge als Top-Level-Domain interpretiert, z.B. **net** für alle NET-Domains (`www.domain.net`).

### Hinweis

Bei der Angabe von URLs können Sie auch das Wildcard-Zeichen `*` für beliebig viele Zeichen verwenden. Verwenden Sie auch in Kombination mit Wildcards abschließende oder führende Punkte, um die Domain-Levels zu kennzeichnen:

`.domainname.*`

`*.domainname.com`

`*.name*.com` (gültig aber nicht empfohlen)

Angaben ohne Punkte wie `*name*` werden als Teile einer Top-Level-Domain interpretiert und sind nicht sinnvoll.

### Warnung

Alle Webseiten auf der Liste der auszulassenden URLs werden ohne weitere Prüfung des Web-Filters oder des WebGuard im Internet-Browser geladen: Bei allen Einträgen in der Liste der auszulassenden URLs werden Einträge des Web-Filters (siehe WebGuard::Suche::Gesperrte Zugriffe) ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt. Schließen Sie deshalb nur vertrauenswürdige URLs von der Suche des WebGuard aus.

### Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene URL (Internetadresse) in das Anzeigefenster übernehmen.

### Löschen

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

### Beispiele: Auszulassende URLs

– `www.avira.com -ODER- www.avira.com/*`

= Alle URLs mit der Domain 'www.avira.com' werden von der Suche des WebGuard ausgenommen: `www.avira.com/en/pages/index.php`, `www.avira.com/en/support/index.html`, `www.avira.com/en/download/index.html`,... URLs mit der Domain `www.avira.de` sind nicht von der Suche des WebGuard ausgenommen.

– `avira.com -ODER- *.avira.com`

= Alle URLs mit der Second- und Top-Level-Domain 'avira.com' werden von der Suche des WebGuard ausgenommen. Die Angabe impliziert alle existierenden Subdomains zu `'avira.com'`: `www.avira.com`, `forum.avira.com`,...

– `avira.-ODER- *.avira.*`

= Alle URLs mit der Second-Level-Domain 'avira' werden von der Suche des WebGuard ausgenommen. Die Angabe impliziert alle existierenden Top-Level-Domains oder Subdomains zu `'avira.'`: `www.avira.com`, `www.avira.de`, `forum.avira.com`,...

– `.*domain*.*`



Alle URLs, die eine Second-Level-Domain mit der Zeichenkette 'domain' enthalten, werden von der Suche des WebGuard ausgenommen: www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

– net -ODER- \*.net

=Alle URLs mit der Top-Level-Domain 'net' werden von der Suche des WebGuard ausgenommen: www.name1.net, www.name2.net,...

### **Warnung**

Geben Sie die URLs, die Sie von der Suche des WebGuard ausschließen möchten, so präzise wie möglich an. Vermeiden Sie die Angabe gesamter Top-Level-Domains oder Teile eines Second-Level-Domainnamens, da die Gefahr besteht, dass Internetseiten, die Malware und unerwünschte Programme verbreiten durch globale Angaben unter Ausnahmen von der Suche des WebGuard ausgeschlossen werden. Es wird empfohlen mindestens die vollständige Second-Level-Domain und die Top-Level-Domain anzugeben: domainname.com

#### 12.6.1.4. Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

AntiVir Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware 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 Malware 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**

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

#### **Advanced Heuristic Analysis and Detection (AHeAD)**

##### **AHeAD aktivieren**

Ihr AntiVir Programm beinhaltet mit der AntiVir AHeAD Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware 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 wird weniger unbekannte Malware erkannt, 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 wird bedeutend mehr unbekannte Malware, mit Fehlmeldungen muss jedoch gerechnet werden.

## 12.6.2 Report

Der WebGuard 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 WebGuard 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 WebGuard wichtige Informationen (zu Funden, 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 WebGuard auch weniger wichtige Informationen in die Reportdatei mit auf.

#### **Vollständig**

Bei aktivierter Option nimmt der WebGuard 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. Bei der Beschränkung der Reportdatei 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 weniger 20% erreicht worden ist.

#### **Reportdatei vor dem Kürzen sichern**

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert. Sicherungsort siehe Konfiguration :: Allgemeines :: Verzeichnisse :: Reportverzeichnis.

#### **Konfiguration in Reportdatei schreiben**

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

**Hinweis**

Wenn Sie keine Beschränkung der Reportdatei angegeben haben, werden automatisch ältere Einträge gelöscht, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es werden so viele Einträge gelöscht bis die Reportdatei eine Größe von 80 MB erreicht hat.

## 12.7 Update

Unter der Rubrik *Update* konfigurieren Sie die automatische Ausführung von Updates und die Verbindung zu den Downloadservern. Sie haben die Möglichkeit, verschiedene Update-Intervalle einzustellen sowie das automatische Update zu aktivieren und zu deaktivieren.

**Hinweis**

Wenn Sie Ihr AntiVir Programm unter dem AntiVir Security Management Center konfigurieren, ist die Konfiguration der automatischen Updates nicht verfügbar.

### Automatisches Update

#### Aktivieren

Bei aktivierter Option werden automatische Updates in dem angegebenen Zeitintervall sowie zu den aktivierten Ereignissen ausgeführt.

#### Automatisches Update alle n Tage / Stunden / Minuten

In diesem Feld können Sie das Intervall angeben, in dem automatische Updates ausgeführt werden sollen. Um das Update-Intervall zu ändern, markieren Sie eine der Zeitangaben im Feld und ändern Sie diese über die Pfeiltasten rechts vom Eingabefeld.

#### Auftrag zusätzlich bei Internet Verbindung starten (DFÜ)

Bei aktivierter Option wird der Update-Auftrag zusätzlich zum festgelegten Update-Intervall bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

#### Auftrag nachholen, wenn die Zeit bereits abgelaufen ist

Bei aktivierter Option werden Update-Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.

### Download

#### Über Webserver

Das Update erfolgt über einen Webserver per HTTP-Verbindung. Sie können einen Webserver des Herstellers im Internet nutzen oder einen Webserver im Intranet, der die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht.

**Hinweis**

Weitere Einstellungen zum Update über einen Webserver finden Sie unter: Konfiguration :: Allgemeines :: Update :: Webserver .

#### Über Dateiserver/Freigegebene Verzeichnisse

Das Update erfolgt über einen Dateiserver im Intranet, der die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht.

### **Hinweis**

Weitere Einstellungen zum Update über einen Dateiserver finden Sie unter: Konfiguration :: Allgemeines :: Update :: Dateiserver .

## 12.7.1 Produktupdate

Unter **Produktupdate** konfigurieren Sie die Ausführung von Produktupdates oder die Benachrichtigung über verfügbare Produktupdates.

### **Produktupdates**

#### **Produktupdates herunterladen und automatisch installieren**

Bei aktivierter Option werden Produktupdates heruntergeladen und automatisch von der Update-Komponente 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.

#### **Produktupdates herunterladen. Falls ein Neustart erforderlich ist, das Update nach dem nächsten Neustart des Systems installieren, ansonsten sofort installieren.**

Bei aktivierter Option werden Produktupdates heruntergeladen, sobald Produktupdates verfügbar sind. Das Update wird automatisch nach dem Download der Update-Dateien installiert, falls kein Neustart erforderlich ist. Wenn es sich um ein Produktupdate handelt, das einen Neustart des Rechners erfordert, wird das Produktupdate nicht sofort nach dem Download der Update-Dateien ausgeführt, sondern erst nach dem nächsten, benutzergesteuerten Neustart des Systems. Dies hat den Vorteil, dass der Neustart nicht zu einem Zeitpunkt ausgeführt wird, zu dem ein Benutzer am Rechner arbeitet. 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 Updater im Control Center unter Übersicht ::Ereignisse.

#### **Erneut benachrichtigen nach n Tag(en)**

Geben Sie in diesem Feld an, nach wie viel Tagen eine erneute Benachrichtigung über verfügbare Produktupdates erfolgen soll, falls das Produktupdate nach der ersten Benachrichtigung nicht durchgeführt wurde.

#### **Keine Produktupdates herunterladen**

Bei aktivierter Option erfolgen keine automatischen Produktupdates oder Benachrichtigungen zu verfügbaren Produktupdates durch 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).

**Hinweis**

Wenn Sie eine Option für ein automatisches Produktupdate aktiviert haben, können Sie unter Neustart-Einstellungen weitere Optionen zur Meldung und zu Abbruchmöglichkeiten des Neustarts konfigurieren.

## 12.7.2 Neustart-Einstellungen

Wenn ein Produktupdate Ihres AntiVir Programms ausgeführt wird, kann ein Neustart Ihres Computersystems erforderlich sein. Falls Sie eine automatische Ausführung von Produktupdates unter Update::Produktupdate eingestellt haben, können Sie unter **Neustart-Einstellungen** zwischen verschiedenen Optionen zur Meldung des Neustarts und zum Abbruch des Neustarts wählen.

**Hinweis**

Beachten Sie bei Ihren Einstellungen zum Neustart, dass Sie in der Konfiguration unter Update::Produktupdate zwischen zwei Optionen zur Ausführung eines Produktupdates mit erforderlichem Rechnerneustart wählen können:

Automatische Ausführung des Produktupdates mit erforderlichem Rechnerneustart bei Verfügbarkeit des Updates: Das Update und der Neustart werden ausgeführt, während ein Benutzer am Rechner arbeitet. Wenn Sie diese Option aktiviert haben, können die Neustart-routinen mit Abbruchmöglichkeit oder mit Erinnerungsfunktion sinnvoll sein.

Ausführung des Produktupdates mit erforderlichem Rechnerneustart nach dem nächsten Systemstart: Das Update und der Neustart werden ausgeführt, nachdem ein Benutzer den Rechner gestartet und sich angemeldet hat. Für diese Option empfehlen sich die automatischen Neustart-routinen.

### Neustart-Einstellungen

#### Neustart des Rechners nach n Sekunden

Bei aktivierter Option wird ein ggf. erforderlicher Neustart nach Ausführung eines Produktupdates nach dem angegebenen Zeitintervall **automatisch** durchgeführt. Es erscheint eine Countdown-Meldung ohne Möglichkeit den Rechnerneustart abzubrechen.

#### Erinnerungsmeldung zum Neustart alle n Sekunden

Bei aktivierter Option wird **nicht automatisch** ein ggf. erforderlicher Neustart nach Ausführung eines Produktupdates durchgeführt. Sie erhalten im angegebenen Zeitintervall Meldungen ohne Abbruchmöglichkeiten für den Neustart. In den Meldungen können Sie den Neustart des Rechners bestätigen oder die Option "**Weiter erinnern**" auswählen.

**Nachfrage, ob Neustart des Rechners durchgeführt werden soll**

Bei aktivierter Option wird **nicht automatisch** ein ggf. erforderlicher Neustart nach Ausführung eines Produktupdates durchgeführt. Sie erhalten einmalig eine Meldung, in der Sie den Neustart bestätigen oder die Neustartroutine abbrechen können.

**Neustart des Rechners ohne Nachfrage**

Bei aktivierter Option wird **automatisch** ein ggf. erforderlicher Neustart nach Ausführung eines Produktupdates durchgeführt. Sie erhalten keine Meldung.

## 12.7.3 Dateiserver

Bei mehreren Computern in einem Netzwerk kann Ihr AntiVir Programm ein Update von einem Dateiserver im Intranet herunterladen, der seinerseits die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht. So kann die Aktualität von AntiVir Programmen auf allen Computern ressourcenschonend sichergestellt werden.

**Hinweis**

Die Konfigurationsrubrik ist nur aktiviert, wenn unter Konfiguration :: Update:: Produktupdate die Option **Über Dateiserver / Freigegebene Verzeichnisse** ausgewählt wurde.

**Download**

Geben Sie den Dateiserver an, auf dem sich die Update-Dateien Ihres AntiVir Programms befinden, sowie die erforderlichen Verzeichnisse '/release/update/'. Folgende Angabe ist erforderlich: file://<IP-Adresse des Dateiservers>/release/update/. Das Verzeichnis 'release' muss ein Verzeichnis sein, das für alle Benutzer freigegeben ist.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, das gewünschte Download-Verzeichnis auszuwählen.

**Server Login****Login Name**

Geben Sie einen Benutzernamen für die Anmeldung am Server ein. Verwenden Sie ein Benutzerkonto mit Zugriffsrechten auf das genutzte, freigegebene Verzeichnis am Server.

**Login Kennwort**

Geben Sie das Passwort des genutzten Benutzerkontos ein. Die eingegebenen Zeichen werden mit \* maskiert.

**Hinweis**

Wenn Sie im Bereich Server Login keine Daten eingeben, wird beim Zugriff auf den Dateiserver keine Authentifizierung durchgeführt. In diesem Fall müssen jedoch ausreichende Benutzerrechte auf dem Dateiserver vorhanden sein.

## 12.7.4 Webserver

Das Update kann direkt über einen Webserver im Internet oder Intranet 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 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 Internetdiensteanbieter, 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 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.

---

#### **Hinweis**

Die Option ist unter Vista nicht verfügbar. Unter Vista wird die DFÜ-Verbindung, die für das Update geöffnet wurde, immer beendet, sobald der Download durchgeführt wurde.

---

### Download

#### Standard-Server

Geben Sie hier die Adressen (URL) der Webserver an, von denen die Updates geladen werden sollen, sowie das erforderliche Update-Verzeichnis 'update'. Folgende Angabe eines Webserver ist gültig: http://<Adresse des Servers>[:Port]/update. Wenn Sie keinen Port angeben, wird Port 80 verwendet. Standardmäßig sind die erreichbaren Webserver der Avira GmbH für das Update eingetragen. Sie können jedoch auch eigene Webserver beispielsweise im Intranet nutzen. Bei der Angabe von mehreren Webservern werden die Server über Kommata getrennt.

#### Standard

Die Schaltfläche stellt die vordefinierten Adressen wieder her.

#### Prioritäts-Server

Geben Sie in diesem Feld die Adresse (URL) des Webservers an, der bei einem Update als erster Server angefragt werden soll, sowie das erforderliche Update-Verzeichnis. Wenn dieser Server nicht erreichbar ist, werden die angegebenen Standard-Server angefragt. Folgende Angabe des Webservers ist gültig: `http://<Adresse des Webservers>[:Port]/update`. Wenn Sie keinen Port angeben, wird Port 80 verwendet.

### 12.7.4.1. 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. Sie konfigurieren die Windows Systemeinstellungen zur Verwendung eines Proxyservers unter

**Systemsteuerung:: Internetoptionen :: Verbindungen :: LAN-Einstellungen**. Im Internet Explorer können Sie im Menü Extras ebenfalls auf die Internetoptionen zugreifen.

##### **Warnung**

Wenn Sie einen Proxyserver nutzen, der eine Authentifizierung erfordert, geben Sie die Daten unter der Option *Verbindung über diesen Proxy* vollständig an. Die Option *Windows Systemeinstellungen verwenden* kann nur für Proxyserver ohne Authentifizierung genutzt werden.

##### 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 den Rechnernamen oder die IP-Adresse des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

##### Port

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

##### Login Name

Geben Sie einen Benutzernamen für die Anmeldung 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



## 12.8 Allgemeines

### 12.8.1 Email

Das AntiVir Programm 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. Folgende Komponenten unterstützen den Versand von Emails:

- Guard: Versenden von Benachrichtigungen
- Scanner: Versenden von Benachrichtigungen
- Updater: Versenden von Benachrichtigungen

#### **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 können mit Authentifizierung an einen SMTP-Server übergeben werden.

##### **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 das Programm zur Überprüfung der eingegebenen Daten eine Test-Email an die Absenderadresse zu senden.

## 12.8.2 Gefahrenkategorien

### Auswahl Gefahrenkategorien

Ihr AntiVir Produkt schützt Sie vor Computerviren.

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

- Backdoor-Steuersoftware (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.

## 12.8.3 Kennwort

Sie können Ihr AntiVir Programm 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 20 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

Ihr AntiVir Programm 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.

<b>Kennwortgeschützer Bereich</b>	<b>Funktion</b>
<b>Control Center</b>	Bei aktivierter Option wird zum Start des Control Center das gesetzte Kennwort benötigt.
Guard aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung von AntiVir Guard das gesetzte Kennwort benötigt.
MailGuard aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des MailGuard das gesetzte Kennwort benötigt.
FireWall aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung der FireWall das gesetzte Kennwort benötigt.
WebGuard aktivieren/ deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des WebGuard das gesetzte Kennwort benötigt.
Rescue-CD aus Internet herunterladen	Bei aktivierter Option wird für den Start des Downloads der Avira Rescue-CD das gesetzte Kennwort benötigt.
<b>Quarantäne</b>	Bei aktivierter Option werden alle 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 das gesetzte Kennwort benötigt.
Erneutes Prüfen betroffener Objekte	Bei aktivierter Option wird zum erneuten Prüfen eines Objekts das gesetzte Kennwort benötigt.
Eigenschaften betroffener Objekte	Bei aktivierter Option wird zur Anzeige der Eigenschaften eines Objekts das gesetzte Kennwort benötigt.

Löschen betroffener Objekte	Bei aktivierter Option wird für das Löschen eines Objekts das gesetzte Kennwort benötigt.
Email an Avira senden	Bei aktivierter Option wird für das Versenden eines Objekts zur Überprüfung an das Avira Malware Research Center das gesetzte Kennwort benötigt.
Kopieren betroffener Objekte	Bei aktivierter Option wird für das Kopieren von betroffenen Objekten das gesetzte Kennwort benötigt.
Hinzufügen und Ändern von Aufträgen	Bei aktivierter Option wird beim Hinzufügen und Ändern von Aufträgen im Planer das gesetzte Kennwort benötigt.
Produktupdates starten	Bei aktivierter Option wird beim Starten des Produktupdates im Menü Update das gesetzte Kennwort benötigt.
<b>Konfiguration</b>	Bei aktivierter Option ist die Konfiguration des Programms nur nach Eingabe des gesetzten Kennworts möglich.
Manuelles Umschalten der Konfiguration	Bei aktivierter Option wird zum manuellen Umschalten auf ein anderes Konfigurationsprofil das gesetzte Kennwort benötigt.
Expertenmodus aktivieren	Bei aktivierter Option wird zur Aktivierung des Expertenmodus das gesetzte Kennwort benötigt.
<b>Installation / Deinstallation</b>	Bei aktivierter Option wird zur Installation bzw. Deinstallation des Programms das gesetzte Kennwort benötigt.

## 12.8.4 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 maximal vergangen sein dürfen. Ist dieses Alter überschritten, wird im Control Center unter Status ein rotes Icon für den Update-Status 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.

### Produktschutz

**Hinweis**

Die Optionen zum Produktschutz sind nicht verfügbar, wenn der Guard bei einer benutzerdefinierten Installation nicht installiert wurde.

**Prozesse vor unerwünschtem Beenden schützen**

Bei aktivierter Option werden alle Prozesse des Programms 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.

**Erweiterter Prozessschutz**

Bei aktivierter Option werden alle Prozesse des Programms vor unerwünschtem Beenden mit erweiterten Methoden geschützt. Der erweiterte Prozessschutz benötigt erheblich mehr Rechnerressourcen als der einfache Prozessschutz. Die Option ist standardmäßig aktiviert. Zum Deaktivieren der Option ist ein Rechnerneustart erforderlich.

**Wichtig**

Der Prozessschutz ist unter Windows XP 64 Bit nicht verfügbar!

**Warnung**

Bei aktiviertem Prozessschutz können Interaktionsprobleme mit anderen Softwareprodukten auftreten. Deaktivieren Sie in diesen Fällen den Prozessschutz.

**Dateien und Registrierungseinträge vor Manipulation schützen**

Bei aktivierter Option werden alle Registry-Einträge des Programms sowie alle Dateien des Programms (Binär- und Konfigurationsdateien) vor Manipulation geschützt. Der Schutz vor Manipulation beinhaltet den Schutz vor schreibendem, löschendem und z.T. lesendem Zugriff auf die Registry-Einträge oder die Programmdateien durch Benutzer oder fremde Programme. Zum Aktivieren der Option ist ein Rechnerneustart erforderlich.

**Warnung**

Beachten Sie, dass bei deaktivierter Option die Reparatur von Computern, die mit bestimmten Arten von Malware infiziert sind, fehlschlagen kann.

**Hinweis**

Bei aktivierter Option sind Änderungen an der Konfiguration, so auch die Änderung von Prüf- oder Update-Aufträgen nur über die Benutzeroberfläche möglich.

**Wichtig**

Der Schutz von Dateien und Registrierungseinträgen ist unter Windows XP 64 Bit nicht verfügbar!

## 12.8.5 WMI

### Unterstützung für Windows Management Instrumentation

Windows Management Instrumentation ist eine grundlegende Windows Verwaltungstechnologie, die es ermöglicht mittels Skript- und Programmiersprachen lesend und schreibend, lokal und remote auf Einstellungen von Windows Rechnern zuzugreifen. Ihr AntiVir Programm unterstützt WMI und stellt Daten (Statusinformationen, Statistik-Daten, Reports, geplante Aufträge etc.) sowie Ereignisse und Methoden (Prozesse stoppen und starten) an einer Schnittstelle zur Verfügung. Sie haben über WMI die Möglichkeit, Betriebsdaten des Programms abzurufen und das Programm zu steuern. Eine vollständige Referenz der WMI-Schnittstelle können Sie beim Hersteller anfordern. Nach der Unterzeichnung einer Geheimhaltungsvereinbarung erhalten Sie die Referenz im PDF-Format.

#### **WMI-Unterstützung aktivieren**

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Betriebsdaten des Programms abzurufen.

#### **Aktivieren/Deaktivieren von Diensten erlauben**

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Dienste des Programms zu aktivieren und zu deaktivieren.

## 12.8.6 Verzeichnisse

### **Temporärer Pfad**

In diesem Eingabefeld tragen Sie den Pfad ein, unter dem temporäre Dateien vom Programm ablegt sollen.

#### **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.

### **Reportverzeichnis**

Dieses Eingabefeld enthält den Pfad zum Report Verzeichnis.



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

### **Standard**

Die Schaltfläche stellt den vordefinierten Pfad zum Reportverzeichnis wieder her.

### **Quarantäneverzeichnis**

Dieses Eingabefeld enthält den Pfad zum Quarantäneverzeichnis.



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

### **Standard**

Die Schaltfläche stellt den vordefinierten Pfad zum Quarantäneverzeichnis wieder her.

## 12.8.7 Warnungen

### 12.8.7.1. 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.

#### **Warnung**

Die Funktionalität wird von den folgenden Betriebssystemen nicht mehr unterstützt:  
Windows Server 2008 und höher  
Windows Vista und höher

### **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.

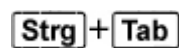
#### **Hinweis**

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

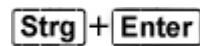
#### Zu sendende Nachricht

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.



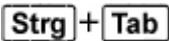
### **Hinweis**

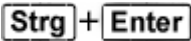
Um diese Option aktivieren zu können, muss unter Allgemeines :: Warnungen :: Netzwerk mindestens ein Empfänger eingetragen sein.

### **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.

## 12.8.7.2. Email

### **Email**

Das AntiVir Programm 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. Folgende Komponenten unterstützen den Versand von Emails:

- Guard: Versenden von Benachrichtigungen
- Scanner: Versenden von Benachrichtigungen
- Updater: Versenden von Benachrichtigungen

### **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 können mit Authentifizierung an einen SMTP-Server übergeben werden.

#### 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 das Programm zur Überprüfung der eingegebenen Daten eine Test-Email an die Absenderadresse zu senden.

### **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.

#### Bearbeiten

Mit der Schaltfläche "Bearbeiten" öffnen Sie das Fenster "Email-Template", in dem Sie die Nachricht zum Ereignis "Fund bei Echtzeitsuche" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Email::Warnungen::Email-Template).

### **Innerhalb des Guard ist ein kritischer Fehler aufgetreten.**

Bei aktivierter Option erhalten Sie eine Email, wenn ein interner kritischer Fehler festgestellt wird.

### **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 mitgesendet werden.

### **Bearbeiten**

Mit der Schaltfläche "Bearbeiten" öffnen Sie das Fenster "Email-Template", in dem Sie die Nachricht zum Ereignis "Kritischer Fehler in Guard" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **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 das Programm 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.

### **Bearbeiten**

Mit der Schaltfläche "Bearbeiten" öffnen Sie das Fenster "Email-Template", in dem Sie die Nachricht zum Ereignis "Fund bei Suche" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **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.

### **Bearbeiten**

Mit der Schaltfläche "Bearbeiten" öffnen Sie das Fenster "Email-Template", in dem Sie die Nachricht zum Ereignis "Ende des Suchlaufs" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **Reportdatei als Anlage beifügen**

Bei aktivierter Option wird beim Versenden von Scanner-Benachrichtigungen die aktuelle Reportdatei der Komponente Scanner als Anlage an die Email angefügt.

### **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.

## **Updater**

Die Komponente Updater kann bei bestimmten Ereignissen Meldungen per Email an einen oder mehrere Empfänger senden.

## **Updater**

### **Email Warnungen**

Bei aktivierter Option versendet die Update-Komponente Email-Nachrichten mit den wichtigsten Daten, wenn ein bestimmtes Ereignis eintritt. Standardmäßig ist diese Option deaktiviert.

### **Benachrichtigungen per Email bei folgenden Ereignissen**

#### **Kein Update erforderlich. Ihr Programm ist auf dem neuesten Stand.**

Bei aktivierter Option wird eine Email versendet, wenn der Updater erfolgreich eine Verbindung zum Download-Server erstellen konnte, am Server jedoch keine neuen Dateien verfügbar sind. Dies bedeutet, dass Ihr AntiVir Programm auf dem aktuellsten Stand ist.

### **Bearbeiten**

Mit der Schaltfläche "Bearbeiten" öffnen Sie das Fenster "Email-Template", in dem Sie die Nachricht zum Ereignis 'Kein Update erforderlich' konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

#### **Update erfolgreich beendet. Es wurden neue Dateien installiert.**

Bei aktivierter Option wird bei allen ausgeführten Updates eine Email versendet: Es kann sich um ein Produktupdate oder eine Aktualisierung der Virendefinitionsdatei oder der Suchengine handeln.

### **Bearbeiten**

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis 'Update erfolgreich-Installation von neuen Dateien' konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **Update erfolgreich beendet. Es ist ein neues Produktupdate verfügbar.**

Bei aktivierter Option wird nur dann eine Email versendet, wenn eine Aktualisierung der Suchengine oder Virendefinitionsdatei ohne Produktupdate ausgeführt wurde, jedoch ein Produktupdate verfügbar ist.

### **Bearbeiten**

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Update erfolgreich-Produktupdate verfügbar" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **Update fehlgeschlagen.**

Bei aktivierter Option wird eine Email versendet, wenn das Update aufgrund eines Fehlers fehlgeschlagen ist.

### **Bearbeiten**

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Update fehlgeschlagen" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

### **Reportdatei als Anlage beifügen**

Bei aktivierter Option wird beim Versenden von Updater-Benachrichtigungen die aktuelle Reportdatei der Komponente Updater als Anlage an die Email angefügt.

### **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.

### **Hinweis**

Bei den folgenden Ereignisse werden immer Warnmeldungen via Email versandt, falls ein SMTP-Server und eine Empfängeradresse für Updater-Benachrichtigungen konfiguriert wurden:

Ein Produktupdate ist für jede weitere Aktualisierung des Programms erforderlich.

Eine Aktualisierung der Suchengine oder der Virendefinitionsdatei konnte nicht ausgeführt werden, da ein Produktupdate erforderlich ist.

Der Versand dieser Warnmeldungen wird unabhängig von Ihren Einstellungen zu den Email-Warnungen der Update-Komponente ausgeführt.

## Email-Template

Im Fenster *Email-Template* konfigurieren Sie die Email-Benachrichtigungen der einzelnen Komponenten zu den aktivierten Ereignissen. Sie können einen Text bis zu maximal 128 Zeichen in der Betreffzeile und einen Text bis zu maximal 1024 Zeichen im Nachrichtenfeld eingeben.

Folgende Variablen können im Email-Betreff und in der Email-Nachricht verwendet werden:

### Global gültige Variablen

Variable	Wert
Windows Umgebungsvariablen	Die Komponente der Email-Benachrichtigungen unterstützt alle Windows Umgebungsvariablen.
%SYSTEM_IP%	IP-Adresse des Rechners
%FQDN%	Vollständiger Domainname (fully qualified domain name)
%TIMESTAMP%	Zeitstempel des Ereignisses: Zeit- und Datumsformate entsprechend den Spracheinstellungen des Betriebssystems
%COMPUTERNAME%	NetBIOS-Computername
%USERNAME%	Name des Benutzers, der auf die Komponente zugreift
%PRODUCTVER%	Produktversion
%PRODUCTNAME%	Produktname
%MODULENAME%	Name der Komponente, die die Email versendet
%MODULEVER%	Version der Komponente, die die Email versendet

### Spezifische Variablen der Komponenten

Variable	Wert	Emails der Komponenten
%ENGINEVER%	Version der verwendeten Suchengine	Guard Scanner
%VDFVER%	Version der verwendeten Virendefinitionsdatei	Guard Scanner
%SOURCE%	Voll qualifizierter Dateiname	Guard
%VIRUSNAME%	Name des Virus oder unerwünschten Programms	Guard
%ACTION%	Aktion, die nach dem	Guard

	Fund ausgeführt wurde	
%MACADDR%	MAC-Adresse der ersten registrierten Netzwerkkarte	Guard
%UPDFILESLIST%	Liste der aktualisierten Dateien	Updater
%UPDATETYPE%	Update-Typ: Update von Suchengine und Virendefinitionsdatei oder Produktupdate mit Aktualisierung von Suchengine und Virendefinitionsdatei	Updater
%UPDATEURL%	URL des Downloadservers, der für das Update verwendet wurde	Updater
%UPDATE_ERROR%	Update-Fehler in Worten	Updater
%DIRCOUNT%	Anzahl durchsuchter Verzeichnisse	Scanner
%FILECOUNT%	Anzahl durchsuchter Dateien	Scanner
%MALWARECOUNT%	Anzahl gefundener Viren oder unerwünschter Programme	Scanner
%REPAIREDCOUNT%	Anzahl reparierter betroffener Dateien	Scanner
%RENAMEDCOUNT%	Anzahl umbenannter betroffener Dateien	Scanner
%DELETEDCOUNT%	Anzahl gelöschter betroffener Dateien	Scanner
%WIPECOUNT%	Anzahl betroffener Dateien, die überschrieben und gelöscht wurden	Scanner
%MOVEDCOUNT%	Anzahl betroffener Dateien, die in die Quarantäne verschoben wurden	Scanner
%WARNINGCOUNT%	Anzahl der Warnungen	Scanner
%ENDTYPE%	Status des Suchlaufendes: Abgebrochen   Erfolgreich beendet	Scanner

%START_TIME%	Startzeitpunkt des Suchlaufs Startzeitpunkt des Updates	Scanner Updater
%END_TIME%	Ende des Suchlaufs Ende des Updates	Scanner Updater
%TIME_TAKEN%	Ausführungsdauer des Suchlaufs in Minuten Ausführungsdauer des Updates in Minuten	Scanner Updater
%LOGFILEPATH%	Pfad und Dateiname der Reportdatei	Scanner Updater

### 12.8.7.3. Akustische Warnungen

#### Akustische Warnung

Beim Fund eines Virus oder einer Malware durch den Scanner oder den Guard ertönt im interaktiven Aktionsmodus ein Warnton. Sie haben die Möglichkeit, den Warnton zu deaktivieren oder zu aktivieren sowie eine alternative Wave-Datei als Warnton auszuwählen.

#### Hinweis

Der Aktionsmodus des Scanner wird in der Konfiguration unter Scanner::Suche::Aktion bei Fund eingestellt. Der Aktionsmodus des Guard wird in der Konfiguration unter Guard::Suche::Aktion bei Fund eingestellt.

#### Keine Warnung

Bei aktivierter Option erfolgt keine akustische Warnung bei einem Virenfund durch den Scanner oder den Guard.

#### Über PC-Lautsprecher abspielen (nur bei interaktivem Modus)

Bei aktivierter Option erfolgt eine akustische Warnung mit dem Standardwarnton beim Fund eines Virus durch den Scanner oder den Guard. Der Warnton wird über den PC internen Lautsprecher abgespielt.

#### Folgende Wave-Datei benutzen (nur bei interaktivem Modus)

Bei aktivierter Option erfolgt bei Fund eines Virus durch den Scanner oder den Guard ein akustisches Warnen mit der ausgewählten Wave-Datei. Die ausgewählte Wave-Datei wird über einen angeschlossenen externen Lautsprecher abgespielt.

#### Wave- Datei

In diesem Eingabefeld können Sie den Namen und den dazugehörigen Pfad einer Audiodatei Ihrer Wahl eintragen. Der Standardwarnton des Programms ist per Default eingetragen.



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

#### Test



Diese Schaltfläche dient zum Testen der ausgewählten Wave-Datei.

#### 12.8.7.4. Warnungen

Ihr AntiVir Programm erzeugt bei bestimmten Ereignissen Desktopbenachrichtigungen, sogenannte Slide-Ups, um Sie über Gefahren sowie erfolgreich ausgeführte oder fehlgeschlagene Programmabläufe, wie z.B. die Ausführung eines Updates, zu informieren. Unter *Warnungen* können Sie die Benachrichtigung bei bestimmten Ereignissen aktivieren oder deaktivieren.

Bei Desktop-Benachrichtigungen besteht die Möglichkeit, die Benachrichtigung direkt im Slide-Up zu deaktivieren. Sie können die Deaktivierung der Benachrichtigung unter *Warnungen* rückgängig machen.

##### **Warnungen**

###### **über verwendete Dial-Up Verbindungen**

Bei aktivierter Option werden Sie mit einer Desktop-Benachrichtigung gewarnt, wenn auf Ihrem Rechner ein Einwahlprogramm über das Telefon- oder das ISDN-Netz eine Wählverbindung aufbaut. Es besteht die Gefahr, dass es sich bei dem Einwahlprogramm um einen unbekanntes und unerwünschten Dialer handelt, der eine kostenpflichtige Verbindung erstellt. (siehe Viren und mehr::Gefahrenkategorien: Dialer).

###### **über erfolgreich aktualisierte Dateien**

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update erfolgreich abgeschlossen wurde und Dateien aktualisiert wurden.

###### **über fehlgeschlagenes Update**

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update fehlgeschlagen ist: Es konnte keine Verbindung zum Downloadserver aufgebaut werden oder die Update-Dateien konnten nicht installiert werden.

###### **dass kein Update notwendig ist**

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update angestoßen wurde, die Installation von Dateien jedoch nicht erforderlich war, da Ihr Programm auf dem aktuellsten Stand ist.

#### 12.8.8 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. Auf der Programmoberfläche unter Ereignisse werden jedoch maximal 20 000 Einträge angezeigt.

## 12.8.9 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.

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 Operations GmbH & Co. KG nicht gestattet.

Ausgabe Q2-2011

Hier verwendete 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.



live free.™