Avira AntiVir Premium

Handbuch für Anwender

AVIRA

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 Premium 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 Premium unter Third Party Licenses.

Inhaltsverzeichnis

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:

Symbol / Bezeichnung	Erläuterung
✓	Steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss.
▸	Steht vor einem Handlungsschritt, den Sie ausführen.
→	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
Warnung	Steht vor einer Warnung bei Gefahr von kritischem Datenverlust.
Hinweis	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:

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

3 Produktinformationen

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

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

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. Inklusive 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
- 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)

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 in Form eines Aktivierungsschlüssels vergeben. Der Aktivierungsschlüssel ist ein Buchstaben-Zahlen-Code, den Sie beim Erwerb des AntiVir Produkts erhalten. Über den Aktivierungsschlüssel sind die genauen Daten Ihrer Lizenz, d.h. welche Programme für welchen Zeitraum lizenziert wurden, erfasst.

Der Aktivierungsschlüssel wird Ihnen in einer Email übermittelt, falls Sie Ihr AntiVir Programm im Internet erworben haben, oder ist auf der Produktverpackung vermerkt.

Um Ihr Programm zu lizenzieren, geben Sie den Aktivierungsschlüssel bei der Aktivierung des Programms ein. Die Produktaktivierung kann bei der Installation erfolgen. Sie können Ihr AntiVir Programm jedoch auch nach der Installation im Lizenzmanager unter Hilfe::Lizenzmanagement aktivieren.

Im Lizenzmanager haben Sie die Möglichkeit, ein Upgrade auf ein Produkt aus der AntiVir Desktop-Produktfamilie anzustoßen: Eine manuelle Deinstallation des alten Produkts und eine manuelle Installation des neuen Produkts sind dadurch nicht erforderlich. Beim Upgrade aus dem Lizenzmanager geben Sie den Aktivierungsschlüssel des Produkts, auf das Sie umsteigen möchten, im Eingabefeld des Lizenzmanagers an. Es erfolgt eine automatische Installation des neuen Produkts.

Über den Lizenzmanager können folgende Produktupgrades automatisch ausgeführt werden:

- Upgrade von Avira AntiVir Personal auf Avira AntiVir Premium
- Upgrade von Avira AntiVir Personal auf Avira Premium Security Suite
- Upgrade von Avira AntiVir Premium auf Avira Premium Security Suite

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
- 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 **Schutzeinstellungen** 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

- 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)
- Aktivierung des Programms
- Ggf. Ausführung eines Updates nach beendeter Installation
- Halten Sie den Lizenzschlüssel für Ihr AntiVir Programm bereit, wenn Sie das 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.

Hinweis
Zur Produktaktivierung kommuniziert Ihr AntiVir Programm über das HTTP-Protokoll und Port 80 (Web-Kommunikation) sowie über das Verschlüsselungsprotokoll SSL und Port 443 mit den Servern der Avira GmbH. Falls Sie eine Firewall nutzen, stellen Sie sicher, dass die benötigten Verbindungen und eingehende oder ausgehende Daten nicht von der Firewall blockiert werden.

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:

▶ 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 Premium*.

▶ 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**.

▶ Überspringen Sie den folgenden Abschnitt "Expressinstallation".

Expressinstallation

Es 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**.

Fortsetzung: Expressinstallation und benutzerdefinierte Installation

Der Lizenz-Assistent wird geöffnet.

Sie haben folgende Optionen zur Aktivierung des Programms zur Auswahl

- Eingabe eines Aktivierungsschlüssels

  Durch die Eingabe Ihres Aktivierungsschlüssels wird Ihr AntiVir Programm mit Ihrer Lizenz aktiviert.

- Auswahl der Option **Produkt testen**

  Wählen Sie **Produkt testen**, wird beim Aktivierungsvorgangs eine Evaluationslizenz generiert, mit das Programm aktiviert wird. Sie können das AntiVir Programm für einen bestimmten Zeitraum in seinem vollen Funktionsumfang testen.

Hinweis
Mit der Option **Gültige hbedv.key Lizenzdatei vorhanden** können Sie eine gültige Lizenzdatei einlesen. Die Lizenzdatei wird beim Vorgang der Produktaktivierung mit einem gültigen Aktivierungsschlüssel generiert und im Programmverzeichnis Ihres AntiVir Programms abgelegt. Nutzen Sie diese Option, wenn Sie eine Produktaktivierung bereits durchgeführt haben und Ihr AntiVir Programm neu installieren möchten.

Hinweis
Bei einigen Verkaufsversionen von AntiVir Produkten ist ein Aktivierungsschlüssel bereits im Produkt hinterlegt. Ein Aktivierungsschlüssel muss daher nicht angegeben werden. Der hinterlegte Aktivierungsschlüssel wird ggf. im Lizenz-Assistenten angezeigt.

Hinweis
Zur Aktivierung des Programms wird eine Verbindung zu den Servern der Avira GmbH erstellt. Unter **Proxy Einstellungen** können Sie die Internetverbindung über einen Proxyserver konfigurieren.

- Wählen Sie einen Aktivierungsvorgang und bestätigen Sie mit **Weiter**

Produktaktivierung

Ein Dialogfenster wird geöffnet, in dem Sie Ihre persönlichen Daten eingeben können.

- Geben Sie Ihre Daten ein und klicken Sie auf **Weiter**

Ihre Daten werden zu den Servern der Avira GmbH übertragen und geprüft. Ihr AntiVir Programm wird mit Ihrer Lizenz aktiviert.

Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt.

- Klicken Sie auf **Weiter**.
- Überspringen Sie den folgenden Abschnitt "Aktivierung über die Auswahl der Option **Gültige hbedv.key vorhanden** ".

Auswahl der Option "Gültige hbedv.key vorhanden"

Ein Dialog zum Einlesen der Lizenzdatei wird geöffnet.

- Wählen Sie die Lizenzdatei hbedv.key mit Ihren Lizenzdaten für das Programm und klicken Sie auf **Öffnen**

Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt.

- Klicken Sie auf **Weiter**

Fortsetzung nach abgeschlossener Aktivierung oder Laden der Lizenzdatei

Die Programmkomponenten werden installiert. Der Installationsfortschritt wird im Dialogfenster angezeigt.

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 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 *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 Premium**
  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.
- *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**.

  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.

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

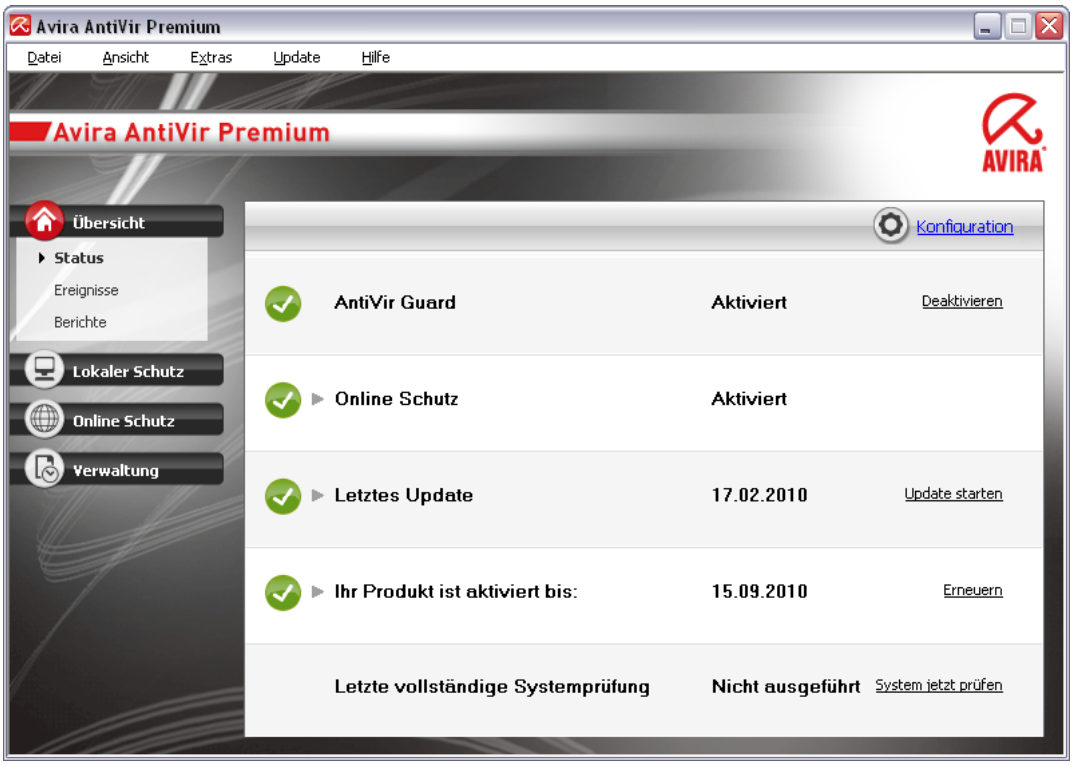
5.1 Oberfläche und Bedienung

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.

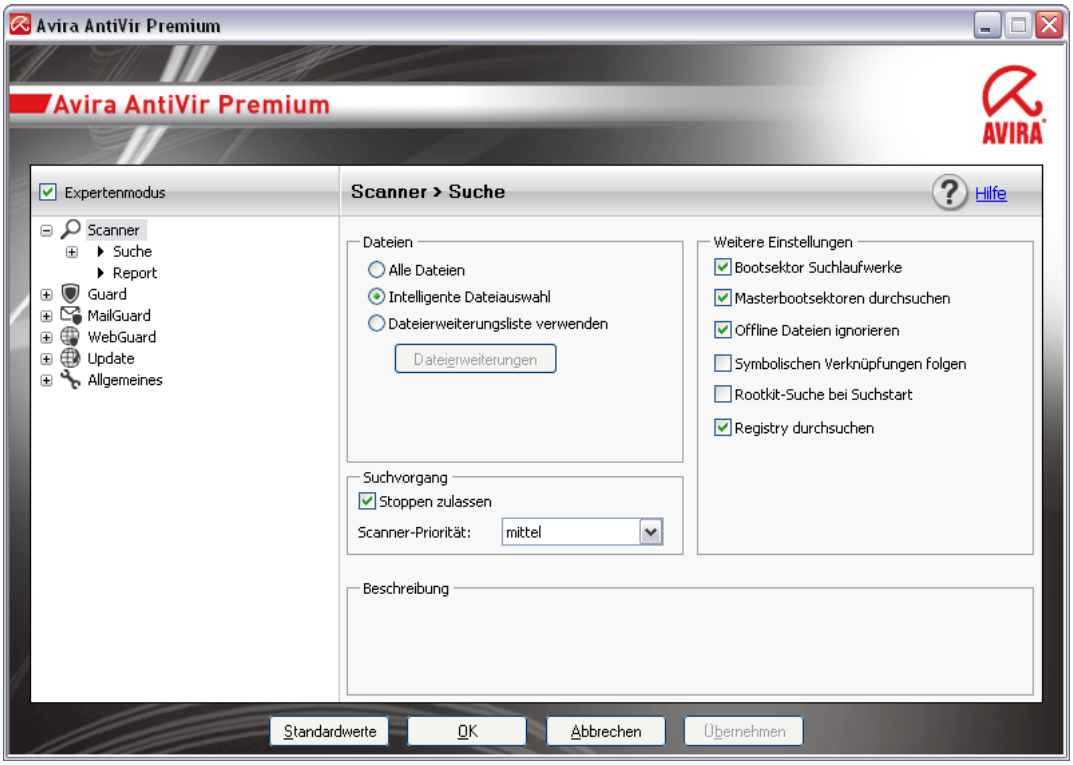
- Die Rubrik MailGuard zeigt Ihnen die vom MailGuard überprüften Emails, deren Eigenschaften sowie weitere statistische Daten.
- Die Rubrik WebGuard zeigt Ihnen Informationen zu überprüften URLs und gefundenen Viren, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".

– **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 Quarantänemanager. 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.

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

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

– **Allgemeines**:

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, Einstellung der Produktupdates

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
	AntiVir Guard ist deaktiviert

Das Tray Icon zeigt den Status des Guard 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.
- **AntiVir starten**: Öffnet das Control Center.
- **AntiVir konfigurieren**: Öffnet die Konfiguration.
- **Update starten**: Startet ein Update.
- **Hilfe**: Öffnet die Online-Hilfe.
- **Über AntiVir Premium:** 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 Produkt aktivieren

Um Ihr AntiVir Produkt zu aktivieren, haben Sie die folgenden Optionen:

- Aktivierung mit einer gültigen Volllizenz

  Zur Aktivierung des Programms mit einer Volllizenz benötigen Sie einen gültigen Aktivierungsschlüssel, über den die Daten Ihrer erworbenen Lizenz erfasst sind. Den Aktivierungsschlüssel haben Sie entweder per Email von uns erhalten oder er ist auf der Produktverpackung vermerkt.

- Aktivierung mit einer Evaluationslizenz

  Ihr AntiVir Programm wird mit einer automatisch generierten Evaluationslizenz aktiviert, mit der Sie das AntiVir Programm in einem begrenzten Zeitraum im vollen Funktionsumfang testen können.

Hinweis
Zur Produktaktivierung oder zur Beantragung einer Testlizenz benötigen Sie eine aktive Internetverbindung.
Falls keine Verbindung zu den Servern der Avira GmbH erstellt werden kann, prüfen Sie ggf. die Einstellungen in der genutzten Firewall: Bei der Produktaktivierung werden Verbindungen über das HTTP-Protokoll und Port 80 (Webkommunikation) und über das Verschlüsselungsprotokoll SSL und Port 443 genutzt. Stellen Sie sicher, dass Ihre Firewall, eingehende und ausgehende Daten nicht blockiert. Prüfen Sie zunächst, ob Sie über Ihren Webbrowser, Webseiten aufrufen können.

So aktivieren Sie Ihr AntiVir Programm:

Wenn Sie Ihr AntiVir Programm noch nicht installiert haben:

- Installieren Sie Ihr AntiVir Programm.

  Während der Installation werden Sie aufgefordert, eine Aktivierungsoption zu wählen

  - *Produkt aktivieren*

    = Aktivierung mit einer gültigen Volllizenz

  - *Produkt testen*

    = Aktivierung mit einer Evaluationslizenz

- Geben Sie für eine Aktivierung mit Volllizenz den Aktivierungsschlüssel an.
- Bestätigen Sie die Auswahl des Aktivierungsverfahrens mit **Weiter**.
- Geben Sie ggf. Ihre persönlichen Daten für eine Registrierung an und bestätigen Sie mit **Weiter**.

  Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt. Ihr AntiVir Programm wurde aktiviert.

- Fahren Sie mit der Installation fort.

Wenn Sie Ihr AntiVir Programm bereits installiert haben:

- Wählen Sie im Control Center den Menüpunkt **Hilfe :: Lizenzmanagement**.

  Es öffnet sich der Lizenz-Assistent, in dem Sie eine Aktivierungsoption wählen können. Die weiteren Schritte der Produktaktivierung sind identisch mit dem oben dargestellten Ablauf.

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: 2 Stunden.

- Geben Sie je nach Auswahl ggf. den Termin an.
- Wählen Sie ggf. Zusatzoptionen (nur je nach Auftragsart verfügbar):
  - **Auftrag zusätzlich bei Internet-Verbindung starten**

    Zusätzlich zur festgelegten Häufigkeit wird der Auftrag bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.
  - **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**

    Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- Klicken Sie auf **Weiter**.

Das Dialogfenster *Auswahl des Darstellungsmodus* erscheint.

- Wählen Sie den Darstellungsmodus des Auftragsfensters:
  - **Minimiert**: nur Fortschrittsbalken
  - **Maximiert**: gesamtes Auftragsfenster
  - **Unsichtbar**: kein Auftragsfenster
- Klicken Sie auf **Fertig stellen**.

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

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

Über folgende Symbole können Sie Aufträge weiter bearbeiten:

 Eigenschaften eines Auftrags ansehen

 Auftrag ändern

 Auftrag löschen

 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: 2 Stunden.

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 Betriebsystem 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.

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.

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.

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):

– **Vertrauenswürdiges 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 Quarantänemanager 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 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.

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 jeweils nur eine einzelne Datei hochladen.

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 Betriebsystem 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 enstprechende 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
- 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.

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 eines 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, Bootsektorviren 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 Bootsektorviren über den Menübefehl **Bootsektorviren 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: 2 Stunden. 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. Standardmäßig wird die existierende Netzwerkverbindung als Verbindung zu den Downloadservern der Avira GmbH genutzt. Sie können diese Standardeinstellung in der Konfiguration unter Allgemeines :: Update anpassen.

8 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

8.1 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.
- 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.

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.

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).

8.2 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.

8.2.1 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-Listenfeld 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-Listenfeld öffnen.
Esc	Ausgewähltes Drop-Down-Listenfeld schließen. Befehl abbrechen und Dialogfeld schließen.
Eingabetaste	Befehl für die aktive Option oder Schaltfläche ausführen.

8.2.2 In der Hilfe

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

8.2.3 Im Control Center

Allgemein

Tastaturbefehl	**Beschreibung**
F1	Hilfe anzeigen
Alt + F4	Control Center schließen

F5	Ansicht aktualisieren
F8	Konfiguration öffnen
F9	Update starten

Rubrik Prüfen

Tastaturbefehl	Beschreibung
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 Quarantäne

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

Rubrik Planer

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

Rubrik Berichte

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

Rubrik Ereignisse

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

8.3 Windows Sicherheitscenter

- ab Windows XP Service Pack 2 -

8.3.1 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.

8.3.2 Das Windows Sicherheitscenter und Ihr AntiVir Programm

Virenschutzsoftware / Schutz vor schädlicher Software

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

Virenschutz NICHT GEFUNDEN

Virenschutz NICHT AKTUELL

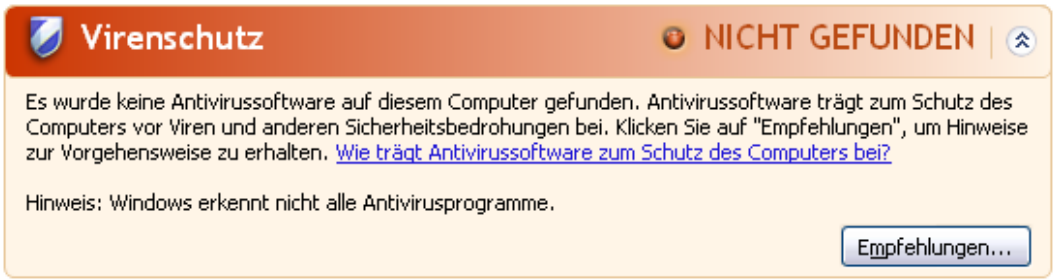
Virenschutz AKTIV

Virenschutz INAKTIV

Virenschutz NICHT ÜBERWACHT

Virenschutz NICHT GEFUNDEN

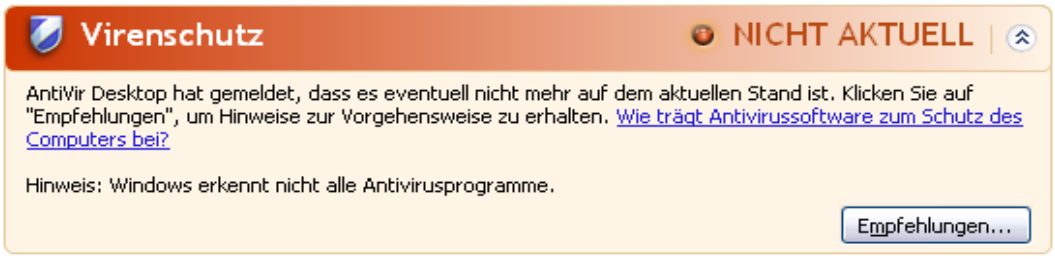
Dieser Hinweis des Windows Sicherheitscenters erscheint, wenn das Windows Sicherheitscenter keine Antivirussoftware auf Ihrem Computer gefunden hat.



Hinweis
Installieren Sie Ihr AntiVir Programm auf Ihrem Computer, um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Virenschutz NICHT AKTUELL

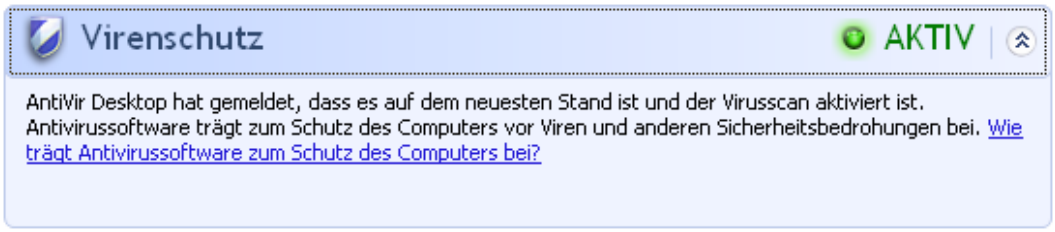
Haben Sie den Windows XP Service Pack 2 bzw. Windows Vista bereits installiert und installieren danach Ihr AntiVir Programm oder aber installieren Sie den Windows XP Service Pack 2 bzw. Windows Vista auf ein System, auf dem Ihr AntiVir Programm bereits installiert war erhalten sie folgende Meldung:



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

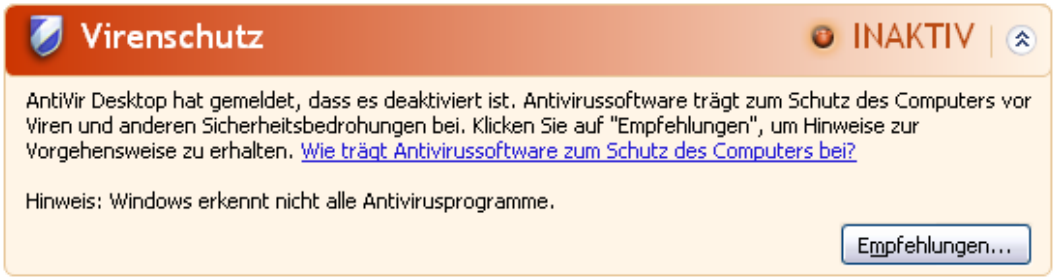
Nach der Installation Ihres AntiVir Programms und einem im Anschluss daran durchgeführten Update erhalten Sie folgenden Hinweis:



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.

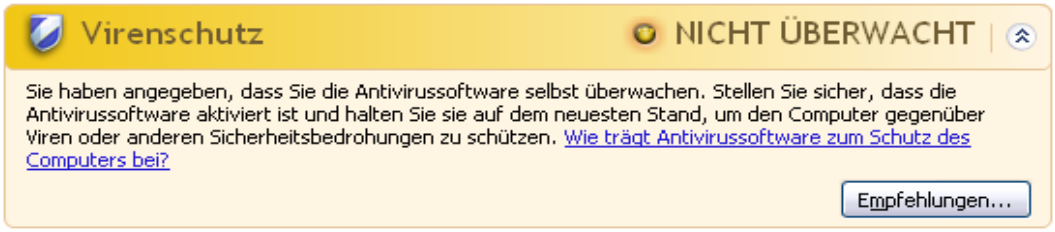


Hinweise
Den AntiVir Guard können Sie unter der Rubrik Übersicht :: Status des Control Center aktivieren bzw. deaktivieren. Sie erkennen zudem, dass der AntiVir Guard aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist.

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.



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!

9 Viren und mehr

9.1 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 überteuerte 0190/0900-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190/0900-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

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

Standardmäßig erkennt 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 verschleierten Dateiendungen (HEUR-DBLEXT)

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

Ihr AntiVir Programm erkennt "Dateien mit verschleierten Dateiendungen". Ist in der Konfiguration unter Gefahrenkategorien die Option **Dateien mit verschleierten Dateiendungen (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. potienzielle 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.

9.2 Viren sowie sonstige Malware

Adware

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

Backdoors

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

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

Bootviren

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

Bot-Net

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

Exploit

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

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

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

Honeypot

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

Makroviren

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

Pharming

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

Phishing

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

Polymorphe Viren

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

Programmviren

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

Rootkit

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

Skriptviren und Würmer

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

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

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

Spyware

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

Trojanische Pferde (kurz Trojaner)

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

Zombie

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

10 Info und Service

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

siehe Kapitel Kontaktadresse

siehe Kapitel Technischer Support

siehe Kapitel Verdächtige Datei

siehe Kapitel Fehlalarm melden

siehe Kapitel Ihr Feedback für mehr Sicherheit

10.1 Kontaktadresse

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

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

10.3 Verdächtige Datei

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

- Wählen Sie die Datei im Quarantänemanager des Control Center aus und wählen Sie über das Kontextmenü oder die entsprechende Schaltfläche den Punkt Datei senden.
- Senden Sie die gewünschte Datei gepackt (WinZIP, PKZip, Arj etc.) im Anhang einer Email an folgende Adresse:
  virus-premium@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

10.4 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-premium@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).

10.5 Ihr Feedback für mehr Sicherheit

Bei Avira steht die Sicherheit unserer Kunden an erster Stelle. Aus diesem Grund beschäftigen wir nicht nur ein eigenes Expertenteam, welches jede einzelne 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-premium@avira.de

11 Referenz: Konfigurationsoptionen

Die Referenz der Konfiguration dokumentiert alle verfügbaren Konfigurationsoptionen.

11.1 Scanner

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

11.1.1 Suche

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

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

Dateien

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

Alle Dateien

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

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

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch 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 Dateiendungen gelöscht, wird dies durch den Text "Keine Dateierweiterungen" unterhalb der Schaltfläche Dateierweiterungen angezeigt.

Dateierweiterungen

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

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

Weitere Einstellungen

Bootsektor Suchlaufwerke

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

Masterbootsektoren durchsuchen

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

Offline Dateien ignorieren

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

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.

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.

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.

Suchvorgang

Stoppen zulassen

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

Scanner-Priorität

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

Niedrig

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

Mittel

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

Hoch

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

11.1.1.1. Aktion bei Fund

Aktion bei Fund

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

Interaktiv

Bei aktivierter Option 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
Standardmäßig ist im Dialogfenster zur Virenbehandlung die Aktion 'In Quarantäne verschieben' vorausgewählt. Über ein Kontextmenü können Sie weitere Aktionen auswählen.

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.

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.

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

Archive durchsuchen

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

Alle Archiv-Typen

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

Smart Extensions

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

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

Rekursionstiefe einschränken

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

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

Maximale Rekursionstiefe

Um die maximale Rekursionstiefe eingeben zu können, muss die Option Rekursionstiefe einschränken aktiviert sein.
Sie können die gewünschte Rekursionstiefe entweder direkt eingeben oder aber mittels der Pfeiltasten rechts vom Eingabefeld ändern. Erlaubte Werte sind 1 bis 99. Der Standardwert ist 20 und wird empfohlen.

Standardwerte

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

Archiv-Liste

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

11.1.1.2. Ausnahmen

Vom Scanner auszulassende Dateiobjekte

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

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

Hinweis
Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

Warnung
Diese Dateien werden bei einem Suchlauf nicht berücksichtigt!

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

Eingabefeld

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

Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei bzw. den gewünschten Pfad auszuwählen.
Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht auf Befall überprüft. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht durchsucht.

Hinzufügen

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

Löschen

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

Hinweis
Wenn Sie eine gesamte Partition zur Liste der auszunehmenden Dateiobjekte hinzufügen, werden nur die Dateien, die direkt unter der Partition gespeichert sind, von der Suche ausgenommen, jedoch nicht Dateien in Verzeichnissen auf der entsprechenden Partition:
Beispiel: Auszulassendes Dateiobjekt: `D:\` = `D:\file.txt` wird von der Suche des Scanner ausgenommen, `D:\folder\file.txt` wird nicht von der Suche ausgenommen.

11.1.1.3. 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.

11.1.2 Report

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

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

Protokollierung

Aus

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

Standard

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

Erweitert

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

Vollständig

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

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

11.2 Guard

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

11.2.1 Suche

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

Suchmodus

Hier wird der Zeitpunkt für das Prüfen einer Datei festgelegt.

Beim Lesen durchsuchen

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

Beim Schreiben durchsuchen

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

Bei Lesen und Schreiben suchen

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

Dateien

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

Alle Dateien

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

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

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch 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 Dateiendungen gelöscht, wird dies durch den Text "Keine Dateierweiterungen" unterhalb der Schaltfläche Dateierweiterungen angezeigt.

Dateierweiterungen

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

Hinweis
Beachten Sie bitte, dass sich die 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.

11.2.1.1. Aktion bei Fund

Aktion bei Fund

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

Interaktiv

Bei aktivierter Option erscheint 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.

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 Quarantänemanager 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 Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung.

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.

11.2.1.2. 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.

11.2.1.3. Ausnahmen

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

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
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 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.

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.

11.2.1.4. 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.

11.2.2 ProActiv

Mit dem Einsatz von Avira AntiVir ProActiv schützen Sie sich vor neuen und unbekannten 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 Anwendungsfilter der erlaubten Anwendungen enthalten sind, alle Programme, die Sie zum Anwendungsfilter 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.

11.2.2.1. Anwendungsfilter: Zu blockierende Anwendungen

Unter *Anwendungsfilter: 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 Anwendungsfilter 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 AntVir 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 Dateiendung angegebenen 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.

11.2.2.2. Anwendungsfilter: Erlaubte Anwendungen

Unter *Anwendungsfilter: 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 Anwendungsfilter 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.

11.2.3 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.

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.

11.3 MailGuard

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

11.3.1 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 Posteingangs-Konto, 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.

11.3.1.1. 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.

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 beim 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!

11.3.1.2. 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.

11.3.1.3. 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 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.

11.3.2 Allgemeines

11.3.2.1. 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

Symbol	Beschreibung
	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.

11.3.2.2. 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.

11.3.3 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.

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.

11.4 WebGuard

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

11.4.1 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.

11.4.1.1. 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.

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 Marlware 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.

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!

11.4.1.2. 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-Emails verbreitet werden. Die Kategorie Betrug und Täuschung umfasst Webseiten mit 'Abonnement-Fallen' und anderen Angeboten von Dienstleistungen, deren Kosten vom Anbieter verschleiert werden.

11.4.1.3. 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

11.4.1.4. 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.

11.4.2 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.

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.

11.5 Update

Unter der Rubrik *Update* konfigurieren Sie die automatische Ausführung von Updates. Sie haben die Möglichkeit, verschiedene Update-Intervalle einzustellen sowie das automatische Update zu aktivieren und zu deaktivieren.

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.

11.5.1 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.

11.5.2 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 Neustartroutinen 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 Neustartroutinen.

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.

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

Verbindung zum Webserver

Vorhandene Verbindung (Netzwerk) verwenden

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

Die folgende Verbindung verwenden:

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

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

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

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

Hinweis
Die automatische Einwahl des Updaters über sogenannte Dial-Up Tools (z.B. SmartSurfer, Oleco, ...) steht momentan 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.

11.6 Allgemeines

11.6.1 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 verschleierten Dateiendungen (HEUR-DBLEXT)
- Phishing
- Anwendung (APPL)

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

Alle aktivieren

Bei aktivierter Option werden sämtliche Typen aktiviert.

Standardwerte

Diese Schaltfläche stellt die vordefinierten Standardwerte wieder her.

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

11.6.2 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.

Kennwortgeschützter Bereich	Funktion
Control Center	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.
WebGuard aktivieren/ deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des WebGuard das gesetzte Kennwort benötigt.
Quarantäne	Bei aktivierter Option werden alle Bereiche des Quarantänemanagers, 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.

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.
Konfiguration	Bei aktivierter Option ist die Konfiguration des Programms nur nach Eingabe des gesetzten Kennworts möglich.
Expertenmodus aktivieren	Bei aktivierter Option wird zur Aktivierung des Expertenmodus das gesetzte Kennwort benötigt.
Installation / Deinstallation	Bei aktivierter Option wird zur Installation bzw. Deinstallation des Programms das gesetzte Kennwort benötigt.

11.6.3 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!

11.6.4 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 an einer Schnittstelle zur Verfügung. Sie haben über WMI die Möglichkeit, Betriebsdaten des Programms abzurufen.

WMI-Unterstützung aktivieren

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Betriebsdaten des Programms abzurufen.

11.6.5 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.

11.6.6 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:	proyx.domain.de	Port:	8080
Adresse:	192.168.1.100	Port:	3128

11.6.7 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.

11.6.8 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.

11.6.9 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.

11.6.10 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 unbekannten 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.

Ausgabe Q2-2011

AVIRA

live free.™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de