Avira AntiVir Server – Windows

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 Server 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 Server 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.

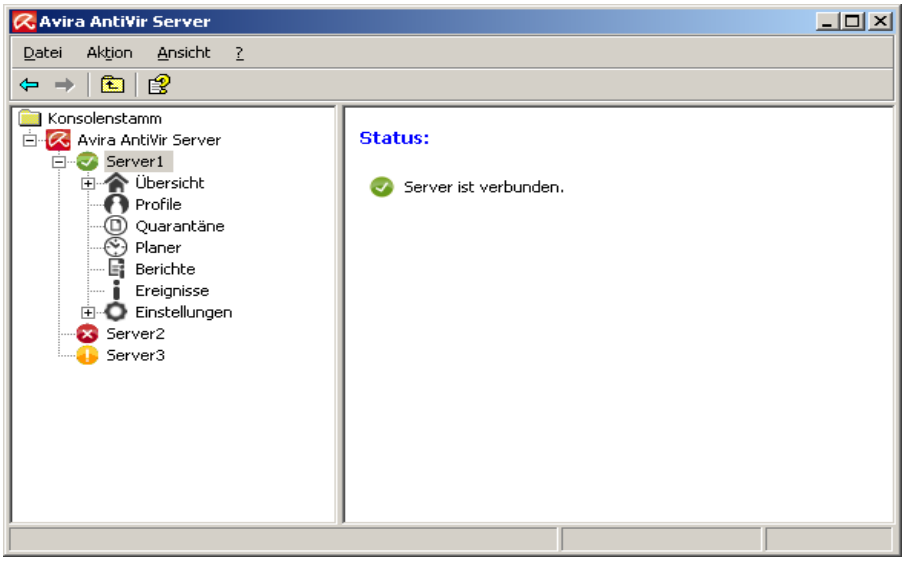
Folgende Hervorhebungen werden verwendet:

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 Produktinformation

3.1 Funktionsweise

Das Schutzpaket Avira AntiVir Server umfasst den Dienst Avira AntiVir Server und die AntiVir Server Konsole. Der Dienst Avira AntiVir Server schützt Ihre Windows Server vor Viren und Malware. AntiVir Server Konsole dient zur Administration, Steuerung und Überwachung der zu schützenden Server bzw. der AntiVir Dienste auf den zu schützenden Servern. Über AntiVir Server Konsole können Sie auf beliebig viele zu schützende Server zugreifen.



Der Dienst Avira AntiVir Server

... schützt Ihre Server vor Viren und Malware. Sie installieren den Dienst auf allen zu schützenden Windows Servern im Netzwerk.

Der AntiVir Server Dienst stellt in einem Paket mit mehreren Programmkomponenten und weiteren Hilfsprogrammen umfangreiche Funktionen zum Schutz Ihres Systems zur Verfügung. Die wichtigsten Komponenten im Überblick:

- Der **Scanner** durchsucht Ihr Computersystem nach Viren und unerwünschten Programmen (Direktsuche). Betroffene Dateien werden je nach Konfiguration gelöscht, repariert oder in die Quarantäne verschoben . Suchläufe des Scanner werden automatisch ausgeführt. Ausführungsintervall und Suchumfang von Suchläufen können konfiguriert werden.
- Der **Guard** läuft im Hintergrund. Er überwacht und repariert, falls nötig, Dateien bei Operationen wie Öffnen, Schreiben und Kopieren in Echtzeit.
- Der **Planer** unterstützt Sie beim Planen von regelmäßigen Aufgaben wie Suchläufen und Updates über Internet bzw. Intranet.
- Der **Updater** hält über eine Internet- bzw. Intranet-Verbindung Ihr Programm immer auf dem aktuellsten Stand.

– Der **Quarantänemanager** verwaltet und überwacht komfortabel die in Quarantäne gestellten Dateien.

AntiVir Server Konsole

... stellt eine Benutzeroberfläche für AntiVir Server Dienste zur Verfügung, mit der Sie AntiVir Server Dienste steuern, konfigurieren und überwachen können. Sie installieren AntiVir Server Konsole auf mindestens einem Rechner mit Netzwerkverbindung zu den zu schützenden Servern. AntiVir Server Konsole kann auch auf den zu schützenden Servern installiert werden.

AntiVir Server Konsole kann sich mit beliebig vielen zu schützenden Server verbinden und bietet Zugriff auf Komponenten, Reports, Ereignisse sowie auf die Konfiguration des verbunden AntiVir Server Dienstes.

3.2 Leistungsumfang

Wesentliche Leistungsmerkmale:

- Konsole zur Überwachung, Administration und Steuerung des gesamten Programms
- Einfache, kennwortgestützte Konfiguration: Unterstützung der Konfiguration durch integrierten Assistenten und kontextsensitive Hilfe
- Konfiguration und Bedienung von getrenntem Rechner aus möglich: Benutzeroberfläche (AntiVir Server Konsole) kann separat vom AntiVir Server Dienst installiert werden
- Netzwerkweite Administration durch das Avira Security Management Center (SMC)
- Scanner (Direktsuche bzw. on-demand scan) mit profilgesteuerter und konfigurierbarer Suche nach allen bekannten Typen von Viren und Malware
- Residenter Virenwächter (Echtzeitsuche bzw. on-access scan) zur ständigen Überwachung sämtlicher Dateizugriffe
- Extrem hohe Viren- und Malware-Erkennung durch innovative Suchtechnologien (Suchengine) inklusive heuristischer Suchverfahren
- Innovative AHeAD (Advanced Heuristic Analysis and Detection) Technologie zur Erkennung unbekannter oder sich schnell verändernder Angreifer für proaktive Sicherheit
- Erkennung aller gebräuchlichen Archivtypen inklusive Erkennung verschachtelter Archive und Smart-Extension-Erkennung
- Umfangreiche Filtermöglichkeiten und File Caching zur Erhöhung der Scan-Geschwindigkeit
- "Multi-Threading-Fähigkeit": Gleichzeitiger Scan vieler Dateien mit hoher Geschwindigkeit
- Konfigurierbare Reaktionen auf einen Fund: Reparieren, Löschen, Verschieben in ein Quarantäneverzeichnis, Sperren, Umbenennen und Isolieren von Programmen oder Dateien; Automatisches Entfernen von Viren und Malware
- Quarantänemanager: Betroffene Dateien können im Quarantäneverzeichnis gelöscht oder an ihrem Ursprungsort wiederhergestellt werden

- Integrierter Planer zur Planung von einmaligen oder wiederkehrenden Aufträgen wie Updates oder Prüfläufen
- Automatisierbare Aktualisierung über Internet oder netzwerkweite Verteilung (ohne Systemunterbrechung)
- Umfassende Protokoll-, Warn- und Benachrichtigungsfunktionen für den Administrator; Versenden von Warnungen in Windows-Netzwerken und per Email (SMTP),SMTP-Authentifizierung möglich
- Schutz vor Änderungen der Programmdateien durch intensiven Selbsttest
- Erweiterter Terminal Server Support
- Rootkit-Schutz (nicht unter Windows XP 64 Bit, Windows 2003 64 Bit, Windows Server 2003 64 Bit)
- Unterstützung für Windows Management Instrumentation

3.3 Systemvoraussetzungen

Avira AntiVir Server stellt für einen erfolgreichen Einsatz folgende Anforderungen an den Dienst Avira AntiVir Server und an AntiVir Server Konsole:

- Computer ab Pentium, mindestens 266 MHz
- Betriebssystem
- Windows XP, SP2 (32 oder 64 Bit) oder
- Windows Vista (32 oder 64 Bit, SP 1 empfohlen) oder
- Windows 7 (32 oder 64 Bit) oder
- Windows Server 2003, SP1 (32 oder 64 Bit) oder
- Windows Server 2008 (32 oder 64 Bit) oder
- Windows Server 2008 R2 (nur 64 Bit)
- Mindestens 150 MB freier Speicherplatz auf der Festplatte (bei Verwendung der Quarantäne und für temporären Speicher mehr)
- Mindestens 512 MB Arbeitsspeicher unter Windows Server 2003
- Mindestens 1024 MB Arbeitsspeicher unter Windows Vista, Windows 7, Windows Server 2008 und Windows Server 2008 R2
- Für die Installation von Avira AntiVir Server: Administrator-Rechte

Internet-Zugang

Für regelmäßige Updates ist es nötig, dass ein Server Ihres Netzwerks einen Internet-Zugang besitzt. Alternativ können die Updates auch von einem File- oder HTTP-Server im Intranet geladen werden. Nähere Informationen finden Sie unter Update.

3.4 Lizenzierung

Um Avira AntiVir Server zu nutzen, benötigen Sie eine Lizenz. Mit der Lizenzdatei *hbedv.key* aktivieren Sie Ihre Lizenz für Avira AntiVir Server. Die Lizenzdatei erhalten Sie von der Avira GmbH per Email. Die Lizenzdatei enthält die Lizenz für alle Produkte, die Sie bei einem Bestellvorgang bestellt haben. Sie erkennen damit die Lizenzbedingungen an.

3.4.1 Lizenzmodelle

Sie können die vielfältigen Funktionen von Avira AntiVir Server mit folgenden Lizenzmodellen nutzen:

- Evaluationsversion: Voller Funktionsumfang, 30 Tage Lizenz
- Vollversion

Die Lizenzierung umfasst eine Lizenz für alle Plattformen und ist abhängig von der Anzahl der Benutzer im Netzwerk, die durch Avira AntiVir Server geschützt werden sollen. Weitere Informationen zu den Lizenzmodellen und zu optionalen Support-Angeboten finden Sie auf unserer Webseite:

http://www.avira.de

Zum Leistungsumfang einer Vollversion gehören:

- Bereitstellung der AntiVir-Version zum Download aus dem Internet
- Vierwöchiger Installationssupport ab Kaufdatum
- Newsletter-Service (per Email)
- Update-Service per Internet

4 Installation und Deinstallation

4.1 Installation

Vor der Installation von Avira AntiVir Server müssen bestimmte Voraussetzungen erfüllt sein:

- Stellen Sie sicher, dass die Systemvoraussetzungen erfüllt sind (siehe Systemvoraussetzungen) und der verwendete Windows Server gestartet ist.
- Stellen Sie sicher, dass Sie am Server als Administrator oder als Benutzer mit Administrator-Rechten angemeldet sind.
- Stellen Sie sicher, dass zur Aktualisierung von Avira AntiVir Server eine Internetverbindung oder eine Netzwerkverbindung zu einem Downloadserver vorhanden ist. Wenn Sie einen Dateiserver nutzen, benötigen Sie ggf. einen Benutzernamen und ein Kennwort für das Server-Login.
- Bei Installation der Vollversion: Stellen Sie sicher, dass eine gültige Lizenzdatei *hbedv.key* vorhanden und in einem lokalen Verzeichnis auf dem Server gespeichert ist.
- Bei Installation vom Dienst Avira AntiVir: Wenn Sie auf den zu schützenden Server remote mit AntiVir Server Konsole zugreifen möchten, stellen Sie sicher, dass folgende Ports geöffnet sind:
  139 (NetBIOS SSN)
  137 (NetBIOS NS)
  138 (NetBIOS DGM)

Installationsarten

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

Express

- Avira AntiVir Server wird mit dem Dienst Avira AntiVir Server, der Konsole AntiVir Server Konsole und allen empfohlenen Programmkomponenten installiert.
- Es kann kein Zielordner für die zu installierenden Programmdateien gewählt werden.

Benutzerdefiniert

- Sie können wählen, ob Sie den Dienst Avira AntiVir Server und/oder die Konsole AntiVir Server Konsole installieren möchten.
- Sie haben die Möglichkeit, Zusatzfunktionalitäten des Dienstes Avira AntiVir Server zur Installation auszuwählen:

AntiVir Rootkit-Schutz: Die Funktionalität beinhaltet das Suchprofil Rookit-Suche, mit dem Sie nach versteckter Malware suchen können.

VMware Offline Scanner: Die Funktionalität beinhaltet das Suchprofil VMware-Image, mit dem Sie offline VMware-Images nach Viren und unerwünschten Programmen durchsuchen können.

Shell Extension: Die Funktionalität erzeugt einen Eintrag im Kontextmenü des Windows Explorer, mit dem Sie Verzeichnisse nach Viren und unerwünschten Programmen durchsuchen können.

AntiVir Systray-Tool: Die Funktionalität erzeugt auf dem zu schützenden Server ein Tray Icon von Avira AntiVir Server in der Notification Area, mit dem Sie den Status von Avira AntiVir Server überwachen und auf weitere Funktionen von Avira AntiVir Server zugreifen können. Die Funktionalität ist in der Expressinstallation enthalten und kann in der benutzerdefinierten Installation abgewählt werden.

– Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden.

Installation ausführen

So installieren Sie Avira AntiVir Server:

– Starten Sie das Setup mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.
Es öffnet sich der Installationsassistent.

– Folgen Sie den Anweisungen des Installationsassistenten. Folgende Installationsschritte werden ausgeführt:

– Ggf. Installation des Microsoft Visual C++ 2008 - Redistributable Kit, wenn das Kit nicht bereits installiert wurde.

Hinweis
Avira AntiVir Server verwendet Runtime Libraries des Microsoft Visual C++ 2008 - Redistributable Kit. Zur Nutzung von Avira AntiVir Server ist daher eine Installation von Microsoft Visual C++ 2008 - Redistributable Kit zwingend erforderlich.

– Bestätigung der Lizenzvereinbarungen

– Auswahl des Setup-Typs (Expressinstallation oder benutzerdefinierte Installation)

– Lizenzierung von Avira AntiVir Server: Laden der Lizenzdatei oder Auswahl einer 30-Tage-Testlizenzierung

– Installation vom Dienst Avira AntiVir Server und/oder AntiVir Server Konsole

Wenn Sie den Dienst Avira AntiVir Server installiert haben, öffnet sich nach der Ausführung der Installation ein Konfigurationsassistent. Sie haben die Möglichkeit, die wichtigsten Einstellungen des installierten Dienstes Avira AntiVir Server zu konfigurieren:

– **Einstellung der AHeAd-Technologie (Advanced Heuristic Analysis and Detection):** Die Einstellung wird für den Scanner und den Guard übernommen.

– **Auswahl erweiterter Gefahrenkategorien:** Durch die Auswahl weiterer Gefahrenkategorien, die von Avira AntiVir Server erkannt und gemeldet werden sollen, können Sie die Schutzfunktion von Avira AntiVir Server anpassen.

– **Auswahl von Produktausnahmen (Guard):** Sie können Softwareprodukte auswählen, die von der Überwachung des Guard (On Access Scanner) ausgenommen sind. Dadurch vermeiden Sie Performanceeinbußen, die durch den Guard entstehen können.

– **Email-Einstellungen wählen:** Sie können die Servereinstellungen für den Email-Versand vornehmen. Avira AntiVir Server nutzt Email-Versand per SMTP beim Versenden von Email-Warnungen an den Administrator von Avira AntiVir Server.

Hinweis
Nach der Installation wird das eigene System von AntiVir Server Konsole (Local Host/ 127.0.0.1) als zu schützender Server automatisch hinzugefügt, selbst wenn kein AntiVir Server Dienst installiert ist.

Hinweis
Wenn Sie Programmkomponenten der aktuellen Avira AntiVir Server Installation hinzufügen oder entfernen möchten, nutzen Sie das Setup von Avira AntiVir Server.

4.2 Deinstallation

Die Deinstallation führen Sie über die Systemsteuerung des Betriebssystems oder über das Setup Ihres AntiVir Programms durch.

Bei der Deinstallation werden die AntiVir-Dienste gestoppt, alle Reportdateien und infizierten Dateien (in der Quarantäne) gelöscht.

Sie können während der Deinstallation angeben, dass die Verzeichnisse mit den Reportdateien und die Quarantäne nicht gelöscht werden.

4.3 Installation und Deinstallation im Netzwerk

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

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

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

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

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

Hier finden Sie Informationen zur Installation und Deinstallation im Netzwerk:

– siehe Kapitel: Kommandozeilenparameter für das Setup-Programm
– siehe Kapitel: Parameter der Datei setup.inf

- siehe Kapitel: Installation im Netzwerk
- siehe Kapitel: Deinstallation im Netzwerk

4.3.1 Installation im Netzwerk

Die Installation kann skriptgesteuert im Batch-Modus ausgeführt werden.

Das Setup ist für folgende Installationen geeignet:

- Erstinstallation über das Netzwerk (unattended setup)

▶ Änderungsinstallation bzw. Update

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

So installieren Sie AntiVir Programme automatisch im Netzwerk:

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

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

▶ Starten Sie die Installation mit dem Parameter /inf oder binden Sie den Parameter in das Login-Skript des Servers ein.

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

4.3.2 Deinstallation im Netzwerk

So deinstallieren Sie AntiVir Programme automatisch im Netzwerk:

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

▶ Starten Sie die Deinstallation mit den Parametern `/inf` und `/AVUNINSTALL` oder binden Sie die Parameter in das Login-Skript des Servers ein.

4.3.3 Kommandozeilenparameter für das Setup-Programm

Für die Installation und Deinstallation verwenden Sie folgende Parameter:

- `/INF=<Skriptname mit Pfad>`

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

Installation: `PRESETUP.EXE /INF=e:\disks\setup.inf`

Deinstallation: `PRESETUP.EXE /INF=e:\disks\setup.inf /AVUNINSTALL`

– /SILENT

Das Setup-Skript läuft komplett ohne Benutzer-Interaktion.

4.3.4 Parameter der Datei setup.inf

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

– `InstallPath`

Zielpfad, in dem Avira AntiVir Server installiert wird. Er muss im Script angegeben werden. Es ist möglich Umgebungsvariablen zu verwenden

Beispiel: InstallPath="%PROGRAMFILES%\Avira\AntiVir Server\"

– `LicenseFile=<Pfad und Dateiname der Lizenzdatei>`

Avira AntiVir Server wird mit der Lizenz installiert. Wenn Sie nur den Dateinamen angeben, wird die Lizenzdatei im Quellverzeichnis des Setups gesucht.

Beispiel: `LicenseFile="A:\hbedv.key"`

– `RestartWindows= 0 | 1`

Falls nach der Installation ein Neustart des Systems erforderlich ist, kann dieser automatisch durchgeführt werden (Standard) oder eine MessageBox angezeigt werden.

`0`: Disabled (Neustart mit Message Box)

`1`: Enabled (Automatischer Neustart)

– `DeleteFolderOnUninstall=1`

Löscht die Konfiguration bei der Deinstallation

– `Guard= 0 | 1`

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

1: AntiVir Guard installieren (Standard)

0: AntiVir Guard nicht installieren

– `RootKit= 0 | 1`

Installiert das Modul AntiVir Rootkit-Schutz . Mit dem Modul wird Malware erkannt, die sich im System versteckt.

1: AntiVir Rootkit-Schutz installieren

0: AntiVir Rootkit-Schutz nicht installieren (Standard)

– `VMWare= 0 | 1`

Installiert den VMWare Offline Scanner. Mit dem Modul können VMWare Images offline nach Viren und Malware durchsucht werden.

1: VMWare Offline Scanner installieren

0: VMWare Offline Scanner nicht installieren (Standard)

– `ShellExtension= 0 | 1`

Installiert die Shell Extension. Über einen Eintrag im Kontextmenü des Windows Explorer können Sie Verzeichnisse direkt nach Viren und unerwünschten Programmen durchsuchen.

1: Shell Extension installieren (Standard)

0: Shell Extension nicht installieren

– `Systray= 0 | 1`

Installiert das Systray Tool. Auf dem zu schützenden Server ist ein Tray Icon von Avira AntiVir Server in der Notification Area sichtbar. Mit dem Tray Icon überwachen Sie den Status von Avira AntiVir Server. Sie können auf weitere Funktionalitäten von Avira AntiVir Server zugreifen.

1: Systray Tool installieren (Standard)

0: Systray Tool nicht installieren

– `GUI= 0 | 1`

Installiert die Benutzeroberfläche AntiVir Server Konsole, mit der Sie die AntiVir Server Dienste auf den zu schützenden Servern remote administrieren und konfigurieren können.

1: Installiert AntiVir Server Konsole (Standard)

0: Installiert nicht AntiVir Server Konsole

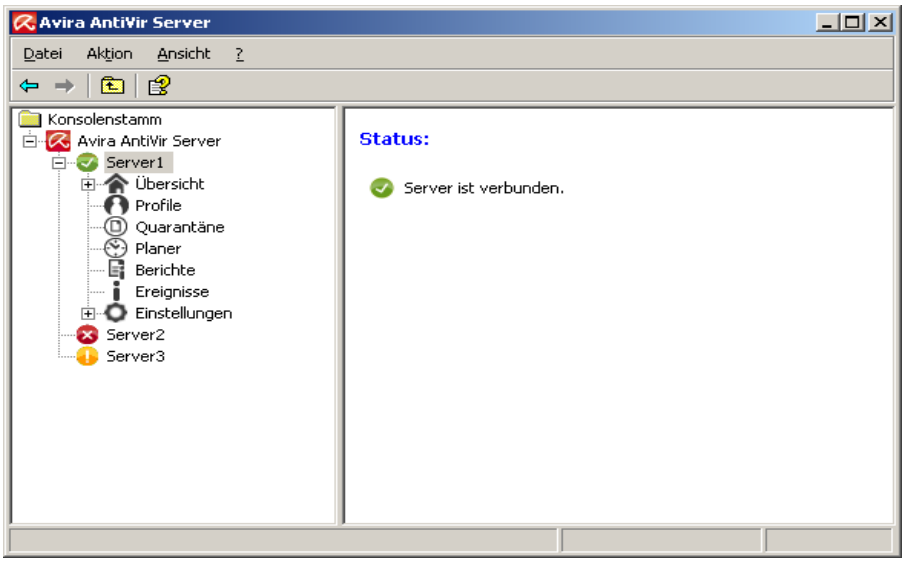
Im Bereich [FEEDBACK] trägt das Setup Fehlercode und Fehlertexte ein, die vom Setup zurückgegeben werden:

Beispiel: `ErrCode=0`
`ErrMsg=Produkt wurde erfolgreich installiert`

5 Benutzeroberfläche und Bedienung

5.1 Benutzeroberfläche: AntiVir Server Konsole

Der Avira AntiVir Server Dienst, der auf zu schützenden Servern installiert ist, wird über **AntiVir Server Konsole** administriert. AntiVir Server Konsole ist ein Snap-In der Microsoft Management Konsole (MMC). Auf AntiVir Server Konsole können Sie beliebig viele zu schützende Server anlegen, um diese auf AntiVir Server Konsole zu konfigurieren und zu überwachen.



Hinweis
Beachten Sie, dass in dieser Hilfe nur die proprietären Elemente von AntiVir Server Konsole dokumentiert sind. Informationen zur MMC und zur manuellen Einbindung eines Snap-In entnehmen Sie dem Benutzerhandbuch oder der Online-Hilfe des Betriebssystems.

Starten und Beenden von AntiVir Server Konsole

Sie starten AntiVir Server Konsole über die Verknüpfung **Avira AntiVir Server Benutzeroberfläche** im Windows Startmenü oder unter **Alle Programme**. Sie können auch AntiVir Server Konsole direkt in der MMC laden. Sie finden die vorkonfigurierte AntiVir Server Konsole im Installationsverzeichnis von AntiVir Server Konsole. Um AntiVir Server Konsole zu beenden, müssen Sie MMC schließen.

Bedienung

- Navigieren Sie über die Konsolenstruktur im linken Fenster der MMC. Navigationselemente werden auch als Objekte im rechten Detailfenster der MMC angezeigt. Sie öffnen diese Objekte im Detailfenster mit Doppelklick. Die Konfiguration befindet sich unter dem Knoten **Einstellungen**. Sie können im Detailfenster verschiedene Konfigurationsrubriken anwählen: Es öffnet sich das Fenster **Einstellungen**, in dem Sie die angewählte Rubrik konfigurieren können.
- Befehle und Aktionen sind über Symbole im Detailfenster sowie über Kontextmenüs zu den einzelnen Konsolenknoten oder zu Objekten im Detailfenster verfügbar.
- Bei der Konfiguration eines Servers müssen Sie Ihre Angaben im Fenster **Einstellungen** mit der Schaltfläche **OK** oder **Übernehmen** bestätigen, um die neuen Einstellungen zu übernehmen. Mit der Schaltfläche **Abbrechen** werden Ihre Angaben verworfen.

AntiVir Server Konsole im Überblick

Avira AntiVir Server

- Anzeige der angelegten Server mit Verbindungsstatus
- Aktionen: Server hinzufügen

Hinweis
Auf der AntiVir Server Konsole werden der lokale AntiVir Server sowie alle AntiVir Server angezeigt, die der angemeldete Benutzer hinzugefügt hat.

Server

- Anzeige des Serverstatus
- Aktionen: Produktupdate starten, Lizenzdatei aktualisieren, Konfiguration neu laden, Reportdatei anzeigen, Server umbenennen, Verbindung beenden, Server verbinden, Server löschen

Übersicht

Übersicht über..

- den Systemstatus (letzte Systemprüfung, letztes Update, Lizenz)
- die statistischen Daten der Echtzeitsuche des Guard und der Direktsuche des Scanner
- die Programmversion
- Kontakt- und Supportadressen

Profile

- Anzeige der Standardprofile und der angelegten Profile für die Direktsuche
- Aktionen: Neue Profile erstellen, Profile umbenennen, Profile löschen

Quarantäne

- Anzeige der Objekte in der Quarantäne
- Aktionen: Objekteigenschaften anzeigen, Objekt wiederherstellen, Datei zur Quarantäne hinzufügen, Objekt an Avira Malware Research Center senden, Objekt löschen

Planer

- Anzeige aller angelegten Prüf- und Update-Aufträge
- Aktionen: Anlegen neuer Aufträge, Auftragseigenschaften anzeigen, Auftrag ändern, Auftrag löschen

Berichte

- Anzeige der Berichte von Suchläufen der Direktsuche und Updates
- Bericht anzeigen, Reportdatei anzeigen, Bericht drucken, Bericht löschen

Ereignisse

- Anzeige aller Ereignisse vom Dienst Avira AntiVir Server auf dem zu schützenden Server
- Aktionen: Ereignisse anzeigen, Ereignisse exportieren, Ereignisse löschen

Einstellungen

- Konfiguration des Diensts Avira AntiVir Server auf dem zu schützenden Server Konfigurationsrubriken:
- **Scanner**: Konfiguration der Direktsuche
- **Guard**: Konfiguration der Echtzeitsuche
- **Allgemeines**: Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche, Kennwortschutz für den Server auf AntiVir Server Konsole, Sicherheitswarnungen bei veraltetem Avira AntiVir Server, verwendete Verzeichnisse, Begrenzung von Berichten und vom Ereignis-Log
- **Update**: Download über Webserver oder Dateiserver, Produktupdates, Konfiguration der Verbindung zum Downloadserver
- **Warnungen**: Konfiguration von Netzwerkwarnungen des Guard und des Scanner
- **Email**: Konfiguration von Email-Warnungen per SMTP von den Modulen Guard, Scanner, Updater

5.2 Benutzeroberfläche: Tray Icon

Nach der Installation des Dienstes Avira AntiVir Server wird auf dem zu schützenden Server in der Notification Area das Tray Icon von Avira AntiVir Server angezeigt. Das Tray Icon zeigt den Status des AntiVir Guard Dienstes an:

Symbol	Beschreibung
	AntiVir Guard ist aktiviert
	AntiVir Guard ist deaktiviert

Über das Kontextmenü des Tray Icons können Sie Funktionen aufrufen. Um das Kontextmenü aufzurufen, klicken Sie mit der rechten Maustaste auf das Tray Icon:

- *AntiVir starten*: Öffnet die AntiVir Server Konsole zur Administration der verbundenen AntiVir Server. Diese Option ist nur verfügbar, wenn eine AntiVir Server Konsole lokal am Rechner installiert wurde und wenn Sie mit Administrator-Rechten am Rechner angemeldet sind.
- *Prüfe 'Meine Dokumente':* Startet das Scanner-Suchprofil "Meine Dokumente": Der Standardspeicherort "Eigene Dateien" des eingeloggten Benutzers wird nach Viren bzw. unerwünschten Programmen durchsucht.
- *Hilfe*: Öffnet die Online-Hilfe.
- *Avira im Internet*: Öffnet das Avira Webportal.

Hinweis
Sie können die AntiVir Server Konsole auch mit Doppelklick auf das Tray Icon öffnen.

5.3 Quickstart

Diese Schritte führen Sie aus, wenn Sie Avira AntiVir Server zum ersten Mal einsetzen:

1. Installation

Installieren Sie den Dienst Avira AntiVir Server auf den Servern, die Sie vor Viren und unerwünschten Programmen schützen möchten. Installieren Sie AntiVir Server Konsole mindestens auf einem Rechner in Ihrem Netzwerk.
siehe Kap. Installation

2. Administration auf AntiVir Server Konsole

Server hinzufügen

Fügen Sie auf AntiVir Server Konsole alle Server hinzu, die Sie auf AntiVir Server Konsole administrieren möchten.
siehe Kap. AntiVir Server Konsole

Für jeden hinzugefügten Server führen Sie die folgenden Schritte aus:

Konfiguration

Konfigurieren Sie den Dienst Avira AntiVir Server auf dem zu schützenden Server. Vergeben Sie ein Kennwort für den Server auf AntiVir Server Konsole.
siehe Kap. Einstellungen und Einstellungen::Allgemeines::Kennwort

Update und Systemprüfung ausführen

Führen Sie zunächst einmalig ein Update aus. Hierfür legen Sie im **Planer** einen Update-Auftrag an. Wählen Sie als Startzeitpunkt "Sofort" aus. Führen Sie eine komplette Systemprüfung durch. Hierfür legen Sie im **Planer** einen Prüfauftrag an. Wählen Sie für den Prüfauftrag das Profil "Lokale Festplatten" und den Startzeitpunkt "Sofort" aus.
siehe Kap. Planer

Suchläufe und Update-Aufträge definieren

Definieren Sie Suchläufe und Update-Aufträge. Um Suchläufe des Scanner zu konfigurieren, legen Sie ggf. zunächst unter **Prüfen** benutzerdefinierte Profile an. Im nächsten Schritt können Sie Suchläufe und Update-Aufträge unter **Planer** anlegen.
siehe Kap. Prüfen und Planer

6 Scanner

6.1 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:

- **Suche im Planer (remote und lokal)**
  Der Planer bietet die Möglichkeit, zeitlich gesteuerte Prüfaufträge auf dem zu schützenden Server durchführen zu lassen.
- **Suche über Profile (remote und lokal)**
  Unter Profile können definierte und konfigurierte Suchprofile auf dem zu schützenden Server angestoßen werden.
- **Shell Extension: Suche über das Kontextmenü im Windows Explorer (nur lokal)**
  Sie haben die Möglichkeit, über den Eintrag **Ausgewählte Dateien mit AntiVir überprüfen** im Verzeichniskontextmenü ein Verzeichnis nach Viren und unerwünschten Programmen zu durchsuchen. Die Funktionalität **Shell Extension** ist eine Zusatzkomponente, die nur nach Auswahl in der benutzerdefinierten Installation verfügbar ist.
- **Durchsuchen von eigenen Dokumenten über das Kontextmenü des Tray Icons (nur lokal)**

  Über den Eintrag **Meine Dokumente** im Kontextmenü des Tray Icons können Sie auf dem zu schützenden Server eine Suche nach Viren und unerwünschten Programmen im Windows Benutzerverzeichnis 'Eigene Dateien' anstoßen.

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 bei allen Suchprofilen über die Aktivierung der entsprechenden Optionen unter **Einstellungen::Scanner::Suche: Weitere Einstellungen**

7 Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität der Suchengine und der Virendefinitionen. Laden Sie deshalb regelmäßig Updates für Avira AntiVir Server von unseren Downloadservern herunter. Zur Ausführung von regelmäßigen Updates ist die Komponente Updater in Avira AntiVir Server integriert. Die Komponente Updater aktualisiert die folgenden Programmkomponenten:

- Virendefinitionsdatei
- Suchengine
- Programmdateien (Produktupdate)

Auf der AntiVir Server Konsole unter Planer können Sie Update-Aufträge einrichten, die in den angegebenen Intervallen von AntiVir Updater ausgeführt werden. Standardmäßig ist nach einer Installation von AntiVir Server ein Update-Auftrag angelegt, der in folgendem Intervall ausgeführt wird: 60 Minuten.

Bei jedem Update-Auftrag werden die Virendefinitionsdatei und die Suchengine auf Aktualität geprüft und ggf. aktualisiert, Produktupdates werden entsprechend der Konfiguration ausgeführt. Auf der AntiVir Server Konsole können Sie im Kontextmenü eines Serverknotens ein Produktupdate manuell anstoßen. Ein Neustart des Systems nach einem Update ist nur beim Produktupdate erforderlich.

Sie können Updates über folgende Server beziehen:

- direkt aus dem **Internet** über einen **Webserver der Avira GmbH**
- über einen **Web- oder Dateiserver im Intranet**, der als Master-Server die Update-Dateien aus dem Internet herunterlädt und sie anderen Servern zur Verfügung stellt. Dies ist sinnvoll, wenn Sie Avira AntiVir Server auf mehreren Computern in einem Netzwerk aktualisieren wollen. Durch die Einrichtung eines Downloadservers im Intranet kann die Aktualität von Avira AntiVir Server auf den zu schützenden Servern ressourcenschonend gewährleistet werden. Um einen funktionierenden Downloadserver im Intranet einzurichten, benötigen Sie einen Server, der die Update-Struktur von Avira AntiVir Server anbietet.

Bei der Nutzung eines Webservers erfolgt der Download per HTTP-Protokoll. Bei der Nutzung eines Dateiservers erfolgt ein Zugriff auf die Update-Dateien über das Netzwerk. Sie konfigurieren das Update auf der AntiVir Server Konsole.

Hinweis
Als Web- oder Dateiserver im Intranet können Sie AntiVir Internet Update Manager (File- oder Webserver unter Windows) nutzen. AntiVir Internet Update Manager spiegelt Downloadserver von AntiVir Produkten (u.a. von Avira AntiVir Server) und ist im Internet auf der Avira Webseite beziehbar:
http://www.avira.de

8 Viren und mehr

8.1 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.

8.2 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 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

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

9.2 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 der AntiVir Server Konsole 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@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/de/support/upload

9.3 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@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).

9.4 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@avira.com

10 Referenz: Konfigurationsoptionen

Die Referenz der Konfiguration dokumentiert alle verfügbaren Konfigurationsoptionen.

10.1 Scanner

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.

Optimierter Suchlauf

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

Hinweis
Die Option ist nur bei Multi-Prozessor-Rechnern verfügbar, wird jedoch in der Konfiguration in jedem Fall angezeigt und kann aktiviert werden: Falls der administrierte Server nicht über mehrere Prozessoren verfügt, wird die Option vom Scanner nicht genutzt.

Symbolischen Verknüpfungen folgen

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

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

Rootkit-Suche bei Suchstart

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

Wichtig
Die Rootkit-Suche ist unter Windows XP 64 Bit, Windows 2003 64 Bit, Windows Server 2003 64 Bit nicht verfügbar!

Wichtig
Die Rootkit-Suche wird remote nicht ausgeführt.

Registry durchsuchen

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

Keine Dateien und Pfade auf Netzlaufwerken durchsuchen

Suchvorgang

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.

10.1.1 Aktion bei Fund

Aktion bei Fund

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

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.

10.1.2 Weitere Aktionen

Programm nach Fund starten

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

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

Programmname

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

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

Argumente

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

Ereignisprotokoll

Ereignisprotokoll verwenden

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

10.1.3 Archive

10.1.4 Archive

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.

10.1.5 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.

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

10.1.6 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.

10.1.7 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.

10.2 Guard

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.

Laufwerke

Lokale Laufwerke

Bei aktivierter Option werden nur Dateien von lokalen Laufwerken wie Festplatten, CD- und Disketten-Laufwerke, MO- und ZIP-Laufwerke, etc. überwacht. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Netzlaufwerke

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

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

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

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

Caching aktivieren

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

10.2.1 Aktion bei Fund

Aktion bei Fund

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

Erweiterte Terminal Server Unterstützung

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

reparieren

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

umbenennen

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

Quarantäne

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

löschen

Die Datei wird gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

ignorieren

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

überschreiben und löschen

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

Standard

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

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

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.

Warnmeldungen anzeigen

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms eine Warnmeldung.

Primäre Aktion

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

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

reparieren

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

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

löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

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

umbenennen

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

ignorieren

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

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

Zugriff verweigern

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

Quarantäne

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

Sekundäre Aktion

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

löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

überschreiben und löschen

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

umbenennen

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

ignorieren

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

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

Zugriff verweigern

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

Quarantäne

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

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

10.2.2 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.

10.2.3 Ausnahmen

Mit diesen Optionen können Sie Ausnahme-Objekte für den Guard (Echtzeitsuche) konfigurieren. Die entsprechenden Objekte werden dann bei der Echtzeitsuche nicht beachtet. Der Guard kann über die Liste der auszulassenden Prozesse deren Dateizugriffe bei der Echtzeitsuche ignorieren. Dies ist zum Beispiel bei Datenbanken oder Backuplösungen sinnvoll.
Beachten Sie bei der Angabe von auszulassenden Prozessen und Dateiobjekten folgendes: Die Liste wird von oben nach unten abgearbeitet. Je länger die Liste ist, desto mehr Prozessorzeit braucht die Abarbeitung der Liste für jeden Zugriff. Halten Sie deshalb die Listen möglichst klein.

Vom Guard auszulassende Prozesse

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

Eingabefeld

In dieses Feld geben Sie den Namen des Prozesses ein, der von der Echtzeitsuche nicht berücksichtigt werden soll. Standardmäßig ist kein Prozess eingegeben.

Hinweis
Sie können bis zu 128 Prozesse eingeben.

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

Hinweis
Sie haben die Möglichkeit, Prozesse ohne vollständige Pfadangabe von der Überwachung des Guard auszunehmen:
anwendung.exe
Dies gilt jedoch ausschließlich für Prozesse, deren ausführbare Dateien auf Laufwerken der Festplatte liegen.
Eine vollständige Pfadangabe ist bei Prozessen erforderlich, deren ausführbare Dateien auf verbundenen Laufwerken, z.B. Netzlaufwerken liegen. Beachten Sie hierzu die allgemeinen Hinweise zur Notation von Ausnahmen auf verbundenen Netzlaufwerken.
Geben Sie keine Ausnahmen für Prozesse an, deren ausführbare Dateien auf dynamischen Laufwerken liegen. Dynamische Laufwerke werden für Wechseldatenträger wie CD, DVD oder USB-Stick verwendet.

Hinweis
Laufwerke müssen wie folgt angegeben werden: [Laufwerksbuchstabe]:\
Das Zeichen Doppelpunkt (:) darf nur zur Angabe von Laufwerken verwendet werden.

Hinweis
Bei der Angabe des Prozesses können Sie die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden:
C:\Programme\Anwendung\anwendung.exe
C:\Programme\Anwendung\anwendun?.exe
C:\Programme\Anwendung\anwend*.exe
C:\Programme\Anwendung*.exe
Um zu vermeiden, dass Prozesse global von der Überwachung des Guard ausgenommen werden, sind Angaben ungültig, die ausschließlich aus folgenden Zeichen bestehen: * (Stern), ? (Fragezeichen), / (Slash), \ (Backslash), . (Punkt), : (Doppelpunkt).

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

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

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

Hinzufügen

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

Löschen

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

Vom Guard auszulassende Dateiobjekte

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

Eingabefeld

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

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

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

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

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

Hinweis
Pro Laufwerk können Sie maximal 20 Ausnahmen mit vollständigem Pfad (beginnend mit dem Laufwerksbuchstaben) angeben.
Bsp.: C:\Programme\Anwendung\Name.log

Die maximale Anzahl von Ausnahmen ohne vollständigen Pfad beträgt 64.
Bsp: *.log
\Rechner1\C\Verzeichnis1

Hinweis
Bei dynamischen Laufwerken, die als Verzeichnis auf einem anderen Laufwerk eingebunden (gemountet) werden, müssen Sie den Aliasnamen des Betriebssystems für das eingebundene Laufwerk in der Liste der Ausnahmen verwenden:
z.B. \Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
Verwenden Sie den Bereitstellungspunkt (mount point) selbst, z.B. C:\DynDrive, wird das dynamische Laufwerk trotzdem durchsucht. Sie können den zu verwendenden Aliasnamen des Betriebssystems aus der Report-Datei des Guard ermitteln.

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

Hinzufügen

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

Löschen

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

Beachten Sie bei der Angabe von Ausnahmen die weiteren Hinweise:

Hinweis
Um Objekte auch dann auszunehmen, wenn darauf mit kurzen DOS-Dateinamen (DOS-Namenskonvention 8.3) zugegriffen wird, muss der entsprechende kurze Dateiname ebenfalls in die Liste eingetragen werden.

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

Beispielsweise:

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

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

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

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

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

Beispiele für auszunehmende Prozesse:

- anwendung.exe

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

- C:\Programme1\anwendung.exe

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

- C:\Programme1*.exe

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

Beispiele für auszunehmende Dateien:

- *.mdb

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

- *.xls*

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

- C:\Verzeichnis*.log

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

- \\Computername1\Freigabe1\

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

– \\1.0.0.0\Freigabe1*.mdb

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

-

10.2.4 Produkte

Vom Guard auszulassende Produkte

In diesem Anzeigebereich können Sie Produkte auswählen, die von der Suche des Guard ausgenommen werden. Alle Anwendungen, Dienste oder Datenbanken des ausgewählten Produkts sind von der Überwachung durch Guard ausgenommen.

10.2.5 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.

10.2.6 Report

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

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Guard kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

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

Erweitert

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

Vollständig

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

Reportdatei beschränken

Größe beschränken auf n MB

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

Reportdatei vor dem Kürzen sichern

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

Konfiguration in Reportdatei schreiben

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

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

10.3 Allgemeines

10.3.1 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.

10.3.2 Kennwort

Sie können den Zugriff auf zu schützende Server in der AntiVir Server Konsole durch ein Kennwort schützen. Das Kennwort des Servers muss immer eingegeben werden, wenn eine Verbindung zum Server erstellt wird. Die Verbindung zu Servern, die durch ein Kennwort geschützt sind, wird getrennt, sobald Sie die AntiVir Server Konsole schließen.

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!

10.3.3 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 diese Alter überschritten, wird in der Status-Übersicht 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.

10.3.4 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 und Methoden (Prozesse stoppen und starten) an einer Schnittstelle zur Verfügung. Sie haben über WMI die Möglichkeit, Betriebsdaten des Programms abzurufen und das Programm zu steuern. Eine vollständige Referenz der WMI-Schnittstelle können Sie beim Hersteller anfordern. Nach der Unterzeichnung einer Geheimhaltungsvereinbarung erhalten Sie die Referenz im PDF-Format.

WMI-Unterstützung aktivieren

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

Aktivieren/Deaktivieren von Diensten erlauben

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Dienste des Programms zu aktivieren und zu deaktivieren.

10.3.5 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.

10.3.6 Berichte

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.

10.3.7 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.

Verwende folgendes Verzeichnis

Bei aktivierter Option wird der im Eingabefeld angezeigte Pfad verwendet.

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

Standard

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

Reportverzeichnis

Dieses Eingabefeld enthält den Pfad zum Report Verzeichnis.

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

Standard

Die Schaltfläche stellt den vordefinierten Pfad zum Reportverzeichnis wieder her.

Quarantäneverzeichnis

Dieses Eingabefeld enthält den Pfad zum Quarantäneverzeichnis.

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

Standard

Die Schaltfläche stellt den vordefinierten Pfad zum Quarantäneverzeichnis wieder her.

10.4 Update

10.4.1 Update

Unter der Rubrik *Update* konfigurieren Sie die Verbindung zu den Downloadservern.

Download

Über Webserver

Das Update erfolgt über einen Webserver per HTTP-Verbindung. Sie können einen Webserver des Herstellers im Internet nutzen oder einen Webserver im Intranet, der die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht.

Hinweis
Konfigurieren Sie den Webserver und ggf. den Proxy-Server, wenn Sie diese Option aktivieren.

Über Dateiserver/Freigegebene Verzeichnisse

Das Update erfolgt über einen Dateiserver im Intranet, der die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht.

Hinweis
Konfigurieren Sie den zu verwendenden Dateiserver, wenn Sie diese Option aktivieren.

Unter **Produktupdate** konfigurieren Sie die Ausführung von Produktupdates oder die Benachrichtigung über verfügbare Produktupdates.

Produktupdates

Produktupdates herunterladen und automatisch installieren

Bei aktivierter Option können Sie einen Zeitpunkt für das Produktupdate festlegen. Geben Sie einen Wochentag und eine Uhrzeit für das Produktupdate an. Zum angegebenen Zeitpunkt wird das Produktupdate ausgeführt, falls 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. Vor der Ausführung eines Produktupdates erhalten Sie eine Warnmeldung auf der AntiVir Server Konsole, mit der der zu schützende Server administriert wird.

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 auf der AntiVir Server Konsole und per Email, falls die Email-Benachrichtigung konfiguriert wurde.

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).

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

Download

Standard-Server

Geben Sie hier die Adressen (URL) der Webserver an, von denen die Updates geladen werden sollen, sowie das erforderliche Update-Verzeichnis 'update'. Folgende Angabe eines Webservers ist gültig: http://<Adresse des Webservers>[:Port]/update. Wenn Sie keinen Port angeben, wird Port 80 verwendet. Standardmäßig sind die erreichbaren Webserver der Avira GmbH für das Update eingetragen. Sie können jedoch auch eigene Webserver beispielsweise im Intranet nutzen. Bei der Angabe von mehreren Webservern werden die Server über Kommata getrennt.

Standard

Die Schaltfläche stellt die vordefinierten Adressen wieder her.

Prioritäts-Server

Geben Sie in diesem Feld die Adresse (URL) des Webservers an, der bei einem Update als erster Server angefragt werden soll, sowie das erforderliche Update-Verzeichnis. Wenn dieser Server nicht erreichbar ist, werden die angegebenen Standard-Server angefragt. Folgende Angabe des Webservers ist gültig: http://<Adresse des Webservers>[:Port]/update. Wenn Sie keinen Port angeben, wird Port 80 verwendet.

10.4.2 Dateiserver

Bei mehreren Computern in einem Netzwerk kann Ihr AntiVir Programm ein Update von einem Dateiserver im Intranet herunterladen, der seinerseits die Update-Dateien von einem Downloadserver des Herstellers im Internet bezieht. So kann die Aktualität von AntiVir Programmen auf allen Computern ressourcenschonend sichergestellt werden.

Hinweis
Die Konfigurationsrubrik ist nur aktiviert, wenn unter Einstellungen::Update::Update die Option **Über Dateiserver / Freigegebene Verzeichnisse** ausgewählt wurde.

Download

Geben Sie den Dateiserver an, auf dem sich die Update-Dateien Ihres AntiVir Programms befinden, sowie die erforderlichen Verzeichnisse '/release/update/'. Folgende Angabe ist erforderlich: file://<IP-Adresse des Dateiservers>/release/update/. Das Verzeichnis 'release' muss ein Verzeichnis sein, das für alle Benutzer freigegeben ist.

Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, das gewünschte Download-Verzeichnis auszuwählen.

Server Login

Login Name

Geben Sie einen Benutzernamen für die Anmeldung am Server ein. Verwenden Sie ein Benutzerkonto mit Zugriffsrechten auf das genutzte, freigegebene Verzeichnis am Server.

Login Kennwort

Geben Sie das Passwort des genutzten Benutzerkontos ein. Die eingegebenen Zeichen werden mit * maskiert.

Hinweis
Wenn Sie im Bereich Server Login keine Daten eingeben, wird beim Zugriff auf den Dateiserver keine Authentifizierung durchgeführt. In diesem Fall müssen jedoch ausreichende Benutzerrechte auf dem Dateiserver vorhanden sein.

10.4.3 Proxy

Proxyserver

Keinen Proxyserver verwenden

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

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

10.5 Warnungen

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

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

Warnung
Die Funktionalität wird von den folgenden Betriebssystemen nicht mehr unterstützt:
Windows Server 2008 und höher
Windows Vista und höher

Nachricht senden an

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

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

Einfügen

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

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

Löschen

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

10.5.1 Guard

Netzwerkwarnungen

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

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

Zu sendende Nachricht

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

Folgende Tastenkombinationen können Sie zum Formatieren der Nachricht verwenden:

Strg + Tab	fügt einen Tabulator ein. Die aktuelle Zeile wird um einige Zeichen nach rechts eingerückt.
Strg + Enter	fügt einen Zeilenumbruch ein.

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

Folgende Platzhalter sind verwendbar:

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

Standard

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

10.5.2 Scanner

Netzwerkwarnungen aktivieren

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

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

Zu sendende Nachricht

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

Folgende Tastenkombinationen können Sie zum Formatieren der Nachricht verwenden:

Strg + Tab	fügt einen Tabulator ein. Die aktuelle Zeile wird um einige Zeichen nach rechts eingerückt.
Strg + Enter	fügt einen Zeilenumbruch ein.

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

Folgende Platzhalter sind verwendbar:

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

Standard

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

10.5.3 Akustische Warnungen

Akustische Warnung

Sie haben die Möglichkeit einen Warnton zu aktivieren, der bei der Suche des Guard einen Virenfund signalisiert. Die akustische Warnung erfolgt nur im Aktionsmodus "*Erweiterte Terminal Server Unterstützung*". Als Warnton kann eine alternative Wave Datei ausgewählt werden.

Hinweis
Sie stellen den Aktionsmodus des Guard unter folgender Rubrik ein: Einstellungen::Guard::Aktion bei Fund

Keine Warnung

Bei aktivierter Option erfolgt keine akustische Warnung bei einem Virenfund des Guard.

Über PC-Lautsprecher abspielen (nur beim Modus Erweiterte Terminal Server Unterstützung)

Bei aktivierter Option erfolgt eine akustische Warnung mit dem Standardwarnton beim Fund eines Virus durch den Guard. Der Warnton wird über den PC internen Lautsprecher abgespielt.

Folgende Wave-Datei benutzen (nur beim Modus Erweiterte Terminal Server Unterstützung)

Bei aktivierter Option erfolgt eine akustische Warnung mit der ausgewählten Wave-Datei beim Fund eines Virus durch den Guard. 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.

10.6 Email

10.6.1 Email

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

Die Nachrichten können hierbei durch unterschiedliche Ereignisse ausgelöst werden. Folgende Komponenten unterstützen den Versand von Emails:

- Guard: Versenden von Benachrichtigungen
- Scanner: Versenden von Benachrichtigungen
- Updater: Versenden von Benachrichtigungen
- Quarantänemanager: Versenden von verdächtigen Dateien an das Avira Malware Research Center

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

Email-Nachrichten

SMTP-Server

Geben Sie hier den Namen des zu verwendenden Hosts an - entweder seine IP-Adresse oder den direkten Hostnamen.
Die maximal mögliche Länge des Hostnamens beträgt 127 Zeichen.

Beispielsweise:

192.168.1.100 oder mail.musterfirma.de.

Absenderadresse

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

Authentifizierung

Einige Mailserver erwarten, dass sich ein Programm vor dem Versenden einer Email gegenüber dem Server authentifiziert (anmeldet). Warnungen per Email können mit Authentifizierung an einen SMTP-Server übergeben werden.

Authentifizierung verwenden

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

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

Test Email senden

Mit Klick auf die Schaltfläche versucht das Programm zur Überprüfung der eingegebenen Daten eine Test-Email an die Absenderadresse zu senden.

10.6.2 Guard

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

Guard

Email Warnungen

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

Benachrichtigung per Email bei folgenden Ereignissen

Bei der Echtzeitsuche wurde ein Fund gemeldet.

Bei aktivierter Option erhalten Sie eine Email mit dem Namen des Virus oder unerwünschten Programms und der betroffenen Datei immer dann, wenn die Echtzeitsuche einen Virus bzw. ein unerwünschtes Programm findet.

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Fund bei Echtzeitsuche" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Email::Warnungen::Email-Template).

Innerhalb des Guard ist ein kritischer Fehler aufgetreten.

Bei aktivierter Option erhalten Sie eine Email, wenn ein interner kritischer Fehler feststellt wird.

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

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Kritischer Fehler in Guard" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Empfänger

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

10.6.3 Scanner

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

Scanner

Email Warnungen aktivieren

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

Benachrichtigung per Email bei folgenden Ereignissen

Bei der Suche wurde ein Fund gemeldet.

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

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Fund bei Suche" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Ende eines geplanten Suchlaufs.

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

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Ende des Suchlaufs" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Reportdatei als Anlage beifügen

Bei aktivierter Option wird beim Versenden von Scanner-Benachrichtigungen die aktuelle Reportdatei der Komponente Scanner als Anlage an die Email angefügt.

Empfängeradresse(n)

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

10.6.4 Updater

Die Komponente Updater kann bei bestimmten Ereignissen Meldungen per Email an einen oder mehrere Empfänger senden.

Updater

Email Warnungen

Bei aktivierter Option versendet die Update-Komponente Email-Nachrichten mit den wichtigsten Daten, wenn ein bestimmtes Ereignis eintritt. Standardmäßig ist diese Option deaktiviert.

Benachrichtigungen per Email bei folgenden Ereignissen

Kein Update erforderlich. Ihr Programm ist auf dem neuesten Stand.

Bei aktivierter Option wird eine Email versendet, wenn der Updater erfolgreich eine Verbindung zum Download-Server erstellen konnte, am Server jedoch keine neuen Dateien verfügbar sind. Dies bedeutet, dass Ihr AntiVir Programm auf dem aktuellsten Stand ist.

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis 'Kein Update erforderlich' konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Update erfolgreich beendet. Es wurden neue Dateien installiert.

Bei aktivierter Option wird bei allen ausgeführten Updates eine Email versendet: Es kann sich um ein Produktupdate oder eine Aktualisierung der Virendefinitionsdatei oder der Suchengine handeln.

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis 'Update erfolgreich-Installation von neuen Dateien' konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Update erfolgreich beendet. Es ist ein neues Produktupdate verfügbar.

Bei aktivierter Option wird nur dann eine Email versendet, wenn eine Aktualisierung der Suchengine oder Virendefinitionsdatei ohne Produktupdate ausgeführt wurde, jedoch ein Produktupdate verfügbar ist.

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Update erfolgreich-Produktupdate verfügbar" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Update fehlgeschlagen.

Bei aktivierter Option wird eine Email versendet, wenn das Update aufgrund eines Fehlers fehlgeschlagen ist.

Bearbeiten

Mit der Schaltfläche "*Bearbeiten*" öffnen Sie das Fenster "*Email-Template*", in dem Sie die Nachricht zum Ereignis "Update fehlgeschlagen" konfigurieren können. Sie haben die Möglichkeit, Texte für den Betreff und die Nachricht der Email einzugeben. Sie können dabei Variablen verwenden (siehe Konfiguration::Allgemeines::Warnungen::Email::Email-Template).

Reportdatei als Anlage beifügen

Bei aktivierter Option wird beim Versenden von Updater-Benachrichtigungen die aktuelle Reportdatei der Komponente Updater als Anlage an die Email angefügt.

Empfänger

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

Hinweis
Bei den folgenden Ereignisse werden immer Warnmeldungen via Email versandt, falls ein SMTP-Server und eine Empfängeradresse für Updater-Benachrichtigungen konfiguriert wurden:
Ein Produktupdate ist für jede weitere Aktualisierung des Programms erforderlich.
Eine Aktualisierung der Suchengine oder der Virendefinitionsdatei konnte nicht ausgeführt werden, da ein Produktupdate erforderlich ist.

Der Versand dieser Warnmeldungen wird unabhängig von Ihren Einstellungen zu den Email-Warnungen der Update-Komponente ausgeführt.

10.6.5 Email-Template

Im Fenster *Email-Template* konfigurieren Sie die Email-Benachrichtigungen der einzelnen Komponenten zu den aktivierten Ereignissen. Sie können einen Text bis zu maximal 128 Zeichen in der Betreffzeile und einen Text bis zu maximal 1024 Zeichen im Nachrichtenfeld eingeben.

Folgende Variablen können im Email-Betreff und in der Email-Nachricht verwendet werden:

Global gültige Variablen

Variable	**Wert**
Windows Umgebungsvariablen	Die Komponente der Email-Benachrichtigungen unterstützt alle Windows Umgebungsvariablen.
%SYSTEM_IP%	IP-Adresse des Rechners
%FQDN%	Vollständiger Domainname (fully qualified domain name)
%TIMESTAMP%	Zeitstempel des Ereignisses: Zeit- und Datumsformate entsprechend den Spracheinstellungen des Betriebssystems
%COMPUTERNAME%	NetBIOS-Computername
%USERNAME%	Name des Benutzers, der auf die Komponente zugreift
%PRODUCTVER%	Produktversion
%PRODUCTNAME%	Produktname
%MODULENAME%	Name der Komponente, die die Email versendet
%MODULEVER%	Version der Komponente, die die Email versendet

Spezifische Variablen der Komponenten

Variable	**Wert**	**Emails der Komponenten**
%ENGINEVER%	Version der verwendeten Suchengine	Guard Scanner
%VDFVER%	Version der verwendeten Virendefinitionsdatei	Guard Scanner
%SOURCE%	Voll qualifizierter Dateiname	Guard
%VIRUSNAME%	Name des Virus oder unerwünschten Programms	Guard
%ACTION%	Aktion, die nach dem	Guard

	Fund ausgeführt wurde	
%MACADDR%	MAC-Adresse der ersten registrierten Netzwerkkarte	Guard
%UPDFILESLIST%	Liste der aktualisierten Dateien	Updater
%UPDATETYPE%	Update-Typ: Update von Suchengine und Virendefinitionsdatei oder Produktupdate mit Aktualisierung von Suchengine und Virendefinitionsdatei	Updater
%UPDATEURL%	URL des Downloadservers, der für das Update verwendet wurde	Updater
%UPDATE_ERROR%	Update-Fehler in Worten	Updater
%DIRCOUNT%	Anzahl durchsuchter Verzeichnisse	Scanner
%FILECOUNT%	Anzahl durchsuchter Dateien	Scanner
%MALWARECOUNT%	Anzahl gefundener Viren oder unerwünschter Programme	Scanner
%REPAIREDCOUNT%	Anzahl reparierter betroffener Dateien	Scanner
%RENAMEDCOUNT%	Anzahl umbenannter betroffener Dateien	Scanner
%DELETEDCOUNT%	Anzahl gelöschter betroffener Dateien	Scanner
%WIPECOUNT%	Anzahl betroffener Dateien, die überschrieben und gelöscht wurden	Scanner
%MOVEDCOUNT%	Anzahl betroffener Dateien, die in die Quarantäne verschoben wurden	Scanner
%WARNINGCOUNT%	Anzahl der Warnungen	Scanner
%ENDTYPE%	Status des Suchlaufendes: Abgebrochen | Erfolgreich beendet	Scanner

%START_TIME%	Startzeitpunkt des Suchlaufs Startzeitpunkt des Updates	Scanner Updater
%END_TIME%	Ende des Suchlaufs Ende des Updates	Scanner Updater
%TIME_TAKEN%	Ausführungsdauer des Suchlaufs in Minuten Ausführungsdauer des Updates in Minuten	Scanner Updater
%LOGFILEPATH%	Pfad und Dateiname der Reportdatei	Scanner Updater

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