Avira Professional Security

Kurzanleitung

AVIRA

Inhaltsverzeichnis

Dieses Dokument soll Sie bei der Installation und optimalen Einrichtung von Avira Professional Security unterstützen. Es beinhaltet wichtige und hilfreiche Einstellungsmöglichkeiten und Empfehlungen des Avira Supports zur Konfiguration des Programms. Ebenfalls sind nützliche Tipps z.B. zur Vorgehensweise bei einem Virusbefall enthalten.

Sämtliche für die Installation benötigten Installationsdateien sowie die Produkthandbücher im PDF-Format finden Sie zum Download auf unserer Internetseite.

1. Setup

Im Downloadbereich auf unserer Homepage finden Sie zwei Setuppakete:
Den sogenannten Webloader mit etwas über 800 Kb und das komplette Installationspaket mit ca. 45 MB.

1.1 Webloader

Der Webloader lädt die aktuellen Programmdateien vor der Ausführung der Installation von den Avira-Webservern herunter. Durch dieses Verfahren wird gewährleistet, dass Avira Professional Security mit einer tagesaktuellen Virendefinitionsdatei installiert wird.

1.2 Komplettes Installationspaket

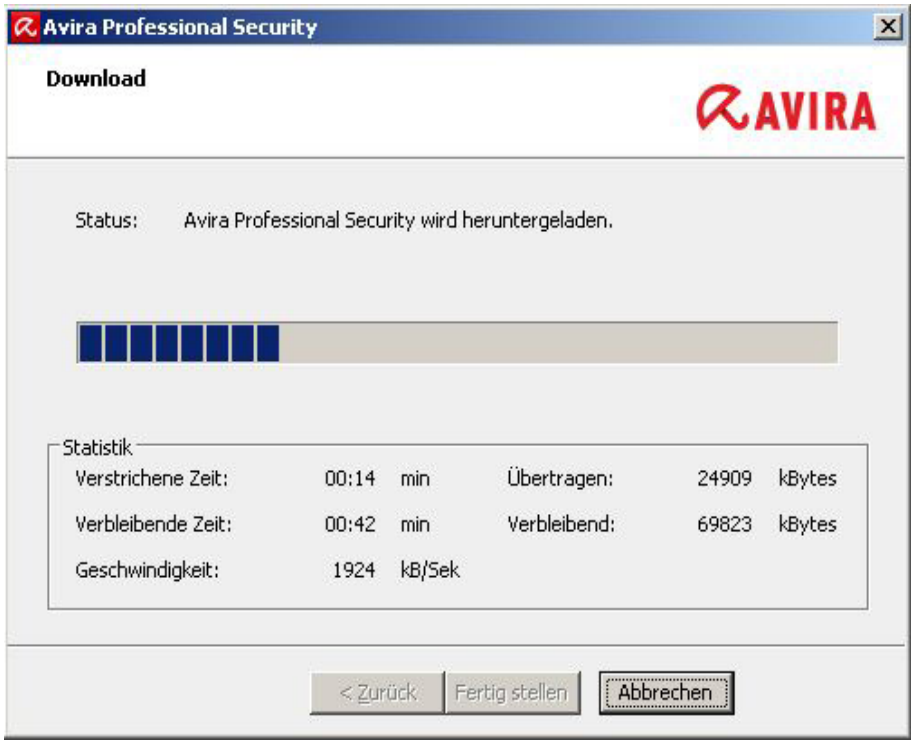
Das Installationspaket enthält sowohl das Installationsprogramm als auch alle benötigten Programmdateien. Bei diesem Installationspaket haben Sie jedoch keine Sprachauswahl der Avira Professional Security. Sollten Sie Avira Professional Security in einer anderen Sprache als Deutsch installieren wollen, so ändern Sie bitte auf der Homepage von Avira entsprechend die Sprache der Seite. Danach wird Ihnen der Download des zur ausgewählten Sprache gehörenden Softwarepaketes angeboten.

Ebenfalls ist darauf zu achten, dass die darin enthaltenen Dateien eventuell nicht aktuell sind.
Wir empfehlen Ihnen daher im Anschluss an die Installation ein Update auszuführen, um auf dem aktuellsten Stand zu sein.

Nachdem Sie die Installationsdatei der Avira Professional Security heruntergeladen haben, starten Sie zunächst die Installationsroutine mit einem Doppelklick auf die Datei
avira_professional_security.exe oder *avira_professional_security_de.exe*.

Im anschließend erscheinenden Assistenten klicken Sie auf weiter.
Falls Sie den Webloader ausgewählt haben, können Sie nun die passende Sprachversion auswählen.

Im weiteren Verlauf lädt der Webloader die benötigten Programmdateien und Virendefinitionsdateien herunter.



Anschließend haben Sie die Möglichkeit, einen Setup-Typ auszuwählen:

Vollständig
- Avira Professional Security wird vollständig mit allen Programmkomponenten (Modulen) installiert
- Die Programmdateien werden in ein vorgegebenes Standardverzeichnis unter C:\Programme\Avira\ installiert

Benutzerdefiniert
- Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden
- Sie haben die Möglichkeit, einzelne Programmkomponenten / Module zur Installation auszuwählen
- Sie können das Erstellen eines Desktop-Icons und einer Programmgruppe im Startmenü deaktivieren

Im benutzerdefinierten Setupmodus können Sie folgende Module auswählen:

- **Echtzeit Scanner** (permanente Überwachung aller Dateizugriffe in Echtzeit)
- **ProActive** (Modul zur Erkennung von Angriffen unbekannter Malware)
- **Email Schutz** (dieses Modul überwacht permanent alle ein- und ausgehenden Emails (POP3, IMAP, SMTP) inklusive der Dateianhänge
- **FireWall** (Regelbasierte Kontrolle über ein- und ausgehenden Internetverkehr)
- **Rootkits Schutz** (Modul zum Aufspüren von potenziellen Rootkits)
- **Browser Schutz** (bietet über den Webbrowser permanenten Schutz vor Viren und Malware)
- **Shell Extension** (direktes Prüfen von Dateien und Verzeichnissen im Windows Explorer)

Avira ProActiv ist die neue verhaltensbasierte Erkennungstechnologie von Avira, die ab der Version 10 integriert ist.

ProActiv schützt Ihren Computer vor neuen und unbekannten Bedrohungen, für die noch keine Virendefinitionen und Heuristiken vorliegen.

Es überwacht das System in Echtzeit und erkennt Angriffe, während diese stattfinden. Dazu überwachen Sensoren das System dauerhaft und melden Auffälligkeiten. Zur Ermittlung des malwaretypischen Verhaltens verwendet die ProActiv-Komponente Regelsets, die vom Avira Malware Research Center entwickelt wurden.

Die Regelsets werden von den Datenbanken der Avira GmbH gespeist. Zur Informationserfassung in den Avira Datenbanken sendet ProActiv Informationen über gemeldete, verdächtige Programme. Sie haben die Möglichkeit, die Datenübermittlung an die Avira Datenbanken zu deaktivieren.

Falls ein Programm ein für Malware typisches Verhalten zeigt, wird dies wie ein Virenfund behandelt und gemeldet.

Hinweis
Die ProActiv-Technologie ist für 64-Bit-Systeme noch nicht verfügbar. Windows 2000 wird generell nicht unterstützt.

Der Email Schutz wird benötigt, falls Sie Ihre Emails über POP3, SMTP oder IMAP empfangen und versenden.
Den Email Schutz kann man als Modul entfernen, falls einer der folgenden Punkte erfüllt ist:

- Sie lassen Emailverkehr bereits durch einen Emailserver überprüfen, beispielsweise durch Avira Exchange Security oder Avira Email-Schutz
- Sie rufen Ihre Emails via Webaccess ab, d.h. Sie greifen z.B. direkt auf die Anbieter gmx.de oder web.de zu

Mit dem Browser Schutz schützen Sie sich vor Viren und Malware, die über Webseiten auf Ihren Computer gelangen, die Sie aus dem Internet in Ihren Webbrowser laden.

Den Browser Schutz kann man als Modul entfernen, falls z.B. der folgenden Punkt erfüllt ist:

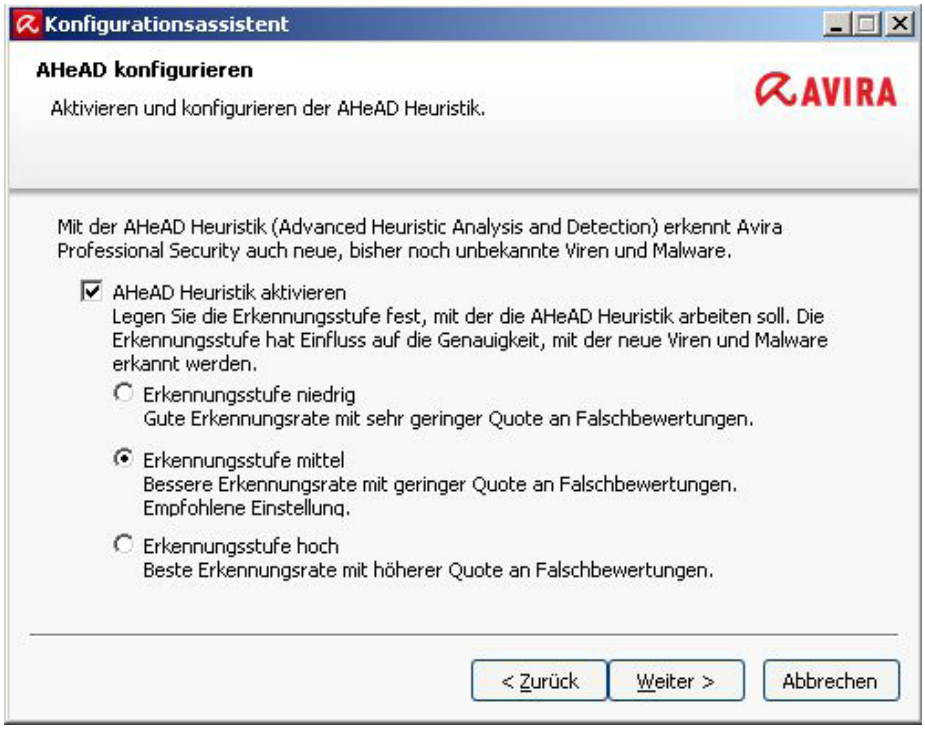
- Falls Sie den http-Verkehr bereits überprüfen lassen, beispielsweise durch den Avira ISA Server oder Avira Browser-Schutz

Die Avira FireWall prüft ein- und ausgehenden Internetverkehr. Mittels Adapter- und Anwendungsregeln kann man die Kommunikation einzelner Anwendungen kontrollieren.

Anschließend erscheint das Dialogfenster „Lizenz installieren“
Wählen Sie das Verzeichnis, in dem Sie die Lizenzdatei „*hbedv.key*“ gespeichert haben.

Sobald Sie die Installation beendet haben, erscheint der Konfigurationsassistent. Dieser leitet Sie einmal durch die grundlegenden Einstellungen der Avira Professional Security.

Im anschließenden Dialogfenster können Sie die Engine konfigurieren und die Erkennungsstufe für die AHeAD-Technologie wählen. Die gewählte Erkennungsstufe wird für die Einstellung der AHeAD-Technologie des Scanners (Direktsuche) und des Echtzeit-Scanners (Echtzeitsuche) übernommen.



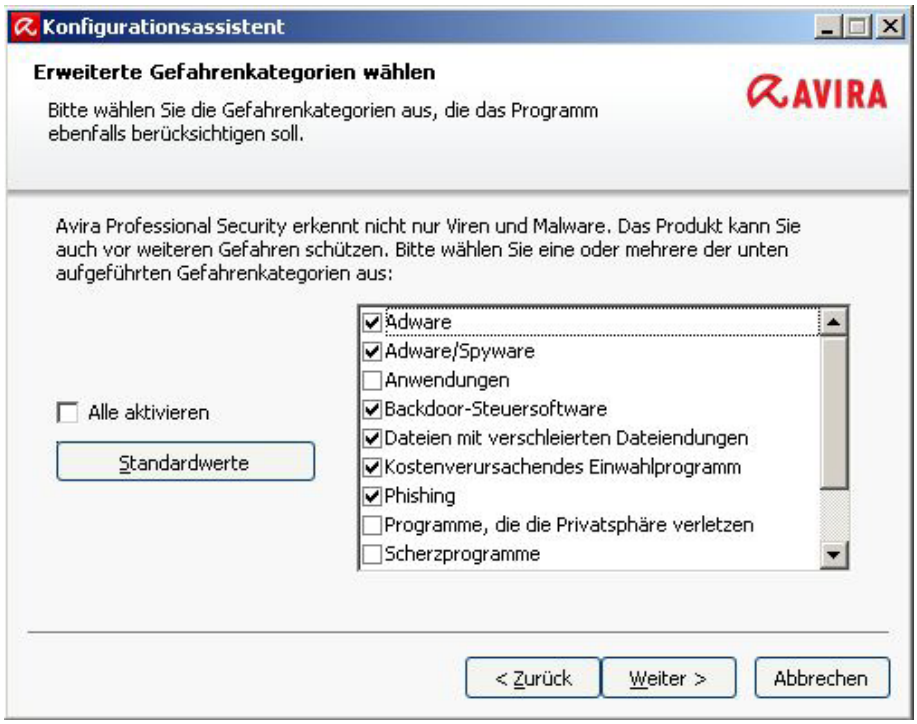
Hinweis
Bitte beachten Sie, dass eine hohe Erkennungsstufe zwar viele unbekannte Malwarearten erkennt, aber auch das Risiko von Fehlerkennungen erhöht.

Was bedeutet der Begriff Heuristik?

Bei der Heuristik handelt es sich um eine Früherkennungsfunktion, die auch unbekannte Viren entdecken kann. Dies geschieht durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Viren typisch sind.

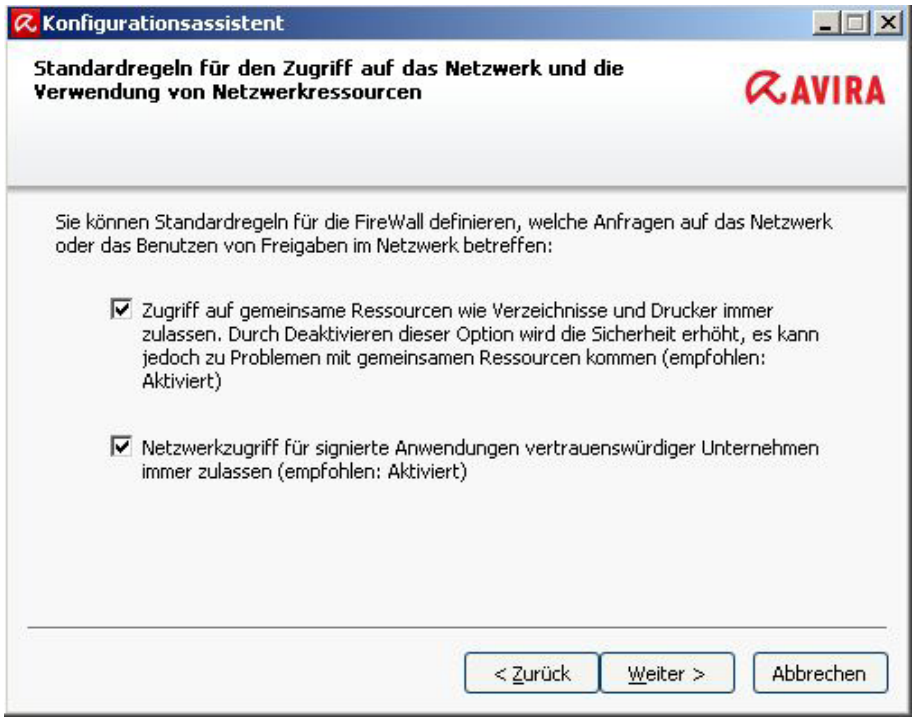
Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um einen Virus handelt; es können auch Fehlerkennungen vorkommen.

Im folgenden Dialogfenster können Sie die erweiterten Gefahrenkategorien auswählen, welche erkannt werden sollen.

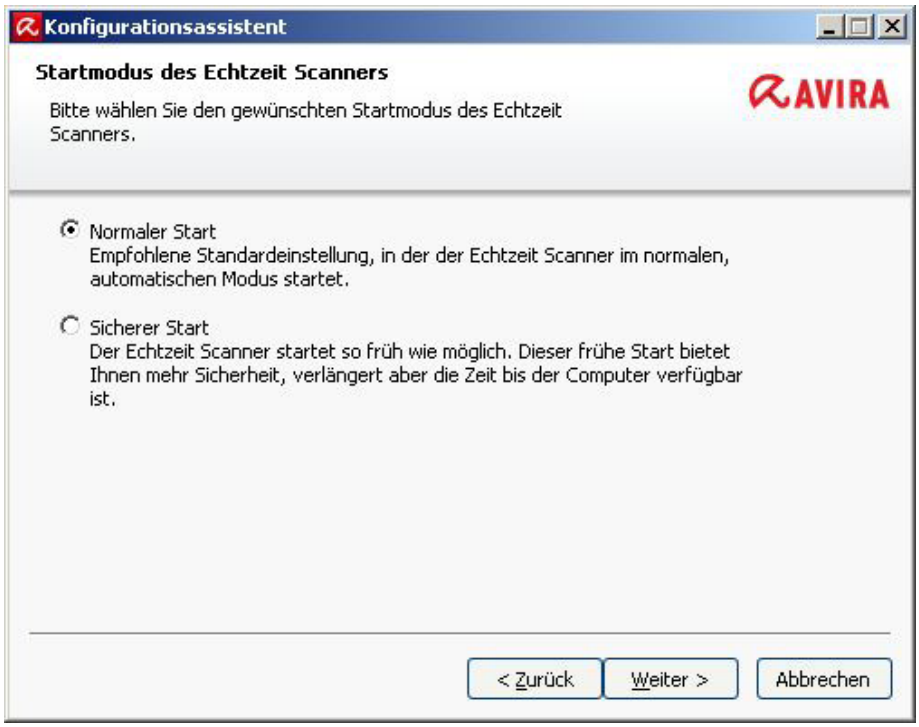


- Standardmäßig sind die oben abgebildeten Optionen aktiviert, da einerseits die Risiken von Adware/Spyware sowie Backdoor-Steuersoftware, Phishing und Dialern am größten sind. Andererseits werden aber gerade viele Administratortools von Avira als „Security Privacy Risk“ erkannt, da Avira nicht unterscheiden kann, ob das Programm nun von einem Admin gewollt dieses Verhalten zeigt oder nicht. Daher haben wir Anwendungen, SPR sowie die Spieleerkennung in unserer Grundkonfiguration ausgenommen

Eine kurze Übersicht über alle Gefahrenkategorien und ihre Bedeutung finden Sie in den Quicktipps am Ende dieser Dokumentation.



Wählen Sie anschließend den Startmodus des Echtzeit-Scanners aus.
Sie haben dort die Möglichkeit, zwischen dem normalen Start und dem sicheren Start zu wählen.



Beim „normalen Start“ wird der Echtzeit-Scanner im normalen, automatischen Modus gestartet. Dies ist der empfohlene Startmodus.

Beim „sicheren Start“ wird der Echtzeit-Scanner so früh wie möglich geladen. Dies erhöht die Sicherheit, kann aber die Startzeit des Computers verlangsamen. Hintergrund ist, dass einige Viren sich beim Start direkt mit dem Betriebssystem laden und so eventuell bereits aktiv sind, bevor der Echtzeit-Scanner geladen ist.

Beim sicheren Start wird zuerst der Echtzeit-Scanner gestartet. Erst wenn dieser komplett geladen und funktionsbereit ist, wird der Start der restlichen Komponenten fortgesetzt, woraus sich die eventuell verlängerte Startzeit des Systems ergibt.

Im folgenden Konfigurationsdialog können Sie die Servereinstellungen für den Email-Versand vornehmen.

Avira Professional Security nutzt diesen Email-Versand per SMTP beim Versenden von Email-Warnungen der jeweiligen Module Echtzeit-Scanner, Scanner und Updater.
Falls Sie Ihre Daten des SMTP Servers nicht wissen oder diese Option nicht nutzen möchten, können Sie diese Felder leer lassen.

Anschließend können Sie noch die Option „Kurze Systemprüfung nach der Installation durchführen“ auswählen, um den Computer nach der Installation kurz zu überprüfen.

2. Konfiguration

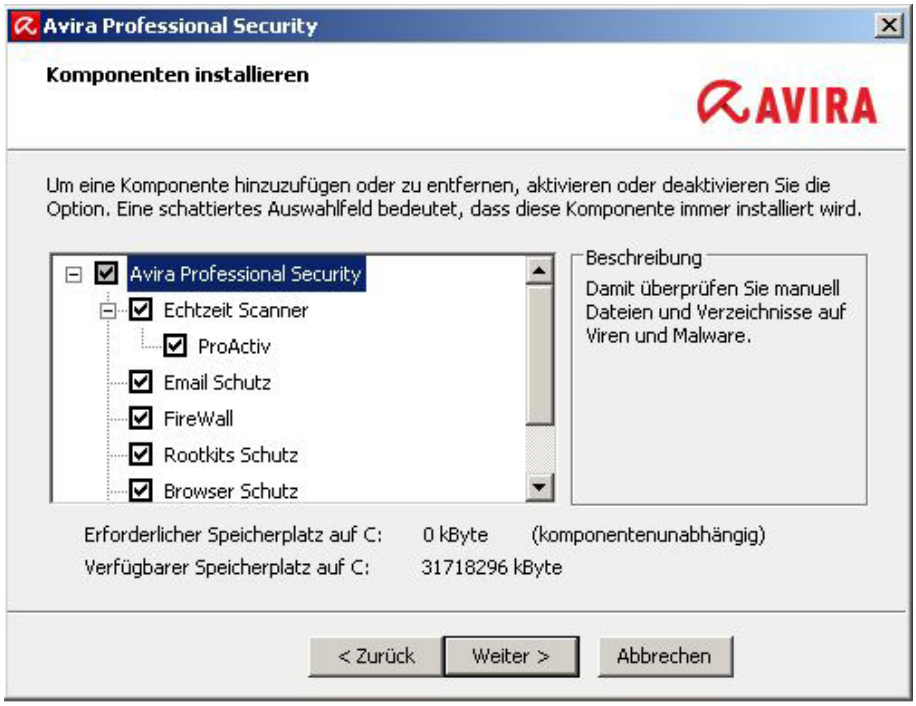
2.1 Module installieren / nachinstallieren bzw. entfernen

Durch eine Änderungsinstallation können verschiedene Module zur Installation ausgewählt und hinzugefügt bzw. entfernt werden.

Dies empfiehlt sich z.B. um Ressourcen zu sparen oder vorhandene Sicherheitslücken zu schließen.

Falls Sie Programmkomponenten der aktuellen Avira Professional Security Installation hinzufügen oder entfernen möchten, wechseln Sie in die Windows-Systemsteuerung auf den Punkt „Software“. Unter Windows Vista / Windows 7 würden Sie dies unter dem Punkt „Programme“ finden.

Wählen Sie Avira Professional Security und klicken Sie auf Ändern. Im Dialog der Avira Professional Security wählen Sie die Option „Programm ändern“. Sie werden durch die Änderungsinstallation geführt.



2.2. Updatekonfiguration zum Avira Update Manager

Falls Sie mehrere Installationen von Avira Professional Security in Ihrem Netzwerk betreiben und diese von einem zentralen Punkt aus updaten möchten, können Sie dies mit unserem kostenlosen Modul „Avira Update Manager“ realisieren.

Dies ist zum Beispiel sinnvoll, wenn nur einer Ihrer Rechner Zugriff zum Internet haben soll, die Virendefinitionen an Ihren Rechnern im Netzwerk aber dennoch immer auf dem neuesten Stand sein sollen. Zudem sparen Sie Netzwerk-Traffic und belasten die Internetverbindung nicht unnötig.

Sie können das hierfür benötigte Tool hier downloaden.

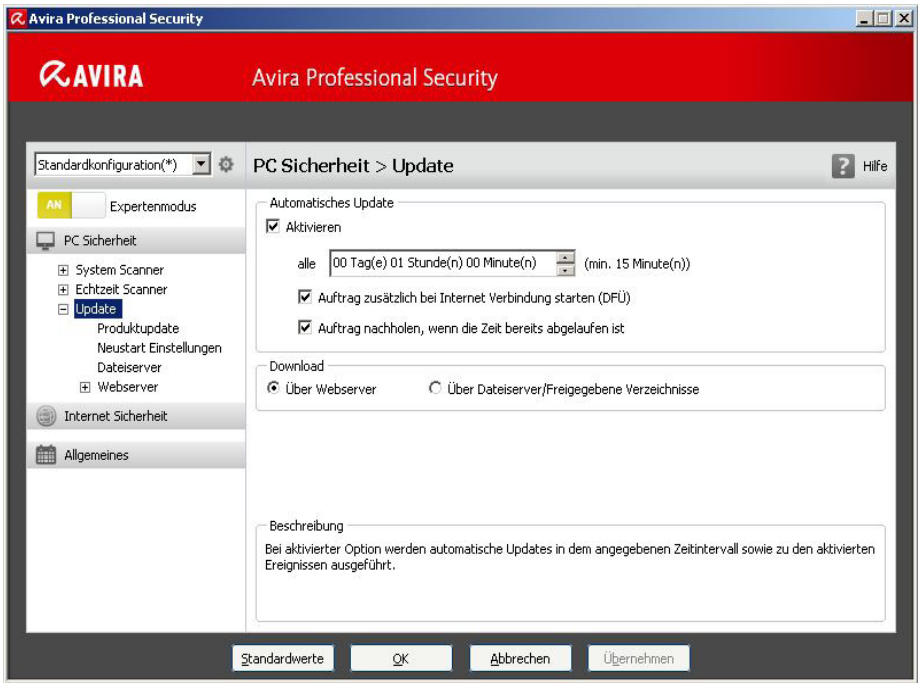
Diese Software können Sie entweder auf einem normalen Arbeitsplatzrechner oder einem Server installieren. Für detaillierte Informationen zur Installation und Konfiguration des Avira Update Managers lesen Sie bitte im entsprechenden Handbuch nach, welches Sie ebenfalls unter oben genanntem Link herunterladen können.

Nach der Installation des Avira Update Managers und dessen Konfiguration lädt dieser die neuen Virendefinitionen der Avira Professional Security zu den geplanten Zeiträumen herunter und speichert sie in seinem Wurzelverzeichnis.

Da der Avira Update Manager gleichzeitig auch einen integrierten Webserver mit dem Port 7080 bereitstellt, können nun alle Workstations im lokalen Netzwerk eine Verbindung zu diesem Verzeichnis aufbauen und sich dort ihre Updates laden.

Um die Avira Professional Security hierfür zu konfigurieren, gehen Sie bitte wie folgt vor:

Öffnen Sie die Konfiguration von Avira Professional Security und aktivieren Sie den „Expertenmodus“.
Gehen Sie im Menübaum auf den Punkt „Allgemeines“ und den Unterpunkt „Update“.
Wählen Sie hier beim Punkt „Download“ die Option „Über Webserver“.



Anschließend gehen Sie bitte auf den Punkt „Webserver“. Hier gibt es zwei Felder, „Prioritäts-Server“ und „Standard-Server“.

Avira Professional Security versucht immer zunächst den Prioritäts-Server zu kontaktieren. Sollte hier keine Verbindung möglich sein, wird versucht eine Verbindung zum Standard-Server aufzubauen.

Daher sollte für die Konfiguration der Updates über den Avira Update Manager (AUM) das Feld des Prioritäts-Servers genutzt werden. Dies ist zum Beispiel interessant, wenn Notebooks im Firmennetz verwendet werden, welche auch außerhalb des Netzwerks regelmäßig mit Updates versorgt werden sollen.

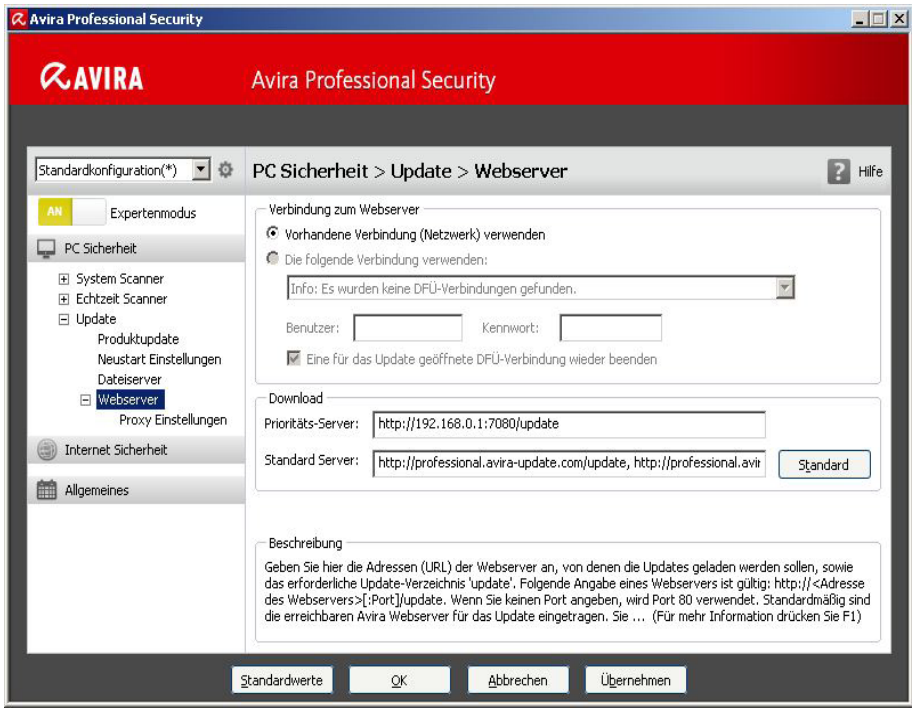
Sollte der AUM-Rechner einmal nicht online sein, wird Avira Professional Security automatisch mit den Standard-Servern versuchen, Kontakt aufzunehmen, sofern Sie sowohl Prioritäts-Server (AUM-Adresse) als auch Standard-Server (Avira-Downloadserver) konfiguriert haben.

Der Eintrag, welchen Sie in diesem Feld nun vornehmen müssen, sieht allgemein beschrieben wie folgt aus:

http:///[IP-Adresse des AUM-Rechners]:7080/update

also beispielhaft so:

http:///192.168.2.1:7080/update



Sie können den Port des Avira Update Managers auch ändern, falls dieser Port in Ihrem Netzwerk schon vergeben sein sollte. Doppelklicken Sie hierfür im Navigationsmenü des Avira Update Managers auf den jeweiligen Server *(Standardmäßig „localhost“)* > *Einstellungen* > *Network*.

Hier können Sie dann den Port des Servers von 7080 auf den von Ihnen gewünschten Port umstellen. Entsprechend ändert sich dann auch der Eintrag, welchen Sie in der Updatekonfiguration von Avira Professional Security vornehmen müssen.

Es ist wichtig, dass der gewählte Port im ganzen Netzwerk und in jeder Firewall der Arbeitsplatzrechner freigegeben wird.

2.3 Produktupdates konfigurieren

In den Konfigurationseinstellungen zum Update von Avira Professional Security finden Sie den Punkt der „Produktupdates“. Avira stellt in unregelmäßigen Abständen Aktualisierungen der Software bereit, um aufgetretene Programmfehler zu beheben oder neue Funktionen anzubieten.

Bei der Einstellung „automatische Produktupdates“, sollten Sie beachten, dass dies mitunter einen *Neustart* mit sich bringt. Dieser wird von Avira Professional Security automatisch initiiert, um den Virenschutz nicht zu unterbrechen.

Sie umgehen diesen erzwungenen Neustart, indem Sie „Benachrichtigen, wenn neue Produktupdates verfügbar sind“ auswählen. Dies konfigurieren Sie über die Konfiguration von Avira Professional Security unter dem Punkt *Allgemeines* > *Update* bei den Optionen zum Punkt „Produktupdates“.

Anschließend können Sie planen, wann dieses Produktupdate installiert werden soll, z.B. in einem Zeitfenster, wo der PC gefahrlos neu booten kann.

2.4 Ausnahmen setzen

Avira Professional Security ist teilweise sehr eng mit dem Betriebssystem verzahnt. Besonders der Echtzeit-Scanner überprüft während des Echtzeitscans die Dateien bei jedem Schreib- oder Lesezugriff.
Deshalb ist es empfehlenswert, bestimmte Programme und deren Prozesse von der Suche mit Avira auszunehmen.

Hierzu gehören z.B. alle Programme, welche mit einer Datenbank im Hintergrund operieren wie Buchhaltungsprogramme oder Finanzsoftware.

Ebenso sind hiervon besonders Backup-Programme betroffen, welche eine Datensicherung Ihres Systems durchführen. Hierbei erfolgt ein Lesezugriff auf alle Dateien Ihres Rechners und der Echtzeit-Scanner prüft laufend jede einzelne Datei, welche das Backupprogramm sichert. Dies kann die Performance Ihres Rechners negativ beeinflussen.

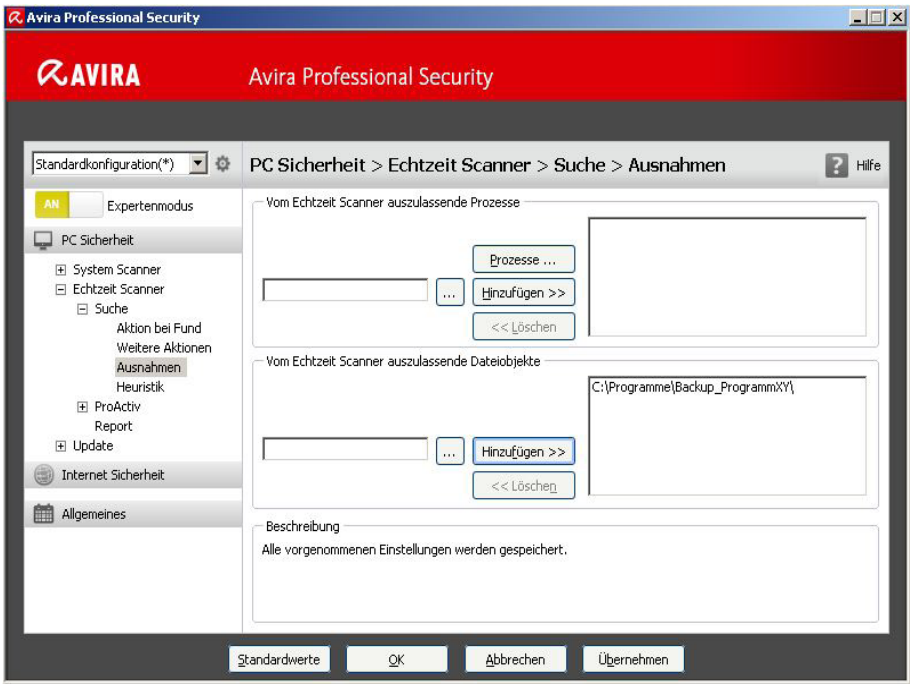
Um ein Verlangsamen Ihres Systems zu vermeiden und derartige Programme von der Suche auszunehmen, gehen Sie bitte wie folgt vor:

- Rufen Sie die Konfiguration von Professional Security auf
- Wechseln Sie in den „Expertenmodus“
- Öffnen Sie im Menübaum die Punkte „Echtzeit-Scanner“ und „Suche“
- Wählen Sie hier den Punkt „Ausnahmen“

Unter dem Punkt „Vom Echtzeit-Scanner auszulassende Dateiobjekte“ müssen Sie nun die Pfade der Programmordner angeben, in welchen die betroffene Software installiert ist. Es ist wichtig, dass am Ende der Pfadangabe ein abschließender „\“ steht, damit Avira den Pfad als Verzeichnis und nicht als Datei erkennt.

Beispielhaft sieht eine Pfadangabe dann so aus:

C:\Programme\Backup_ProgrammXY



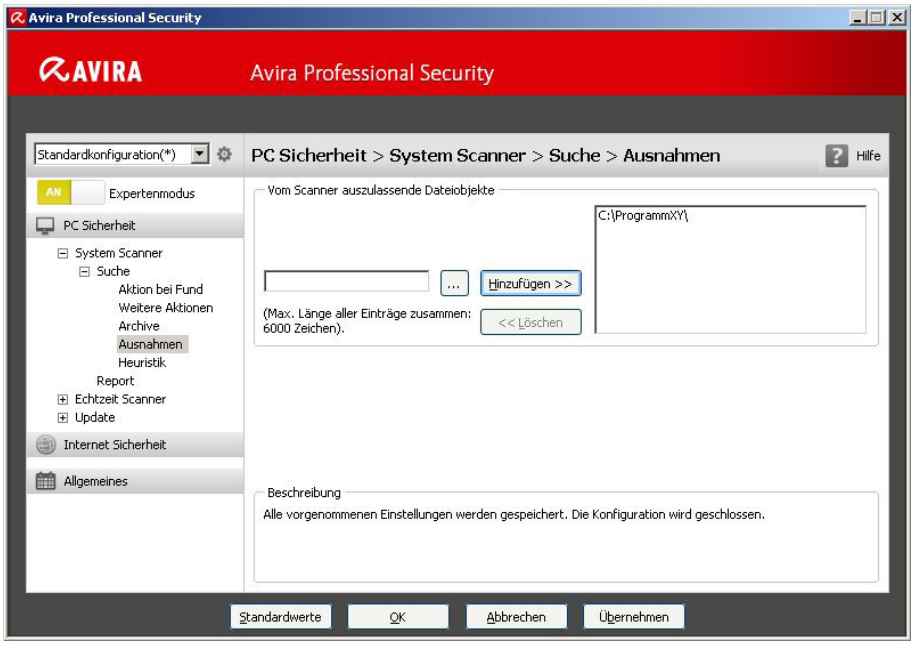
Darüber hinaus ist es beim Echtzeit-Scanner wichtig, die Prozesse der jeweiligen auszunehmenden Software ebenfalls von der Suche auszuschließen.

Gerade diese laufenden Prozesse, wie z.B. von Backupsoftware initialisieren Zugriffe auf Dateien. Wird also der Prozess an sich nicht ausgenommen, greift der Echtzeit-Scanner bei jedem Lesezugriff mit ein.

Stellen Sie daher bei aktivierter Software über Ihren Taskmanager fest, welche Prozesse die Software verwendet und tragen Sie diese unter „Vom Echtzeit-Scanner auszulassende Prozesse“ ein.

Wird lediglich das Programmverzeichnis als Dateiobjekt von der Echtzeit-Scannersuche ausgenommen, bedeutet dies, dass der Echtzeit-Scanner in diesem Verzeichnis nicht aktiv werden wird. Dies betrifft jedoch nicht alle aktiven Prozesse im Taskmanager.

Für das Ausführen des Scanners ist es ebenfalls wichtig, hier die Programmordner der betroffenen Software von der Scannersuche auszunehmen. Dies geschieht unter dem Punkt *Scanner* > *Suche* > *Ausnahmen* analog zu den Einstellungen im Echtzeit-Scanner:



2.5. Konfigurationsprofile

Avira Professional Security bietet die Möglichkeit, mehrere Konfigurationsprofile anzulegen. Ein Konfigurationsprofil ist ein komplettes Set von Konfigurationseinstellungen, das per Mausklick oder automatisch gewechselt werden kann. Konfigurationsprofile sind besonders hilfreich in Unternehmensnetzwerken, in denen z.B. auch Notebooks eingesetzt werden.

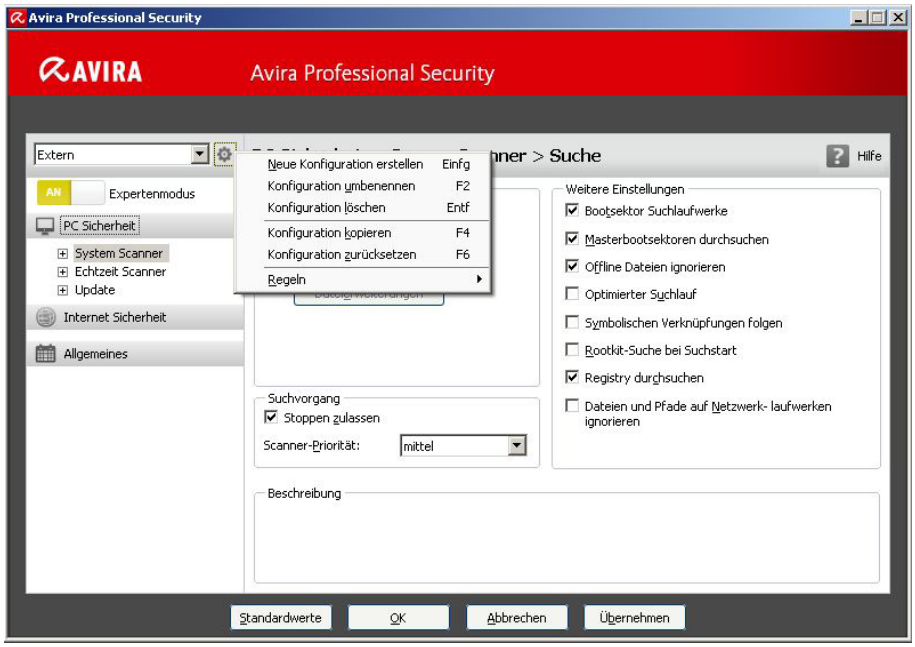
War es bislang für diese Geräte nur möglich, beim Update über Standard- und Prioritäts-Server die Updates zu planen, kann man nun für diese Geräte zwei komplett individuelle Profile mit unterschiedlichen Konfigurationen anlegen.

Beispielsweise eines für die Verwendung innerhalb des Firmennetzwerks und eines, welches aktiv werden soll, sobald das Notebook außerhalb der Firma ist.

Wird im Unternehmen ein Proxy verwendet um Updates zu laden bzw. wird im Unternehmen der Browser Schutz oder Email Schutz nicht benötigt, so kann dies in einem speziellen Profil eingestellt werden. Die Optionen ändern sich dann mit dem Profilwechsel, sobald das Notebook das interne Firmennetz verlässt.

Um ein neues Konfigurationsprofil zu erstellen und zu konfigurieren gehen Sie bitte wie folgt vor:

- Öffnen Sie die Konfiguration von Professional Security
- Klicken Sie auf den linken oberen Button für „Neue Konfiguration erstellen“ (siehe Screenshot)
- Definieren Sie einen Namen für das Profil und konfigurieren es am besten im Experternmodus



Für den Wechsel zwischen den Profilen gibt es nun mehrere Möglichkeiten, sogenannte Regeln, die gesetzt werden können.
Die Profile lassen sich manuell oder automatisch wechseln, je nachdem, in welchem Netzwerk sich der Rechner befindet.

Der manuelle Wechsel zwischen Konfigurationsprofilen erfolgt über das Kontextmenü im System Tray (durch Rechtsklick auf das Symbol). Dort finden Sie den Punkt „Profil wechseln“ zur Auswahl eines anderen Profils.

Für das automatische Wechseln muss in der Konfiguration der Professional Security eine Regel definiert werden, welche festlegt, wann ein bestimmtes Profil aktiviert werden soll.

Um die entsprechenden Regel zu setzen, klicken Sie bitte mit der rechten Maustaste auf das entsprechende Profil in der Konfiguration und wählen den Punkt „Regeln“.
Hier gibt es folgende Punkte: „Keine“, „Standardregel“ und „Standard-Gateway“.

Diese Regeln beziehen sich alle auf die IP-Adresse des Standard-Gateways.
Sie werden vom Dienst des Avira Planers überwacht, der automatisch auf das entsprechende Profil umschaltet, sobald die definierte Regel erfüllt ist.

Mit der Regel „Standard-Gateway“ sollte immer jenes Profil ausgewählt werden, welches im internen Firmennetz betrieben wird.

Sobald der Rechner aus dem Netzwerk entfernt wird, ändert sich damit auch das Gateway und Avira Professional Security wird automatisch auf das Profil umschalten, welches die Regel „Standardregel“ erhalten hat.

Für den Fall, dass ein Notebook an zwei oder sogar drei Firmenstandorten mit jeweils unterschiedlichen Netzwerkkonfigurationen eingesetzt wird, können Sie auch für diesen Fall eigene Konfigurationsprofile einstellen und jedes über eine eigene „Standard-Gateway“-Regel dem jeweiligen Netzwerk zuweisen.

3. Aufträge im Planer anlegen

Die Avira Professional Security besitzt einen integrierten Planer zur Planung von einmaligen oder wiederkehrenden Aufgaben wie z.B. Updates oder Suchläufe.

Diesen Planer sollten Sie nach der erstmaligen Installation einrichten, damit Updates und Suchläufe automatisiert durchgeführt werden.

Starten Sie dazu das „Avira Control Center“ und wählen Sie dort den Punkt *Verwaltung* > *Planer* aus.
Wählen Sie in der Symbolleiste „Neuen Auftrag mit dem Wizard erstellen“ aus.
Definieren Sie anschließend einen Namen (z. B. Internetupdate oder wöchentlicher Suchlauf) und eine kurze Beschreibung für den Auftrag.

Stellen Sie die Art des Auftrages ein (im Falle des Updates wählen Sie bitte „Update-Auftrag“ aus, möchten Sie einen Auftrag für einen Suchlauf erstellen, wählen Sie „Prüfauftrag“).

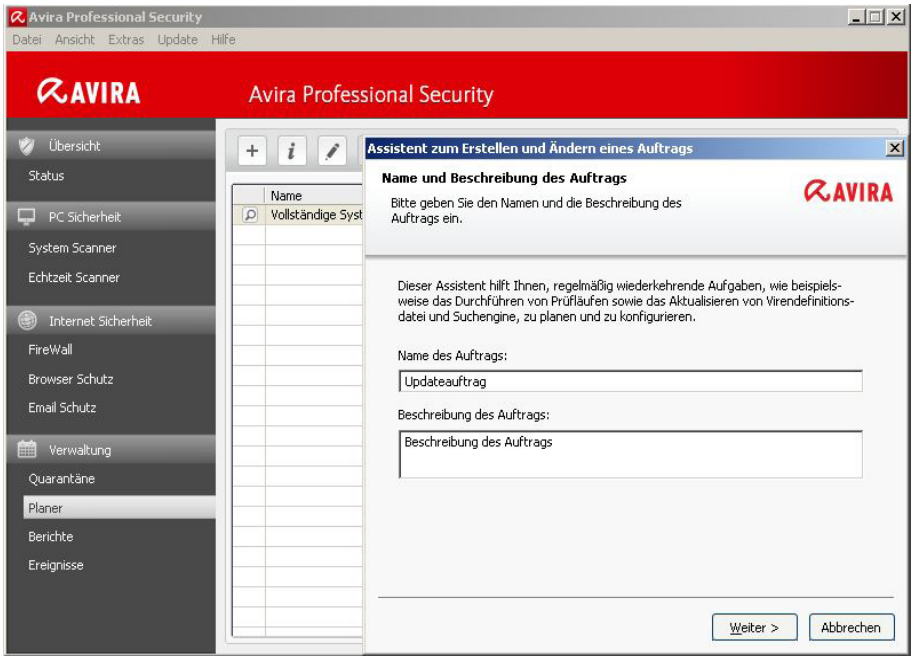
Bei einem „Prüfauftrag“ können Sie anschließend definieren, mit welchem Profil dieser durchgeführt werden soll. Weitere Informationen zum Thema Suchprofile finden Sie im Abschnitt 4 dieses Dokuments.

Konfigurieren Sie anschließend, wann der Auftrag ausgeführt werden soll (z.B. Sofort / Täglich / Wöchentlich / Intervall / Einmalig).

Abschließend definieren Sie, in welchem Darstellungsmodus der Auftrag durchgeführt wird. Im Darstellungsmodus „unsichtbar“ läuft der gesamte Prozess im Hintergrund ab.

Der Modus „minimiert“ erzeugt ein kleines Kontrollfenster auf dem Desktop, welches Sie über den Fortschritt der Aktion informiert. Der Modus „maximiert“ erzeugt ein größeres Fenster mit zusätzlichen Detailinfos zum laufenden Auftrag.

Prüfen Sie bitte, ob der Auftrag als „Aktiviert“ in der Übersicht angezeigt wird. Der entsprechende Haken muss hierfür gesetzt sein.



Hinweis
Wir empfehlen Ihnen beim Update ein stündliches Intervall und einen wöchentlichen Prüfauftrag.

Wir nehmen täglich ca. 5 Updates unserer Virendefinitionen/Engine vor. Durch stündliche Updates können Sie sichergehen, dass Ihr Schutz auch wirklich noch aktuell ist. Die wöchentliche Systemprüfung dient außerdem der maximalen Sicherheit.

Zu häufige Suchläufe würden eventuell die Systemperformance zu stark belasten. Zu seltene Suchläufe bringen die Gefahr, dass sich neue Viren auf dem PC einnisten, die eventuell kurz nach dem Suchlauf erkannt würden.

Wird nur alle paar Wochen oder gar Monate einmal eine Systemprüfung durchgeführt, wird dieser Virus trotz aktuellstem Schutz möglicherweise erst dann von Avira entdeckt, sofern ihn der Echtzeit-Scanner nicht vorher aufgespürt hat.

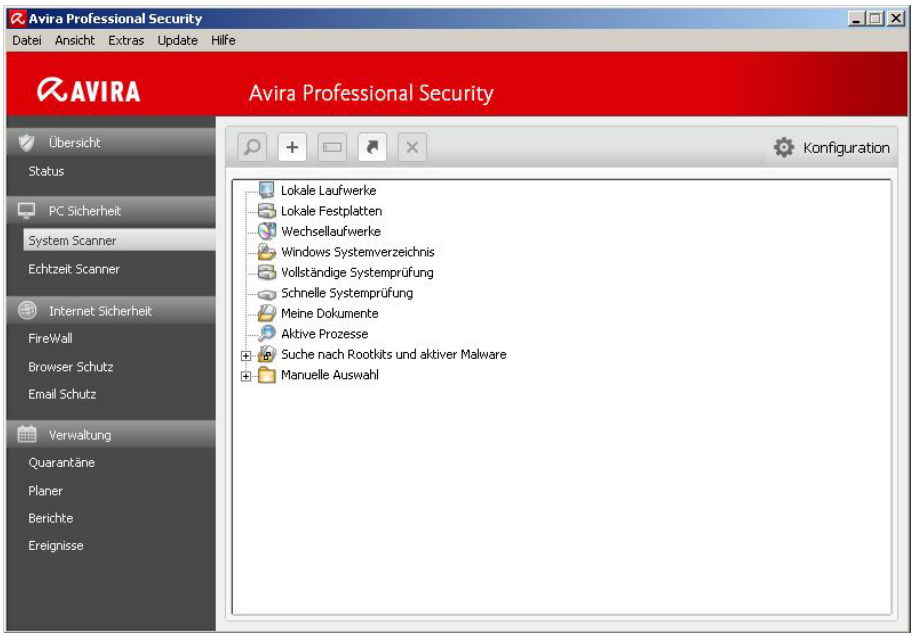
Daher stellt eine wöchentliche Systemprüfung ein ausgewogenes Verhältnis aus geringer Performancebelastung und optimaler Sicherheit des Systems dar.

4. Verschiedene Suchprofile

Im Falle eines vermuteten Virenbefalls oder zur allgemeinen, schnellen Sicherstellung, dass das System frei von Viren ist, hat Avira vordefinierte Suchprofile erstellt und die Möglichkeit gegeben, eigene Suchprofile anzulegen.

Mithilfe dieser Profile ist es möglich, die Virensuche des Scanners effektiver auszuführen, so dass nur spezielle Bereiche bzw. Laufwerke oder Verzeichnisse des Systems überprüft werden.
Im Folgenden geben wir zunächst einen Überblick über die vordefinierten Suchprofile, sowie die Möglichkeit, die Suche auf die eigenen Bedürfnisse anzupassen.

Sie finden die Profile zur Scannersuche unter dem Punkt „Lokaler Schutz“ und dem Unterpunkt „Prüfen“ im Kontrollcenter von Avira Professional Security.



Die Auswahl des richtigen Suchprofils richtet sich danach, welche Dateien durchsucht werden sollen bzw. für die Suche ausgelassen werden können.

Besteht ein genereller Virenverdacht, der aber auf die lokalen Festplatten eingegrenzt werden kann, verkürzt das Profil „Lokale Festplatten“ erheblich den Suchlauf. Bei der Auswahl „Lokale Laufwerke“ werden auch CD-Laufwerke sowie Wechselmedien durchsucht.

Neue, unbekannte USB-Sticks, die am Rechner eingesteckt werden, sollten auch geprüft werden. Da hierbei keine vollständige Systemprüfung notwendig ist, kann man mit dem Profil „Wechsellaufwerke“ speziell diesen Laufwerkstyp abdecken und sicherstellen, dass auf den neu angeschlossenen Geräten kein Virus enthalten ist.

Bei Verdacht auf einen Virenbefall kann man prüfen, ob dieser Virus gerade als aktiver Prozess läuft. Mit dem Suchprofil „Aktive Prozesse“ werden nur die derzeit in Ausführung stehenden Prozesse gescannt.

Die folgende Liste zeigt eine Übersicht der vordefinierten Profile und mögliche Szenarien, bei denen diese Anwendung stattfinden kann:

Suchprofil	Erklärung	Szenario
Lokale Laufwerke	Dieses Profil überprüft alle lokalen Laufwerke	Bei Virenverdacht, wenn unklar ist, auf welchem Laufwerk der Virus sich befindet.
Lokale Festplatten	Dieses Profil überprüft nur die lokalen Festplattan auf Ihrem System	Falls man sicher ist, dass der Virus auf den Festplatten ist und nicht auf Wechselmedien und man diese gezielt prüfen möchte
Wechsellaufwerke	Dieses Profil überprüft alle verfügbaren Wechsellaufwerke	Falls man schnell verifizieren will, ob hinzugefügte Wechselmedien virenfrei sind.
Windows Systemverzeichnis	Überprüft nur das Systemverzeichnis von Windows (C:\Windows\System32)	Falls man sicher gehen will, dass die Systemdateien von Windows sauber sind. Viele Viren schreiben sich in das Systemverzeichnis, somit ist dies eine erste Anlaufstelle im Verdachtsfall
Vollständige Systemprüfung	Führt vollständige Prüfung mit speziellen Suchoptionen durch und wird mit der GUI (Server-Übersicht) synchronisiert	Falls unbekannt ist, ob und wo ein Virus sich eingenistet hat
Meine Dokumente	Überprüft Ordner „Eigene Dateien“ des jeweils angemeldeten Benutzers	Standardmäßig speichert Windows Downloads etc. z.B. in den Eigenen Dateien des Nutzers. Somit kann auch hier gezielt gesucht werden
Aktive Prozesse	Überprüft alle aktiven Prozesse	Prüft, ob sich unter den laufenden Prozessen ein Virus befindet
Suche nach Rootkits	Überprüft System auf aktive Rootkits (Software, die nach dem Einbruch in das Computersystem mit den herkömmlichen Methoden der Malware-Erkennung nicht gefunden werden kann).	Im konkreten Verdachtsfall anzuwenden

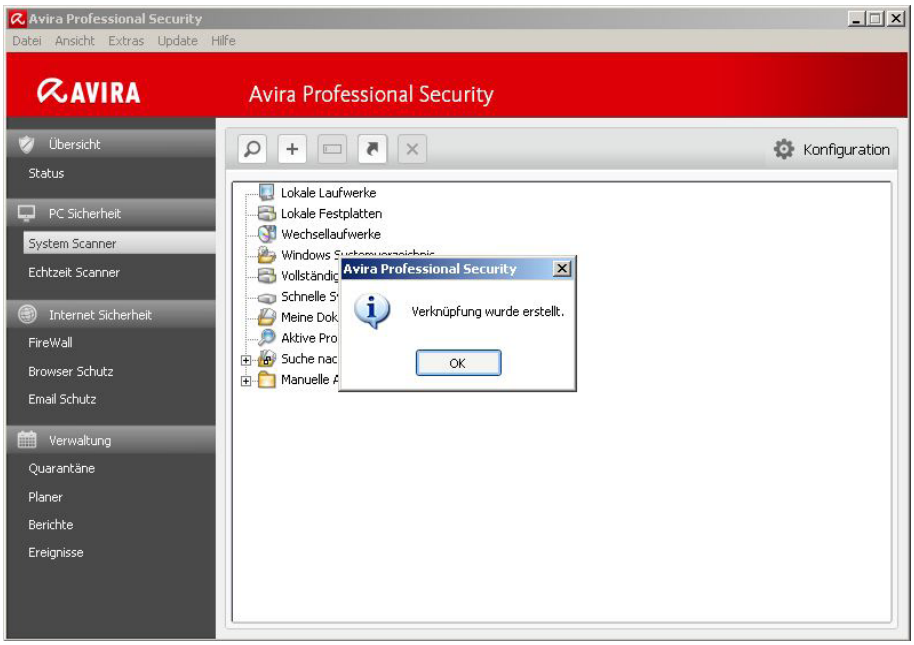
Um die Suche auf speziellen Laufwerken und Verzeichnissen manuell einzustellen, gibt es neben dem Standardprofil „Manuelle Auswahl“ auch noch die Möglichkeit, sich eigene Suchprofile zu erstellen. Diese sind dann ebenso konfigurierbar, wie die manuelle Auswahl.

In der manuellen Auswahl und in eigens erstellen Suchprofilen haben Sie zudem die Möglichkeit, bestimmte Dateitypen von der Suche auszunehmen oder diese explizit durchsuchen zu lassen.

Klicken Sie mit der rechten Maustaste auf das jeweilige Suchprofil und wählen Sie die Option „Dateifilter“ aus. Über den Punkt „Benutzerdefiniert“ können nun Dateiendungen aus der Liste gelöscht oder hinzugefügt werden.

Für ein spezielles Suchprofil können Sie auch eine Verknüpfung anlegen, durch welche mit nur einem Klick vom Desktop aus z.B. alle Wechsellaufwerke durchsucht werden können.

Sie können die selbst erstellten Profile im Planer verwenden, um gezielt jene Verzeichnisse prüfen zu lassen, welche Sie vordefiniert haben, z.B. ein spezielles lokales Laufwerk auf welchem häufig externe Daten hinzugefügt werden und ein Netzlaufwerk, welches mit dem PC verbunden ist und das ebenfalls geprüft werden soll.



5. Quarantäne

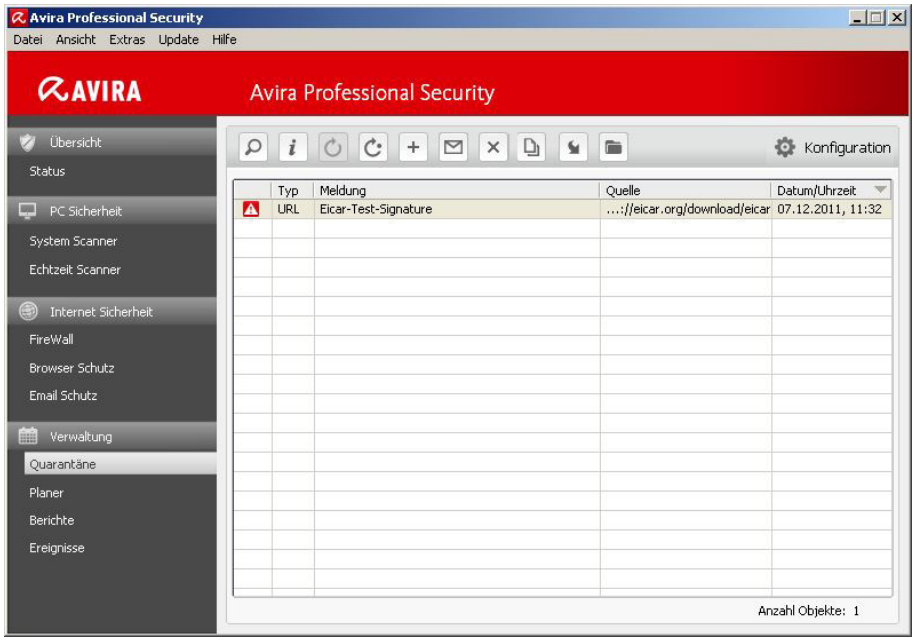
Wird bei einem Suchlauf ein Virus oder eine verdächtige Datei gefunden, wird dieser bei entsprechender Einstellung in die Quarantäne verschoben.
Die Datei wird in ein speziell verschlüsseltes Format (*.qua) gepackt und in das Quarantäne - Verzeichnis INFECTED auf Ihrer Festplatte verschoben, sodass kein direkter Zugriff mehr möglich ist.

Dieses Verzeichnis befindet sich standardmäßig bei Windows2000 / XP unter:
C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir Desktop\INFECTED

Bei Windows Vista / Windows 7 befindet sich dieses Verzeichnis unter:
C:\ProgramData\Avira\AntiVir Desktop\INFECTED

Dateien in diesem Verzeichnis können später im Quarantänemanager repariert oder falls nötig an das Avira Malware Research Center geschickt werden.

In die Quarantäneverwaltung der Avira Professional Security gelangen Sie, indem Sie das Avira Control Center starten und den Punkt *Verwaltung* > *Quarantäne* auswählen.



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

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

Bei heuristischen Treffern beginnt der Name des Fundes entweder mit „HEUR/..“, um einen Treffer der Advanced Heuristic Analysis and Detection (AHeAD) anzuzeigen oder endet auf „.gen“, falls es sich um eine generische Datei handelt.
Eine generische Erkennungsroutine wird verwendet, um gemeinsame Familienmerkmale der verschiedenen Varianten zu erkennen.

Diese generische Erkennungsroutine wurde entwickelt, um unbekannte Varianten bereits bekannter Viren zu erkennen und wird kontinuierlich weiterentwickelt.
Bei einem heuristischen Fund der AHeAD hingegen ist die Datei aufgrund ihres Verhaltens auffällig geworden.

Es handelt sich hierbei also nicht zwangsweise um eine infizierte Datei sondern nur um einen Fund, der eventuell einen neuen, noch nicht bekannten Virus darstellt. Daher sollte auch dieser Fund zur Analyse eingesendet werden.

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

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

Hinweis
Die Größe der Dateien die Sie hochladen, ist begrenzt auf 20 MB ungepackt oder 8 MB gepackt.
Sie können mehrere Dateien gleichzeitig hochladen, indem Sie alle Dateien die Sie hochladen möchten, markieren und dann auf die Schaltfläche „Objekt senden“ klicken.

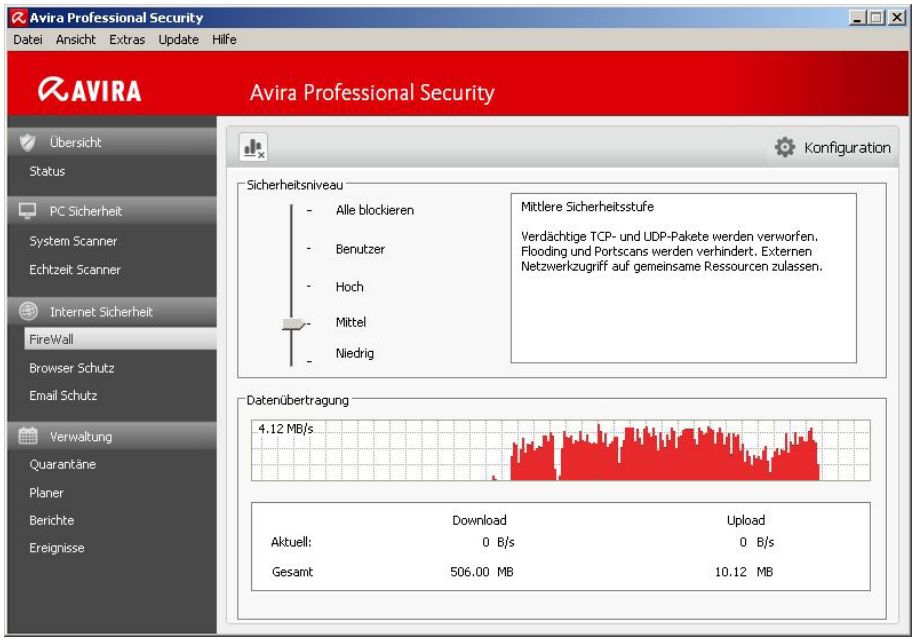
Sie sollten zudem nach 5 bis 10 Tagen ein Update auf die neuesten Virendefinitionen machen und die verdächtigen Objekte in der Quarantäne markieren und erneut prüfen lassen (Taste „F2“ drücken oder Rechtsklick und „Objekt erneut prüfen“).

Sollten die Dateien immer noch gemeldet werden, sind es aller Wahrscheinlichkeit nach echte Viren und können gelöscht werden. Werden sie nicht länger gemeldet, so hat es sich um Fehlalarme gehandelt und Sie können die Objekte wiederherstellen.

6. Avira FireWall

Seit Avira Professional Security 10 ist eine Desktop-Firewall integriert. Mit dieser Komponente haben Sie die Möglichkeit, ein- und ausgehenden Internetverkehr zu kontrollieren. Zum einen gibt es einen Schieberegler, mit dem man ein vordefiniertes Sicherheitsniveau einstellen kann.

Standardmäßig ist das Sichheitsniveau auf „Mittel“ eingestellt, damit der Rechner im Netzwerk gesehen werden kann und damit die Datei- und Druckerfreigabe funktioniert.



Zum anderen stehen Ihnen vordefinierte Adapter- und Anwendungsregeln zur Verfügung, welche natürlich auch individuell angepasst bzw. erweitert werden können.

Wollen Sie z.B. den Firefox Browser hinzufügen, gehen Sie folgendermaßen vor:

Öffnen Sie die Konfiguration und navigieren dort unter *FireWall* > *Anwendungsregel* > *Anwendung hinzufügen*.

Nun öffnet sich ein Fenster und listet Ihnen alle Anwendungen auf, die vor kurzem benutzt wurden. Wird die von Ihnen gesuchte Anwendung nicht aufgezeigt, können Sie danach suchen, indem Sie „Nach weiteren Anwendungen suchen“ auswählen.

Anschließend ist die Anwendung als neue Regel hinzugefügt und man kann definieren, wie diese von der Avira FireWall behandelt wird.

Hier wird zwischen verschiedenen Modi bzw. Aktionen unterschieden:

Modus:

- *Privilegiert:* Anwendungen werden unabhängig von den Adapterregeln bzw. Sicherheitsniveau behandelt. D.h. erst werden die Anwendungsregeln, dann die Adapterregeln beachtet

- *Gefiltert*: Erst werden die Adapterregeln, dann die Anwendungsregeln beachtet. Sollte also ein Port in den Adapterregeln gesperrt sein (z.B. Port 80), können Anwendung diesen Port nicht zur Kommunikation nutzen (z.B. Webbrowser).

Aktion:

- *Erlauben:* Anwendung darf mit dem Internet kommunizieren
- *Ablehnen:* Anwendung darf nicht mit dem Internet kommunizieren
- *Fragen:* Der Benutzer wird gefragt, welche der oben genannten Aktionen ausgeführt werden soll.

7. Quicktipps

7.1 Vorgehensweise bei Virenbefall

Sollte der Echtzeit-Scanner oder der Scanner einen Virus auf Ihrem System erkannt haben, empfiehlt es sich, das komplette System gründlich nach weiteren infizierten Dateien überprüfen zu lassen. Da im normalen Betrieb von Windows viele Programme exklusiven Schreib – und Lesezugriff auf Dateien besitzen, ist ein Suchlauf im abgesicherten Modus sinnvoll.

Sie gelangen in den abgesicherten Modus, indem Sie Ihr System neu starten und beim Bootvorgang die Taste F8 drücken. Danach wählen Sie im erscheinenden Menü den Punkt „im abgesicherten Modus starten“.

Hierbei erhält der Scanner von Avira alle nötigen Schreibrechte auf alle System – und Programmdateien und kann bei einem Fund Dateien gegebenenfalls reparieren, sofern eine Reparaturroutine für den betreffenden Virus hinterlegt ist.

Bitte achten Sie im Vorfeld darauf, dass Sie die Systemwiederherstellung von Windows deaktiviert haben. Sie deaktivieren diese unter *Start* > *Programme* > *Zubehör* > *Systemprogramme* > *Systemwiederherstellung*.

7.2 Web-Filter des Browser Schutz

Der Browser Schutz sperrt in der Standardeinstellung Seiten, welche bekanntermaßen Spam, Malware oder Phishing beinhalten. Darüber hinaus werden auch Betrugsseiten sogenannter „Abofallen“ gesperrt, sowie Seiten, welche auf diese Seiten verlinken.

Hierbei handelt es sich um Angebote für Dienstleistungen mit geringem bis nichtigem Wert, für welche eine versteckte aber nicht statthafte Gebühr erhoben wird. Dieser Fakt ist bei diesen Seiten meist nur in den AGBs ersichtlich, weshalb der Anspruch der Betreiber auf Zahlung laut Verbraucherschutz nicht gegeben ist.

Über das Setzen von Ausnahmen bzw. das Deaktivieren einzelner Webfilter-Gruppen kann die Sperrung von Seiten in diesem Webfilter aufgehoben werden.
Gehen Sie hierzu in die Konfiguration von Avira Professional Security, aktivieren Sie den Expertenmodus und klicken Sie im Menüstamm auf *Browser Schutz* > *Suche* > *Gesperrte Zugriffe*.

Hier sehen Sie den Punkt „Web Filter aktivieren“ und darunter die einzelnen Kategorien, welche Sie nun an- oder abwählen können.

7.3 LSP Reset bei Problemen mit Browser- und Email Schutz

Sollte es zu Problemen mit dem Browser Schutz oder Email Schutz kommen, z.B. dass die Module beim Systemstart nicht mehr starten oder sich gar nicht mehr starten lassen, hängt dies oft mit Fehlern im LSP zusammen (Layered Service Provider, ein Programm das sich im TCP/IP-Socket befindet).

Hierbei kann es helfen, die Module komplett zu deinstallieren und danach den LSP auf Ausgangswerte zurückzusetzen. Zum Reparieren wird hierfür eine CMD-Console benötigt, in welcher ‚netsh winsock reset' eingegeben werden muss.
Danach muss der Rechner neu gestartet werden und Email Schutz und/oder Browser Schutz können neu installiert werden.

Hinweis
Hierfür darf kein Registry Schutz auf dem Rechner bestehen. Sollten zudem andere Programme noch Eintragungen im LSP vorgenommen haben, wären diese damit auch gelöscht, was bedeutet, dass diese Programme nach einem LSP Reset nicht mehr korrekt arbeiten würden.

Ein Beispiel hierfür wäre z.B. AVM FritzProtect, welches einen Eintrag im LSP mit dem Namen „Sarah LSP" erzeugt, ohne den das Programm nicht funktioniert.

Um festzustellen, welche Eintragungen sich im LSP befinden, können Sie unseren Supportcollector benutzen welcher den LSP-Stack ausliest.

7.4 Protokolle die vom Email Schutz überprüft werden können

Der Email Schutz dient zur permanenten Kontrolle Ihrer Emails auf Viren und Malware; inklusive Überprüfung der Email-Anhänge.

POP3 (eingehende Emails) werden standardmäßig (falls der Email Schutz installiert wurde) überprüft.
Eine SMTP Überprüfung (ausgehende Emails durchsuchen) können Sie ebenfalls in der Konfiguration der Professional Security unter *Konfiguration* > *Email Schutz* aktivieren.

Die Überprüfung über das Protokoll IMAP ist ebenfalls möglich, diese können Sie in der Konfiguration der Avira Professional Security unter *Konfiguration* > *Email Schutz* > *IMAP-Konten überwachen* aktivieren.

Im Gegensatz zum Protokoll POP3 verbleiben die Emails auf dem Server und werden dort verwaltet.

7.5 Manuelles Einfügen der Lizenzdatei

Falls Sie Ihre Lizenz verlängert haben und diese nicht über den Button „Lizenzdatei laden“ im Hauptprogramm von Professional Security laden können, besteht die Möglichkeit, diese Datei (hbedv.key) auch direkt ins Hauptverzeichnis von Avira zu kopieren (*C:\Programme\Avira\AntiVir Desktop*).

Dies hat denselben Effekt wie ein Einlesen der Datei im Programm selbst über den Punkt „Hilfe“ und „Lizenzdatei laden“.

7.6 Übernahme der Konfiguration bei mehrfacher Installation

Falls Sie Avira Professional Security auf mehreren PCs installieren und eine einmal definierte Konfiguration auch auf den anderen PCs einspielen möchten, gelingt dies über die Konfigurationsdatei „*avwin.ini*“. Sie finden diese unter folgendem Pfad:

Windows XP
C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir Desktop\CONFIG\avwin.ini

Windows 7
C:\Programm Data\Avira\AntiVir Desktop\CONFIG\avwin.ini

Sie können diese Datei nun entweder nachträglich von einem PC zum anderen kopieren und somit die Konfiguration verändern (bei deaktiviertem Prozessschutz und deaktivierten Avira Diensten) oder Sie geben bei einer Installation über die Kommandozeile, z.B. bei einem Logon-Skript den Pfad zur avwin.ini Datei an, welche dann bei der Installation eingespielt wird.

Für die automatische Installation von Avira Professional Security arbeitet das Setup-Programm mit der Steuerdatei setup.inf. Das Setup-Programm (presetup.exe) ist im Installationspaket von Avira Professional Security enthalten.

Die Setup-Datei von Professional Security ist ein selbstentpackendes WinRAR-Archiv, welches Sie mit WinRAR öffnen und dessen Inhalt so entpacken können. In diesem Archiv befinden sich auch die Dateien „presetup.exe“ und „setup.inf“ welche für die Installation im Netzwerk notwendig sind.

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.

Mit einem Login-Skript des Servers oder über AMC kann Avira Professional Security komfortabel im Netzwerk verteilt werden.

So installieren Sie Avira Professional Security 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 von Avira Professional Security mit dem Parameter /inf
- oder binden Sie den Parameter in das Login-Skript des Servers ein (Beispiele: `presetup.exe /inf="c:\temp\setup.inf"`)
- Die Installation läuft automatisch ab
- Alle Angaben zu Pfaden oder Dateien müssen in „..." gesetzt werden

7.7 Erweiterte Gefahrenkategorien

Kostenverursachende Einwahlprogramme (DIALER)
Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende PremAUM-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Einige Dialer ersetzen die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine Kosten verursachende, oft horrend überteuerte 0190/0900-Nummer an.

Spiele (GAMES)
Untersuchungen haben ergeben, dass die für Computerspiele 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.

Witzprogramme (JOKES)
Die Witzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren.
Aber Vorsicht! Alle Symptome von Witzprogrammen könnten auch von einem Virus oder einem Trojaner stammen.

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.

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.

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.

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

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.

Phishing
Phishing, auch bekannt als brand spoofing, ist eine raffinierte Form des Datendiebstahls, der auf Kunden bzw. potenzielle Kunden von Internet Service Providern, Banken, Online-Banking Diensten, Registrierungsbehörden abzielt.
Durch eine Weitergabe der eigenen Email-Adresse im Internet, das Ausfüllen von Online-Formularen, dem Beitritt von Newsgroups oder Webseiten ist es möglich, dass Ihre Daten von sog. „Internet crawling spiders“ gestohlen und ohne Ihre Erlaubnis dazu verwendet werden, einen Betrug oder andere Verbrechen zu begehen.

Anwendung (APPL)
Bei der Bezeichnung APPL handelt es sich um eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.
Avira Professional Security erkennt „Anwendung (APPL)“. Ist in der Konfiguration unter „Erweiterte Gefahrenkategorien“ die Option Anwendung (APPL) mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Avira Professional Security ein solches Verhalten bemerkt.

Ausgabe Q4-2011

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