Avira Server 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 unter

http://www.avira.com/de/support-download

1. Setupmodi

Nachdem Sie die Installationsdatei der Avira Server Security heruntergeladen haben und auf Ihrem PC entpackt haben, starten Sie zunächst die Installation der Server Security durch einen Doppelklick auf die Datei avira_server_security_de.exe.

Im anschließend erscheinenden Assistenten klicken Sie auf „weiter“.
Sie haben dann nachfolgend die Möglichkeit, einen Setup-Typ auszuwählen:

1.1 Express

Avira Server Security wird vollständig mit dem Dienst Avira Server Security und der Konsole Server Security Console installiert. Es kann kein Zielordner für die zu installierenden Programmdateien gewählt werden.

1.2 Benutzerdefiniert

Sie können wählen, ob Sie den Dienst Avira Server Security und/oder die Server Security Console installieren möchten.
Hier können Sie ebenfalls die Server Security Console auf einer Workstation installieren um Remote auf den Serverdienst zugreifen zu können.

Hinweis
Bei der Installation des Dienstes Avira Server Security: Falls Sie auf den zu schützenden Server remote mit der Server Security Konsole zugreifen möchten, stellen Sie bitte sicher, dass folgende Ports geöffnet sind:

139 (NetBIOS SSN)
137 (NetBIOS NS)
138 (NetBIOS DGM)

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

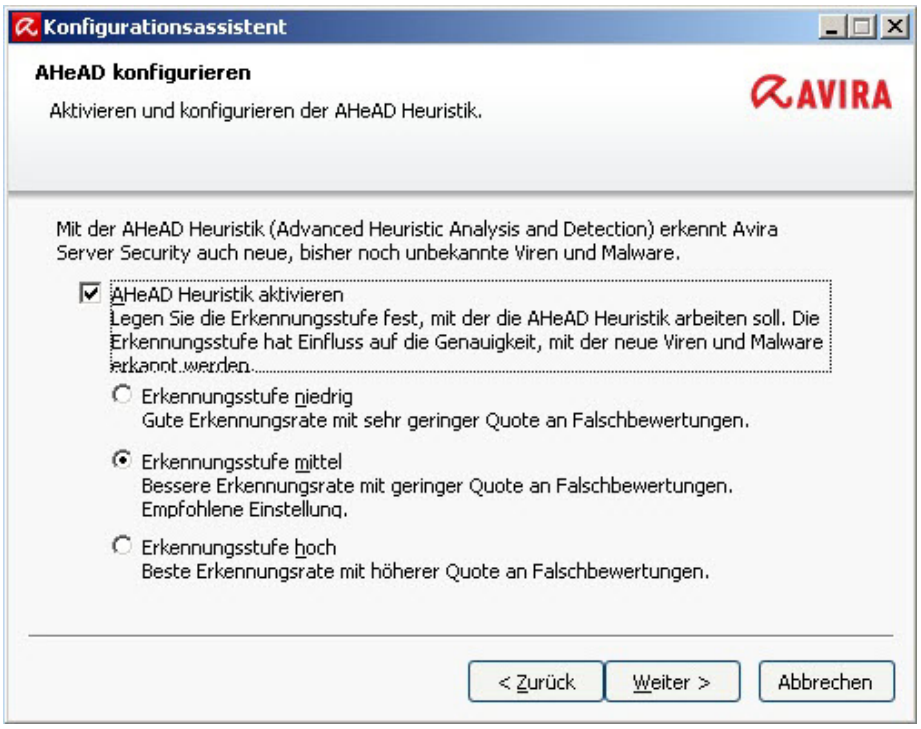
Nun erscheint das Dialogfenster „Lizenz installieren“.
Wählen Sie das Verzeichnis, in dem Sie die Lizenzdatei (hbedv.key) gespeichert haben. Alternativ können Sie auswählen, ob Sie den Server für 30 Tage testen möchten.Anschließend wird die Installation gestartet.
Ggf. wird ebenfalls die Installation des Microsoft Visual C++ 2008 - Redistributable Kit begonnen, falls das Kit nicht bereits installiert wurde.

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

Der Link zum Download des Redistributable Kit lautet:

http://www.microsoft.com/downloads/de-de/details.spx?displaylang=de&FamilyID=a5c84275-3b97-4ab7-a40d-3802b2af5fc2

Sobald Sie die Installation beendet haben, erscheint der Konfigurationsassistent. Dieser leitet Sie einmal durch die grundlegenden Einstellungen der Server Security. Im anschließenden Dialogfenster können Sie die Engine konfigurieren und die Erkennungsstufe für die AHeAD Heuristik aktivieren.
Die gewählte Erkennungsstufe wird für die Einstellung der AHeAD-Technologie des System-Scanner (Direktsuche) und des Echtzeit-Scanner (Echtzeitsuche) übernommen.



Hinweis
Bitte beachten Sie, dass eine zu hohe Erkennungsstufe zwar viele unbekannte Malware erkennt, aber Sie müssen in diesem Fall auch mit höheren Fehlerkennungen rechnen.

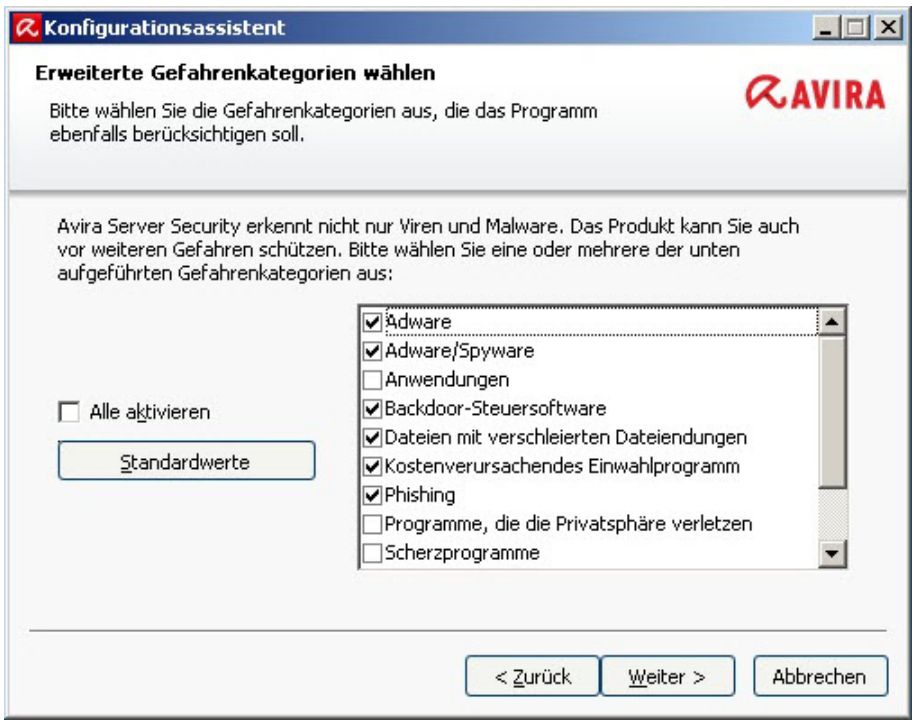
Was bedeutet der Begriff Heuristik?

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.

Dabei bedeutet dies 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.



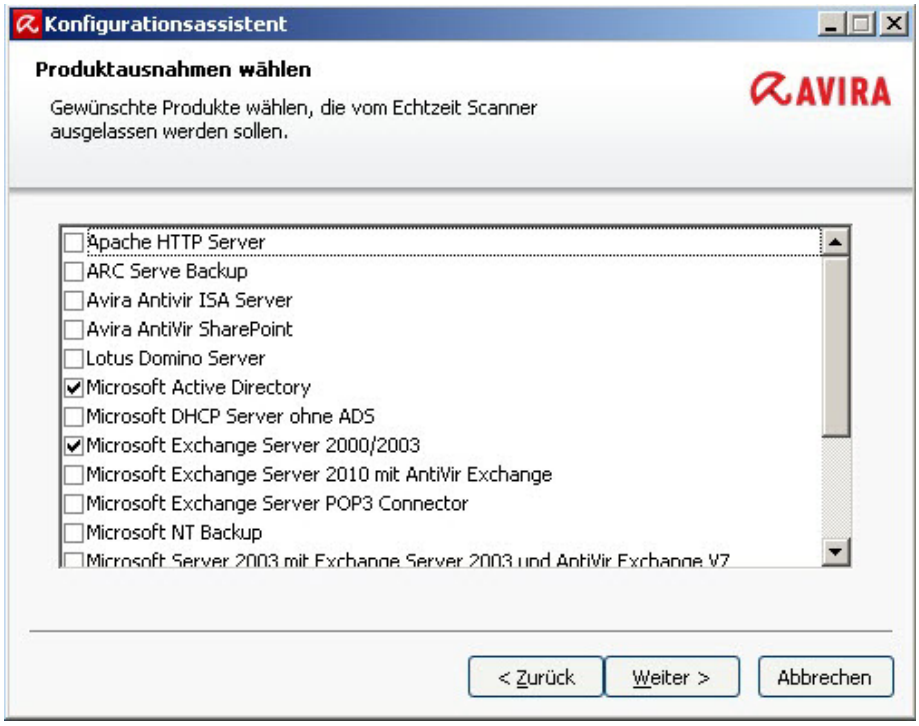
Standardmäßig sind die oben gesehenen Optionen aktiviert, da einerseits die Risiken von Adware/Spyware sowie Backdoor-Steuersoftware, Phishing und Dialern am Größten sind.

Andererseits werden aber gerade viele Administratortools von Avira als „Security Privacy Risk“ (SPR) 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 im Anschluss die gewünschten Produkte aus, die von der Überwachung des Echtzeit-Scanner (On Access Scanner) ausgelassen werden sollen. Dadurch vermeiden Sie Performanceeinbußen und Seiteneffekte, die durch den Echtzeit-Scanner entstehen können.

Dabei sind von Avira bereits die häufigsten Programme vordefiniert. Sollten Sie eines dieser Programme nutzen, nehmen Sie es bitte von der Suche durch entsprechendes Hakensetzen aus.



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

Server Security nutzt diesen Email-Versand per SMTP beim Versenden von Email-Warnungen von den jeweiligen Modulen 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.

2. Konfiguration

2.1 Updatekonfiguration zum Avira Update Manager

Falls Sie mehrere Installationen von Server Security oder 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 Traffic und belasten die Internetverbindung nicht unnötig.

Sie finden das hierfür benötigte Tool unter folgendem Link:

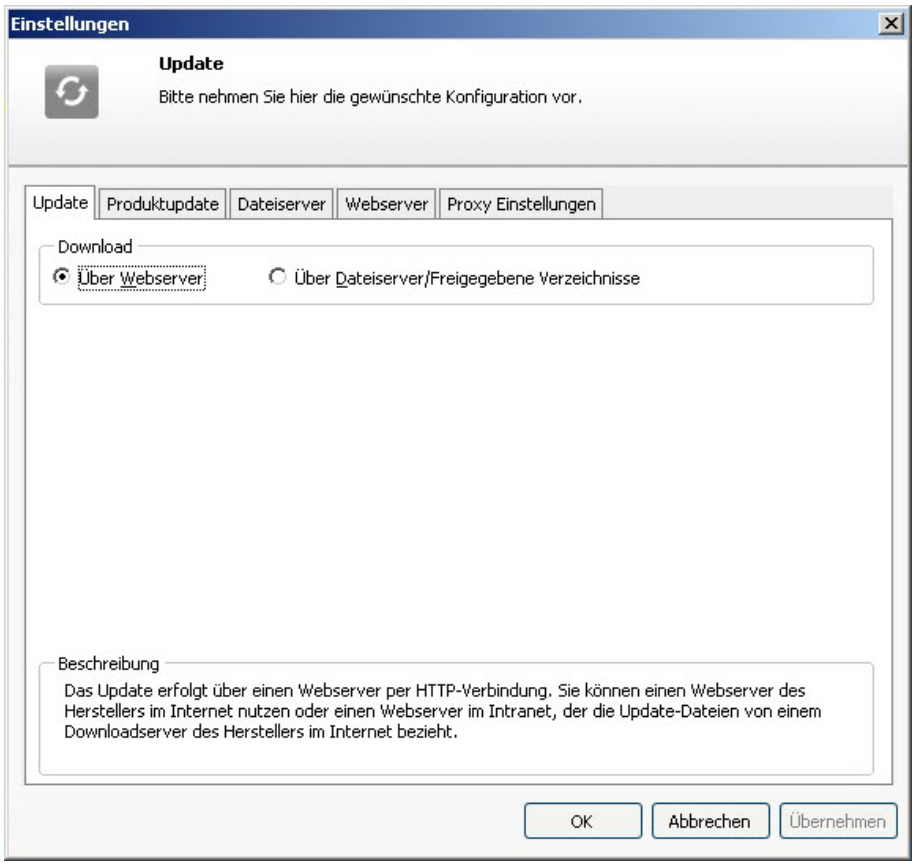
http://www.avira.com/de/support-download-avira-server-security

Diese Software können Sie entweder auf einem normalen Arbeitsplatzrechner oder einem Server installieren. Bei einem Arbeitsplatzrechner ist darauf zu achten, dass maximal 10 gleichzeitige Netzwerkverbindungen möglich sind. Für detaillierte Informationen zur Installation und Konfiguration des Avira Update Managers lesen Sie bitte im entsprechenden Handbuch nach, welches Sie ebenfalls unter obigem Link herunterladen können.

Nach der Installation des Avira Update Managers und dessen Konfiguration lädt dieser die neuen Virendefinitionen der Server 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 den Server Security hierfür zu konfigurieren, gehen Sie bitte wie folgt vor:

- Öffnen Sie die Konfiguration der Server Security
- Gehen Sie im Menübaum auf den Punkt „Einstellungen“ und „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“.

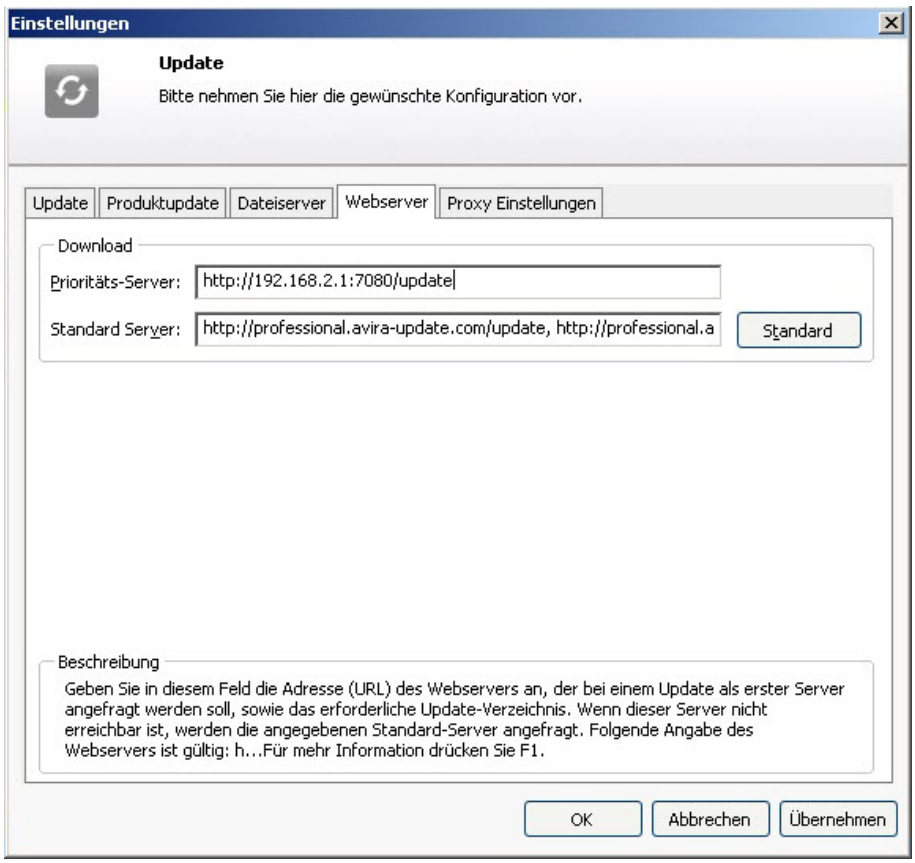
Server Security versucht immer zunächst den Prioritäts-Server zu kontaktieren. Sollte hier keine Verbindung möglich sein, wird versucht eine Verbindung zum Standard-Server aufzubauen.
Daher sollte für die Konfiguration der Updates über den Avira Update Manager (AUM) das Feld des Prioritäts-Servers genutzt 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 Server 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

Anhand eines Beispiels: 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 > Netzwerk*.

Hier kann der Port des Servers von 7080 auf den von Ihnen gewünschten Port umgestellt werden. Entsprechend ändert sich dann auch der Eintrag, welchen Sie in der Updatekonfiguration von Professional Security vornehmen müssen.
Es ist wichtig, dass der gewählte Port im ganzen Netzwerk und in jeder Firewall der Arbeitsplatzrechner freigegeben wird.

2.2 Produktupdates konfigurieren

In den Konfigurationseinstellungen zum Update von Server 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.
Wenn Sie hier einstellen, dass Sie Produktupdates automatisch herunterladen und installieren wollen, müssen Sie beachten, dass dafür mitunter ein Server-Neustart erforderlich ist. Dieser wird von Server Security dann automatisch initiiert, um den Virenschutz nicht zu unterbrechen.

Sie umgehen diesen erzwungenen Neustart, indem Sie einstellen, dass Sie bei neuen Produktupdates lediglich benachrichtigt werden wollen. Dies konfigurieren Sie über die Konfiguration von Server Security unter dem Punkt *Einstellungen* > *Update* bei den Optionen zum Punkt „Produktupdates“.

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

2.3 Ausnahmen setzen

Da Server Security mitunter sehr tief mit dem Betriebssystem verzahnt ist und besonders auch der Echtzeit-Scanner während des Echtzeitscans bei jedem Schreib- oder Lesezugriff auf Dateien diese Dateien prüft, ist es sehr empfehlenswert, bestimmte Programme und deren Prozesse von der Suche mit Avira auszunehmen.

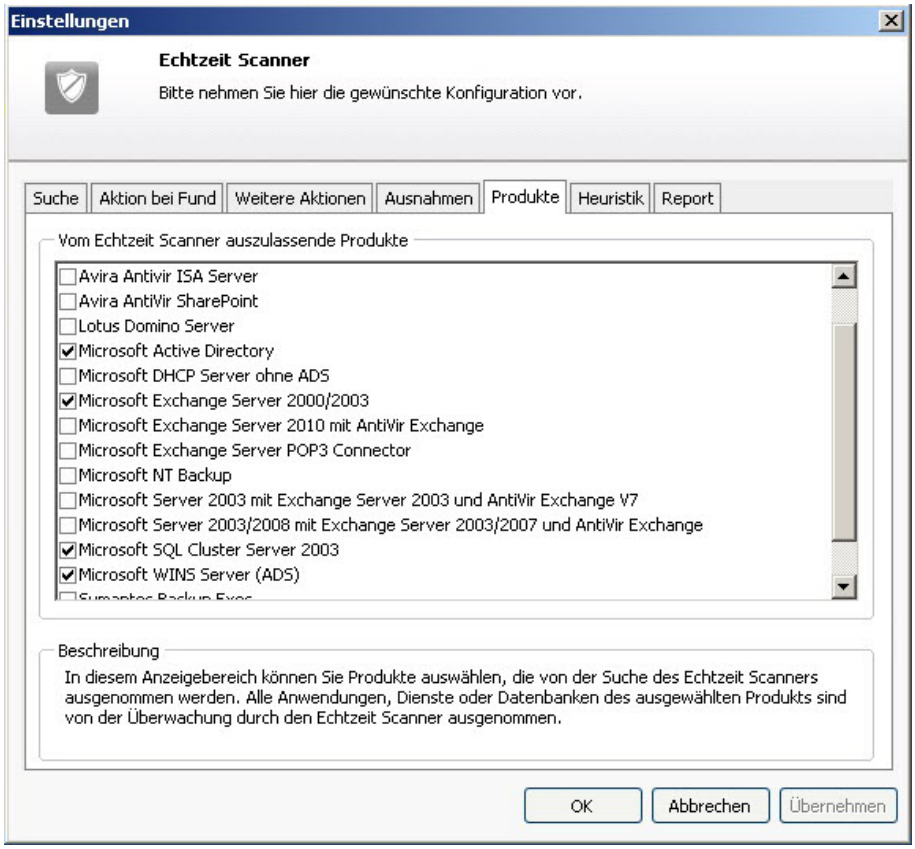
Hierzu gehören z.B. alle Programme, welche mit einer Datenbank im Hintergrund operieren wie unter anderem Buchhaltungsprogramme, Mailserver, Webserver oder Finanzsoftware.

Ebenso sind hiervon besonders Backup-Programme betroffen, welche eine Datensicherung Ihres Systems durchführen, da hierbei ein Lesezugriff auf alle Dateien Ihres Rechners erfolgt und der Echtzeit-Scanner ebenfalls laufend jede einzelne Datei prüft, 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 Server Security auf
- Gehen Sie auf den Menüpunkt „Einstellungen“
- Öffnen Sie im Menübaum den Punkt „Echtzeit-Scanner“
- Wählen Sie hier den Punkt „Produkte“

Unter dem Punkt „Produkte“ sind von Avira bereits vordefiniert die häufigsten Programme, welche in ihrer Verwendung die Leistung des Systems bremsen, sofern sie nicht von der Echtzeit-Scannersuche ausgenommen werden. Sollten Sie eines dieser Programme nutzen, nehmen Sie es bitte von der Suche durch entsprechendes Anhaken aus.



Sollten Sie darüber hinaus noch Backup-Software oder andere Software auf Datenbankbasis verwenden, welche in dieser Liste nicht aufgeführt ist, gehen Sie bitte auf 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:

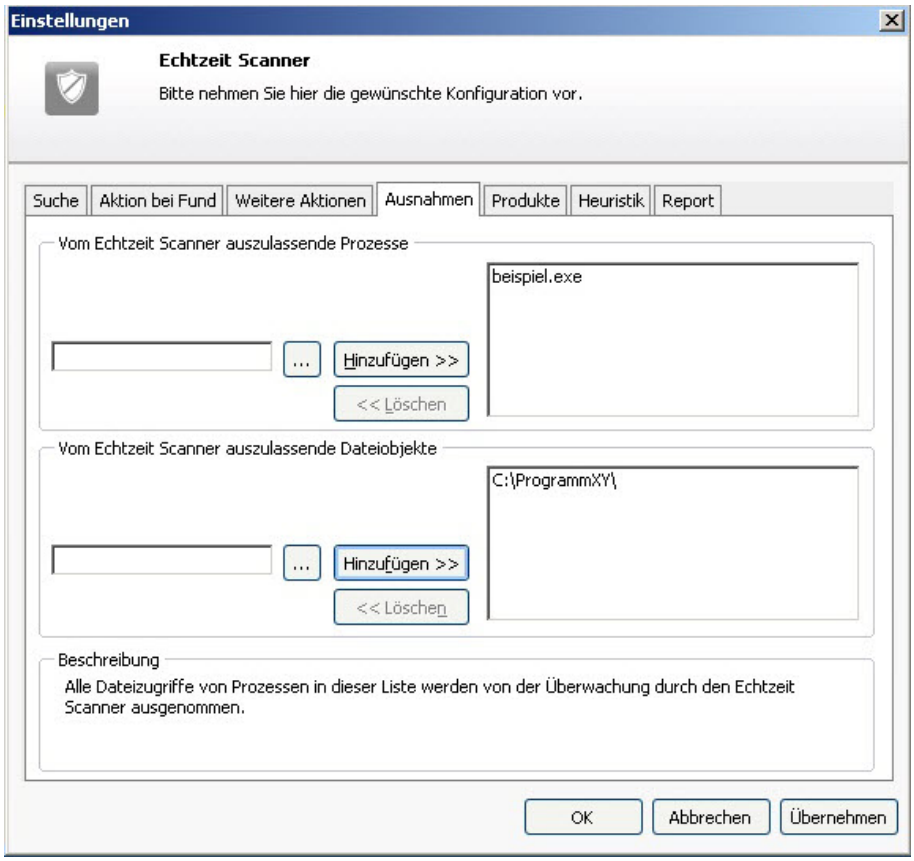
C:\Programme\Backup_ProgrammXY\

Darüber hinaus ist es beim Echtzeit-Scanner wichtig, die Prozesse der jeweiligen auszunehmenden Software mit von der Suche auszuschließen.
Dies hat den Hintergrund, dass gerade diese laufenden Prozesse z.B. von Backup-Software Zugriffe auf Dateien initialisieren. Wird also der Prozess an sich nicht ausgenommen, greift auch hier der Echtzeit-Scanner wieder 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.

Ein aktiver Prozess, z.B. eines Backup-Programms, benötigt fortwährend Lese – bzw. Schreibzugriffe auf die Platte, bei welchen der Echtzeit-Scanner alles in Echtzeit überprüfen würde, wenn der entsprechende Prozess nicht ausgenommen würde.

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 dann nicht alle aktiven Prozesse im Taskmanager.



Selbiges ist ebenfalls auch unter dem Punkt *Scanner* > *Ausnahmen* zu tun, wobei Sie hier lediglich die Pfadangaben und keine Prozesse anzugeben brauchen.

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.

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

Wir nehmen täglich bis zu 5 Updates unserer Virendefinitionen/ Engine vor. Aus diesem Grund sollte stündlich geprüft werden, ob der Schutz auch wirklich noch aktuell ist. Ebenfalls dient die wöchentliche Systemprüfung 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 Server einnisten, die in unseren Updates erst einen Tag später enthalten sind.

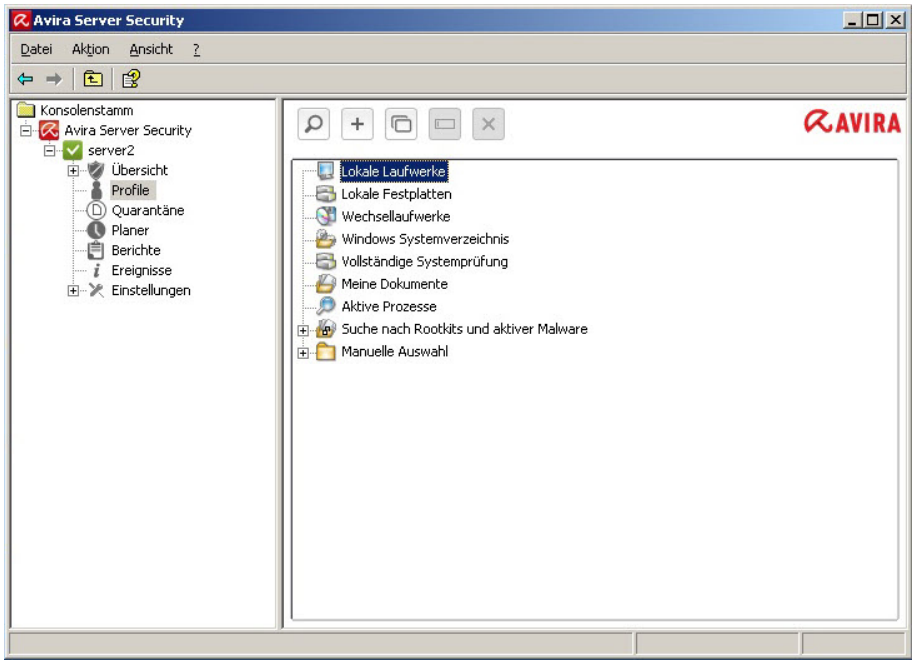
Wird alle paar Wochen oder gar Monate einmal eine Systemprüfung durchgeführt, wird dieser Virus trotz aktuellstem Schutz möglicherweise auch erst dann von Avira entdeckt, sofern ihn der Echtzeit-Scanner nicht vorher aufgespürt hat.
Daher ist die wöchentliche Systemprüfung die beste ausgewogene Mischung aus geringer Performancebelastung und optimaler Sicherheit des Systems.

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.

Falls ein genereller Virenverdacht besteht, man diesen aber auf die lokalen Festplatten eingrenzen kann, bringt es z.B. eine erheblich verkürzte Suchlaufzeit, falls man das Profil „Lokale Festplatten“ wählt, statt „Lokale Laufwerke“, da hier auch CD-Laufwerke sowie Wechselmedien durchsucht werden.

Ebenfalls kann der Fall vorliegen, dass neue, unbekannte USB-Sticks am Server eingesteckt werden und diese geprüft werden sollen. Da hierbei nicht gleich eine komplette Systemprüfung von Nöten ist, kann man mit dem Profil „Wechsellaufwerke“ speziell diesen Laufwerkstyp abdecken und sicherstellen, dass auf den neu angeschlossenen Geräten kein Virus enthalten ist.

Falls der Verdacht auf einen Virenbefall besteht und man zunächst prüfen möchte, ob dieser Virus eventuell sogar gerade als aktiver Prozess läuft, kann man dies mit dem Suchprofil „Aktive Prozesse“ schnell überprüfen, welches nur die derzeit in Ausführung stehenden Prozesse einer Virenprüfung unterzieht.

Die folgende Liste zeigt eine Übersicht der vordefinierten Profile und mögliche Szenarien bei denen Sie diese Anwendung finden können:

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

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.

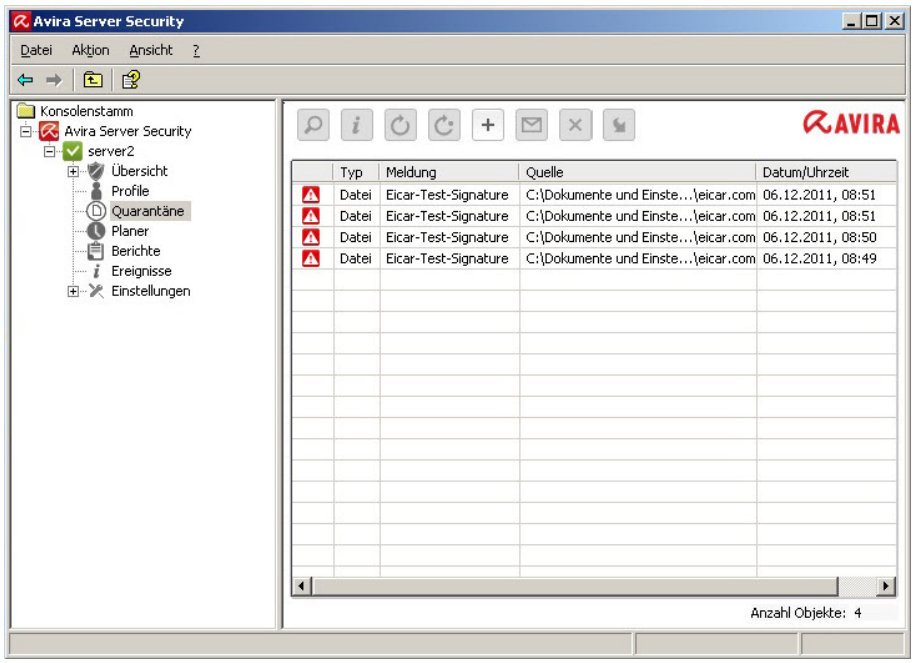
5. Quarantäne

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 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: Server 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 können, 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 einigen Tagen (zwischen 5 und 10) die verdächtigen Objekte in der Quarantäne markieren und erneut prüfen lassen (durch drücken von „F2“ oder Rechtklick 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. Quicktipps

6.1 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.
Da auf Serverbetriebssystemen kein abgesicherter Modus verfügbar ist, empfehlen wir bei einem definitiven Befall, das System mit unserer Rescue CD zu booten und mit dieser den PC zu reinigen.

Die Rescue CD erhalten Sie unter folgendem Link:

http://www.avira.com/de/support-download

6.2 Manuelles Einfügen der Lizenzdatei

Wenn Sie Ihre Lizenz verlängert haben besteht die Möglichkeit, diese Datei (hbedv. key) auch direkt ins Hauptverzeichnis von Avira zu kopieren (C:\Programme\Avira\AntiVir Server).
Ebenso können Sie die Lizenzdatei in der Serverkonsole einfügen, indem Sie den Server Security mit der rechten Maustaste auswählen und den Punkt „Lizenzdatei aktualisieren“ wählen.

6.3 Übernahme der Konfiguration bei mehrfacher Installation

Wenn 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 „avnetnt.ini“. Sie finden diese unter folgendem Pfad:

Windows Server 2003:
C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir Server\config\avnetnt.ini

Windows Server 2008:
C:\Programm Data\Avira\AntiVir Server\config\avnetnt.ini

Sie können diese Datei nun entweder nachträglich von einem Server zum anderen kopieren und somit die Konfiguration umändern (bei deaktivierten Avira Diensten), oder Sie geben bei einer Installation über die Kommandozeile, z.B. bei einem Logon-Skript den Pfad zur avnetnt.ini Datei an, welche dann bei der Installation eingespielt wird. Nähere Informationen hierzu erhalten Sie im Handbuch von Server Security unter dem Punkt „Kommandozeilenparameter für das Setup-Programm“.

6.4 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 kostenverursachende, oft horrend überteuerte 0190/0900-Nummer an.

Spiele (GAMES)
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.

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 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