Avira Internet Security
FireWall

Kurzanleitung

AVIRA

Inhaltsverzeichnis

1. Grundwissen zur Firewall

Eine Firewall arbeitet mit Netzwerkprotokollen wie z.B. TCP, UDP, IP, etc.

Ein einfaches Beispiel für den Verbindungsaufbau des TCP-Protokolls nennt man auch Handshake-Verfahren. Damit soll Ihnen erklärt werden, wie eine Kommunikation von zwei Rechnern im Internet zustande kommt.

- Computer A schickt ein Paket, in dem steht, dass er eine Verbindung zu Computer B aufbauen möchte
- Darauf antwortet Computer B, dass er dazu bereit ist
- Computer A bestätigt anschließend Computer B, dass er verstanden hat, dass Computer B bereit ist
- Die Verbindung zwischen Computer A und Computer B ist damit hergestellt, und der eigentliche Datenaustausch kann beginnen

2. Begriffserklärung

TCP
Das „Transmission Control Protocol“ (TCP) (zu dt. Übertragungssteuerungsprotokoll) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen.

UDP
Das „User Datagram Protocol“ (UDP) ist ein minimales, verbindungsloses Netzwerkprotokoll.
Um die Daten, die mit UDP versendet werden, dem richtigen Programm auf dem Zielrechner zukommen zu lassen, werden bei UDP sogenannte Ports verwendet. Dazu wird bei UDP die Portnummer des Dienstes mit gesendet, der die Daten erhalten soll. Zusätzlich bietet UDP die Möglichkeit, einer Integritätsüberprüfung an, indem eine Prüfsumme mitgesendet wird. Dadurch kann eine fehlerhafte Übertragung erkannt werden.

Flooding
„Flooding“ (engl. überfluten) bezeichnet das Überschwemmen eines Netzwerkes mit Paketen. Flooding kann den Datenverkehr in einem Netzwerk (oder eines einzelnen Rechners) lahmlegen, da der Rechner oder das Netzwerk mit einer Masse von Anfragen überschwemmt wird und dadurch nicht mehr reagieren kann. Man kann dies mit einem Stau auf der Autobahn vergleichen.

Ports
Einen „Port“ kann man mit einer Hausnummer vergleichen. Nur ist der Unterschied, dass ein Haus, in diesem Falle der Computer, auch mehrere Nummern haben kann. Ein Port ist ein Teil einer Adresse, der ankommende Pakete einer Anwendung zuordnet.

Beispiel
Port 110, zuständig für Dienst POP3, gewährleistet den Zugriff auf den Email-Server. Bestimmte Applikationen verwenden Portnummern, die ihnen von der IANA fest zugeordnet und allgemein bekannt sind. Sie liegen üblicherweise von 0 bis 1023, und werden als „Well Known Ports“ bezeichnet.
Von Port 1024 bis 49151 befinden sich die Registered Ports. Anwendungshersteller können bei Bedarf Ports für eigene Protokolle registrieren lassen, ähnlich wie Domainnamen.

Die Registrierung hat den Vorteil, dass eine Anwendung anhand der Portnummer identifiziert werden kann, allerdings nur wenn die Anwendung auch den bei der IANA eingetragenen Port verwendet. Die restlichen Ports von Portnummer 49152 bis 65535 sind so genannte „Dynamic“ und/oder „Private Ports“. Weitere Informationen finden Sie hier.

Portscan
Portscans werden unter anderem ausgeführt um freie Ports auf dem Rechner auszuspähen.
Wenn ein Rechner, einen Serverdienst für andere zur Verfügung stellt, öffnet er einen TCP/IP- oder UDP-Port, oder auch beides oder mehrere. Ein Webserver muss den Port 80 geöffnet haben. Ein Portscan ermittelt nun, welche Ports auf dem Rechner geöffnet sind.

IP
Um einen bestimmten Computer ansprechen zu können, identifiziert ihn das „Internetprotokoll“ (IP) mit einer eindeutigen IP-Adresse. Wenn Sie an einen Freund einen Brief schicken möchten, müssen Sie die Straße und den Ort angeben. Genau so funktioniert es auch mit der IP-Adresse.

Host-Datei
Manchmal wird die Host-Datei dazu verwendet, bekannte Werbeserver zu blockieren, indem der Localhost (127.0.0.1) eingetragen wird, damit alle Anfragen an das eigene System gesendet werden.

Die Besonderheit dieser Methode gegenüber den zu installierenden Werbefiltern ist, dass diese Sperrung systemweit Gültigkeit hat, also nicht nur auf einen Browser beschränkt ist. Darüber hinaus kann man solche Filter auch gegen manche Schadprogramme einsetzen, wenn diese Anweisungen von bereits bekannten Servern abzurufen versuchen.

URL
Als Uniform Resource Locator (URL, dt. „einheitlicher Quellenanzeiger“) bezeichnet man eine Unterart von Uniform Resource Identifier (URIs). URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise HTTP oder FTP) und den Ort (engl. location) der Ressource in Computernetzwerken.

Da URLs die erste und häufigste Art von URIs darstellen, werden die Begriffe häufig als Synonym verwendet.

In der Umgangssprache wird URL häufig als Synonym für Internetadresse wie z.B. „www.avira.de“ verwendet.

Slide-Up
Als Slide-Up versteht man ein kleines Fenster, dass entweder rechts oben oder rechts unten, langsam auf ihrem Bildschirm erscheint und nach einer Eingabe (Interaktion) oder nach einer gewissen Zeit selbstständig wieder verschwindet.

3. Einstellungsmöglichkeiten

3.1. Sicherheitsniveau

Zuerst gilt es zu entscheiden, welches Sicherheitsniveau eingestellt werden sollte. Eine zu hohe Einstellung des Sicherheitsniveaus kann dazu führen, dass bestimmte Systemfunktionen nicht mehr gewährleistet sind.

Eine zu niedrige Einstellung dagegen kann bewirken, dass die Firewall nicht alle Zugriffe auf Ihren Rechner blockiert.

Allgemein gilt: Ist der PC nicht an ein lokales Netzwerk angeschlossen und befindet sich kein netzwerkfähiges Gerät (z.B. Netzwerkdrucker) in der Umgebung des PCs, kann das Sicherheitsniveau auf „Hoch“ eingestellt bleiben.

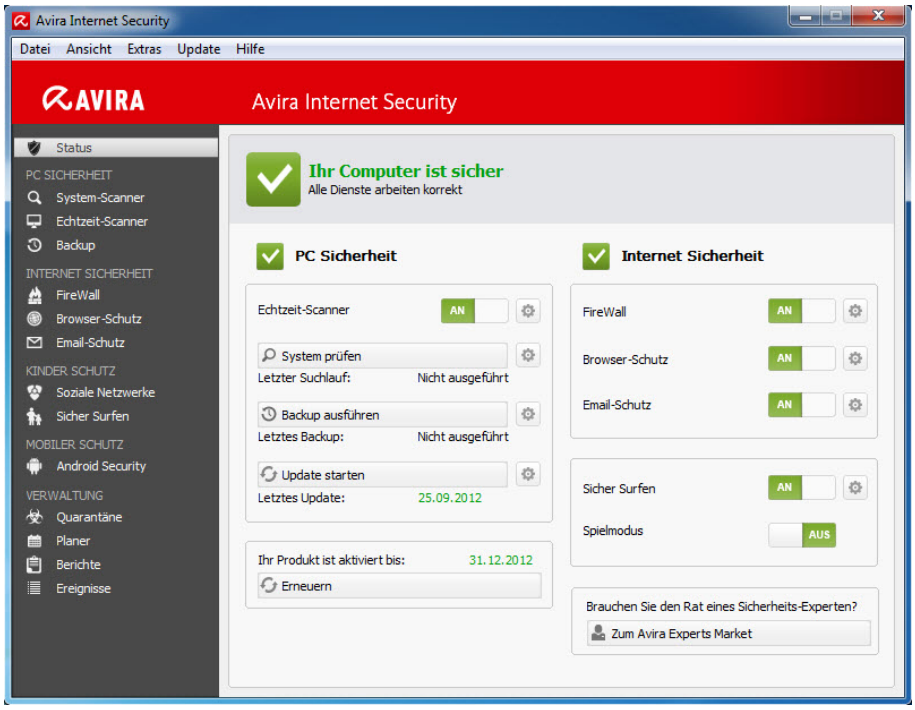
Das bedeutet, der Computer ist im Netzwerk unsichtbar. Des Weiteren werden Verbindungen von außen blockiert und Flooding und Portscan verhindert. Dies ist die Standardeinstellung nach der Installation der Avira Internet Security.

Sollte sich der PC jedoch in einer Netzwerkumgebung befinden oder der PC auf Netzwerkgeräte wie z.B. Netzwerkdrucker zugreifen, sollte das Sicherheitsniveau auf „Mittel“ gestellt werden.

Sonst kann es unter Umständen dazu führen, dass der Netzwerkdrucker blockiert wird bzw. nicht erkannt wird, da Sie der Firewall nicht mitgeteilt haben, dass ein Drucker vorhanden ist.

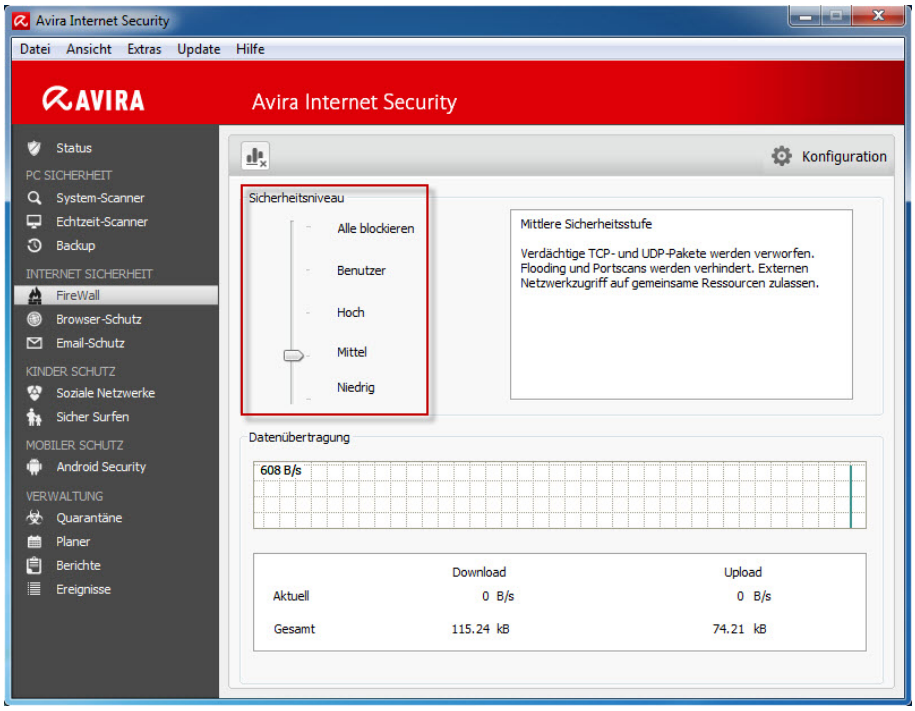
Hierzu gehen Sie wie folgt vor:

► Starten Sie das Avira Control Center



Dies wird am einfachsten durch einen Doppelklick mit der linken Maustaste auf das Schirmsymbol erreicht. Dieses Symbol befindet sich in der Taskleiste, unten rechts neben der Systemuhrzeit. Alternativ kann das Control Center über einen Doppelklick auf das bei der Installation angelegten Symbols auf dem Desktop gestartet werden.

► FireWall-Einstellungen öffnen



Ein Klick auf „FireWall“ im Untermenü „INTERNET SICHERHEIT“ öffnet die Konfiguration der Avira FireWall. Diese erscheint rechts im Hauptfenster des Control Centers.

► Sicherheitsniveau der FireWall anpassen

Durch Anklicken und Festhalten des Sicherheitsniveau-Reglers der FireWall lässt sich diese anpassen. Die möglichen Stufen sind „Alle blockieren“, „Benutzer“, „Hoch“, Mittel“, „Niedrig“. Eine Beschreibung der Stufen finden Sie direkt rechts neben dem Sicherheitsniveau-Schieber.

Stellen Sie hier das Niveau auf „Mittel“, falls Probleme mit Netzwerkdruckern, externen Festplatten oder ähnlichen Netzwerkverbindungen auftreten sollten.

3.1.1 Alle blockieren

Alle Netzwerkverbindungen werden blockiert.

3.1.2 Benutzer

Mit dieser Option können Benutzerdefinierte Regeln konfiguriert werden.

3.1.3 Hoch

Der Computer ist im Netzwerk unsichtbar und die Verbindungen von außen werden blockiert. Flooding und Portscan werden verhindert.

3.1.4 Mittel

Im Vergleich zur FireWall-Einstellung „Hoch“, ist der Rechner im Netzwerk sichtbar und bekommt somit TCP- und UDP Anfragen. Diese werden aber verworfen.

TCP- und UDP-Pakete, die unerwartet eintreffen oder empfangen werden, werden nicht bearbeitet und nicht entgegengenommen. Flooding und Portscan werden verhindert.

Auch unter der Stufe „Mittel“ können gegebenenfalls Probleme mit dem Netzwerk auftreten. In diesem Fall sollten Sie das Level auf „Niedrig“ heruntersetzen.

Das Preset Level (vorkonfigurierte Regeln) ist unter dem Sicherheitsniveau „Mittel“ ein wenig ausgeprägter, d.h. unter „Mittel“ werden verschiedene TCP und UDP-Paketanfragen erkannt und automatisch verarbeitet. Andere werden verworfen.

3.1.5 Niedrig

Auch unter der Stufe „Niedrig“ haben Sie noch den Schutz der Avira FireWall. Es werden nicht wie bei der Stufe „Mittel“ Flooding und Portscan verhindert, sondern nur noch erkannt. Dies sind die gängigsten Arten, eine „Lücke“ auf Ihrem Rechner ausfindig zu machen.

Sind die Einstellungen für Sie nicht ausreichend oder verschiedene Ports müssen für eine Anwendung frei geschaltet werden, so können Sie unter Punkt 3.2 Konfiguration weitere Einstellungen vornehmen.

3.2. Konfiguration

Klicken Sie mit der rechten Maustaste auf das Trayicon in der Taskleiste und wählen Sie den Punkt „Avira Internet Security konfigurieren“ aus.
Sie haben auch die Möglichkeit, über das Avira Control Center die Konfiguration zu starten, indem sie das Control Center öffnen, F8 drücken oder über *Extras* > *Konfiguration* gehen.

In der Konfiguration finden Sie auf der linken Seite unter „Internet Sicherheit“ den Punkt „FireWall“. Aktivieren Sie den *Expertenmodus*, um alle Einstellungen sehen und ändern zu können. Hier können Sie folgende Einstellungen konfigurieren:

- Adapterregeln
- Anwendungsregeln
- Vertrauenswürdige Anbieter
- Einstellungen
- Popup-Einstellungen

3.2.1 Adapterregel

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

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

Eine vordefinierte Adapterregel ist abhängig vom Sicherheitsniveau. Sie können das Sicherheitsniveau über das Avira Control Center wie unter Punkt 3.1 beschrieben ändern, oder die Adapterregeln auf Ihre Bedürfnisse anpassen.
Haben Sie die Adapterregeln auf Ihre Bedürfnisse angepasst, wird unter der Rubrik FireWall des Avira Internet Security Control Center im Bereich Sicherheitsniveau der Regler auf Benutzer platziert.

Eingehende Regeln

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

Beispiel

Sie wollen die IP- Adresse 10.40.30.20 hinzufügen.

Wenn Sie auf **Hinzufügen** klicken, öffnet sich ein neues Fenster mit verschiedenen vordefinierten Regeln. Dort wählen Sie „Eingehende IP-Regel“ aus und bestätigen mit **OK.**

In Ihren „Eingehenden Regeln“ finden Sie nun den Punkt „Eingehende IP-Regel“. Wählen Sie diesen aus. Es ist auch möglich den Punkt umzubenennen.

Sie können nun im unten markierten Kasten die IP und deren Maske eintragen und diese entweder zulassen oder sperren. Ebenso besteht die Option, ob das Paket in die Reportdatei geschrieben werden soll oder nicht.

Ausgehende Regeln

Ausgehende Regeln dienen zur Kontrolle des ausgehenden Datenverkehrs durch die Avira FireWall. Sie können eine ausgehende Regel für die folgenden Protokolle definieren:

- IP
- ICMP
- UDP
- TCP

Um Einstellungen zur „Ausgehenden Regel“ vorzunehmen, gehen Sie genauso vor wie bei der „Eingehenden Regel“.

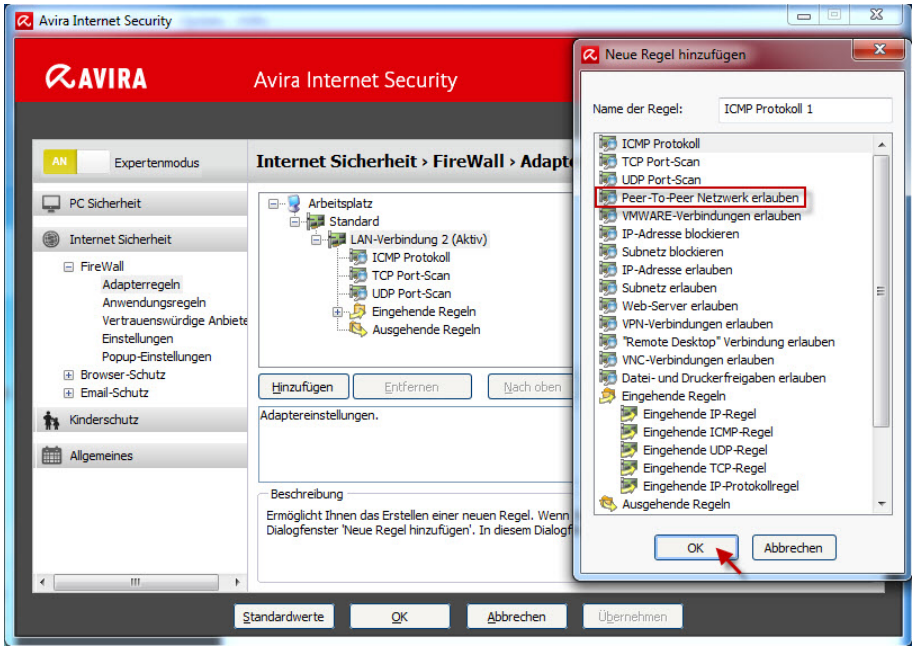
Beispiele

- Peer to Peer

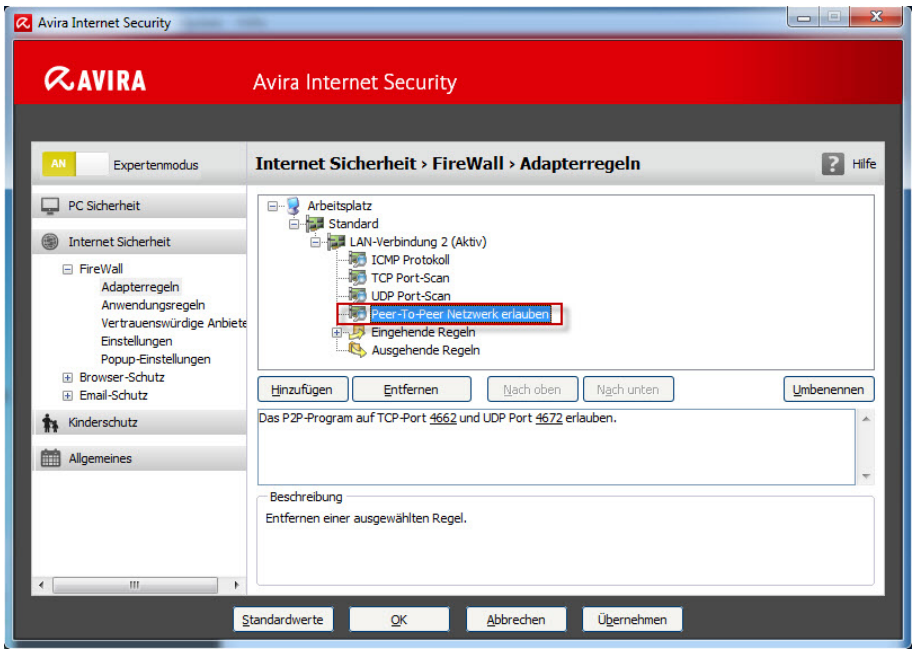
Sollten Sie z.B. Tauschsysteme, Dateisysteme oder File-Sharing-Systeme verwenden, können Sie dieses vorgefertigte Template verwenden.

Über folgenden Pfad können Sie die neue Regel hinzufügen:
Internet Sicherheit > FireWall > Adapterregeln > LAN-Verbindung 2 (Aktiv)

Drücken Sie den Button **Hinzufügen** und wählen Sie im erscheinenden Fenster „Peer-To-Peer Netzwerk erlauben“ aus und bestätigen Sie mit **OK**.

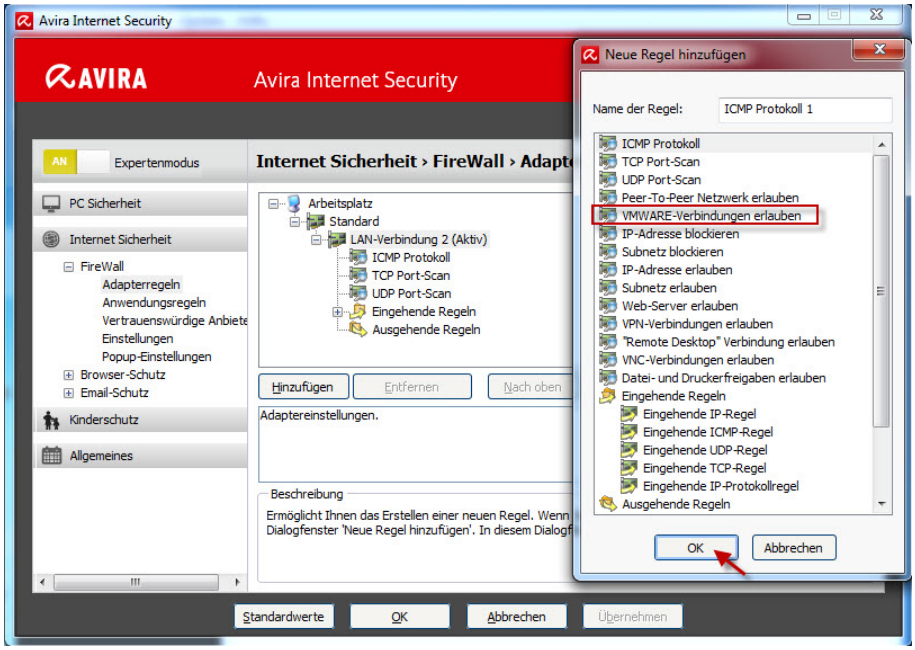


Sie müssen in diesem Fall nur noch die benötigten TCP- und UDP-Ports freigeben.



- VMware

Sollte der Internetzugriff von Ihrer VMware nicht möglich sein, müssen Sie diese über folgendes Template freischalten.

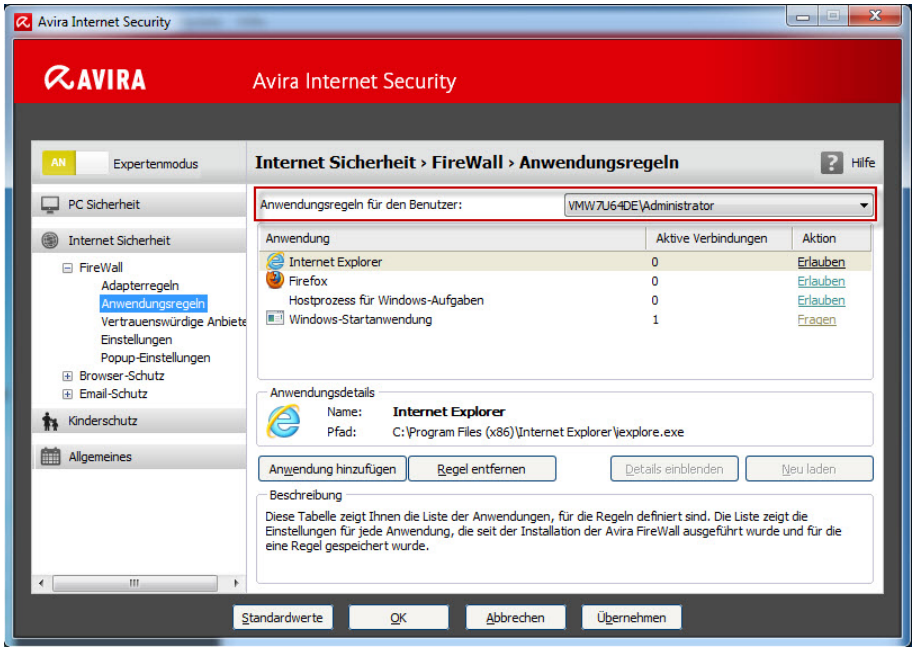


Um die Einstellungen zur „VMWARE-Verbindungen erlauben“ vorzunehmen, gehen Sie genauso vor wie bei der vorherigen „Peer-To-Peer Netzwerk erlauben“ Regel.

3.2.2 Anwendungsregeln

Diese Liste enthält alle Anwender im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, für den Sie Regeln erstellen möchten.

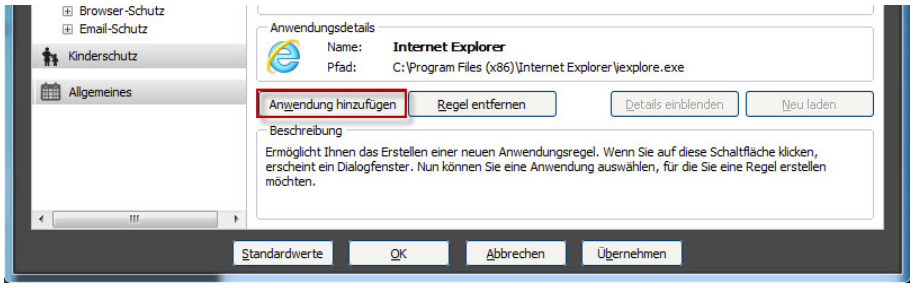
Falls Sie kein Anwender mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.



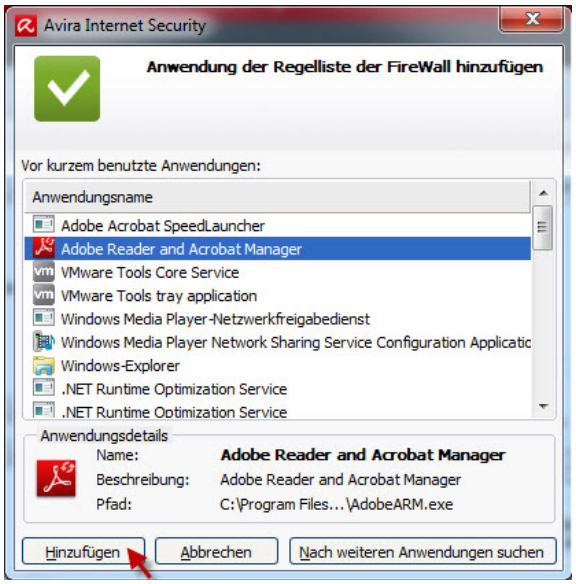
Beispiel
So kann ein Administrator dafür sorgen, dass ein Webbrowser keinen Internetzugriff erhält, oder ein Chatprogramm nicht ausgeführt werden kann.

Anwendung hinzufügen

Wenn Sie auf den Button **Anwendung hinzufügen** klicken, öffnet sich ein neues Fenster mit den Programmen, die auf Ihrem Rechner installiert sind.

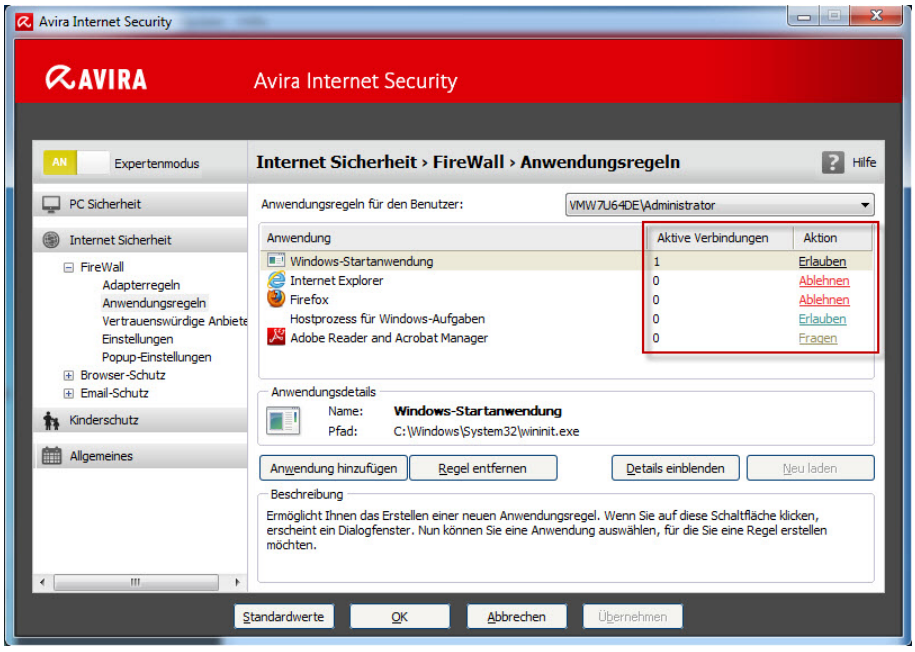


Durch einfaches Anklicken wird die Anwendung markiert und kann von Ihnen über den Button **Hinzufügen** zur Liste aufgenommen werden.



Anwendungseinstellungen

Dort können Sie die Aktive Verbindung zwischen „Immer erlauben“ und „Immer ablehnen“ ändern. Bei gefiltertem Modus werden die Adapterregeln und die Anwendungsregeln überprüft, im privilegierten Modus hingegen werden nur die Anwendungsregeln kontrolliert.
Ebenso kann die Aktion von „Erlauben“ auf „Ablehnen“ oder „Fragen“ geändert werden. Stellen Sie die Aktion auf „Fragen“, werden Sie immer vor der Ausführung des Programms von Avira gefragt, ob Sie wirklich das Programm starten wollen. Bei „Ablehnen“ wird das Programm von der Avira FireWall geblockt.



3.2.3 Vertrauenswürdige Anbieter

Unter „Vertrauenswürdige Anbieter“ wird eine Liste von vertrauenswürdigen Software-Herstellern angezeigt.

Sie können Hersteller aus der Liste entfernen oder hinzufügen, indem Sie die Option „Diesem Anbieter immer vertrauen“ im Popup-Fenster „Netzwerkereignis“ nutzen.

Sie können den Netzzugriff von Anwendungen, die von den aufgelisteten Anbietern signiert sind, standardmäßig erlauben, indem Sie die Option „Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen“ aktivieren.

3.2.4 Vertrauenswürdige Anbieter für Benutzer

Diese Liste enthält alle Benutzer im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, dessen Liste vertrauenswürdiger Anbieter Sie einsehen oder pflegen möchten.

Falls Sie kein Benutzer mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.

Erstellte Anwendungen automatisch zulassen

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

Die Option ist standardmäßig aktiviert.

Wir empfehlen Ihnen die Standardeinstellung aktiviert zu lassen, da wir die vollen Kontaktdaten der Anbieter haben.

Des Weiteren handelt es sich hierbei um lizenzierte Softwarefirmen. Daher werden die Anbieter in der Liste von uns als vertrauenswürdig eingestuft.

Anbieter

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

Entfernen

Um einen Anbieter endgültig aus der Liste der vertrauenswürdigen Anbieter zu entfernen, markieren sie den Eintrag und drücken Sie auf **OK** im Fenster der Konfiguration.

Neu laden

Die vorgenommenen Änderungen werden rückgängig gemacht. Die letzte gespeicherte Liste wird geladen.

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

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

3.2.5 Einstellungen

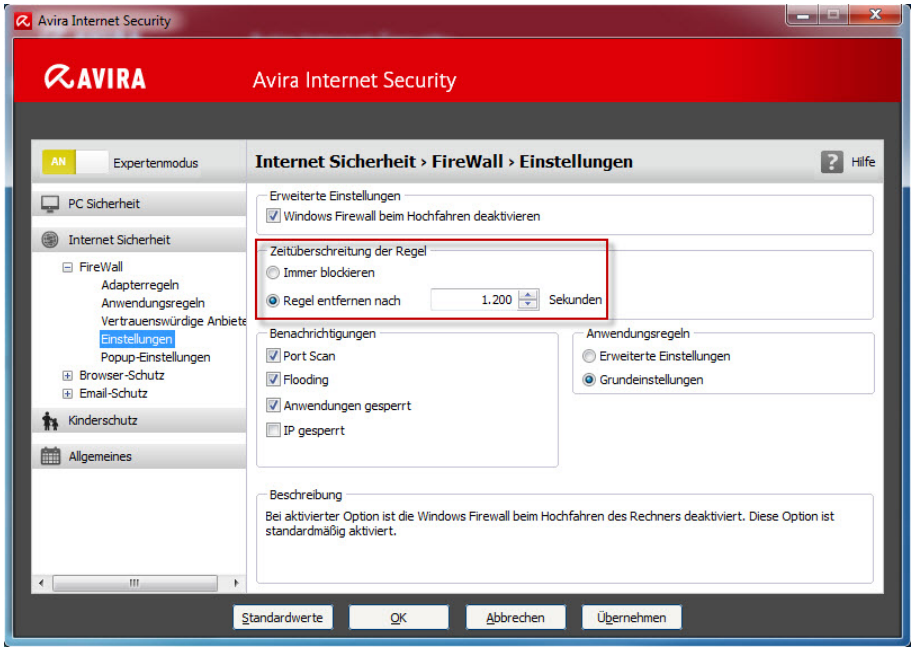
Zeitüberschreitung der Regel

- Immer blockieren

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

- Regel entfernen nach n Sekunden

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan (siehe Begriffserklärung) automatisch erstellt wurde, nach der von Ihnen angegebenen Zeit wieder entfernt. Diese Option ist standardmäßig aktiviert (siehe Abb. auf der nächsten Seite).

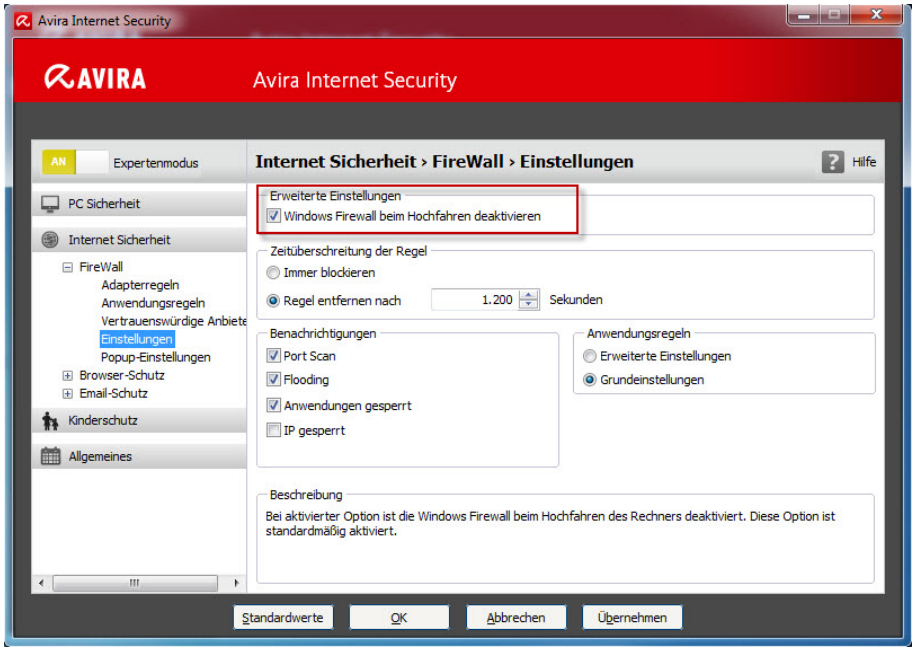


Erweiterte Einstellungen

- Windows Firewall beim Hochfahren deaktivieren

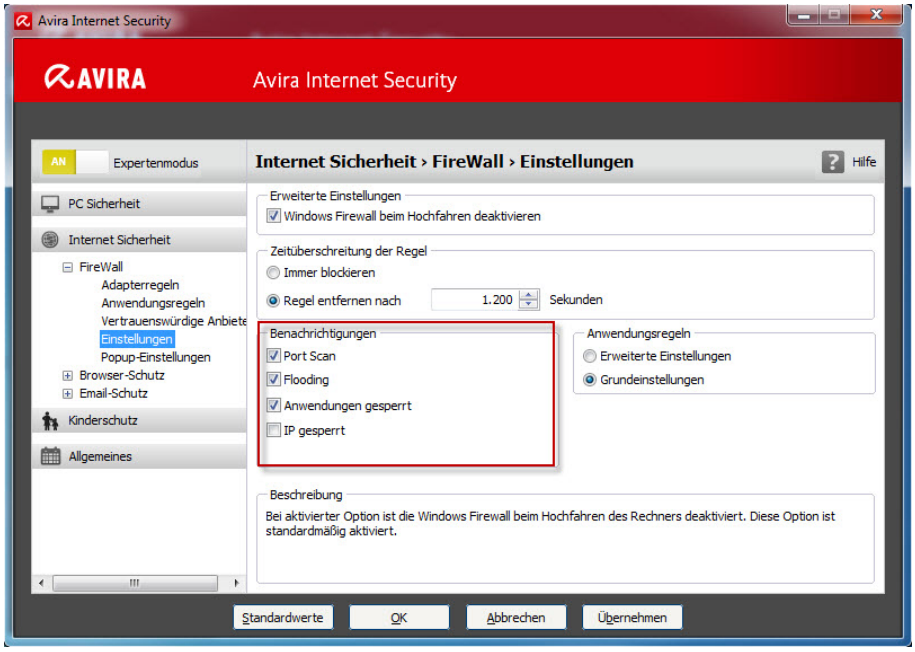
Bei aktivierter Option ist die Windows Firewall beim Hochfahren des Rechners deaktiviert.

Diese Option ist standardmäßig aktiviert, da die Verwendung von zwei gleichzeitig laufenden Desktop Firewalls unter Umständen Probleme hervorruft, da diese sich gegenseitig behindern können.



Benachrichtigungen

Unter Benachrichtigungen legen Sie fest, bei welchen Ereignissen Sie eine Desktop-benachrichtigung der FireWall erhalten möchten.



- Portscan

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

Portscans sind in der Regel nicht unbedingt schädlich, deuten aber darauf hin, dass eventuell ein Angriff auf Ihr System stattfinden kann.

- Flooding

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der FireWall eine Flooding-Attacke erkannt wurde. Flooding-Attacken können unter Umständen Ihr Netzwerk mit Datenmengen „überfluten“, und Ihr Netzwerk lahmlegen.

- Anwendungen wurden blockiert

Sollte eine Anwendung versuchen, eine Verbindung nach außen herzustellen, die Sie nicht in der FireWall zugelassen haben, oder die nicht privilegiert ist, dann wird Sie von der Avira FireWall blockiert und Sie bekommen eine Desktopbenachrichtigung.

In dieser Benachrichtigung wird Ihnen die Anwendung und der Grund der Blockade mitgeteilt.

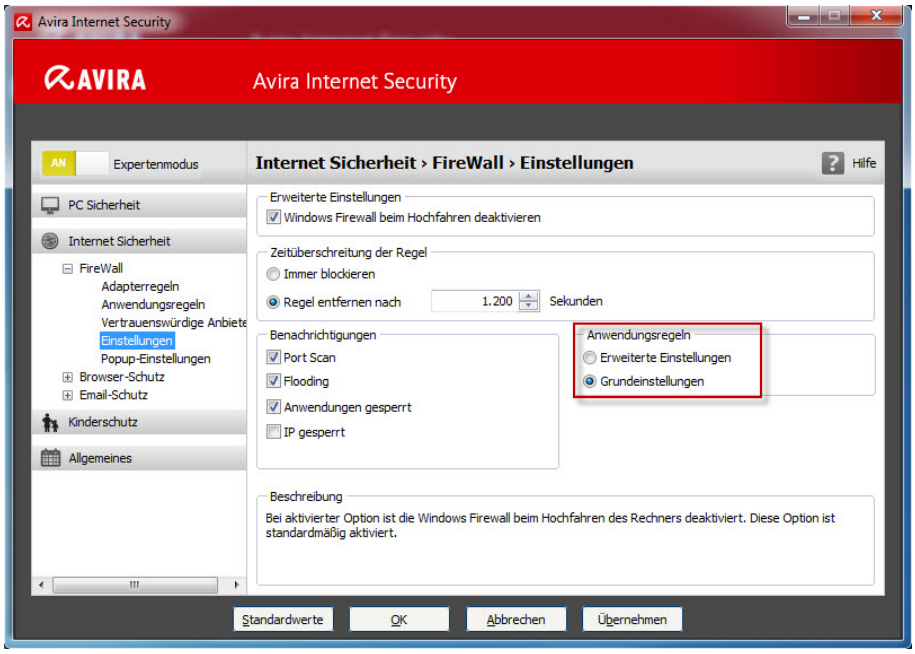
- IP blockiert

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

Wir empfehlen diese Option nicht zu aktivieren, da es im Internet sehr häufig ungewollte IP Adressanfragen auf Rechner gibt, und Sie deshalb ständig Desktopmeldungen erhalten würden.

Anwendungsregeln

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



- Erweiterte Einstellungen

Bei aktivierter Option haben Sie die Möglichkeit, verschiedene Netzwerkzugänge einer Anwendung individuell zu regeln, d.h. hier haben Sie die Möglichkeit, für eine Anwendung eine eigene Anwendungsregel zu erstellen.
Sie können den Verkehr der Anwendung individuell regeln oder die Anwendung nur abhören.

- Grundeinstellungen

Bei aktivierter Option kann nur eine einzige Aktion für verschiedene Netzwerkzugänge der Anwendung eingestellt werden. Das reicht in der Regel aus, um Anwendungen zuzulassen oder zurückzuweisen.

3.2.6 Popup Einstellungen

Popup Einstellungen

- Startblock des Prozesses überprüfen

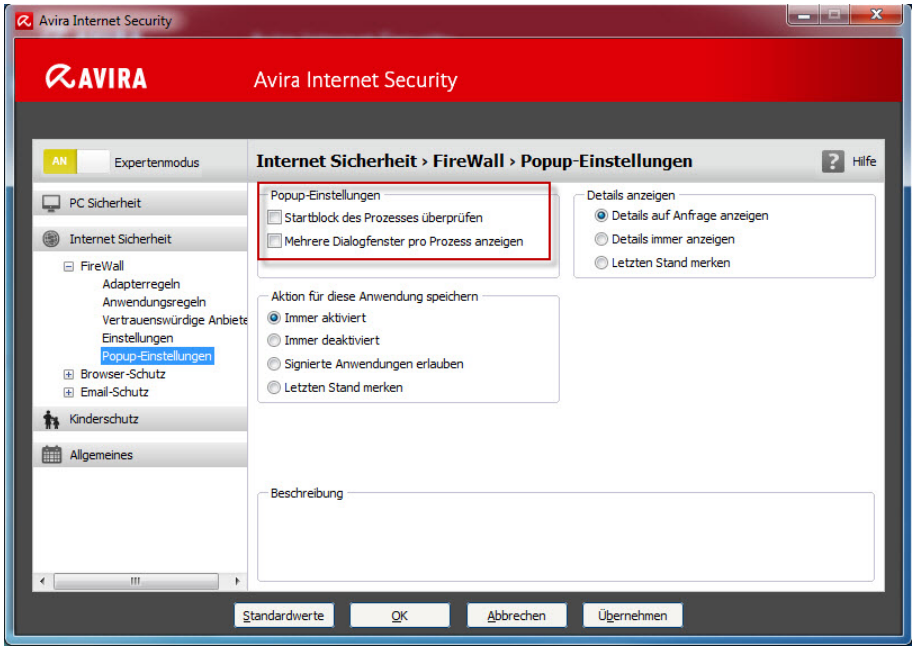
Bei aktivierter Option erfolgt eine präzisere Überprüfung des Prozessstapels. Die FireWall geht dann davon aus, dass jeder Prozess im Stapel, der nicht vertrauenswürdig ist, derjenige ist, über dessen Kindprozess auf das Netzwerk zugegriffen wird. Deshalb wird in diesem Fall für jeden nicht vertrauenswürdigen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

Diese Option ist standardmäßig deaktiviert. Wir empfehlen Ihnen, diese Standardeinstellung beizubehalten, da Sie sonst mit einer Flut von Popups rechnen müssen.

- Mehrere Dialogfenster pro Prozess anzeigen

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

Diese Option ist standardmäßig deaktiviert. Wir empfehlen Ihnen, diese Standardeinstellungen beizubehalten, damit Sie pro Prozess nur ein Popup-Fenster erhalten.



Aktion für diese Anwendung speichern

- Immer aktiv

Bei Auswahl dieser Option ist die Option „Aktion für diese Anwendung speichern“ des Dialogfensters „Netzwerkereignis“ standardmäßig aktiviert.

- Immer deaktiviert

Bei Auswahl dieser Option ist die Option „Aktion für diese Anwendung speichern“ des Dialogfensters „Netzwerkereignis“ standardmäßig deaktiviert.

- Signierte Anwendung erlauben

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

- Letzten Stand merken

Bei Auswahl dieser Option wird die Aktivierung der Option „Aktion für diese Anwendung speichern“ des Dialogfensters „Netzwerkereignis“ gehandhabt wie beim letzten Netzwerkereignis. Wurde beim letzten Netzwerkereignis die Option „Aktion für diese Anwendung speichern“ aktiviert, ist die Option beim folgenden Netzwerkereignis aktiv.
Wurde beim letzten Netzwerkereignis die Option „Aktion für diese Anwendung speichern“ deaktiviert, ist die Option beim folgenden Netzwerkereignis deaktiviert.

Wir empfehlen Ihnen, diese Option beizubehalten, damit alle Ihre Aktionen in Verbindung mit der jeweiligen Anwendung automatisch gespeichert werden.

Details anzeigen

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

- Details auf Anfrage anzeigen

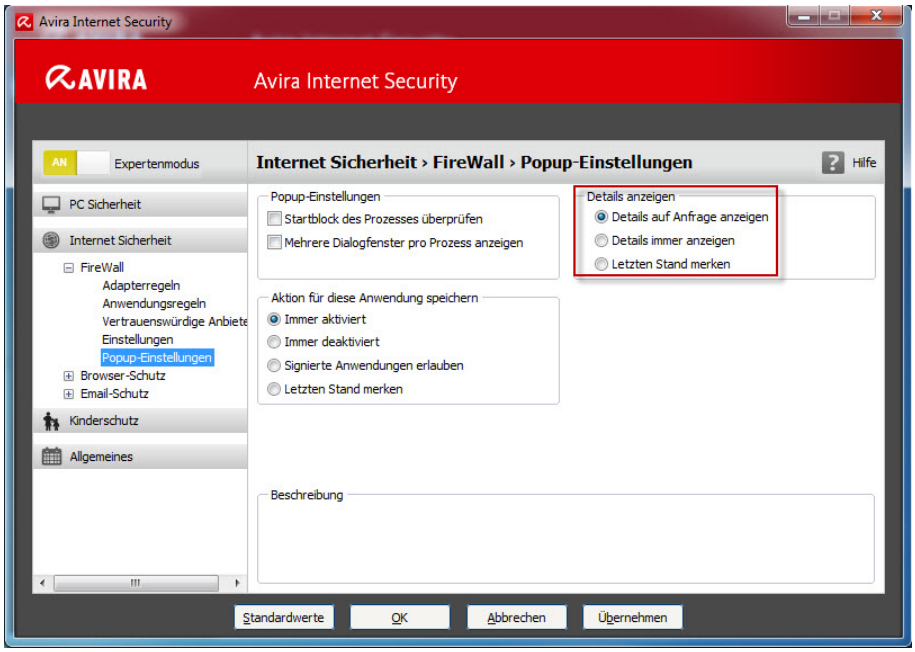
Bei aktivierter Option werden die Detailinformationen im Fenster Netzwerkereignis nur auf Anfrage angezeigt, d.h. eine Anzeige der Detailinformationen erfolgt mit Klick auf die Schaltfläche **Details einblenden** im Fenster Netzwerkereignis.

- Details immer anzeigen

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

- Letzten Stand merken

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



4. Allgemeines zum „Kinderschutz“

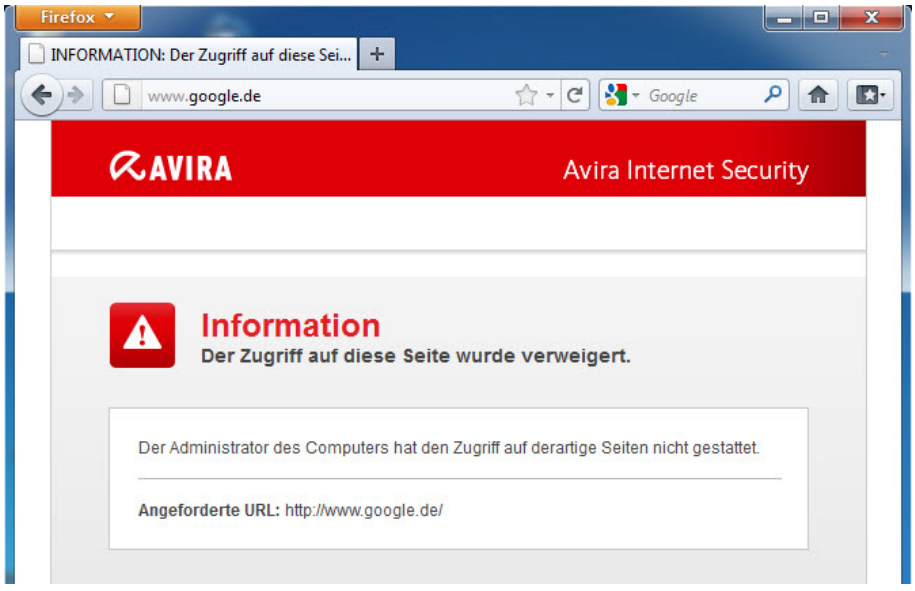
Avira Internet Security besitzt eine Kinderschutzfunktion zum Filtern unerwünschter oder illegaler Internetangebote. Den Benutzern des Computers können Nutzerrollen zugewiesen werden. Eine Nutzerrolle ist konfigurierbar und kann verbotene oder erlaubte URLs (Internetadressen) sowie verbotene Inhaltskategorien umfassen.

Beim Blockieren von Internetinhalten nach bestimmten Kategorien werden leistungsstarke URL-Filterlisten verwendet, in denen URLs anhand der Inhalte der Internetseiten in Inhaltsgruppen kategorisiert sind. Die URL-Filterlisten werden täglich aktualisiert, angepasst, erweitert und unterstützen Sprachen aus dem europäischen Sprachraum (Deutsch, Englisch, Französisch, Italienisch, Russisch,...).

Die Rollen Kind, Jugendlicher, Erwachsener sind mit den entsprechenden verbotenen Kategorien vorkonfiguriert. Um den „Sicher Surfen“ zu konfigurieren, müssen Sie ihn aktivieren.

Ist „Sicher Surfen“ aktiv, werden beim Navigieren im Internet alle im Browser angeforderten Webseiten anhand der Nutzerrolle geprüft. Bei verbotenen Webseiten wird die Webseite blockiert und eine Meldung im Browser angezeigt.

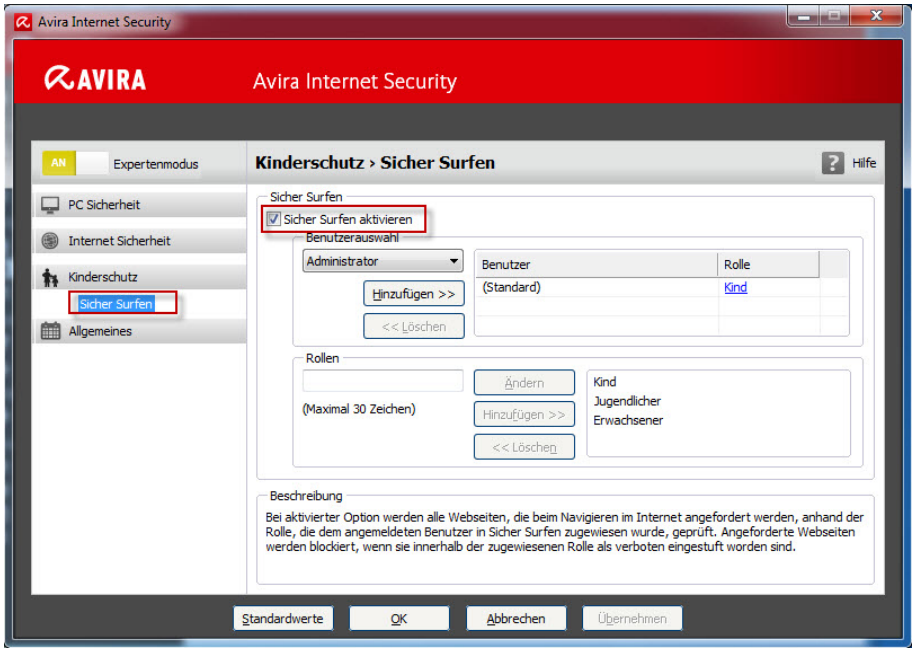
Beispiel
Wenn eine gesperrte Seite aufgerufen wird, erscheint folgendes im Browserfenster.



4.1 „Sicher Surfen“ im „Kinderschutz“ aktivieren

Um „Sicher Surfen“ zu aktivieren, öffnen Sie das Avira Control Center.

Dort finden Sie auf der linken Seite die Kategorie „Kinderschutz“. Wählen Sie den Unterpunkt „Sicher Surfen“ und setzen dann oben auf der rechten Seite den Haken bei „Sicher Surfen aktivieren“.



4.2 Benutzerauswahl

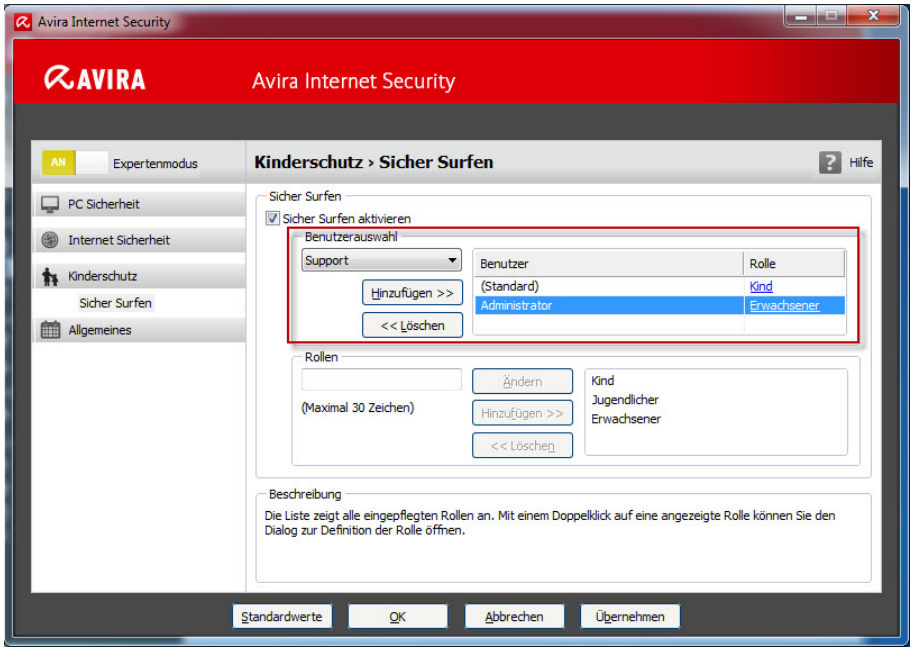
In der Auswahlliste unter „Benutzerauswahl“ befinden sich alle Benutzer des Systems. Wählen Sie einen Benutzer aus und klicken Sie auf **Hinzufügen**.
Der Benutzer erscheint rechts daneben mit der Standardeinstellung in der Rolle als „Kind“.

Sie können die Rolle des Benutzers durch einfaches Klicken auf den Rollen-Namen des jeweiligen Benutzers ändern.

Standardmäßig stehen drei eingepflegte Rollen zur Auswahl:

- Kind
- Jugendlicher
- Erwachsener

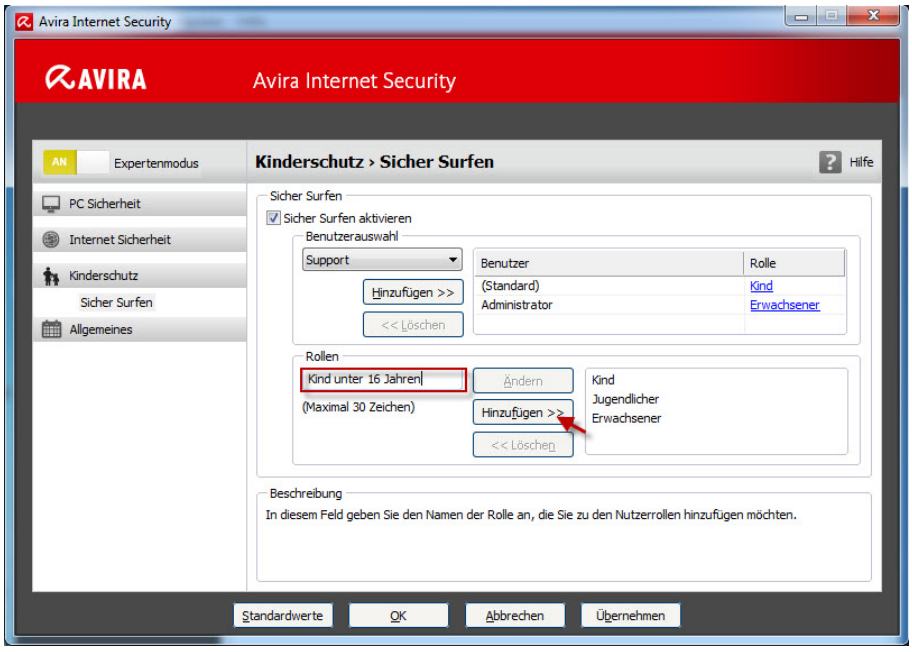
Nähere Informationen zur weiteren Konfiguration der Rollen finden Sie im nächsten Kapitel.



4.3 Rollen

Sie können entweder neue Rollen zu den bestehenden hinzufügen oder die bestehenden ändern. Um neue Rollen hinzuzufügen, geben Sie den Rollennamen in das freie Feld ein. Beachten Sie, dass der Name nicht länger als 30 Zeichen sein darf.

Beispiel
„Kind unter 16 Jahren“ soll hinzugefügt werden.



Klicken Sie auf **Hinzufügen**. Die neue Rolle erscheint im rechten Feld. Um die Rolle

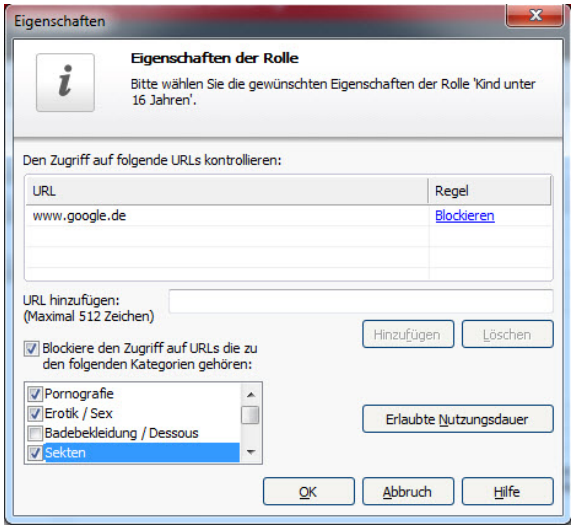
„Kind unter 16 Jahren“ zu konfigurieren, wählen Sie diese aus und klicken auf **Ändern**.

4.3.1 Eigenschaften von Rollen

Hier können Sie URLs hinzufügen und den Zugriff auf URLs, die zu bestimmten Kategorien gehören, sperren lassen.

Beispiel
Die Suchmaschine „www.google.de“ und URLs der Kategorie Pornografie, Erotik/Sex und Sekten sollen blockiert werden.

Nachdem Sie die URL hinzugefügt haben, aktivieren Sie mit einem Häkchen die Kategorie „Blockiere den Zugriff auf URLs die zu den folgenden Kategorien gehören:“ Im darunter liegenden Fenster können Sie jetzt die gewünschten Zugriffe blockieren.

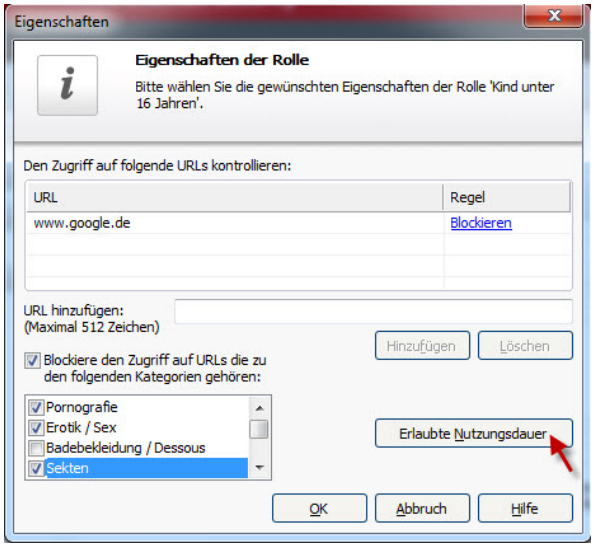


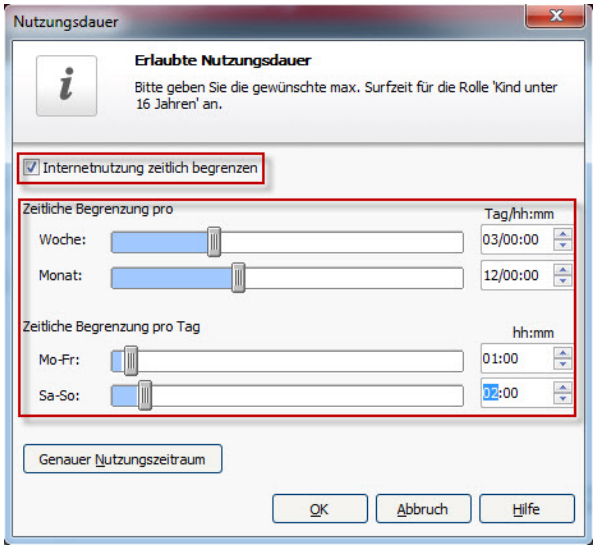
Die Kategorien wurden von einer riesigen Datenbank der Firma Cobion bereitgestellt. Des Weiteren greift der Webfilter auf eine Datenbank der Verbraucherschutzzentrale Hamburg zu.

Sollte Ihnen eine Seite auffallen, die Ihres Erachtens auf eine Kategorie zutreffen sollte, können Sie diese über Test-a-Site kategorisieren, bzw. überprüfen lassen.

Zusätzlich besteht die Möglichkeit über den Button **Erlaubte Nutzungsdauer** die Internetnutzung für die angelegte Rolle zeitlich zu begrenzen.

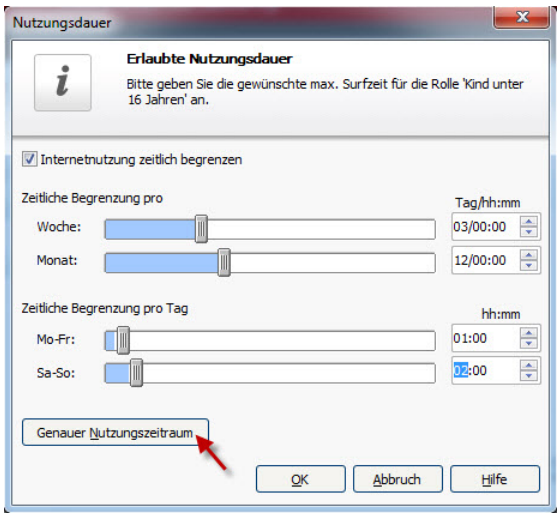
Nach dem Klick auf den Button **Erlaubte Nutzungsdauer**, aktivieren Sie im neuen Fenster die Kategorie „Internetnutzung zeitlich begrenzen“. Danach haben Sie die Möglichkeit, die gewünschte maximale Surfzeit für die aktuelle Rolle zu konfigurieren.

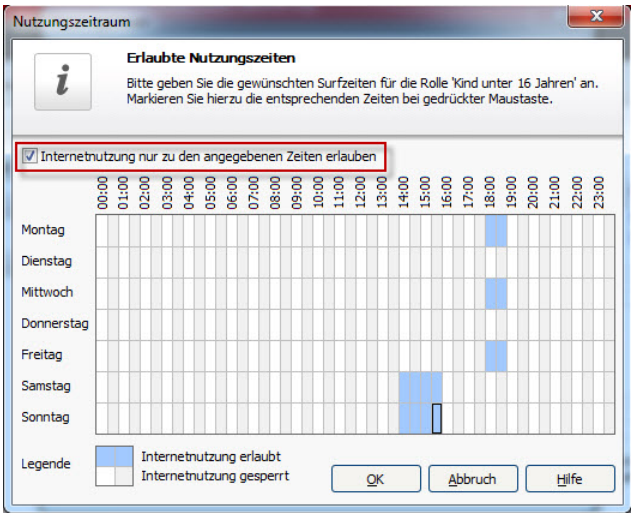




Über den Button **Genauer Nutzungszeitraum** können Sie die Surfzeiten individuell konfigurieren.

Aktivieren Sie mit einem Häkchen die Kategorie „Internetnutzung zu den angegebenen Zeiten erlauben“ und markieren sie mit dem Mauszeiger in der Wochentabelle die gewünschten Surfzeiten. Das Zeitfenster für erlaubtes Internetsurfen kann variabel zwischen 30 min und 24 Stunden pro Tag gesetzt werden.





5. Änderung der Update-Intervalle

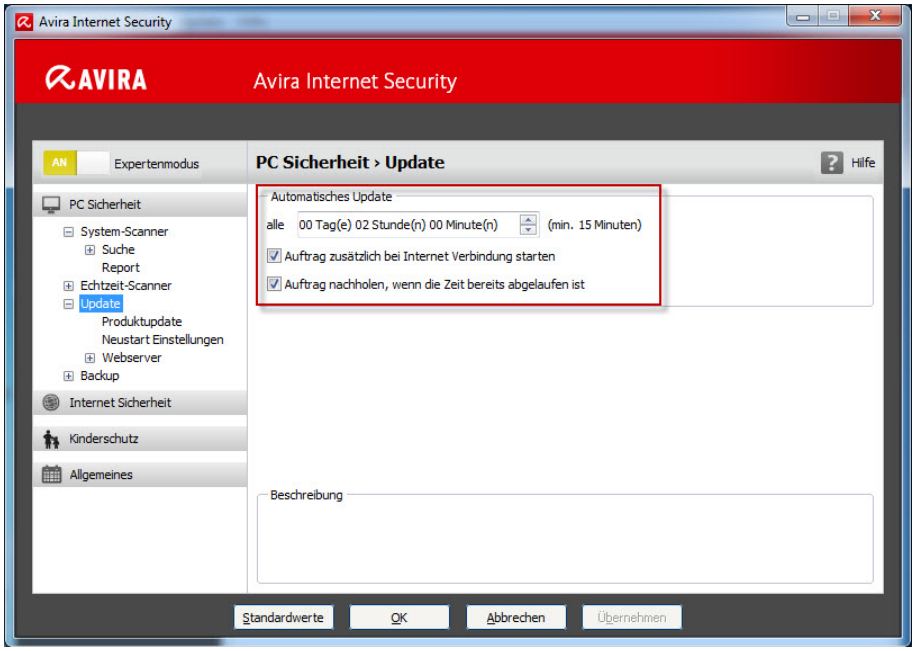
Das Update der Virendefinitionen ist auf einen Intervall von zwei Stunden voreingestellt. Sollte ein anderer Zeitpunkt oder ein häufigeres Update erforderlich sein, kann diese Einstellung wie folgt verändert werden.

► Starten des Avira Control Center

► Schalten Sie den *Expertenmodus* über *Extras* > *Konfiguration* an

Klicken Sie in der Avira Benutzeroberfläche auf den Menüpunkt PC *Sicherheit* > *Update* auf der linken Seite. Im Hauptfenster der Benutzeroberfläche erscheint jetzt die Oberfläche, in welcher alle eingestellten Updateaufträge angezeigt werden.

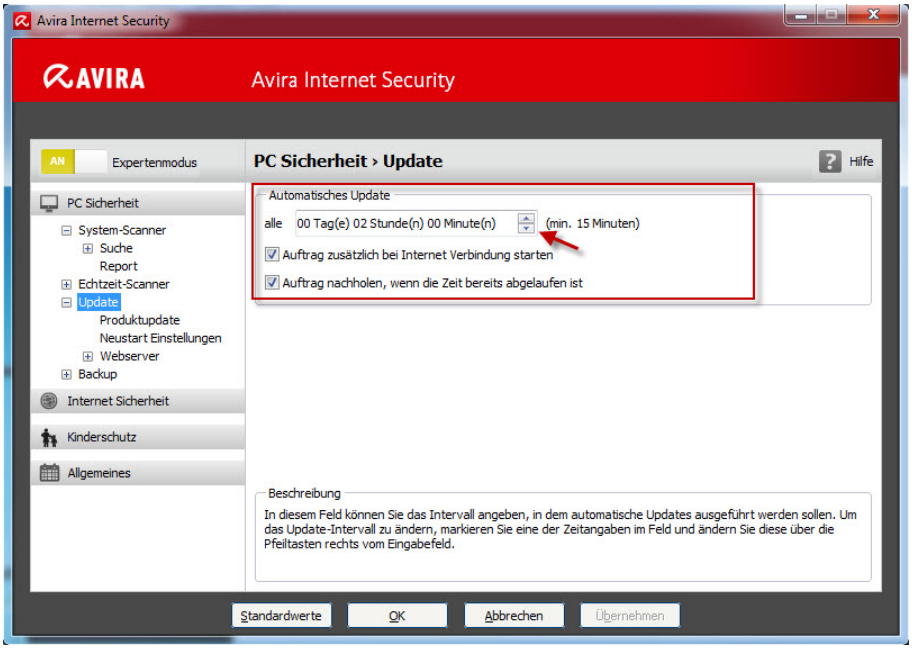
Vorkonfiguriert ist hier ein Update alle zwei Stunden mit zusätzlich aktiviertem Auftrag bei Internetverbindung ein Update zu starten.



5.1 Änderung des Update-Auftrags

In dem Feld „Automatisches Update“ können Sie das Intervall angeben, in dem automatische Updates ausgeführt werden sollen.

Um das Update-Intervall zu ändern, markieren Sie eine der Zeitangaben im Feld und ändern Sie diese über die Pfeiltasten rechts vom Eingabefeld.



Bei aktivierter Option „Auftrag zusätzlich bei Internet Verbindung starten“ werden Update-Aufträge zusätzlich zum festgelegten Update-Intervall bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

Mit der Option „Auftrag nachholen, wenn die Zeit bereits abgelaufen ist“ besteht die Möglichkeit, Update-Aufträge, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, nachträglich durchzuführen.

5.2 Produktupdate

Unter dem Menüpunkt „Produktupdate“ haben Sie vier verschiedene Konfigurationsmöglichkeiten, wie ein Update ausgeführt werden soll.

- Produktupdates herunterladen und automatisch installieren (empfohlen)

  Sobald Produktupdates verfügbar sind, werden diese heruntergeladen und automatisch installiert.

- Produktupdates herunterladen. Falls ein Neustart erforderlich ist, das Update nach dem nächsten Neustart des Systems installieren, ansonsten sofort installieren

  Sobald Produktupdates verfügbar sind werden diese heruntergeladen und automatisch installiert, unter der Voraussetzung, dass kein Neustart des Rechners erforderlich ist. Ansonsten werden sie erst nach dem nächsten, benutzergesteuerten Neustart des Systems installiert.

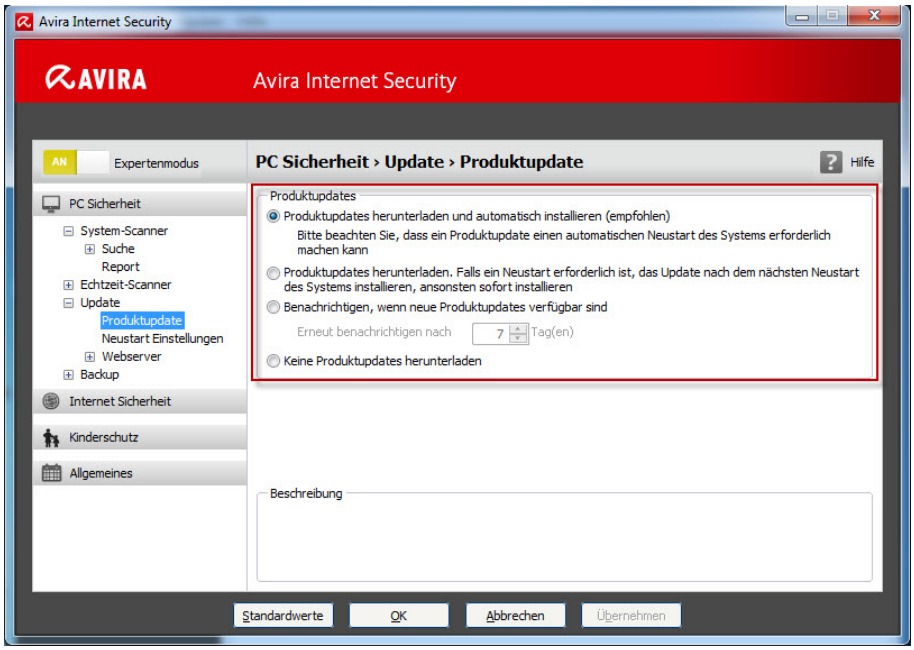
- Benachrichtigen, wenn neue Produktupdates verfügbar sind

  Bei dieser Option erhalten Sie nur eine Desktopbenachrichtigung in Form eines Popup-Fensters, wenn neue Produktupdates verfügbar sind.

- Keine Produktupdates herunterladen

  Hiermit erfolgen keine automatischen Produktupdates oder Benachrichtigungen bei verfügbaren Produktupdates durch den Updater.

Hinweis
Ein Update der Virendefinitionsdatei und der Suchengine erfolgt bei jedem ausgeführten Update unabhängig von den Einstellungen zum Produktupdate.



5.3 Neustart Einstellungen

Falls Sie eine automatische Ausführung von Produktupdates unter *Update* > *Produktupdates* eingestellt haben, können Sie bei „Neustart Einstellungen“ zwischen verschiedenen Optionen zur Meldung des Neustarts und Abbruch des Neustarts wählen.

- Neustart des Rechners nach n Sekunden

  Diese Option führt nach dem angegebenen Zeitintervall automatisch den Neustart aus, der nach einem Produktupdate erforderlich ist. Es erscheint eine Countdown-Meldung ohne Möglichkeit den Rechnerneustart abzubrechen.

- Periodische Neustarterinnerung

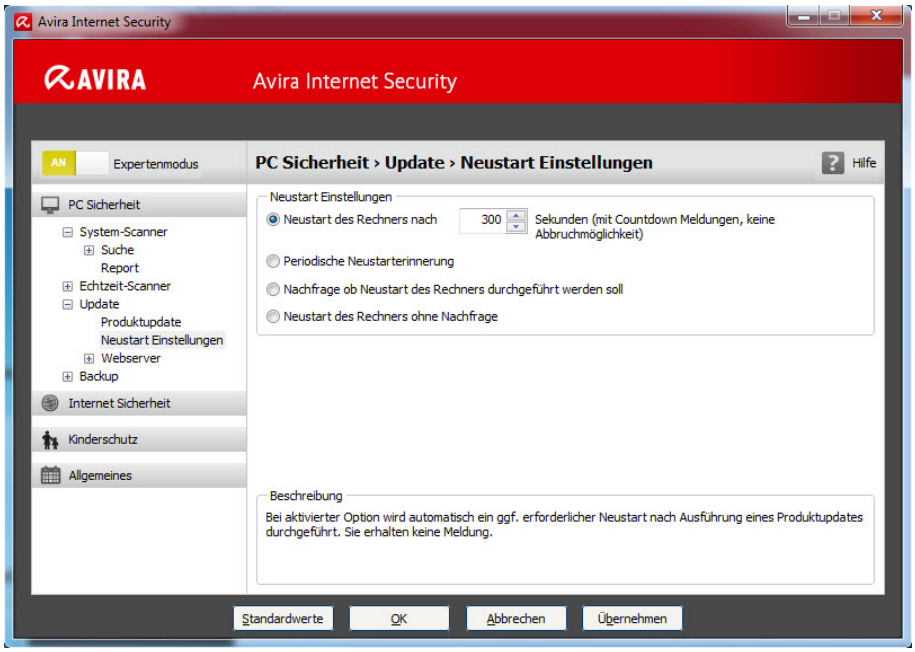
  Der erforderliche Neustart wird nicht automatisch durchgeführt. Sie erhalten im angegebenen Zeitintervall Meldungen ohne Abbruchmöglichkeiten für den Neustart. In den Meldungen können Sie den Neustart des Rechners bestätigen oder die Option „Weiter erinnern“ auswählen.

- Nachfrage ob Neustart des Rechners durchgeführt werden soll

  Bei dieser Option erhalten Sie eine einmalige Meldung, in der Sie den Neustart bestätigen oder abbrechen können

- Neustart des Rechners ohne Nachfrage

  Hiermit wird automatisch der erforderliche Neustart des Rechners durchgeführt. Sie erhalten keine Meldung



Ergänzungen zu diesem Dokument finden Sie:

- In der Onlinehilfe über das Programm (Taste F1)
- Im Avira Benutzerhandbuch
- In unserer Wissensdatenbank

Ausgabe Q3-2012

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