AVG Internet Security

Gebruikershandleiding

Documentrevisie AVG.01 (9/16/2015)

Inhoud

1. Inleiding

Deze gebruikershandleiding bevat uitgebreide informatie voor gebruikers van **AVG Internet Security**.

AVG Internet Security biedt een meerlagige beveiliging voor uw online activiteiten, zodat u zich geen zorgen hoeft te maken over identiteitsdiefstal, virussen of het bezoeken van schadelijke sites. Met AVG Protective Cloud Technology en AVG Community Protection Network voor het verzamelen van informatie over de nieuwste bedreigingen, die we delen met onze community, zodat u de beste bescherming krijgt. U kunt veilig online winkelen en bankieren, zorgeloos actief zijn op sociale netwerken of surfen en zoeken in de wetenschap dat u in realtime wordt beschermd.

Mogelijk wilt u nog andere bronnen van informatie gebruiken:

- ***Help-bestand***: een onderdeel *Problemen oplossen* is rechtstreeks vanuit het Help-bestand in **AVG Internet Security** *beschikbaar (druk op F1 vanuit een willekeurig dialoogvenster in de toepassing om het Help-bestand te openen)*. Deze sectie biedt een lijst met de meest voorkomende situaties waarin een gebruiker behoefte heeft aan professionele hulp met betrekking tot een technisch probleem. Selecteer de situatie die uw probleem het beste beschrijft en klik op de koppeling om gedetailleerde instructies weer te geven voor het oplossen van het probleem.

- ***Ondersteuningscentrum op de AVG-website***: het is ook mogelijk om naar een oplossing voor uw probleem te zoeken op de website van AVG (*http://www.avg.com/*). In de sectie ***Ondersteuning*** vindt u een overzicht van thematische groepen over verkoopproblemen en technische problemen, een gestructureerde sectie met veelgestelde vragen en alle beschikbare contactgegevens.

- ***AVG ThreatLabs***: een speciale AVG-website (*http://www.avg.com/about-viruses*) over virussen met overzichtelijke informatie over online bedreigingen. Daarnaast vindt u hier instructies voor het verwijderen van virussen en spyware en advies met betrekking tot hoe u beveiligd kunt blijven.

- ***Discussieforum***: u kunt ook gebruikmaken van het AVG-discussieforum op http://community.avg.com/.

2. AVG-installatievereisten

2.1. Ondersteunde besturingssystemen

AVG Internet Security is ontworpen om werkstations met de volgende besturingssystemen te beschermen:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (alle edities)
- Windows 7 (alle edities)
- Windows 8 (alle edities)
- Windows 10 (alle edities)

(en mogelijk hogere servicepacks voor bepaalde besturingssystemen)

***Opmerking**: Het onderdeel Identiteit wordt niet ondersteund in Windows XP x64. Onder deze besturingssystemen kunt u AVG Internet Security installeren zonder het onderdeel Identity Protection.*

2.2. Minimale en aanbevolen hardwarevereisten

Minimale hardwarevereisten voor **AVG Internet Security**:

- Intel Pentium CPU van 1,5 GHz of sneller
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM-geheugen
- 1.3 GB beschikbare ruimte op de vaste schijf *(voor de installatie)*

Aanbevolen hardwarevereisten voor **AVG Internet Security**:

- Intel Pentium CPU van 1,8 GHz of sneller
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM-geheugen
- 1.6 GB beschikbare ruimte op de vaste schijf *(voor de installatie)*

3. AVG-installatieprocedure

Als u **AVG Internet Security** op uw computer wilt installeren, moet u over het meest recente installatiebestand beschikken. Download het installatiebestand van de AVG-website (http://www.avg.com/) om er zeker van te zijn dat u de meest recente versie van **AVG Internet Security** installeert. In de sectie ***Ondersteuning*** vindt u een gestructureerd overzicht van de installatiebestanden voor elke versie van AVG. Als u het installatiebestand hebt gedownload en opgeslagen op uw vaste schijf, kunt u de installatieprocedure starten. De installatie heeft de vorm van een reeks eenvoudige en begrijpelijke dialoogvensters. Elk dialoogvenster bevat een beknopte beschrijving van de afzonderlijke stap van het installatieproces. Hieronder volgt een gedetailleerde uitleg van elk dialoogvenster:

3.1. Welkom!

Het installatieproces start met het dialoogvenster ***Welkom bij AVG Internet Security***:

Taalselectie

In dit dialoogvenster kunt u de taal selecteren die voor het installatieproces wordt gebruikt. Klik op de keuzelijst naast de optie ***Taal*** om het taalmenu te openen. Selecteer de gewenste taal. Het installatieproces wordt vervolgens voortgezet in de taal die u hebt gekozen. Dit is ook de taal waarin de toepassing wordt geïnstalleerd. U hebt wel de optie om over te schakelen naar het Engels, dat altijd standaard wordt geïnstalleerd als tweede taal.

Licentieovereenkomst voor eindgebruikers en privacybeleid.

Voordat u het installatieproces voortzet, raden we u aan om kennis te nemen van de ***Licentieovereenkomst voor eindgebruikers*** en het ***privacybeleid***. U kunt beide documenten openen via de actieve koppelingen onder in het dialoogvenster. Klik op de hyperlinks om een nieuw dialoog- of browservenster te openen met de

volledige tekst van het betreffende document. Lees deze juridisch bindende documenten zorgvuldig door. Door te klikken op de knop ***Doorgaan*** bevestigt u dat u instemt met de documenten.

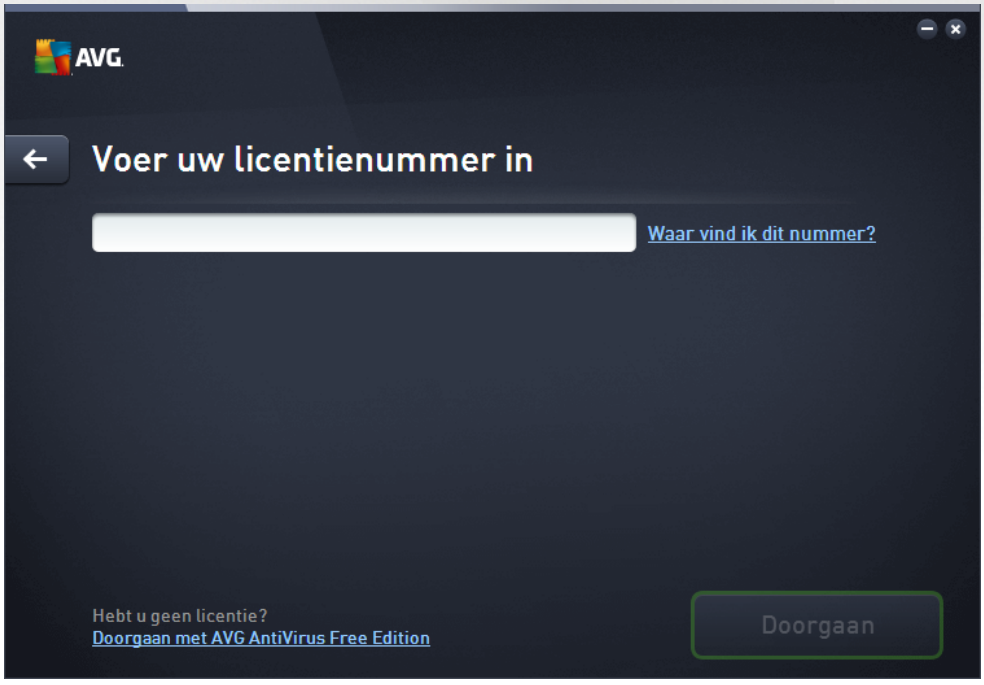
Doorgaan met de installatie

Door te klikken op de knop ***Doorgaan*** gaat u door met de installatie. U wordt gevraagd om uw licentienummer op te geven. Als u dat hebt gedaan, verloopt de installatie verder volledig automatisch. We raden de meeste gebruikers aan om deze standaardoptie te gebruiken. **AVG Internet Security** wordt dan geïnstalleerd met alle vooraf door de leverancier ingestelde instellingen. Die configuratie combineert maximale bescherming met een efficiënt gebruik van bronnen. Als het in de toekomst nodig mocht zijn om de configuratie aan te passen, kunt u dat altijd rechtstreeks in de toepassing doen.

Het alternatief is de optie ***Custom Installation (Aangepaste installatie)*** die beschikbaar is als hyperlink onder de knop ***Doorgaan***. Een aangepaste installatie wordt alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om de toepassing te installeren met afwijkende instellingen, bijvoorbeeld om te voldoen aan specifieke systeemvereisten. Als u deze keuze maakt, wordt na het opgeven van uw licentienummer het dialoogvenster ***Customize your installation (Uw installatie aanpassen)*** geopend, waar u de gewenste instellingen kunt opgeven.

3.2. Voer uw licentienummer in

In het dialoogvenster ***Licentie activeren*** wordt u gevraagd uw licentienummer in het tekstveld in te voeren:



Waar vindt u uw licentienummer

Het verkoopnummer staat op de cd-hoes in de **AVG Internet Security**-doos. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van **AVG Internet Security** online. U moet dat nummer precies zo typen als het wordt weergegeven. Als u beschikt over de digitale versie van het

licentienummer (*in de e-mail*), wordt u aangeraden het nummer te kopiëren en te plakken.

Kopiëren en plakken gebruiken

Gebruik ***kopiëren en plakken*** om uw **AVG Internet Security**-licentienummer in het programma te plakken, zodat u er zeker van kunt zijn dat het nummer op de juiste wijze wordt ingevoerd. Ga als volgt te werk:

- Open het e-mailbericht dat uw licentienummer bevat.
- Klik met de linkermuisknop aan het begin van het licentienummer, houd de muisknop ingedrukt, sleep de muiswijzer naar het einde van het nummer en laat vervolgens de knop los. Het nummer is nu gemarkeerd.
- Druk op de toets ***Ctrl***, houd deze toets ingedrukt en druk vervolgens op ***C***. Het nummer wordt gekopieerd.
- Klik op de positie waar u het gekopieerde nummer wilt plakken.
- Druk op de toets ***Ctrl***, houd deze toets ingedrukt en druk vervolgens op ***V***. Het nummer wordt op de geselecteerde locatie geplakt.

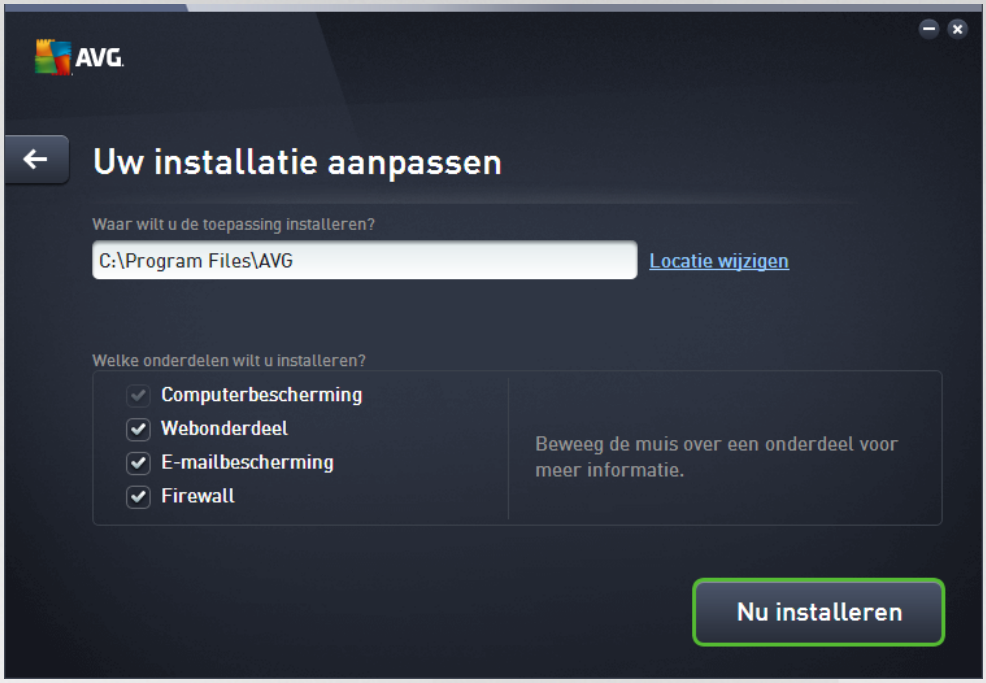
Knoppen

Zoals in de meeste installatievensters zijn er drie knoppen beschikbaar:

- ***Annuleren*** - klik hierop om het installatieproces onmiddellijk af te sluiten; **AVG Internet Security** wordt niet geïnstalleerd.
- ***Terug*** - klik hierop als u wilt terugkeren naar het vorige installatievenster.
- ***Volgende*** - klik hierop als u de installatie wilt voortzetten en wilt doorgaan met de volgende stap.

3.3. Uw installatie aanpassen

In het dialoogvenster ***Aangepaste opties*** kunt u gedetailleerde instellingen opgeven voor de installatie:



In het dialoogvenster ***Onderdelen selecteren*** staat een overzicht van alle onderdelen van **AVG Internet Security** die kunnen worden geïnstalleerd. Als de standaardinstellingen niet voldoen, kunt u onderdelen toevoegen of verwijderen. ***U kunt echter alleen kiezen uit onderdelen die deel uitmaken van de door u gekochte AVG Edition!*** Als u in de lijst ***Onderdelen selecteren*** een item selecteert, wordt rechts een korte beschrijving van het onderdeel weergegeven. Raadpleeg het hoofdstuk Onderdelenoverzicht van deze documentatie voor meer informatie over de functionaliteit van de onderdelen, Klik op de knop ***Standaard*** om de standaardconfiguratie, ingesteld door de leverancier, te herstellen.

In deze stap kunt u ook beslissen of u varianten van het product in een andere taal wilt installeren *(de toepassing wordt standaard geïnstalleerd in de taal die u hebt geselecteerd als communicatietaal voor de installatie en in het Engels)*.

Knoppen

Zoals in de meeste installatievensters zijn er drie knoppen beschikbaar:

- ***Annuleren*** - klik hierop om het installatieproces onmiddellijk af te sluiten; **AVG Internet Security** wordt niet geïnstalleerd.
- ***Terug*** - klik hierop als u wilt terugkeren naar het vorige installatievenster.
- ***Volgende*** - klik hierop als u de installatie wilt voortzetten en wilt doorgaan met de volgende stap.

3.4. AVG installeren

In het dialoogvenster ***Voortgang installatie*** wordt de voortgang van de installatieprocedure weergegeven, u hoeft zelf niets te doen.

Nadat het installatieproces is voltooid, wordt automatisch het volgende dialoogvenster weergegeven.

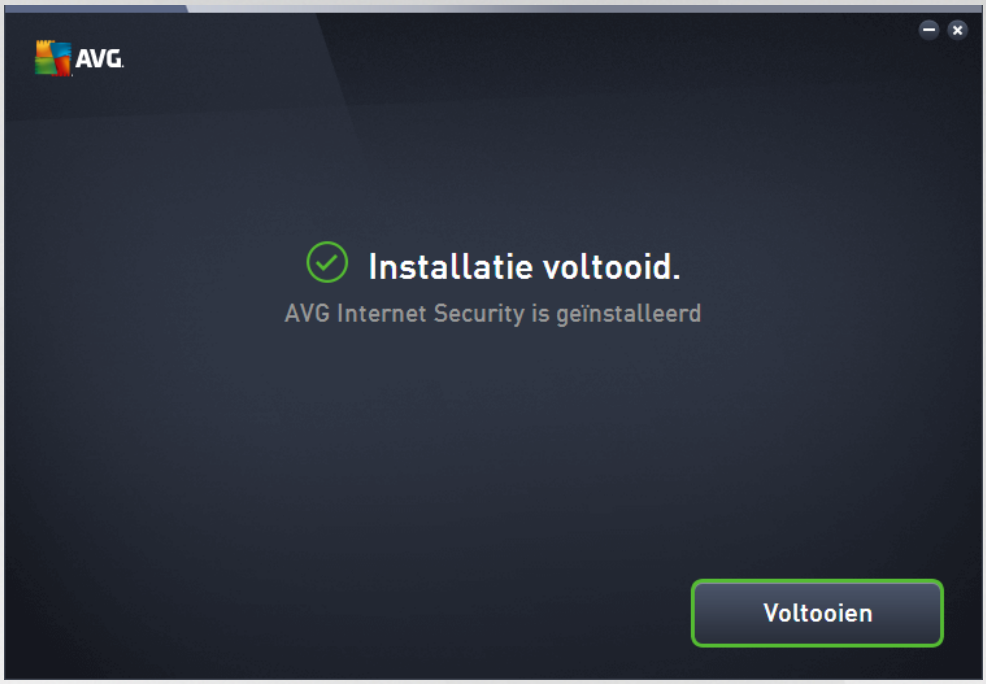
Knoppen

Dit dialoogvenster bevat twee knoppen:

- ***Minimaliseren*** - de installatie kan enkele minuten in beslag nemen. Klik op de knop om het dialoogvenster te minimaliseren. Het dialoogvenster wordt weer weergegeven als de installatie is voltooid.
- ***Annuleren*** - gebruik deze knop alleen als u het huidige installatieproces wilt beëindigen. **AVG Internet Security** wordt in dat geval niet geïnstalleerd.

3.5. Installatie voltooid

Het dialoogvenster ***Gefeliciteerd*** vormt de bevestiging van het feit dat **AVG Internet Security** is geïnstalleerd en geconfigureerd:



Programma voor productverbetering en privacybeleid

Hier kunt u aangeven of u wilt deelnemen aan het ***programma voor productverbetering*** (*zie het hoofdstuk AVG Geavanceerde instellingen / Productverbeteringsprogramma* voor meer informatie) waarmee anoniem gegevens worden verzameld over gedetecteerde bedreigingen om de algehele veiligheid op internet te vergroten. Alle gegevens worden als vertrouwelijk en in overeenstemming met het privacybeleid van AVG beschouwd. Klik op de koppeling ***Privacybeleid*** om naar de AVG-website (http://www.avg.com/) met de volledige tekst van het AVG-privacybeleid te gaan. Als u instemt, laat u de optie ingeschakeld *(standaardinstelling)*.

Klik op ***Voltooien*** om de installatieprocedure te voltooien.

4. Na de installatie

4.1. Updateschema virusdatabase

Na de installatie *(en zo nodig na opnieuw opstarten)* voert **AVG Internet Security** automatisch een update uit voor de virusdatabase en voor alle onderdelen, en worden alle functies ingeschakeld. Dat kan enkele minuten duren. Tijdens het updateproces wordt informatie over de update weergegeven in het hoofdvenster. Wacht tot het updateproces is voltooid en **AVG Internet Security** volledig gereed is om u te beschermen!

4.2. Productregistratie

Neem nadat u de installatie van **AVG Internet Security** hebt voltooid even de tijd om uw product online te registreren op de AVG-website (*http://www.avg.com/*). Na de registratie beschikt u over volledige toegang tot uw AVG-gebruikersaccount, de nieuwsbrief van AVG Update en andere services die alleen beschikbaar zijn voor geregistreerde gebruikers. De eenvoudigste manier waarop u het programma kunt registreren, is door dit rechtstreeks vanuit de gebruikersinterface van **AVG Internet Security** te doen. Selecteer Opties / Nu registreren in het menu. De pagina ***Registratie*** op de AVG-website (*http://www.avg.com/*) wordt geopend. Volg de instructies op deze pagina.

4.3. Toegang tot gebruikersinterface

Het AVG-hoofddialoogvenster kan op verscheidene manieren worden geopend:

- dubbelklik op het AVG-pictogram in het systeemvak
- dubbelklik op het pictogram van AVG op het bureaublad
- via het menu ***Start / Alle programma's / AVG / AVG Protection***

4.4. Volledige computerscan

Het risico bestaat dat er een computervirus naar uw computer is overgebracht voordat u **AVG Internet Security** hebt geïnstalleerd. Voer daarom een volledige scan van de computer uit om zeker te weten dat uw pc niet geïnfecteerd is. De eerste scan kan behoorlijk lang duren *(ongeveer een uur)*, maar het is wel raadzaam om deze eerste scan te starten om er zeker van te zijn dat uw computer niet is geïnfiltreerd door een bedreiging. Zie voor instructies voor het uitvoeren van een scan van uw computer het hoofdstuk AVG scannen.

4.5. De EICAR-test

Als u zeker wilt weten of **AVG Internet Security** juist is geïnstalleerd, kunt u de EICAR-test uitvoeren.

De EICAR-test is een standaardmethode die absoluut veilig is, waarmee u kunt testen of uw antivirussysteem goed functioneert. U kunt het Eicar-virus doorgeven omdat het geen echt virus betreft en omdat het geen viruscodefragmenten bevat. De meeste producten reageren op deze test alsof het een echt virus betreft (*het bestand heeft meestal een duidelijke naam, zoals "EICAR-AV-Test"*). U kunt het Eicar-virus downloaden vanaf de Eicar-website op www.eicar.com. U vindt hier ook de benodigde informatie voor het uitvoeren van de Eicar-test.

Download het bestand *eicar.com* en sla het op naar uw lokale vaste schijf. Direct nadat u de download van het

testbestand bevestigt, wordt in **AVG Internet Security** gereageerd met een waarschuwing. Deze waarschuwing toont aan dat AVG goed op uw computer is geïnstalleerd.

Als het EICAR-testbestand door AVG niet als virus wordt gedetecteerd, moet u uw programmaconfiguratie opnieuw controleren.

4.6. AVG-standaardconfiguratie

De standaardconfiguratie (*de manier waarop de toepassing direct na de installatie is ingesteld*) van **AVG Internet Security** is door de leverancier van de software zo ingesteld dat alle onderdelen en functies optimaal presteren. ***Wijzig de configuratie van AVG alleen als u hier een goede reden voor hebt. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers.*** Als u de configuratie van AVG wilt wijzigen om deze aan uw wensen aan te passen, gaat u naar AVG Geavanceerde instellingen: selecteer *Opties/Geavanceerde instellingen* en bewerk de AVG-configuratie in het dialoogvenster Geavanceerde instellingen dat wordt geopend.

5. AVG gebruikersinterface

AVG Internet Security opent met het hoofdvenster:

Het hoofdvenster is onderverdeeld in een aantal secties:

- ***De navigatiebalk in het bovenste gedeelte*** van het hoofdvenster bestaat uit vier actieve koppelingen *(Vindt u AVG leuk, Rapporten, Ondersteuning, Opties).* Details >>
- ***Informatie over beveiligingsstatus*** biedt algemene informatie over de huidige status van uw **AVG Internet Security**. Details >>
- ***Het overzicht van geïnstalleerde onderdelen*** vindt u in een horizontale strook blokken in het midden van het hoofdvenster. De onderdelen worden weergegeven als lichtgroene blokken. In de blokken worden de pictogrammen voor de betreffende onderdelen en informatie over de onderdeelstatus weergegeven. Details >>
- ***Mijn apps*** worden weergegeven in de strook onder het midden van het hoofdvenster en bieden u een overzicht van aanvullende toepassingen voor **AVG Internet Security** die al op uw computer zijn geïnstalleerd of worden aanbevolen. Details >>
- ***Snelkoppelingen voor scannen/bijwerken*** bevinden zich in de onderste strook blokken in het hoofdvenster. Via deze knoppen hebt u direct toegang tot de belangrijkste en meest gebruikte functies van AVG. Details >>

Buiten het hoofdvenster van **AVG Internet Security** bevindt zich nog een optie die u kunt gebruiken om toegang te krijgen tot de toepassing:

- Het ***systeemvakpictogram*** bevindt zich in de rechterbenedenhoek van het beeldscherm *(in het systeemvak)* en bevat informatie over de huidige status van **AVG Internet Security**. Details >>

5.1. Navigatiebalk

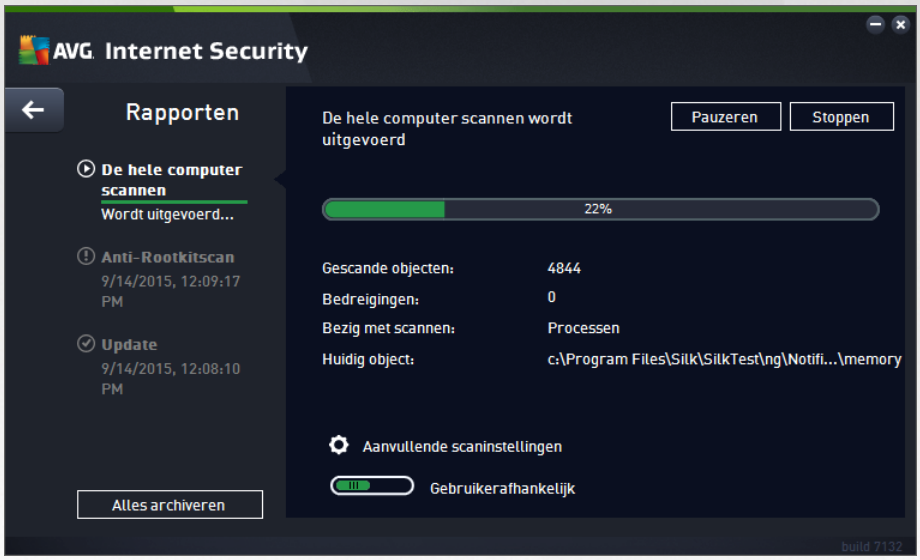
De ***navigatiebalk*** boven aan het hoofdvenster bestaat uit verschillende actieve koppelingen. De navigatiebalk bevat de volgende knoppen:

5.1.1. Volg ons op Facebook

Klik op de koppeling om verbinding te maken met de AVG Facebook-community en om de meest recente AVG-informatie, nieuws, tips en trucs te delen voor een optimale internetbeveiliging.

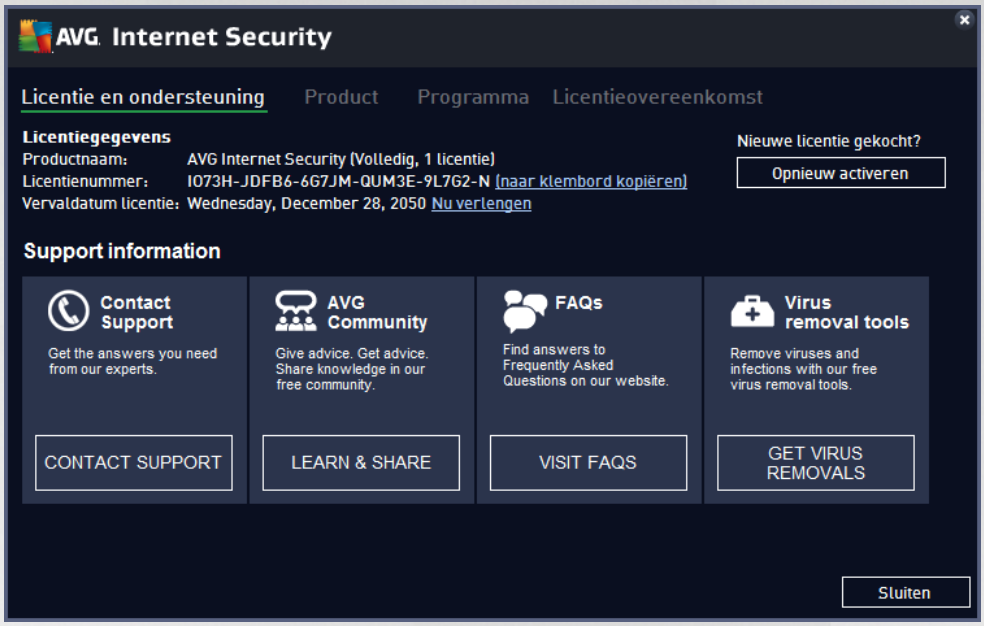
5.1.2. Rapporten

Hiermee opent u een nieuw dialoogvenster ***Rapporten*** met een overzicht van alle relevante rapporten over eerder gestarte scans en updateprocessen. Als de scan of update momenteel wordt uitgevoerd, wordt er een draaiende cirkel weergegeven naast de tekst ***Rapporten*** in de navigatiebalk in de hoofdgebruikersinterface. Klik hierop om het dialoogvenster te openen waarin de voortgang van het actieve proces wordt weergegeven:



5.1.3. Ondersteuning

Hiermee opent u een nieuw dialoogvenster met vier tabbladen waar u alle relevante informatie over **AVG Internet Security** kunt vinden:



- ***Licentie en ondersteuning*** - dit tabblad bevat informatie over de productnaam, het licentienummer en de vervaldatum. In het onderste gedeelte van het dialoogvenster vindt u een duidelijk overzicht van alle manieren waarop u contact kunt opnemen met de klantenondersteuning. Op het tabblad zijn de volgende actieve koppelingen en knoppen beschikbaar:

    - *Opnieuw activeren / Activeren* - klik hierop om het nieuwe dialoogvenster voor het ***activeren van de AVG-software*** te openen. Vul uw licentienummer in het betreffende veld in als u uw verkoopnummer *(het nummer dat u tijdens de installatie van AVG Internet Security hebt ingevoerd) wilt vervangen* of uw huidige licentienummer wilt vervangen door een ander *(bijvoorbeeld wanneer u een upgrade naar een hoger AVG-product uitvoert)*.

    - *Naar klembord kopiëren* - gebruik deze koppeling om het licentienummer te kopiëren. Op deze manier kunt u er zeker van zijn dat het licentienummer correct wordt ingevoerd.

    - *Nu verlengen* - we raden u aan om uw licentie voor **AVG Internet Security** tijdig te verlengen (minstens één maand voordat uw huidige licentie verloopt). U wordt tijdig op de hoogte gesteld van de naderende verloopdatum. Klik op deze koppeling als u doorverwezen wilt worden naar de AVG-website *(http://www.avg.com/)* waar u gedetailleerde informatie vindt over de status van uw licentie, de verloopdatum en de verlengings-/upgrade-aanbieding.

- ***Product*** - dit tabblad bevat een overzicht van de belangrijkste technische gegevens over **AVG Internet Security**, zoals productinformatie, geïnstalleerde onderdelen en geïnstalleerde e-mailbescherming.

- ***Programma*** - op dit tabblad vindt u informatie over de versie van het programmabestand en over code van derden die in het product worden gebruikt.

- ***Licentieovereenkomst*** - dit tabblad bevat de volledige tekst van de licentieovereenkomst tussen u en

AVG Technologies.

5.1.4. Opties

De onderhoudsfuncties voor **AVG Internet Security** zijn toegankelijk via het menu ***Opties***. Klik op de pijl om de vervolgkeuzelijst te openen:

- ***Computer scannen*** - een scan van de volledige computer wordt gestart.
- ***Geselecteerde map scannen*** - hiermee wordt overgeschakeld naar de scaninterface van AVG zodat u in de bestandsstructuur van uw computermappen en bestanden kunt selecteren die moeten worden gescand.
- ***Bestand scannen*** - u kunt in de bestandsstructuur van de computer een afzonderlijk bestand selecteren dat u wilt scannen. Klik op deze optie om een nieuw venster te openen met de bestandsstructuur van de computer. Selecteer het gewenste bestand en bevestig de start van het scannen.
- ***Update*** - hiermee kunt u automatisch de updateprocedure voor **AVG Internet Security** starten.
- ***Bijwerken vanuit directory*** - het updateproces wordt uitgevoerd op basis van de updatebestanden in een opgegeven map op de lokale vaste schijf. Deze optie wordt echter alleen aanbevolen als noodprocedure, bijvoorbeeld onder omstandigheden waarbij er geen verbinding is met internet (uw computer is bijvoorbeeld geïnfecteerd en afgesloten van internet; uw computer is aangesloten op een netwerk zonder verbinding met internet, enz.). Selecteer in het venster dat wordt geopend de map waarin u eerder het updatebestand hebt opgeslagen, en start de updateprocedure.
- ***Quarantaine*** - hiermee opent u de interface voor de quarantaineruimte waar AVG alle verwijderde infecties in plaatst. In de quarantaine worden de geïnfecteerde bestanden geïsoleerd, zodat de veiligheid van uw computer gewaarborgd blijft en de bestanden in de toekomst mogelijk kunnen worden hersteld.
- ***Historie*** - biedt specifieke submenuopties:
  - *Scanresultaten* - hiermee opent u een dialoogvenster met een overzicht van scanresultaten.
  - *Resultaten Resident Shield* - hiermee opent u een dialoogvenster met een overzicht van bedreigingen die zijn gedetecteerd door Resident Shield.
  - *Resultaten Identity Protection* - hiermee opent u een dialoogvenster met een overzicht van bedreigingen die zijn gedetecteerd door het onderdeel Identity Protection.
  - *Resultaten E-mail Protection* - hiermee opent u een dialoogvenster met een overzicht van e-mailbijlagen die als gevaarlijk zijn aangemerkt door het onderdeel E-mail Protection.
  - *Resultaten Online Shield* - hiermee opent u een dialoogvenster met een overzicht van bedreigingen die zijn gedetecteerd door Online Shield.
  - *Logboek eventhistorie* - hiermee opent u het dialoogvenster met de geschiedenis van alle vastgelegde acties van **AVG Internet Security**.
  - *Firewall logboek* - hiermee opent u een dialoogvenster met een gedetailleerd overzicht van alle Firewall-acties.

- ***Geavanceerde instellingen*** - hiermee opent u het dialoogvenster Geavanceerde instellingen van AVG waarin u de configuratie van **AVG Internet Security** kunt bewerken. Doorgaans is het raadzaam de standaardinstellingen aan te houden zoals deze zijn ingesteld door de leverancier van de software.

- ***Firewall-instellingen*** - hiermee opent u een afzonderlijk dialoogvenster voor de geavanceerde configuratie van het onderdeel Firewall.

- ***Inhoud van Help*** - hiermee opent u de Help-bestanden van AVG.

- ***Ondersteuning*** - hiermee opent u het dialoogvenster voor ondersteuning met alle contactgegevens en ondersteuningsinformatie.

- ***Uw AVG-Web*** - hiermee opent u de website van AVG (*http://www.avg.com/*).

- ***Over virussen en bedreigingen*** - hiermee opent u de online virusencyclopedie op de AVG-website (*http://www.avg.com/*) waarin u gedetailleerde informatie over een herkend virus kunt vinden.

- ***Activeren/Opnieuw activeren*** - hiermee opent u het dialoogvenster voor activeren met het licentienummer dat u hebt opgegeven tijdens het installatieproces. In dit dialoogvenster kunt u uw licentienummer bewerken om het verkoopnummer (*het nummer waarmee u AVG hebt geïnstalleerd*) of het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*) te vervangen. Als u de proefversie van **AVG Internet Security** gebruikt, worden de laatste twee items weergegeven als ***Nu kopen*** en ***Activeren*** zodat u meteen de volledige versie van het programma kunt aanschaffen. Als u **AVG Internet Security** hebt geïnstalleerd met een verkoopnummer, worden deze items weergegeven als ***Registreren*** en ***Activeren***:

- ***Nu registreren/MyAccount*** - hiermee maakt u verbinding met de registratiepagina van de AVG-website (*http://www.avg.com/*). Voer uw registratiegegevens in. Uitsluitend klanten die hun AVG-product registreren, komen in aanmerking voor gratis technische ondersteuning.

- ***Info AVG*** - hiermee opent u een nieuw dialoogvenster met vier tabbladen met informatie over uw aangeschafte licentie en de beschikbare ondersteuning, product- en programma-informatie en de volledige licentieovereenkomst. *(Hetzelfde dialoogvenster kan worden geopend via de koppeling Ondersteuning in het hoofdnavigatievenster.)*

5.2. Informatie over beveiligingsstatus

Het gedeelte ***Info Beveiligingsstatus*** bevindt zich in het bovenste deel van het hoofdvenster van **AVG Internet Security**. In deze sectie staat altijd informatie over de huidige beveiligingsstatus van **AVG Internet Security**. Hieronder volgt een overzicht van de pictogrammen die in deze sectie kunnen worden weergegeven, en hun betekenis:

 - het groene pictogram geeft aan dat ***AVG Internet Security volledig functioneel is.*** Uw computer is volledig beveiligd, de bestanden zijn bijgewerkt en alle geïnstalleerde onderdelen werken correct.

 - het gele pictogram duidt op de waarschuwing dat ***een of meer onderdelen niet correct zijn geconfigureerd*** en dat u de betreffende eigenschappen/instellingen moet controleren. Er is geen wezenlijk probleem opgetreden in **AVG Internet Security**; waarschijnlijk hebt u gewoon om de een of andere reden een onderdeel uitgeschakeld. De beveiliging is nog steeds ingeschakeld. Neem echter wel even de tijd om de instellingen van het probleemonderdeel te controleren. Het onjuist geconfigureerde onderdeel wordt met een oranje strook weergegeven in de hoofdgebruikersinterface.

Het gele pictogram wordt ook weergegeven als u de foutstatus van een onderdeel hebt genegeerd. De optie ***Foutstatus negeren*** is toegankelijk via Geavanceerde instellingen / Foutstatus negeren. Hier kunt u aangeven dat u zich bewust bent van de foutstatus van een onderdeel en dat u om welke reden ook **AVG Internet Security** zo wilt instellen dat u niet wordt gewaarschuwd via het systeemvakpictogram. Het kan zijn dat u deze optie in een specifieke situatie moet gebruiken. U wordt in een dergelijk geval echter aangeraden om de optie ***Foutstatus negeren*** zo snel mogelijk uit te schakelen.

Het gele pictogram wordt bovendien weergegeven als **AVG Internet Security** vereist dat uw computer opnieuw moet worden opgestart (***Opnieuw opstarten noodzakelijk***). Start in dit geval uw computer opnieuw op.

 - het oranje pictogram geeft aan dat ***AVG Internet Security een kritieke status heeft***. Een of meer onderdelen functioneren niet correct en **AVG Internet Security** kunnen uw computer niet beschermen. Besteed onmiddellijk aandacht aan het probleem en probeer het te verhelpen. Als het u niet lukt de fout zelf te herstellen, neemt u contact op met het team voor technische ondersteuning van AVG.

In gevallen waarin AVG Internet Security niet is ingesteld voor optimale prestaties, wordt er naast de informatie over de beveiligingsstatus een nieuwe knop met de naam Klik om dit te herstellen (of Klik om alles te herstellen als het probleem meerdere onderdelen betreft) weergegeven. Klik op de knop om het programma automatisch te controleren en te configureren. U kunt op deze wijze AVG Internet Security instellen voor maximale prestaties en een maximaal beveiligingsniveau.

We raden u nadrukkelijk aan het ***gedeelte met informatie over de beveiligingsstatus*** goed in de gaten te houden en in het geval van een probleem direct te proberen het probleem op te lossen. Uw computer loopt anders gevaar.

Opmerking: *AVG Internet Security u kunt ook, wanneer u maar wilt, statusinformatie opvragen via het systeemvakpictogram.*

5.3. Overzicht van onderdelen

Het ***overzicht van geïnstalleerde onderdelen*** vindt u in een horizontale strook blokken in het midden van het hoofdvenster. De onderdelen worden weergegeven als lichtgroene blokken. In de blokken worden de pictogrammen voor de betreffende onderdelen weergegeven. Elk blok biedt informatie over de huidige beschermingsstatus. Als het onderdeel correct is geconfigureerd en volledig functioneel is, wordt de informatie in groene letters weergegeven. Als het onderdeel is beëindigd, de functionaliteit beperkt is of er een fout is opgetreden, wordt er een waarschuwing in een oranje tekstveld weergegeven. ***U wordt in dat geval sterk aangeraden de instellingen van het betreffende onderdeel te controleren.***

Beweeg de muisaanwijzer over het onderdeel om een korte tekst weer te geven onder in het hoofdvenster. De tekst vormt een elementaire inleiding op de functionaliteit van het onderdeel. Daarnaast wordt informatie over de huidige status van het onderdeel gegeven en wordt aangegeven welke services van het onderdeel niet goed zijn geconfigureerd.

Lijst met geïnstalleerde onderdelen

In **AVG Internet Security** bevat het ***Overzicht van onderdelen*** informatie over de volgende onderdelen:

- ***Computer*** - dit onderdeel omvat twee services: ***AntiVirus Shield*** detecteert virussen, spyware, wormen, Trojaanse paarden, ongewenste uitvoerbare bestanden of bibliotheken op uw systeem en beschermt u tegen schadelijke adware. ***Anti-Rootkit*** scant op gevaarlijke rootkits verborgen in

toepassingen, stuurprogramma's of bibliotheken. Details >>

- ***Surfen*** - beschermt u tegen webaanvallen terwijl u zoekt en surft op internet. Details >>
- ***Identiteit*** - Met het onderdeel wordt de service ***Identity Shield*** uitgevoerd die uw digitale bezittingen continu tegen nieuwe en onbekende bedreigingen op internet beschermt. Details >>
- ***E-mails*** - controleert uw binnenkomende e-mailberichten op spam en blokkeert virussen, phishingaanvallen of andere bedreigingen. Details >>
- ***Firewall*** - controleert alle communicatie op elke netwerkpoort om u te beschermen tegen kwaadaardige aanvallen. Details >>

Beschikbare acties

- ***Beweeg de muis over een onderdeelpictogram*** om dit binnen het onderdelenoverzicht te markeren. Dan wordt in het onderste deel van de gebruikersinterface ook de beschrijving van de basisfunctionaliteit van het onderdeel weergegeven.
- ***Klik op het pictogram van een onderdeel*** om de interface voor het onderdeel te openen waarin informatie wordt weergegeven over de huidige status van het onderdeel en waarin u toegang hebt tot de configuratie en statistische gegevens.

5.4. Mijn apps

In de sectie ***Mijn apps*** *(de groene blokken onder de ingestelde onderdelen)* vindt u een overzicht van aanvullende AVG-toepassingen die al zijn geïnstalleerd of worden aanbevolen. De blokken worden onder bepaalde voorwaarden weergegeven en kunnen voor de volgende toepassingen staan:

- ***Mobile protection*** is een toepassing die uw mobiele telefoon beschermt tegen virussen en malware. Daarnaast kunt u hiermee uw smartphone extern traceren als u deze kwijtraakt.
- ***LiveKive*** is speciaal bedoeld voor online gegevensback-ups op beveiligde servers. LiveKive maakt automatisch back-ups van al uw bestanden, foto's en muziek op één veilige plaats, zodat u deze kunt delen met familie en vrienden en zodat deze bereikbaar zijn vanaf elk apparaat met toegang tot internet, waaronder iPhones en apparaten met Android.
- ***Family Safety*** helpt u uw kinderen beschermen tegen onbehoorlijke websites, media-inhoud en online zoekopdrachten en rapporteert over hun online activiteiten. AVG Family Safety maakt gebruik van controletechnologie om de activiteiten van uw kind in chatrooms en op sociale netwerksites in de gaten te houden. Als het woorden, zinnen of taalgebruik detecteert die worden gebruikt om kinderen online te benadelen, ontvangt u direct een sms- of e-mailbericht. U kunt voor elk van uw kinderen een passend niveau aan bescherming instellen en hen afzonderlijk volgen met behulp van unieke aanmeldingen.
- De toepassing ***PC TuneUp*** is een geavanceerd hulpmiddel voor gedetailleerde analyses en correcties van het systeem op het gebied van de wijze waarop de snelheid en algehele prestaties van uw computer kunnen worden verbeterd.
- De ***AVG Toolbar*** is beschikbaar in uw internetbrowser en beschermt u terwijl u op internet surft.

Klik op een blok voor gedetailleerde informatie over een van de toepassingen in ***Mijn apps***. Vervolgens wordt u doorverwezen naar de speciale AVG-webpagina waar u het onderdeel direct kunt downloaden.

5.5. Snelkoppelingen voor scannen/bijwerken

Snelkoppelingen bevinden zich onder in de gebruikersinterface van **AVG Internet Security**. Deze koppelingen bieden onmiddellijk toegang tot de belangrijkste en meest gebruikte functies van de toepassing, zoals scannen en bijwerken De snelkoppelingen zijn toegankelijk vanuit alle dialoogvensters in de gebruikersinterface:

- ***Nu scannen*** - deze knop bestaat uit twee gedeelten. Volg de koppeling ***Nu scannen*** om de scan De hele computer scannen te starten. U kunt de voortgang bekijken in het automatisch geopende venster Rapporten. Met de knop ***Opties*** opent u het dialoogvenster ***Scanopties*** waarin u geplande scans kunt beheren en parameters voor De hele computer scannen / Mappen of bestanden scannen kunt configureren. *(Zie het hoofdstuk AVG scannen voor gedetailleerde informatie)*

- ***Fix performance*** - met deze knop opent u de service ***PC Analyzer***, een geavanceerd hulpmiddel voor gedetailleerde systeemanalyse en -correctie, om te achterhalen hoe de snelheid en de prestaties van de computer verbeterd kunnen worden.

- ***Nu bijwerken*** - klik op deze knop om de productupdate direct te starten. U wordt over de updateresultaten geïnformeerd in het dialoogvenster dat wordt weergegeven boven het AVG-pictogram in het systeemvak. *(Zie het hoofdstuk AVG-updates voor gedetailleerde informatie)*

5.6. Systeemvak pictogram

Het ***AVG-systeemvakpictogram*** *(op de Windows-taakbalk, rechts onder in de hoek van uw scherm)* geeft de status van **AVG Internet Security** aan. Het pictogram is altijd zichtbaar in het systeemvak, ongeacht of de gebruikersinterface van **AVG Internet Security** is geopend of gesloten:

Weergave van het AVG-systeemvakpictogram

- Als alle kleuren worden weergegeven, zonder dat er elementen aan het pictogram zijn toegevoegd, geeft het pictogram aan dat alle **AVG Internet Security** onderdelen actief en naar behoren werken. Dit pictogram wordt echter op dezelfde wijze weergegeven als een van de onderdelen niet naar behoren werkt en de gebruiker heeft besloten om de onderdeelstatus te negeren. *(Als u hebt bevestigd dat de onderdeelstatus moet worden genegeerd, geeft u daarmee aan dat u zich bewust bent van de foutstatus van het onderdeel, maar dat u niet wilt worden gewaarschuwd over situatie.)*

- Het pictogram met een uitroepteken geeft aan dat er op een onderdeel *(of meerdere onderdelen)*

een foutstatus van toepassing is. Besteed altijd aandacht aan een dergelijke waarschuwing en probeer het configuratieprobleem op te lossen als een onderdeel niet goed is ingesteld. Als u wijzigingen in de configuratie van een onderdeel wilt aanbrengen, dubbelklikt u op het systeemvakpictogram om de gebruikersinterface van de toepassing te openen. Raadpleeg de sectie over beveiligingsstatusinformatie voor gedetailleerde informatie over op welk onderdeel een foutstatus van toepassing is.

-  Het is tevens mogelijk dat het systeemvakpictogram in alle kleuren wordt weergegeven met een knipperende, roterende lichtstraal. Deze grafische weergave geeft aan dat er momenteel een update wordt uitgevoerd.

-  De alternatieve weergave van het pictogram met verschillende kleuren met een pijl geeft aan dat er **AVG Internet Security** scans worden uitgevoerd.

Informatie bij het AVG-systeemvakpictogram

Het ***AVG-systeemvakpictogram*** biedt bovendien informatie over huidige activiteiten in **AVG Internet Security** en over mogelijke statuswijzigingen in het programma (*bijvoorbeeld de automatische start van een geplande scan of update, een Firewall-profielwijziging, een statuswijziging van een onderdeel of wanneer zich een foutstatus voordoet*) via een pop-upvenster dat wordt geopend vanuit het systeemvakpictogram van AVG.

Acties die toegankelijk zijn via het AVG-systeemvakpictogram

Het ***AVG-systeemvakpictogram*** kan tevens worden gebruikt als een koppeling voor het openen van de gebruikersinterface van **AVG Internet Security**. Dubbelklik op het pictogram. Als u met de rechtermuisknop op het systeemvakpictogram klikt, opent u een snelmenu met de volgende opties:

- ***AVG openen*** - hiermee opent u de gebruikersinterface van **AVG Internet Security**.

- ***Beveiliging door AVG tijdelijk uitschakelen*** - met deze optie kunt u de volledige bescherming door **AVG Internet Security** direct uitschakelen. Maak alleen gebruik van deze optie als het absoluut noodzakelijk is! In de meeste gevallen is het niet nodig om **AVG Internet Security** uit te schakelen voordat u nieuwe software of stuurprogramma's installeert, zelfs niet als het installatieprogramma of de softwarewizard voorstelt eerst lopende programma's en toepassingen uit te schakelen om ervoor te zorgen dat er zich geen ongewenste onderbrekingen voordoen tijdens het installatieproces. Als u **AVG Internet Security** toch tijdelijk moet uitschakelen, moet u de beveiliging zo snel mogelijk opnieuw inschakelen. Uw computer is kwetsbaar en kan worden aangevallen als u verbonden bent met internet of een netwerk gedurende de tijd dat uw beveiliging is uitgeschakeld.

- ***Scan*** - klik om het snelmenu met vooraf gedefinieerde scans (*De hele computer scannen* en *Mappen of bestanden scannen*) te openen en selecteer de gewenste scan. De scan wordt onmiddellijk gestart.

- ***Firewall*** - klik om het snelmenu te openen voor snelle toegang tot alle beschikbare Firewall-modi. Maak uw selectie in het overzicht en klik om te bevestigen dat u de ingestelde Firewall-modus wilt wijzigen.

- ***Scans worden uitgevoerd...*** - dit item wordt uitsluitend weergegeven wanneer er een scan op uw computer wordt uitgevoerd. U kunt vervolgens de scanprioriteit voor die scan wijzigen, de scan onderbreken of afbreken. Bovendien zijn de volgende acties mogelijk: *Prioriteit instellen voor alle*

scans, Alle scans onderbreken en *Alle scans afbreken*.

- ***Fix performance*** - klik om het onderdeel PC Analyzer te starten.
- ***Aanmelden bij AVG MyAccount*** - hiermee opent u de MyAccount-startpagina waar u uw abonnementsproducten kunt beheren, extra bescherming kunt aanschaffen, installatiebestanden kunt downloaden, eerdere bestellingen en facturen kunt bekijken en uw persoonlijke gegevens kunt beheren.
- ***Nu bijwerken*** - een update onmiddellijk starten.
- ***Help*** - het Help-bestand op de startpagina openen.

5.7. AVG Advisor

AVG Advies is ontworpen om problemen te detecteren waardoor uw computer trager wordt of een beveiligingsrisico loopt, en suggesties te geven om het probleem op te lossen. Als uw computer *(internet, algehele prestaties)* plotseling trager wordt, is het doorgaans niet direct duidelijk wat de oorzaak is en hoe het probleem moet worden opgelost. Daarom is ***AVG Advies*** ontwikkeld: hiermee wordt een melding in het systeemvak weergegeven waarin de mogelijke oorzaak wordt beschreven en wordt aangegeven hoe u het probleem kunt oplossen. ***AVG Advies*** controleert voortdurend alle actieve processen op uw computer op mogelijke problemen en biedt tips voor het voorkomen van het probleem.

AVG Advies is zichtbaar in de vorm van een zwevend pop-upvenster boven het systeemvak:

AVG Advies controleert het volgende:

- ***de staat van geopende webbrowsers***. Webbrowsers kunnen het geheugen overbelasten, vooral als er gedurende langere tijd meerdere tabbladen of vensters geopend zijn, en te veel systeembronnen verbruiken waardoor uw computer trager wordt. In dergelijke situaties kunt u de webbrowser het beste opnieuw openen.
- ***Actieve peer-to-peer-verbindingen***. Wanneer u het P2P-protocol hebt gebruikt voor het delen van bestanden, kan de verbinding soms actief blijven en wordt een bepaalde hoeveelheid bandbreedte verbruikt. Als gevolg daarvan kan uw internetverbinding trager worden.
- ***Onbekend netwerk met een bekende naam***. Dit is doorgaans alleen van toepassing op gebruikers die verbinding met verschillende netwerken maken, doorgaans met draagbare computers: als een nieuw, onbekend netwerk dezelfde naam heeft als een bekend, veelgebruikt netwerk *(zoals Thuis of MijnWifi)*, kan dit verwarrend zijn en kunt u per ongeluk verbinding met een volledig onbekend en mogelijk onveilig netwerk maken. ***AVG Advies*** kan dit helpen voorkomen door u te waarschuwen dat de bekende naam voor een nieuw netwerk staat. Wanneer u hebt bepaald dat het onbekende netwerk veilig is, kunt u het opslaan in een ***AVG Advies***-lijst met bekende netwerken om te voorkomen dat

voor dit netwerk nog waarschuwingen worden weergegeven.

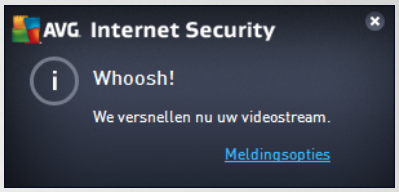
In al deze situaties waarschuwt ***AVG Advies*** u dat een probleem kan optreden en geeft het de naam en het pictogram weer van het proces of de toepassing dat het probleem veroorzaakt. ***AVG Advies*** geeft bovendien aan welke stappen kunnen worden uitgevoerd om mogelijke problemen te voorkomen.

Ondersteunde webbrowsers

De functie werkt met de volgende webbrowsers: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

Met AVG Accelerator worden online video's soepeler afgespeeld en worden extra downloads eenvoudiger. Wanneer de videoacceleratie wordt uitgevoerd, wordt u daarvan in kennis gesteld via een pop-upvenster bij het systeemvak.



6. AVG-onderdelen

6.1. Computerbescherming

Het onderdeel ***Computer*** omvat twee belangrijke beveiligingsservices: ***AntiVirus*** en ***Gegevenskluis***:

- ***AntiVirus*** bestaat uit een scanengine die alle bestanden, de systeemgebieden van de computer en verwisselbare media *(zoals USB-sticks)* en scant op bekende virussen. Gedetecteerde virussen worden geblokkeerd zodat ze geen schade kunnen aanrichten. Vervolgens worden de virussen verwijderd of in Quarantaine geplaatst. U merkt niets van dit proces aangezien deze zogenaamde residente beveiliging "op de achtergrond"wordt uitgevoerd. AntiVirus maakt ook gebruik van heuristische scanmethoden waarbij bestanden worden gescand op typische viruskenmerken. Dat betekent dat AntiVirus een nieuw, nog onbekend virus kan detecteren, als dat virus bepaalde typerende kenmerken heeft van bestaande virussen. **AVG Internet Security** kan ook mogelijk ongewenste uitvoerbare toepassingen of DLL-bibliotheken op het systeem detecteren en analyseren *(verschillende soorten spyware, adware etc.)*. Daarnaast scant AntiVirus uw systeemregister op verdachte sleutels en tijdelijke internetbestanden. U kunt hierbij instellen dat alle mogelijk ongewenste items op dezelfde wijze moeten worden verwerkt als andere infecties.

- Met de functie ***Gegevenskluis*** kunt u veilige virtuele kluizen maken om waardevolle of gevoelige gegevens in op te slaan. De inhoud van een Gegevenskluis wordt gecodeerd en beveiligd met een wachtwoord zodat niemand toegang krijgt zonder autorisatie.

Dialoogvensteropties

U schakelt tussen de twee gedeelten van het dialoogvenster door te klikken. Het actieve deelvenster wordt weergegeven met een lichtere kleur blauw. In beide gedeelten van het dialoogvenster vindt u de volgende opties. Hun functionaliteit komt overeen, ongeacht tot welke beveiligingsservice ze behoren *(AntiVirus of Gegevenskluis)*:

Ingeschakeld / Uitgeschakeld - de knop doet u mogelijk denken aan een verkeerslicht, zowel qua uiterlijk als qua functionaliteit. Klik om te schakelen tussen de twee posities. Groen staat voor ***Ingeschakeld***. Dit betekent dat de beveiligingsservice AntiVirus actief en volledig functioneel is. Rood staat voor ***Uitgeschakeld***. Dit betekent dat de service is gedeactiveerd. Als u geen goede reden hebt om de service te deactiveren, raden we u sterk aan de standaardinstellingen voor alle beveiligingsconfiguraties te behouden. Met de standaardinstellingen bent u verzekerd van een optimale balans tussen prestaties en beveiliging. Als u de service om welke reden dan ook wilt deactiveren, wordt u direct over het mogelijke risico geïnformeerd door middel van een rood ***waarschuwingsteken*** en het bericht dat u niet volledig bent beschermd. ***Activeer de service weer zo snel mogelijk.***

Instellingen - klik op de knop om te worden omgeleid naar de interface Geavanceerde instellingen. Het betreffende dialoogvenster wordt geopend en u kunt de geselecteerde service configureren, bijvoorbeeld AntiVirus. In de interface voor geavanceerde instellingen kunt u de configuratie van de beveiligingsservices in **AVG Internet Security** wijzigen, maar voor elke configuratie kan gelden dat deze alleen wordt aanbevolen voor ervaren gebruikers.

Pijl - gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar de hoofdgebruikersinterface met het overzicht van de onderdelen.

Een gegevenskluis maken

In het gedeelte ***Gegevenskluis*** van het dialoogvenster ***Computerbescherming*** vindt u de knop ***Kluis maken***. Klik op de knop om een nieuw dialoogvenster met dezelfde naam te openen, waar u de parameters van uw geplande kluis kunt opgeven. Vul alle benodigde informatie in en volg de instructies in de toepassing:

Eerst moet u de kluis een naam geven en een sterk wachtwoord instellen:

- ***Kluisnaam*** - om een nieuwe gegevenskluis te maken moet u eerst een passende naam kiezen waar u de kluis aan herkent. Als u de computer deelt met andere gezinsleden, wilt u behalve een aanduiding van de inhoud van de kluis ook misschien uw naam erin opnemen, bijvoorbeeld *E-mail van pa*.

- ***Wachtwoord maken / opnieuw invoeren*** - bedenk een wachtwoord voor uw gegevenskluis en voer het in de bijbehorende tekstvelden in. De grafische indicator rechts geeft aan of uw wachtwoord zwak *(relatief eenvoudig te achterhalen met speciale software)* of sterk is. We raden u aan een wachtwoord van minstens gemiddelde sterkte te maken. U kunt uw wachtwoord sterker maken door hoofdletters, cijfers en andere tekens zoals punten en streepjes te gebruiken. Als u er zeker van wilt zijn dat u het wachtwoord goed typt, kunt u het selectievakje ***Wachtwoord weergeven*** inschakelen *(als er niemand meekijkt)*.

- ***Wachtwoordhint*** - we raden u ten zeerste aan om ook een nuttige wachtwoordhint te maken, om u te helpen uw wachtwoord te herinneren als u het vergeten bent. Gegevenskluis is bedoeld om uw bestanden veilig te houden door alleen toegang te bieden op basis van een wachtwoord. Hier zijn geen andere oplossingen voor. Als u het wachtwoord vergeet, hebt u geen toegang meer tot de gegevens in uw gegevenskluis!

Nadat u alle benodigde gegevens in de tekstvelden hebt ingevuld, klikt u op de knop ***Volgende*** om door te gaan met de volgende stap:

In dit dialoogvenster ziet u de volgende configuratieopties:

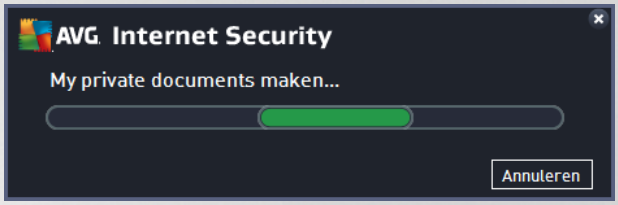
- ***Locatie*** meldt waar de gegevenskluis fysiek wordt geplaatst. Blader naar een passende bestemming op uw harde schijf of kies de vooraf gedefinieerde locatie, de map *Documenten*. Wanneer u een gegevenskluis hebt gemaakt, kunt u de locatie niet meer wijzigen.

- ***Grootte*** - u kunt vooraf de grootte van uw gegevenskluis instellen, waarmee u de benodigde ruimte op de schijf toekent aan de gegevenskluis. De waarde mag niet te klein *(minder dan u nodig hebt)* of te groot *(te veel schijfruimte wordt onnodig in beslag genomen)* instellen. Als u al weet wat u in de gegevenskluis wilt bewaren, kunt u alle bestanden in één map zetten en met de koppeling ***Map selecteren*** de totale grootte automatisch berekenen. U kunt de grootte desgewenst later aanpassen aan uw wensen.

- ***Toegang*** - met de selectievakjes van dit gedeelte maakt u handige snelkoppelingen om uw gegevenskluis te beveiligen.

Een gegevenskluis gebruiken

Wanneer u tevreden bent over de instellingen, klikt u op de knop ***Kluis maken***. Het dialoogvenster ***Gegevenskluis is nu gereed*** wordt nu weergegeven om aan te geven dat u uw bestanden nu kunt opslaan in de kluis. De kluis is nu open en u krijgt direct toegang. Bij elke volgende poging om toegang te krijgen tot de kluis wordt u uitgenodigd de kluis te ontgrendelen met het wachtwoord dat u hebt opgegeven:



Als u uw nieuwe gegevenskluis wilt gebruiken, moet u deze eerst openen door op de knop ***Nu openen*** te klikken. Na het openen wordt de gegevenskluis op uw computer weergegeven als een nieuwe virtuele schijf. Wijs de gewenste letter uit de vervolgkeuzelijst toe (*u kunt kiezen uit de momenteel beschikbare schijven*). Het is over het algemeen niet mogelijk om C *(meestal de vaste schijf)*, A *(diskettestation)* of D *(dvd-station)* te kiezen. Elke keer dat u een gegevenskluis ontgrendelt, kunt u een andere beschikbare stationsletter kiezen.

Uw gegevenskluis ontgrendelen

Bij elke volgende poging om toegang te krijgen tot de gegevenskluis wordt u uitgenodigd de kluis te ontgrendelen met het wachtwoord dat u hebt opgegeven:

Typ in het tekstveld uw wachtwoord ter controle en klik op de knop ***Ontgrendelen***. Als u een geheugensteuntje nodig hebt, klikt u op ***Hint*** om de wachtwoordhint weer te geven die u hebt opgegeven toen u de gegevenskluis maakte. De nieuwe gegevenskluis wordt in het overzicht van uw gegevenskluizen weergegeven als ONTGRENDELD. Vervolgens kunt u bestanden toevoegen aan en verwijderen uit de kluis.

6.2. Bescherming van Surfen

Het onderdeel ***Surfen*** omvat twee services: ***LinkScanner Surf-Shield*** en ***Online Shield***:

- ***LinkScanner Surf-Shield*** beschermt u tegen het toenemende gevaar van kortstondige bedreigingen op internet. Deze bedreigingen kunnen zich op elk type website verbergen, of het nu een website van

de overheid, van een bekend merk of een klein bedrijf betreft, en zijn zelden langer dan 24 uur op dezelfde site aanwezig. LinkScanner analyseert alle pagina's die zijn gekoppeld aan de webpagina die u bezoekt en zorgt zo voor realtime beveiliging op het enige moment dat telt - het moment dat u op het punt staat op een koppeling te klikken. ***LinkScanner Surf-Shield is niet bedoeld voor serverplatforms.***

- ***Online Shield*** is een vorm van interne, realtime bescherming. De inhoud van bezochte webpagina's (en van de bestanden die daarvan eventueel deel uitmaken) wordt gescand zelfs voordat deze wordt weergegeven in uw webbrowser of wordt gedownload naar uw computer. Als Online Shield detecteert dat de pagina die u wilt bezoeken bijvoorbeeld een gevaarlijk Javascript bevat, wordt weergave van die pagina verhinderd. Bovendien herkent Web Shield malware op pagina's en verhindert het onmiddellijk dat de malware wordt gedownload, zodat de malware uw computer nooit bereikt. Dit krachtige schild blokkeert de schadelijke inhoud van webpagina's die u probeert te openen en voorkomt dat deze naar uw computer wordt gedownload. Als de functie is ingeschakeld, wordt automatisch verhinderd dat een webpagina wordt geopend als u op een koppeling klikt of de URL typt van een gevaarlijke site, en zo wordt voorkomen dat u per ongeluk geïnfecteerd raakt. U kunt al door een webpagina met een exploit worden geïnfecteerd door de betreffende site alleen maar te bezoeken. ***Online Shield is niet bedoeld voor serverplatforms.***

Dialoogvensteropties

U schakelt tussen de twee gedeelten van het dialoogvenster door te klikken. Het actieve deelvenster wordt weergegeven met een lichtere kleur blauw. In beide gedeelten van het dialoogvenster vindt u de volgende opties. Hun functionaliteit komt overeen, ongeacht tot welke beveiligingsservice ze behoren *(LinkScanner Surf-Shield of Online Shield)*:

 ***Ingeschakeld / Uitgeschakeld*** - de knop doet u mogelijk denken aan een verkeerslicht, zowel qua uiterlijk als qua functionaliteit. Klik om te schakelen tussen de twee posities. Groen staat voor ***Ingeschakeld***. Dit betekent dat de beveiligingsservice LinkScanner Surf-Shield/Online Shield actief en volledig functioneel is. Rood staat voor ***Uitgeschakeld***. Dit betekent dat de service is gedeactiveerd. Als u geen goede reden hebt om de service te deactiveren, raden we u sterk aan de standaardinstellingen voor alle beveiligingsconfiguraties te behouden. Met de standaardinstellingen bent u verzekerd van een

optimale balans tussen prestaties en beveiliging. Als u de service om welke reden dan ook wilt deactiveren, wordt u direct over het mogelijke risico geïnformeerd door middel van een rood ***waarschuwingsteken*** en het bericht dat u niet volledig bent beschermd. ***Activeer de service weer zo snel mogelijk.***

 ***Instellingen*** - klik op de knop om te worden omgeleid naar de interface Geavanceerde instellingen. Het betreffende dialoogvenster wordt geopend en u kunt de geselecteerde service configureren (LinkScanner Surf-Shield of Online Shield). In de interface voor geavanceerde instellingen kunt u de configuratie van de beveiligingsservices in **AVG Internet Security** wijzigen, maar voor elke configuratie kan gelden dat deze alleen wordt aanbevolen voor ervaren gebruikers.

 ***Pijl*** - gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar de hoofdgebruikersinterface met het overzicht van de onderdelen.

6.3. Identity Protection

Met het onderdeel ***Identity Protection*** wordt de service ***Identity Shield*** uitgevoerd die uw digitale bezittingen continu beschermt tegen nieuwe en onbekende bedreigingen op internet:

- ***Identity Protection*** is een anti-malwareservice die u beschermt tegen allerlei vormen van malware (*zoals spyware, bots en identiteitsdiefstal*) via gedragsherkenningstechnologieën, en die zonder vertraging bescherming biedt tegen nieuwe virussen. Identity Protection is gericht op het voorkomen van diefstal van uw wachtwoorden, bankrekeninggegevens, creditcardnummers en andere waardevolle persoonlijke digitale informatie door allerlei vormen van schadelijke software *(malware)* die uw pc bedreigen. Het product controleert of alle programma's die worden uitgevoerd op uw pc correct functioneren. Identity Protection detecteert en blokkeert verdacht gedrag en beveiligt uw computer tegen alle nieuwe schadelijke software. Het onderdeel Identity Protection beveiligt uw computer in realtime tegen nieuwe en zelfs onbekende bedreigingen. Het onderdeel bewaakt alle *(ook verborgen)* processen en meer dan 285 verschillende gedragspatronen. Het onderdeel kan vaststellen of er iets schadelijks op uw systeem plaatsvindt. Daardoor kan het bedreigingen aan het licht brengen die zelfs nog niet zijn beschreven in de virusdatabases. Als een onbekend stukje code op uw computer arriveert, wordt dit onmiddellijk gecontroleerd op schadelijk gedrag en wordt dit item gevolgd. Als wordt geconstateerd dat het bestand schadelijk is, wordt dit door Identity Protection verwijderd naar Quarantaine en worden alle wijzigingen in het systeem ongedaan gemaakt *(code-injecties, wijzigingen van het register, het openen van poorten, enzovoort)*. U hoeft geen scan te starten om beveiligd te zijn. De technologie is zeer proactief, behoeft nauwelijks te worden bijgewerkt, en is altijd waakzaam.

Dialoogvensteropties

Het dialoogvenster bevat de volgende opties:

Ingeschakeld / Uitgeschakeld - de knop doet u mogelijk denken aan een verkeerslicht, zowel qua uiterlijk als qua functionaliteit. Klik om te schakelen tussen de twee posities. Groen staat voor ***Ingeschakeld***. Dit betekent dat Identity Protection actief en volledig functioneel is. Rood staat voor ***Uitgeschakeld***. Dit betekent dat de service is gedeactiveerd. Als u geen goede reden hebt om de service te deactiveren, raden we u sterk aan de standaardinstellingen voor alle beveiligingsconfiguraties te behouden. Met de standaardinstellingen bent u verzekerd van een optimale balans tussen prestaties en beveiliging. Als u de service om welke reden dan ook wilt deactiveren, wordt u direct over het mogelijke risico geïnformeerd door middel van een rood ***waarschuwingsteken*** en het bericht dat u niet volledig bent beschermd. ***Activeer de service weer zo snel mogelijk.***

Instellingen - klik op de knop om te worden omgeleid naar de interface Geavanceerde instellingen. Het betreffende dialoogvenster wordt geopend en u kunt de geselecteerde service configureren (Identity Protection). In de interface voor geavanceerde instellingen kunt u de configuratie van de beveiligingsservices in **AVG Internet Security** wijzigen, maar voor elke configuratie kan gelden dat deze alleen wordt aanbevolen voor ervaren gebruikers.

Pijl - gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar de hoofdgebruikersinterface met het overzicht van de onderdelen.

Helaas is de Identity Alert-service niet opgenomen in **AVG Internet Security**. Als u dit type bescherming wilt gebruiken, klikt u op de knop ***Upgraden om te activeren*** om te worden omgeleid naar de webpagina waar u de licentie voor Identity Alert kunt aanschaffen.

Ook voor AVG Premium Security geldt dat de service Identity Alert momenteel alleen beschikbaar is in bepaalde regio's: de Verenigde Staten, het Verenigd Koninkrijk, Canada en Ierland.

6.4. E-mailbescherming

Het onderdeel ***E-mail Protection*** beschikt over de volgende twee beveiligingsservices: ***E-mailscanner*** en ***Anti-Spam*** *(de service Anti-Spam is alleen toegankelijk in Internet Security / Premium Security)*.

- ***E-mailscanner***: e-mail is een van de belangrijkste bronnen voor virussen en Trojaanse paarden. Phishing en spam maken van e-mail een nog grotere risicofactor. Gratis e-mailaccounts hebben meer last van dergelijke kwaadaardige e-mail (*omdat daarin zelden antispamtechnologie wordt toegepast*), terwijl thuisgebruikers daar veelal van afhankelijk zijn. Thuisgebruikers stellen zich ook vaak gemakkelijk bloot aan aanvallen via e-mail, omdat ze op onbekende sites surfen en op online formulieren persoonlijke gegevens *(bijvoorbeeld het e-mailadres)* invullen. Bedrijven maken meestal gebruik van bedrijfsaccounts voor e-mail en schakelen spamfilters en dergelijke in om de risico's te beperken. Het onderdeel E-mail Protection is verantwoordelijk voor het scannen van alle verstuurde of ontvangen e-mailberichten. Wanneer een virus in een e-mail wordt ontdekt, wordt het onmiddellijk naar Quarantaine verplaatst. Het onderdeel kan ook bepaalde typen e-mailbijlagen filteren en een certificatietekst toevoegen aan infectievrije berichten. ***E-mailscanner is niet bedoeld voor serverplatforms.***

- ***Anti-Spam*** controleert alle binnenkomende e-mailberichten en markeert ongewenste e-mails als spam. *(Spam verwijst naar ongewenste e-mailberichten, die meestal reclame maken voor een product of service en naar grote aantallen e-mailadressen tegelijk gestuurd worden, waardoor de postbussen van ontvangers vol raken. Spam verwijst niet naar wettige commerciële e-mail waarvoor klanten hun toestemming hebben gegeven.)*. Anti-Spam kan het onderwerp wijzigen van e-mail (*die is herkend als spam*) door er een speciale tekst aan toe te voegen. U kunt dan in uw e-mailclient de e-mails gemakkelijk filteren Anti-Spam maakt gebruik van verschillende analysemethoden om de afzonderlijke e-mailberichten te verwerken. Dit biedt de best mogelijke bescherming tegen ongewenste e-mailberichten. Anti-Spam maakt voor spamdetectie gebruik van een database die regelmatig wordt bijgewerkt. U kunt ook RBL-servers *(openbare databases met e-mailadressen van bekende spammers)* gebruiken en handmatig e-mailadressen toevoegen aan uw Witte lijst *(nooit als spam markeren)* en Zwarte lijst *(altijd markeren als spam)*.

Dialoogvensteropties

U schakelt tussen de twee gedeelten van het dialoogvenster door te klikken. Het actieve deelvenster wordt weergegeven met een lichtere kleur blauw. In beide gedeelten van het dialoogvenster vindt u de volgende opties. Hun functionaliteit komt overeen, ongeacht tot welke beveiligingsservice ze behoren *(E-mailscanner of Anti-Spam)*:

 ***Ingeschakeld / Uitgeschakeld*** - de knop doet u mogelijk denken aan een verkeerslicht, zowel qua uiterlijk als qua functionaliteit. Klik om te schakelen tussen de twee posities. Groen staat voor ***Ingeschakeld***. Dit betekent dat de beveiligingsservice actief en volledig functioneel is. Rood staat voor ***Uitgeschakeld***. Dit betekent dat de service is gedeactiveerd. Als u geen goede reden hebt om de service te deactiveren, raden we u sterk aan de standaardinstellingen voor alle beveiligingsconfiguraties te behouden. Met de standaardinstellingen bent u verzekerd van een optimale balans tussen prestaties en beveiliging. Als u de service om welke reden dan ook wilt deactiveren, wordt u direct over het mogelijke risico geïnformeerd door middel van een rood ***waarschuwingsteken*** en het bericht dat u niet volledig bent beschermd. ***Activeer de service weer zo snel mogelijk.***

 ***Instellingen*** - klik op de knop om te worden omgeleid naar de interface Geavanceerde instellingen. Het betreffende dialoogvenster wordt geopend en u kunt de geselecteerde service configureren (E-mailscanner of Anti-Spam). In de interface voor geavanceerde instellingen kunt u de configuratie van de beveiligingsservices in **AVG Internet Security** wijzigen, maar voor elke configuratie kan gelden dat deze alleen wordt aanbevolen voor ervaren gebruikers.

 ***Pijl*** - gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar de hoofdgebruikersinterface met het overzicht van de onderdelen.

6.5. Firewall

Firewall is een systeem dat een toegangsbeleid afdwingt tussen twee of meer netwerken door verkeer te blokkeren of toe te staan. Firewall bevat een reeks regels die het interne netwerk beschermen tegen aanvallen van *buitenaf (meestal van internet)* en die alle communicatie via elke netwerkpoort beheren. De communicatie wordt aan de hand van de gedefinieerde regels beoordeeld en vervolgens toegestaan of geblokkeerd. Als Firewall indringingspogingen detecteert, worden deze pogingen geblokkeerd en krijgt de indringer geen toegang tot de computer. Firewall wordt geconfigureerd om interne/externe communicatie *(in beide richtingen, binnenkomend en uitgaand)* door opgegeven poorten en voor opgegeven software toe te staan of te weigeren. Firewall kan bijvoorbeeld worden geconfigureerd om alleen gegevensstromen van internet (zowel binnenkomend als uitgaand) toe te staan via Microsoft Explorer. Elke poging om internetgegevens te verzenden of ontvangen via een andere browser wordt dan geblokkeerd. De firewall beschermt uw persoonsgebonden informatie en verhindert dat die vanaf uw computer wordt verzonden zonder uw toestemming. Dit onderdeel bepaalt hoe uw computer gegevens met andere computers op internet of in een lokaal netwerk uitwisselt. Binnen een organisatie beveiligt Firewall ook afzonderlijke computers tegen aanvallen die door interne gebruikers op andere computers op het netwerk worden uitgevoerd.

In **AVG Internet Security** beheert ***Firewall*** alle verkeer op de afzonderlijke netwerkpoorten op uw computer. Firewall beoordeelt op basis van de gedefinieerde regels toepassingen die worden uitgevoerd op de computer *(en die u wilt verbinden met internet/het lokale netwerk)* of toepassingen die de computer van buitenaf benaderen om verbinding te maken met de pc. Voor al deze toepassingen wordt bepaald of de communicatie op de netwerkpoorten wordt toegestaan of verboden. Als de toepassing onbekend is *(een toepassing waarvoor geen Firewall-regels zijn opgegeven)*, wordt u standaard gevraagd of u de communicatie wilt toestaan of blokkeren.

AVG Firewall is niet bedoeld voor serverplatforms.

Aanbeveling: *over het algemeen is het niet raadzaam om meer dan één firewall op één computer te*

gebruiken. De computer wordt niet beter beveiligd als u meer firewalls installeert. Het is waarschijnlijker dat er conflicten tussen deze twee programma's optreden. Daarom raden we u aan slechts één firewall op uw computer te gebruiken en alle andere firewalls te deactiveren om zo het risico op mogelijke conflicten en hiermee verbonden problemen te voorkomen.

***Opmerking:** na de installatie van AVG Internet Security moet de computer mogelijk opnieuw worden opgestart voor het onderdeel Firewall. In dat geval wordt er een dialoogvenster geopend waarin wordt aangegeven dat opnieuw opstarten vereist is. In het dialoogvenster kunt u op de knop **Nu opnieuw starten** klikken. Pas als u opnieuw hebt opgestart, is het onderdeel Firewall volledig geactiveerd. Daarnaast worden alle bewerkingsopties in het dialoogvenster uitgeschakeld. Negeer deze waarschuwing niet en start de pc zo snel mogelijk opnieuw op.*

Beschikbare Firewall-modi

Met Firewall kunt u specifieke regels voor het beveiligingsniveau definiëren, afhankelijk van of de computer zich in een domein bevindt, een zelfstandige computer is of zelfs een notebook is. Voor deze opties zijn verschillende beveiligingsniveaus vereist. De niveaus worden bepaald door de betreffende profielen. Kortom, een Firewall-modus is een specifieke configuratie van het onderdeel Firewall. U kunt een aantal van dergelijke vooraf gedefinieerde configuraties gebruiken.

- ***Automatisch*** - in deze modus wordt al het netwerkverkeer automatisch afgehandeld. U wordt niet gevraagd beslissingen te nemen. Verbindingen worden toegestaan voor bekende toepassingen. Daarnaast wordt voor de toepassing een regel gemaakt waarin wordt aangegeven dat de toepassing in de toekomst altijd verbinding kan maken. Voor andere toepassingen wordt op basis van het gedrag van de toepassing beslist of de verbinding moet worden toegestaan. In dergelijke gevallen wordt er echter geen regel gemaakt. Dit betekent dat de toepassing altijd wordt gecontroleerd als deze probeert verbinding te maken. De automatische modus is een niet-inbreukmakende modus en wordt aanbevolen voor de meeste gebruikers.

- ***Interactief*** - deze modus is handig als u volledige controle wilt over al het netwerkverkeer naar en van uw computer. Firewall controleert het verkeer voor u en er wordt een melding weergegeven zodra er wordt geprobeerd te communiceren of gegevens te verzenden. Op deze manier kunt u bepalen wat wel

en niet is toegestaan. Alleen aanbevolen voor ervaren gebruikers.

- ***Toegang tot internet blokkeren*** - de internetverbinding wordt volledig geblokkeerd. U hebt geen toegang tot internet en niemand kan extern toegang verkrijgen tot uw computer. Gebruik deze modus alleen in speciale gevallen en voor een beperkte tijd.

- ***Firewallbescherming uitschakelen (niet aanbevolen)*** - wanneer u Firewall uitschakelt, is al het netwerkverkeer van en naar uw computer toegestaan. Uw computer is in dat geval kwetsbaar voor aanvallen van hackers. Ga altijd zorgvuldig om met deze optie.

Er is nog een specifieke automatische modus beschikbaar in Firewall. Deze modus wordt op de achtergrond geactiveerd als het onderdeel Computer of Identiteit wordt uitgeschakeld en uw computer als gevolg daarvan kwetsbaarder is. In dergelijke gevallen worden alleen bekende en absoluut veilige toepassingen automatisch toegestaan. In alle andere gevallen wordt u gevraagd een beslissing te nemen. Dit wordt gedaan ter compensatie van de uitgeschakelde beveiligingsonderdelen en om uw computer veilig te houden.

We raden u ten sterkste aan de firewall niet uit te schakelen! Als het echter echt nodig is om het onderdeel Firewall uit te schakelen, kunt u dat doen door de modus Firewallbescherming uitschakelen te selecteren in bovenstaande lijst met firewallmodi.

Dialoogvensteropties

Het dialoogvenster biedt een overzicht van algemene informatie over de status van het onderdeel Firewall:

- ***Firewallmodus*** - biedt informatie over de geselecteerde modus. Gebruik de knop ***Wijziging*** om over te schakelen naar de interface met Firewall-instellingen als u de huidige modus wilt wijzigen *(zie de vorige paragraaf voor een beschrijving en aanbevelingen voor het gebruik van Firewall-profielen)*.

- ***Bestanden en printers delen*** - hier wordt aangegeven of het delen van bestanden en printers *(in beide richtingen)* momenteel is toegestaan. Bestanden en printers delen heeft betrekking op alle bestanden of mappen die u markeert als Gedeeld in Windows en alle gemeenschappelijke stations, printers, scanners en vergelijkbare apparaten. Het delen van dergelijke items is alleen gewenst in netwerken die kunnen worden beschouwd als veilig *(bijvoorbeeld thuis, op het werk of op school)*. Wanneer u echter bent verbonden met een openbaar netwerk *(zoals een Wi-Fi-hotspot op een luchthaven of in een internetcafé)*, kunt u beter niets delen.

- ***Verbonden met*** - hier wordt de naam weergegeven van het netwerk waarmee u momenteel verbonden bent. In Windows XP komt de naam van het netwerk overeen met de naam die u voor het specifieke netwerk opgeeft als u voor het eerst verbinding maakt. In Windows Vista en hoger wordt de netwerknaam automatisch opgehaald uit Netwerkcentrum.

- ***Standaardwaarde herstellen*** - klik op deze knop om de huidige Firewall-configuratie te overschrijven en de standaardconfiguratie op basis van automatische detectie te herstellen.

Het dialoogvenster bevat de volgende grafische opties:

 ***Instellingen*** - klik op deze knop om te worden doorverwezen naar de interface met Firewall-instellingen waar u de Firewall-configuratie kunt wijzigen. Alleen ervaren gebruikers dienen wijzigingen aan te brengen in de configuratie.

 ***Pijl*** - gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar

de hoofdgebruikersinterface met het overzicht van de onderdelen.

6.6. PC Analyzer

Het onderdeel ***PC Analyzer*** is een geavanceerd hulpmiddel voor gedetailleerde systeemanalyse en -correctie om te achterhalen hoe de snelheid en prestaties van de computer verbeterd kunnen worden. U opent dit onderdeel met de knop ***Fix performance*** in het venster met de hoofdgebruikersinterface of met dezelfde optie in het snelmenu van het pictogram van AVG in het systeemvak. De voortgang en de resultaten van de analyse worden in de grafiek weergegeven:

De volgende categorieën kunnen worden geanalyseerd: registerfouten, ongewenste bestanden, fragmentatie en verbroken snelkoppelingen:

- ***Registerfouten*** - het aantal fouten in het Windows-register die uw computer trager kunnen maken of foutmeldingen kunnen veroorzaken.
- ***Ongewenste bestanden*** - het aantal bestanden dat schijfruimte inneemt, maar dat u hoogstwaarschijnlijk niet meer nodig hebt. Het gaat daarbij vooral om bestanden in tijdelijke mappen en in de Prullenbak.
- ***Fragmentatie*** - het percentage van de vaste schijf dat is gefragmenteerd (al lange tijd in gebruik is waardoor de meeste bestanden zich nu verspreid op de vaste schijf bevinden).
- ***Verbroken koppelingen*** - koppelingen die niet langer naar behoren functioneren, naar niet-bestaande locaties leiden, enz., worden gemeld.

Het resultatenoverzicht bevat het aantal systeemproblemen geclassificeerd op basis van de geteste categorieën. De resultaten van de analyse worden bovendien grafisch weergegeven op een as in de kolom ***Ernst***.

Knoppen

- ***Analyse stoppen*** (*weergegeven voor de start van de analyse*) - hiermee kunt u de analyse van de computer onderbreken.

- ***Nu repareren*** *(weergegeven als de analyse is voltooid*) - helaas is de functionaliteit van PC Analyzer in **AVG Internet Security** beperkt tot het analyseren van de huidige status van uw pc. AVG heeft echter een geavanceerd hulpmiddel voor gedetailleerde systeemanalyse en -correctie om te achterhalen hoe de snelheid en prestaties van de computer verbeterd kunnen worden. Klik op de knop om te worden omgeleid naar een website die meer informatie bevat.

7. AVG Geavanceerde instellingen

Het dialoogvenster voor een geavanceerde configuratie van **AVG Internet Security** wordt geopend in een nieuw dialoogvenster, ***Geavanceerde AVG instellingen***. Het venster is onderverdeeld in twee secties. Het linker deelvenster bevat een boomstructuur voor navigatie naar de opties voor programmaconfiguratie. Selecteer het onderdeel (*of een deel daarvan*) waarvoor u de configuratie wilt wijzigen om het bijbehorende dialoogvenster in het rechterdeelvenster te openen.

7.1. Weergave

Het eerste onderdeel van de navigatiestructuur, ***Weergave***, verwijst naar de algemene instellingen van de **AVG Internet Security**-gebruikersinterface en bevat een aantal basisopties die betrekking hebben op het gedrag van de toepassing:

Taalselectie

U kunt in de vervolgkeuzelijst in de sectie ***Taalselectie*** de gewenste taal kiezen. De geselecteerde taal wordt vervolgens gebruikt voor de gehele **AVG Internet Security**-gebruikersinterface. De vervolgkeuzelijst bevat alleen de talen die u eerder tijdens het installatieproces hebt geïnstalleerd plus Engels (*Engels wordt altijd automatisch geïnstalleerd*). Als u het op een andere taal instellen van **AVG Internet Security** wilt voltooien, moet u de toepassing opnieuw starten. Ga als volgt te werk:

- Selecteer in de vervolgkeuzelijst de gewenste taal voor de toepassing
- Bevestig uw keuze door op de knop ***Toepassen*** te klikken *(deze knop wordt in de rechterbenedenhoek van het dialoogvenster weergegeven)*
- Druk op de knop ***OK*** om te bevestigen

- Er wordt een nieuw dialoogvenster weergegeven met de vermelding dat voor het wijzigen van de taal van de toepassing opnieuw opstarten nodig is van **AVG Internet Security**

- Druk op de knop ***AVG nu opnieuw starten*** om in te stemmen met het opnieuw opstarten van het programma en wacht totdat de taalwijziging van kracht wordt:

Systeemvakmeldingen

Hier kunt u opgeven dat systeemvakmeldingen over de status van de **AVG Internet Security**-toepassing moeten worden onderdrukt. De systeemmeldingen worden standaard weergegeven. U wordt sterk aangeraden deze configuratie te behouden. Systeemmeldingen bieden bijvoorbeeld informatie over het starten van het scan- of updateproces, of over statuswijzigingen van een **AVG Internet Security** -onderdeel. Het is belangrijk dat u deze meldingen niet negeert.

Wanneer u echter om welke reden dan ook besluit dat u niet op deze wijze wilt worden geïnformeerd of dat u alleen bepaalde meldingen *(met betrekking tot een specifiek AVG Internet Security-onderdeel)* wilt weergeven, kunt u uw voorkeuren instellen door de volgende opties in of uit te schakelen:

- ***Systeemvakwaarschuwingen weergeven*** *(standaard ingeschakeld)* - standaard worden alle waarschuwingen weergegeven. Schakel dit selectievakje uit als u de weergave van alle systeemmeldingen volledig wilt uitschakelen. Als u de optie inschakelt, kunt u selecteren welke meldingen u wilt weergeven:

  - ***Meldingen van updates*** *(standaard ingeschakeld)* - bepaal of informatie over het starten, de voortgang en het voltooien van het updateproces van **AVG Internet Security** moet worden weergegeven.

  - ***Meldingen van Resident Shield over automatische verwijdering van bedreigingen*** *(standaard ingeschakeld)* - bepaal of informatie over het opslaan, kopiëren en openen van bestanden moet worden weergegeven (*deze instelling wordt alleen weergegeven als de Resident Shield-optie voor automatisch herstel is ingeschakeld*).

  - ***Meldingen van scanner*** *(standaard ingeschakeld)* - bepaal of informatie over het automatisch starten van geplande scans, de voortgang en de resultaten moet worden weergegeven.

  - ***Meldingen van Firewall*** *(standaard ingeschakeld)* - bepaal of informatie over statussen en processen van Firewall, zoals waarschuwingen over het activeren en deactiveren van het onderdeel, meldingen van geblokkeerd verkeer, enzovoort, moet worden weergegeven. Onder dit item vindt u nog twee specifieke selectieopties *(zie het hoofdstuk Firewall in dit document voor gedetailleerde uitleg over deze opties)*:

    - ***Netwerkverbindingspunten*** *(standaard uitgeschakeld)* - wanneer u verbinding maakt met een netwerk, wordt door Firewall aangegeven of het een bekend netwerk betreft en hoe de instellingen voor het delen van bestanden en printers zijn geconfigureerd.

- ***Geblokkeerde toepassingen*** *(standaard ingeschakeld)* - wanneer een onbekende of verdachte toepassing probeert verbinding te maken met een netwerk, wordt dit door Firewall verhinderd en wordt er een melding weergegeven. Op deze manier blijft u op de hoogte. Daarom raden we u aan deze functie altijd ingeschakeld te houden.

- ***Meldingen van E-mailscanner*** *(standaard ingeschakeld)* - bepaal of u informatie over het scannen van alle binnenkomende en uitgaande e-mailberichten wilt weergeven.

- ***Statistische meldingen*** *(standaard ingeschakeld)* - zorg ervoor dat deze optie is ingeschakeld als er regelmatig statistische gegevensmeldingen moeten worden weergegeven in het systeemvak.

- ***Meldingen van AVG accelerator*** *(standaard ingeschakeld)* - bepaal of u informatie over activiteiten van ***AVG accelerator*** wilt weergeven. Met ***AVG accelerator*** worden online video's vloeiender afgespeeld en worden extra downloads vergemakkelijkt.

- ***Meldingen van Opstarttijd verbeteren*** *(standaard uitgeschakeld)* - bepaal of u meldingen over de verbeterde opstarttijd van uw computer wilt weergeven.

- ***Meldingen van AVG Advies*** *(standaard ingeschakeld)* - bepaal of informatie over activiteiten van AVG Advies moet worden weergegeven in het systeemvak.

Gamingmodus

Deze AVG-functie is ontworpen voor schermvullende toepassingen, waarbij AVG-meldingen (*die bijvoorbeeld worden weergegeven wanneer een geplande scan wordt gestart*) een storend effect kunnen hebben (*de toepassing zou geminimaliseerd kunnen worden of de afbeeldingen kunnen beschadigd worden*). Als u dit wilt voorkomen, laat u het selectievakje ***Schakel de Gamingmodus in wanneer een toepassing wordt uitgevoerd die het volledige scherm beslaat*** ingeschakeld (*standaardinstelling*).

7.2. Geluiden

In het dialoogvenster ***Geluidsinstellingen*** kunt u instellen of u via een geluidssignaal in kennis gesteld wilt worden van specifieke acties van **AVG Internet Security**:

De instellingen zijn uitsluitend geldig voor de huidige gebruikersaccount. Dit betekent dat iedere gebruiker op de computer eigen geluidsinstellingen kan gebruiken. Als u geluidsmeldingen wilt gebruiken, laat u het selectievakje ***Geluid gebeurtenissen inschakelen*** ingeschakeld (*de optie is standaard ingeschakeld*), zodat de lijst met alle relevante acties is geactiveerd. Daarnaast is het mogelijk wenselijk om de optie ***Speel geen geluiden af als een schermvullende toepassing actief is*** in te schakelen zodat geluidssignalen worden onderdrukt wanneer deze hinderlijk kunnen zijn *(zie ook de sectie Gamingmodus in het hoofdstuk Geavanceerde instellingen/Weergave in dit document)*.

Knoppen

- ***Bladeren*** - klik nadat u de gewenste gebeurtenis in de lijst hebt geselecteerd op de knop ***Bladeren*** om op uw vaste schijf het geluidsbestand te selecteren dat u eraan wilt toekennen. *(Houd er rekening mee dat er momenteel uitsluitend ondersteuning wordt geboden voor *.wav-geluiden.)*

- ***Afspelen*** - als u het geselecteerde geluid wilt beluisteren, markeert u de gebeurtenis in de lijst en klikt u op de knop ***Afspelen***.

- ***Verwijderen*** - gebruik de knop ***Verwijderen*** om het geluid te verwijderen dat aan een specifieke gebeurtenis is toegewezen.

7.3. Beveiliging door AVG tijdelijk uitschakelen

In het dialoogvenster ***Beveiliging door AVG tijdelijk uitschakelen*** kunt u de volledige bescherming door **AVG Internet Security** in één keer uitschakelen.

Maak alleen gebruik van deze optie als het absoluut noodzakelijk is!

In de meeste gevallen is het ***niet nodig*** om **AVG Internet Security** uit te schakelen voordat u nieuwe software of stuurprogramma's installeert, zelfs niet als het installatieprogramma of de softwarewizard voorstelt eerst lopende programma's en toepassingen uit te schakelen om ervoor te zorgen dat er zich geen ongewenste onderbrekingen voordoen tijdens het installatieproces. Als er problemen optreden tijdens de installatie, probeert u eerst de residente bescherming uit te schakelen *(schakel in het gekoppelde dialoogvenster de optie **Resident Shield inschakelen** uit)*. Als u **AVG Internet Security** tijdelijk moet uitschakelen, moet u de beveiliging zo snel mogelijk opnieuw inschakelen. Uw computer is kwetsbaar en kan worden aangevallen als u verbonden bent met internet of een netwerk gedurende de tijd dat uw bescherming is uitgeschakeld.

De AVG-beveiliging tijdelijk uitschakelen

Klik op de knop ***Beveiliging door AVG tijdelijk uitschakelen***. Stel in het dialoogvenster ***Beveiliging door AVG tijdelijk uitschakelen*** in hoe lang **AVG Internet Security** moet worden uitgeschakeld. De beveiliging wordt standaard 10 minuten uitgeschakeld. Dit is over het algemeen voldoende voor veelvoorkomende taken, zoals het installeren van nieuwe software, enzovoort. U kunt voor een langere periode kiezen, maar doe dit alleen als het echt nodig is. Nadien worden alle uitgeschakelde onderdelen weer automatisch ingeschakeld. U kunt de AVG-bescherming uiterlijk uitschakelen tot de computer opnieuw wordt opgestart. Daarnaast is een aparte optie voor het uitschakelen van het onderdeel ***Firewall*** beschikbaar in het dialoogvenster ***Beveiliging door AVG tijdelijk uitschakelen***. Schakel het selectievakje ***Beveiliging door Firewall uitschakelen*** in.

7.4. Computerbescherming

7.4.1. AntiVirus

AntiVirus en ***Resident Shield*** beschermen uw computer continu tegen alle bekende typen virussen, spyware en malware in het algemeen, *inclusief inactieve malware (malware die is gedownload, maar nog niet geactiveerd)*.

U kunt in het dialoogvenster ***Instellingen AntiVirus*** de volledige residente bescherming activeren of deactiveren door het selectievakje ***Inschakelen Resident Shield*** in of uit te schakelen (*deze optie is standaard ingeschakeld*). Daarnaast kunt u opgeven welke functies van de residente bescherming u wilt activeren:

- ***Vragen voor het verwijderen van bedreigingen*** (*standaard ingeschakeld*) - schakel dit selectievakje in om ervoor te zorgen dat Resident Shield geen automatische acties uitvoert. In plaats daarvan wordt er een dialoogvenster weergegeven waarin de gedetecteerde bedreiging wordt beschreven en waarin u kunt opgeven hoe moet worden omgegaan met de bedreiging. Als u dit selectievakje niet inschakelt, wordt de infectie in **AVG Internet Security** automatisch hersteld of, als dit niet mogelijk is, verplaatst naar Quarantaine.

- ***Rapporteer bedreigingen door mogelijk ongewenste programma's en spyware*** (*standaard ingeschakeld*) - schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de beveiling van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) - schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel ter bevordering van de veiligheid van uw computer, al kunnen er ook legale programma's door worden geblokkeerd; om die reden is de functie standaard uitgeschakeld.

- ***Bestanden scannen bij sluiten*** (*standaard uitgeschakeld*) - hiermee zorgt u ervoor dat AVG actieve objecten (zoals toepassingen, documenten, enzovoort) scant wanneer deze worden geopend en wanneer deze worden gesloten. Deze functie beschermt uw computer tegen bepaalde typen geavanceerde virussen.

- ***Bootsector van verwisselbare media scannen*** (*standaard ingeschakeld*) - aanvinken om de bootsector van USB-sticks, externe schijven en andere verwisselbare media op bedreigingen te controleren.

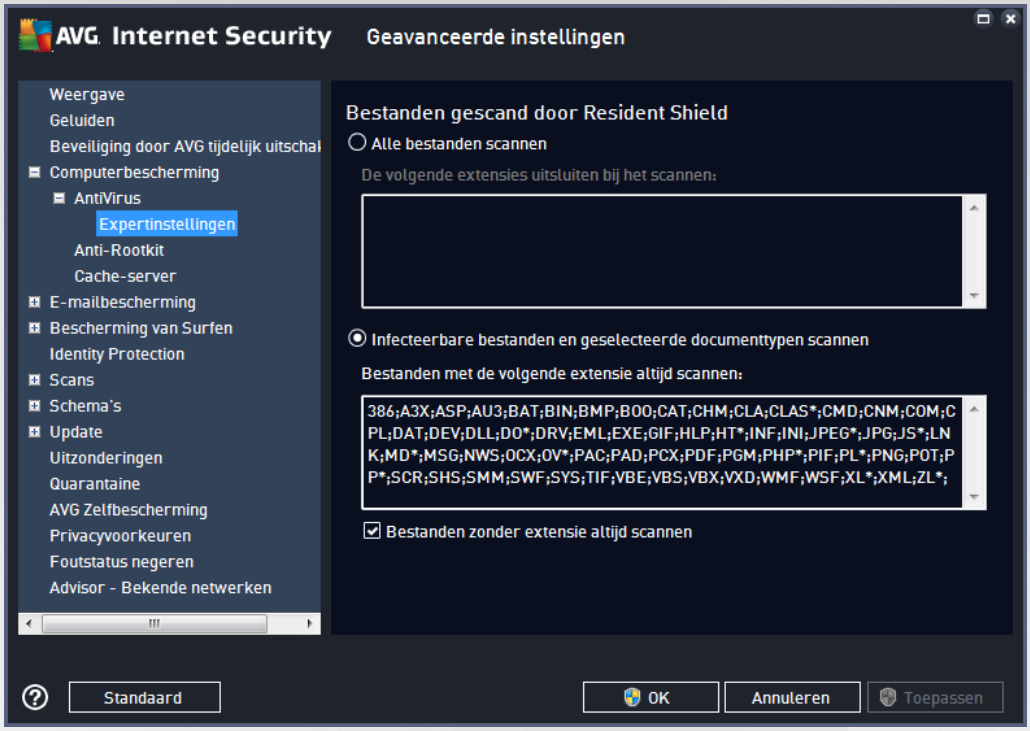
- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - er worden voor het detecteren heuristische analyses gebruikt (*dynamische emulatie van instructies van gescande objecten in een virtuele computeromgeving*).

- ***Bestanden scannen waarnaar in het register wordt verwezen*** (*standaard ingeschakeld*) - hiermee worden alle uitvoerbare bestanden gescand die zijn toegevoegd aan het opstartregister. Zo wordt voorkomen dat een bekende infectie wordt uitgevoerd wanneer de computer opnieuw wordt opgestart.

- ***Grondig scannen inschakelen*** (*standaard uitgeschakeld*) - in specifieke situaties (*in geval van extreme nood*) kunt u deze optie inschakelen zodat de meest grondige algoritmes worden geactiveerd waarmee alle mogelijk bedreigende objecten zeer grondig worden gecontroleerd. Deze manier van scannen kost echter erg veel tijd.

- ***Beveiliging van Instant Messaging en P2P-downloads inschakelen*** (*standaard ingeschakeld*) - schakel deze optie in als u wilt controleren of chatberichten (*zoals AIM, Yahoo!, ICQ, Skype en MSN Messenger*) en gegevens gedownload in P2P-netwerken *(mogelijk gevaarlijke netwerken waarin directe verbindingen tussen clients, zonder server, zijn toegestaan, doorgaans om muziekbestanden te delen)* gevrijwaard zijn van virussen.

In het dialoogvenster ***Bestanden gescand door Resident Shield*** kunt u opgeven welke bestanden gescand moeten worden (*aan de hand van de extensies*):



Schakel het selectievakje ***Alle bestanden scannen*** of ***Infecteerbare bestanden en geselecteerde documenttypen scannen*** in. We raden u aan de standaardinstelling niet te wijzigen als u de optimale balans tussen scansnelheid en bescherming wilt behouden. Op deze manier worden alleen infecteerbare bestanden gescand. In het betreffende gedeelte van het dialoogvenster vindt u tevens een bewerkbare lijst met extensies voor bestanden die worden gescand.

Schakel het selectievakje ***Bestanden zonder extensie altijd scannen*** (*standaard ingeschakeld*) in om er zeker van te zijn dat bestanden zonder extensie en met een onbekende bestandsindeling door Resident Shield worden gescand. We raden u aan deze functie ingeschakeld te laten omdat bestanden zonder extensie verdacht zijn.

7.4.2. Anti-Rootkit

In het dialoogvenster ***Anti-Rootkit instellingen*** kunt u de configuratie en de specifieke parameters voor het controleren op rootkits van de service ***Anti-Rootkit*** bewerken. Het scannen op rootkits is een standaardproces in De hele computer scannen:

Via de opties ***Toepassingen scannen*** en ***Stuurprogramma's scannen*** kunt u gedetailleerd opgeven wat moet worden opgenomen in de rootkitscan. Deze instellingen zijn bedoeld voor geavanceerde gebruikers en we raden u aan geen opties uit te schakelen. U kunt ook de scanmodus kiezen:

- ***Snelle rootkitscan*** - scannen van alle lopende processen, geladen stuurprogramma's en de systeemmap (*standaard c:\Windows*)
- ***Volledige rootkitscan*** - Scant alle lopende processen, geladen stuurprogramma's en de systeemmap (*standaard c:\Windows*) plus alle locale schijven (*inclusief flash-stations, maar exclusief diskette-/cd-stations*)

7.4.3. Cache-server

Het dialoogvenster ***Instellingen Cache-server*** heeft betrekking op het cacheserverproces dat is ontworpen met het oog op het verhogen van de snelheid van alle typen **AVG Internet Security**-scans:

De cacheserver verzamelt en bewaart informatie over vertrouwde bestanden (*een bestand wordt beschouwd als een vertrouwd bestand als het is ondertekend met een digitale handtekening die afkomstig is van een vertrouwde bron*). Deze bestanden worden vervolgens automatisch als veilig beschouwd en hoeven niet opnieuw te worden gescand.

Het dialoogvenster ***Cache-server Instellingen*** biedt de volgende configuratieopties:

- ***Caching ingeschakeld*** (*standaard ingeschakeld*) - Schakel het selectievakje uit om de ***Cache-server*** uit te schakelen en het cachegeheugen te legen. Let op: het scannen kan trager verlopen, en de prestaties van de computer kunnen te wensen over laten, omdat elk afzonderlijk bestand dat wordt gebruikt, eerst moet worden gescand op virussen en spyware.

- ***Toevoegen nieuwe bestanden aan cache inschakelen*** (*standaard ingeschakeld*) - Schakel dit selectievakje uit om te verhinderen dat nog meer bestanden worden toegevoegd aan het cachegeheugen. Alle bestanden die al zijn opgeslagen in de cache, blijven daar totdat het cachen helemaal wordt uitgeschakeld, of tot de eerstvolgende update van de virusdatabase.

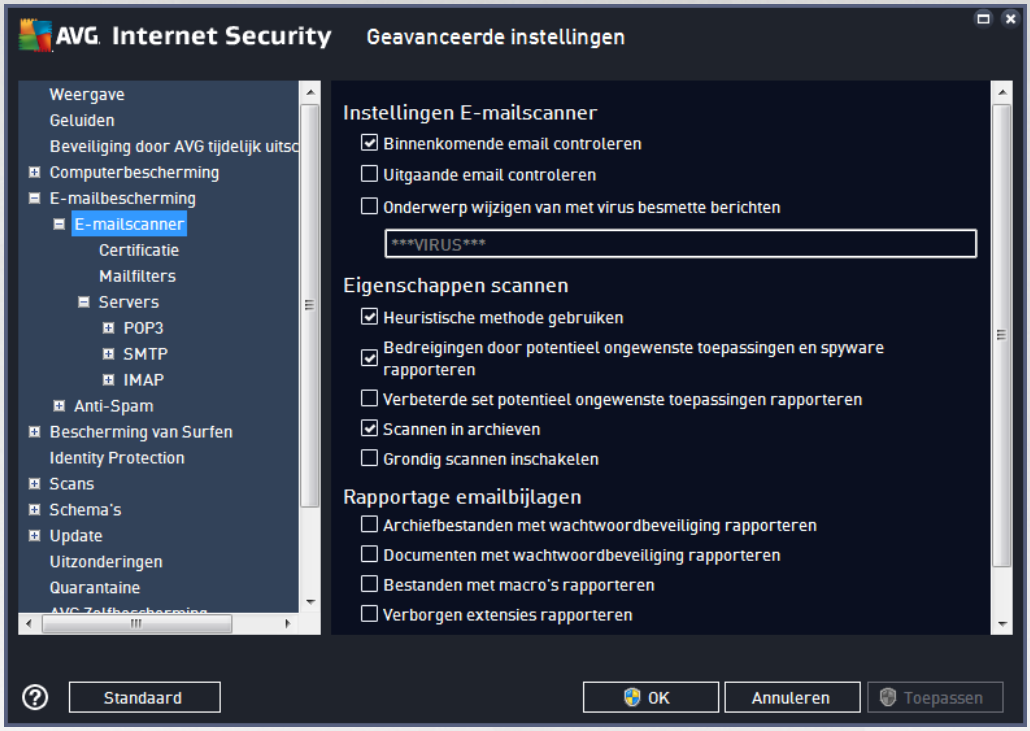
U wordt met klem aangeraden om de standaardinstellingen te behouden en beide opties ingeschakeld te laten, tenzij u over een goede reden beschikt om de cacheserver uit te schakelen. Als u dat niet doet, kan dit de snelheid en prestaties van uw systeem sterk beïnvloeden.

7.5. E-Mail Scanner

In dit gedeelte kunt u de gedetailleerde configuratie van E-mailscanner en Anti-Spam bewerken:

7.5.1. E-Mail Scanner

Het dialoogvenster ***E-mailscanner*** is onderverdeeld in drie gedeelten:



Instellingen E-mailscanner

In dit gedeelte kunt u het volgende instellen voor binnenkomende en uitgaande e-mailberichten:

- ***Binnenkomende e-mail controleren*** (*standaard ingeschakeld*) - schakel dit selectievakje in om alle bij uw e-mailclient binnenkomende e-mail te controleren
- ***Uitgaande e-mail controleren*** (*standaard uitgeschakeld*) - schakel dit selectievakje in om alle vanaf uw e-mailaccount verzonden e-mail te controleren
- ***Onderwerp wijzigen van met virus besmette berichten*** (*standaard uitgeschakeld*) - als u wilt worden gewaarschuwd als er een geïnfecteerd e-mailbericht wordt gedetecteerd, schakelt u dit selectievakje in en vult u de gewenste tekst in het tekstveld in. Die tekst wordt vervolgens toegevoegd aan het veld "Onderwerp" van elk geïnfecteerd e-mailbericht zodat het bericht beter kan worden herkend en kan worden gefilterd. We raden u aan de standaardtekst ***VIRUS*** niet te wijzigen.

Eigenschappen scannen

Scaneigenschappen – in dit gedeelte kunt u opgeven hoe e-mailberichten moeten worden gescand:

- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - schakel dit selectievakje in om gebruik

te maken van de heuristische detectiemethode voor het scannen van e-mailberichten. Als deze optie is ingeschakeld, kunt u e-mailbijlagen niet alleen op extensie filteren, maar wordt ook de feitelijke inhoud van de bijlage gecontroleerd. De filtering kan worden ingesteld in het dialoogvenster Mailfiltering.

- ***Rapporteer bedreigingen door mogelijk ongewenste programma's en spyware*** (*standaard ingeschakeld*) - schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste toepassingen rapporteren*** (*standaard uitgeschakeld*) - schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Scannen in archieven*** (*standaard ingeschakeld*) - schakel het selectievakje in om de inhoud van archiefbestanden te scannen die aan e-mailberichten zijn gekoppeld als bijlage.

- ***Grondig scannen inschakelen*** (*standaard uitgeschakeld*) - onder bepaalde omstandigheden (*bijvoorbeeld wanneer u vermoedt dat de computer is geïnfecteerd door een virus of is aangevallen*) kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

Rapportage e-mailbijlagen

In dit gedeelte kunt u extra rapportages instellen omtrent potentieel gevaarlijke of verdachte bestanden. Er wordt geen waarschuwingsvenster weergegeven, er wordt alleen een certificeringstekst toegevoegd aan het eind van het e-mailbericht en al deze rapporten worden vermeld in het dialoogvenster Detectie e-mailbescherming:

- ***Archieven met wachtwoordbeveiliging rapporteren*** - archieven (*ZIP, RAR etc.*) die beveiligd zijn met een wachtwoord, kunnen niet op virussen worden gescand. Schakel het selectievakje in om dergelijke documenten als potentieel gevaarlijk te rapporteren.

- ***Documenten met wachtwoordbeveiliging rapporteren*** - documenten die beveiligd zijn met een wachtwoord, kunnen niet op virussen worden gescand. Schakel het selectievakje in om dergelijke documenten als potentieel gevaarlijk te rapporteren.

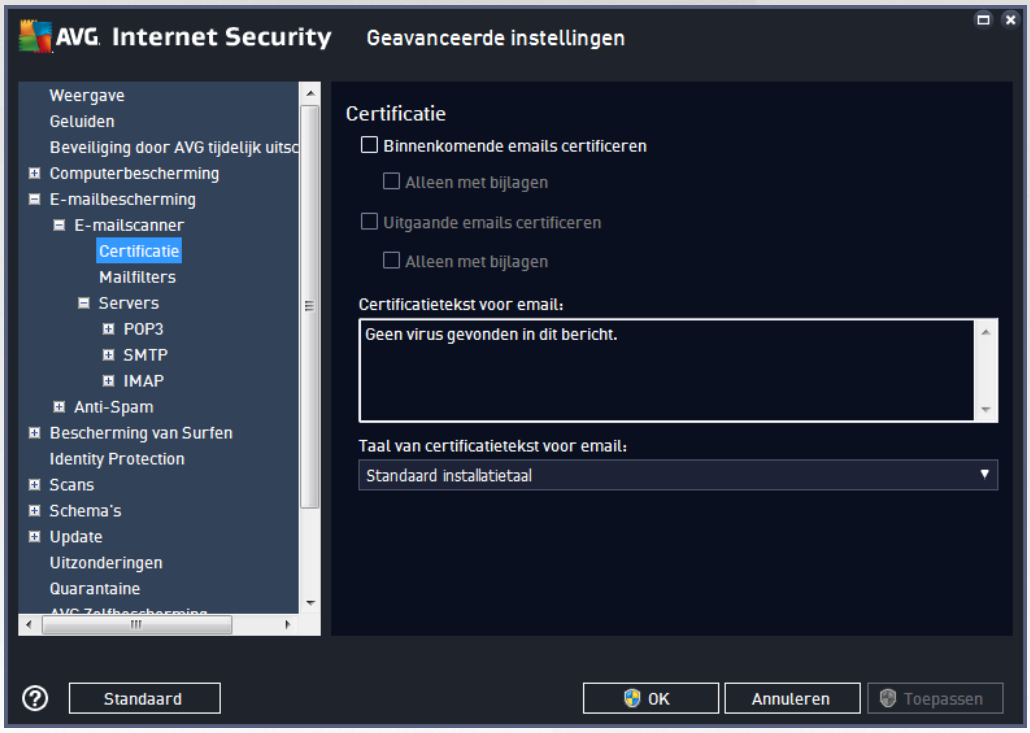
- ***Bestanden met een macro rapporteren*** - een macro is een aantal vooraf gedefinieerde stappen van een bewerking, bedoeld om bepaalde taken voor een gebruiker te vergemakkelijken (*MS Word-macro's zijn alom bekend*). Daarom kan een macro potentieel gevaarlijke instructies bevatten. Als u dit selectievakje inschakelt, worden bestanden met macro's als verdacht gerapporteerd.

- ***Verborgen extensies rapporteren*** - dankzij een verborgen extensie ziet het verdachte uitvoerbare bestand "something.txt.exe" er bijvoorbeeld uit als het onschuldige tekstbestand "something.txt". Schakel het selectievakje in om dergelijke bestanden als potentieel gevaarlijk te rapporteren.

- ***Gerapporteerde bijlagen verplaatsen naar Quarantaine*** - geef op of u via e-mail op de hoogte wilt

worden gesteld van de detectie van met wachtwoord beveiligde archiefbestanden, met een wachtwoord beveiligde documenten, bestanden met macro's en/of bestanden met verborgen extensies die als bijlagen aan gescande e-mail zijn gekoppeld. Geef, als bij het scannen een dergelijk bericht wordt gedetecteerd, op of het geïnfecteerde object moet worden verplaatst naar de Quarantaine.

In het dialoogvenster ***Certificatie*** kunt u de selectievakjes inschakelen als u binnenkomende e-mail (***Binnenkomende e-mails certificeren***) en/of uitgaande e-mail (***Uitgaande e-mails certificeren***) wilt certificeren. U kunt voor elk van deze opties de parameter ***Alleen met bijlagen*** inschakelen zodat de certificatie uitsluitend wordt toegevoegd aan e-mailberichten met bijlagen:



Certificatietekst bestaat standaard uit basisinformatie waarin wordt vermeld dat er *geen virussen in dit bericht zijn gevonden.* Deze informatie kan echter worden uitgebreid of gewijzigd op basis van uw behoeften. U kunt de gewenste tekst voor de certificatie invoeren in het veld ***Certificatietekst voor e-mail***. Bij ***Taal van certificatietekst voor e-mail*** kunt u instellen in welke taal het automatisch gegenereerde gedeelte van de certificatie (*Geen virus gevonden in dit bericht*) moet worden weergegeven.

Opmerking: *houd er rekening mee dat alleen de standaardtekst wordt weergegeven in de ingestelde taal en dat aangepaste tekst niet automatisch wordt vertaald.*

In het dialoogvenster ***Bijlagefilter*** kunt u parameters instellen voor het scannen van bijlagen bij e-mailberichten.Standaard is de optie ***Bijlagen verwijderen*** uitgeschakeld. Als u besluit die functie in te schakelen, worden bijlagen bij e-mailberichten automatisch verwijderd als deze worden herkend als geïnfecteerd of potentieel gevaarlijk. Als u wilt opgeven dat bepaalde typen bijlagen moeten worden verwijderd, schakelt u een van de volgende opties in:

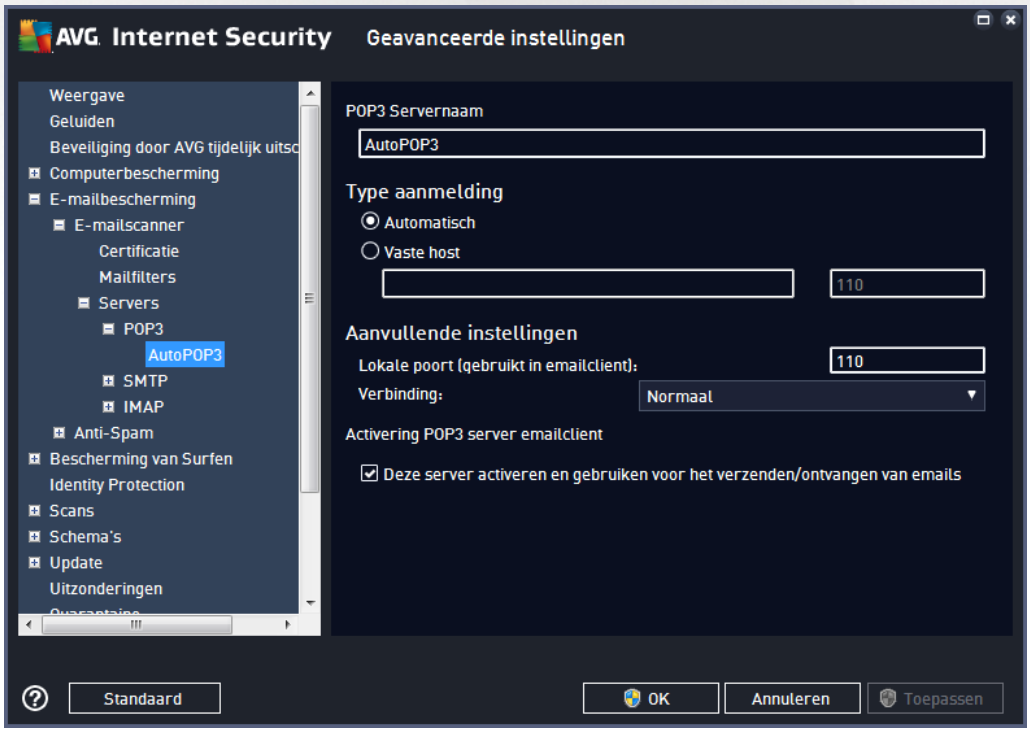
- ***Alle uitvoerbare bestanden verwijderen*** - alle bestanden met de extensie *.exe worden verwijderd
- ***Alle documenten verwijderen*** - alle bestanden met de extensie *.doc, *.docx, *.xls en *.xlsx worden verwijderd
- ***Bestanden met deze kommagescheiden extensies verwijderen*** - alle bestanden met de nader te specificeren extensies worden verwijderd

In de sectie ***Servers*** kunt u parameters voor de E-mailscanner-servers bewerken:

- POP3-server
- SMTP-server
- IMAP-server

U kunt ook nieuw servers voor binnenkomende of uitgaande mail opgeven met de knop ***Server toevoegen***.

In dit dialoogvenster kunt u een nieuwe e-mailscanner instellen die gebruikmaakt van het POP3-protocol voor binnenkomende e-mail:

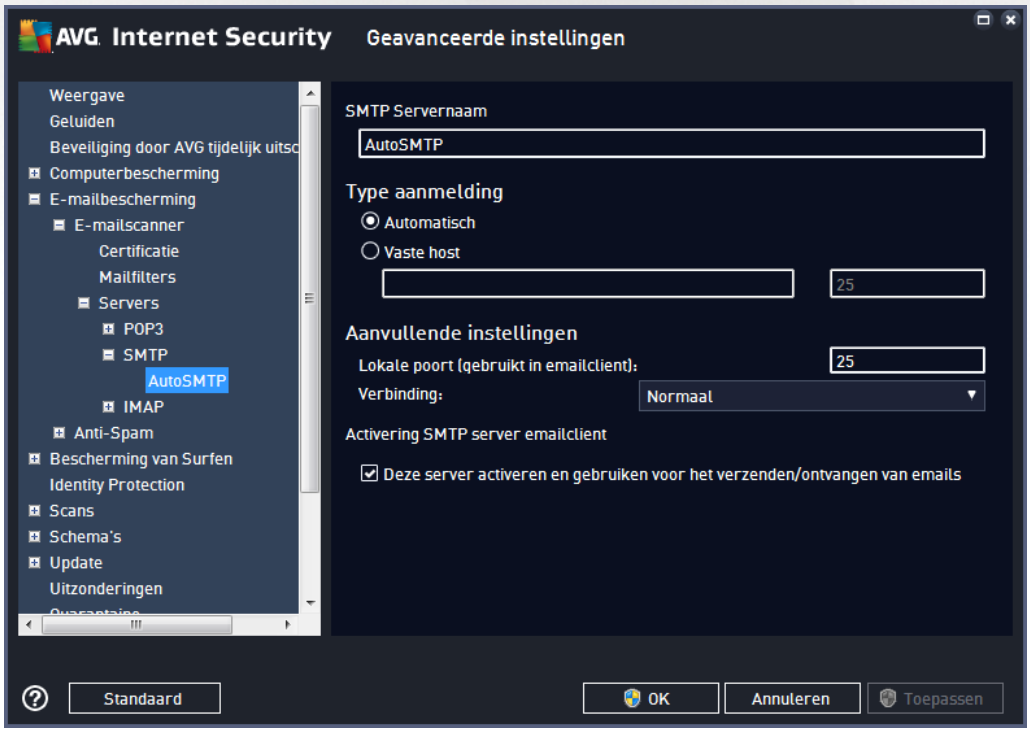


- ***POP3 Servernaam*** - in dit veld kunt u de naam opgeven van nieuwe servers (*als u een POP3-server*

wilt opgeven, klikt u met de rechtermuisknop op het POP3-item in de navigatiestructuur links).

- ***Type aanmelding*** - hiermee bepaalt u de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
    - ***Automatisch*** - aanmelding wordt automatisch uitgevoerd, met behulp van de instellingen voor uw e-mailclient.
    - ***Vaste host*** - in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. De aanmeldingsnaam blijft hetzelfde. U kunt een domeinnaam gebruiken (*bijvoorbeeld pop.acme.com*), evenals een IP-adres (*bijvoorbeeld 123.45.67.89*). Als de mailserver een niet-standaardpoort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (*bijvoorbeeld pop.acme.com:8200*). De standaardpoort voor POP3-communicatie is 110.
- ***Aanvullende instellingen*** - hiermee geeft u gedetailleerdere parameters op:
    - ***Lokale poort*** - de poort waarop de communicatie van de e-mailtoepassing kan worden verwacht. U moet deze poort dan in uw e-mailtoepassing opgeven als de poort voor POP3-communicatie.
    - ***Verbinding*** - met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (*Normaal/SSL/SSL-standaard*). Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is ook alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
- ***Activering POP3 server e-mailclient*** - schakel dit selectievakje in/uit om de opgegeven POP3-server in of uit te schakelen

In dit dialoogvenster kunt u een nieuwe e-mailscanner instellen die gebruikmaakt van het SMTP-protocol voor uitgaande e-mail:



- ***SMTP Servernaam*** - in dit veld kunt u de naam opgeven van nieuwe servers (*als u een SMTP-server*

wilt opgeven, klikt u met de rechtermuisknop op het SMTP-item in de navigatiestructuur links). Voor automatisch gemaakte AutoSMTP-servers is dit veld uitgeschakeld.

- ***Type aanmelding*** - hiermee bepaalt u de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
    - ***Automatisch*** - aanmelding wordt automatisch uitgevoerd, met behulp van de instellingen voor uw e-mailclient
    - ***Vaste host*** - in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. U kunt een domeinnaam gebruiken (*bijvoorbeeld smtp.acme.com*), maar ook een IP-adres (*bijvoorbeeld 123.45.67.89*). Als de mailserver een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (*bijvoorbeeld smtp.acme.com:8200*). De standaardpoort voor SMTP-communicatie is 25.
- ***Aanvullende instellingen*** - hiermee geeft u gedetailleerdere parameters op:
    - ***Lokale poort*** - de poort waarop de communicatie van de e-mailtoepassing kan worden verwacht. U moet vervolgens in uw mailtoepassing deze poort specificeren als poort voor SMTP-communicatie.
    - ***Verbinding*** - met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (*Normaal/SSL/SSL-standaard*). Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zodat ze niet door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
- ***Activering SMTP server e-mailclient*** - schakel dit selectievakje in/uit om de opgegeven SMTP-server in of uit te schakelen

In dit dialoogvenster kunt u een nieuwe e-mailscanner instellen die gebruikmaakt van het IMAP-protocol voor uitgaande e-mail:

- ***IMAP servernaam*** - in dit veld kunt u de naam opgeven van nieuwe servers (*als u een IMAP-server*

wilt toevoegen, klikt u met de rechtermuisknop op het IMAP-item in de navigatiestructuur links).

- ***Type aanmelding*** - hiermee bepaalt u de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
    - ***Automatisch*** - aanmelding wordt automatisch uitgevoerd, met behulp van de instellingen voor uw e-mailclient
    - ***Vaste host*** - in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. U kunt een domeinnaam gebruiken (*bijvoorbeeld smtp.acme.com*), maar ook een IP-adres (*bijvoorbeeld 123.45.67.89*). *Als de mailserver een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (bijvoorbeeld smtp.acme.com:8200*). De standaardpoort voor IMAP-communicatie is 143.
- ***Aanvullende instellingen*** - hiermee geeft u gedetailleerdere parameters op:
    - ***Lokale poort gebruikt in*** - de poort waarop de communicatie van de e-mailtoepassing kan worden verwacht. U moet vervolgens in uw mailtoepassing deze poort specificeren als poort voor SMTP-communicatie.
    - ***Verbinding*** - *met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (Normaal/SSL/SSL-standaard).* Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
- ***Activering IMAP server e-mailclient*** - schakel dit selectievakje in/uit om de opgegeven IMAP-server in of uit te schakelen

7.5.2. Anti-Spam

In het dialoogvenster ***Anti-Spam instellingen*** kunt u het selectievakje ***Anti-Spam inschakelen*** in- en uitschakelen om het scannen van e-mail op spam in of uit te schakelen. De optie is standaard ingeschakeld en zoals gebruikelijk wordt u aangeraden deze instelling alleen te wijzigen als u daar een goede reden voor hebt.

In dit dialoogvenster kunt u bovendien meer of minder agressieve scoremaatregelen selecteren. Het ***Anti-Spam*** filter wijst een score aan elk bericht toe (*bijvoorbeeld in hoeverre de inhoud van het bericht spam benadert*) op basis van verschillende dynamische scantechnieken. U kunt de optie ***Bericht als spam markeren als score hoger is dan*** aanpassen door de waarde in te voeren of door de schuifregelaar naar links of rechts te slepen.

Het bereik met waarden loopt van 50 t/m 90. Hieronder volgt een algemeen overzicht van de scoredrempel.

- ***Waarde 80-90*** - e-mailberichten waarvan de kans groot is dat deze spam bevatten, worden uitgefilterd. Het kan zijn dat sommige niet-spamberichten ook gefilterd worden.
- ***Waarde 60-79*** - een vrij agressieve configuratie. E-mailberichten die mogelijk spam zijn, worden uitgefilterd. Er worden waarschijnlijk ook niet-spamberichten als spam aangeduid.
- ***Waarde 50-59*** - een zeer agressieve configuratie. Zowel niet-spamberichten als echte spamberichten worden uitgefilterd. ***Deze instelling wordt afgeraden voor normaal gebruik.***

In het dialoogvenster ***Anti-Spam instellingen*** kunt u tevens instellen wat er met gedetecteerde spamberichten moet gebeuren:

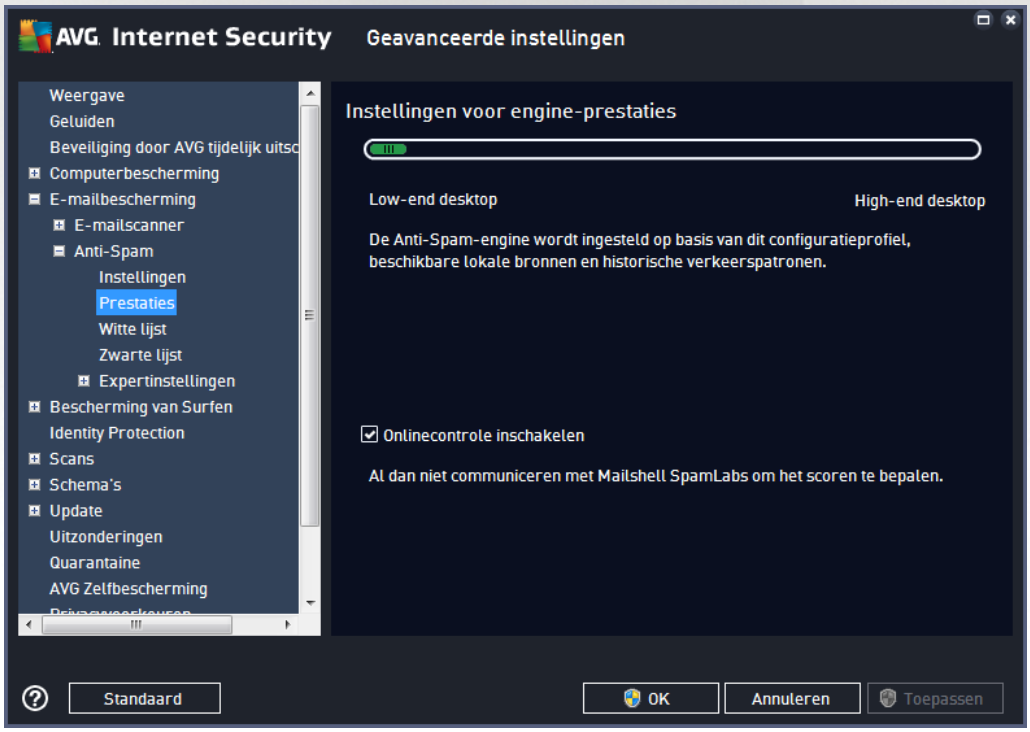
- ***Bericht verplaatsen naar spammap*** *(alleen Microsoft Outlook-invoegtoepassing)* - schakel dit selectievakje in als elk gedetecteerd spambericht automatisch naar de daarvoor aangewezen map in uw e-mailclient MS Outlook moet worden verplaatst. Op dit moment wordt deze functie nog niet ondersteund door andere e-mailclients.

- ***Ontvangers van verzonden e-mails toevoegen aan de witte lijst*** - schakel dit selectievakje in om aan te geven dat alle ontvangers van verzonden e-mails kunnen worden vertrouwd en dat e-mail die vanaf hun e-mailadressen wordt verzonden eveneens kan worden vertrouwd.

- ***Onderwerp wijzigen voor berichten die als SPAM gemarkeerd zijn*** - schakel dit selectievakje in als u alle berichten die als spam worden gedetecteerd, wilt markeren met een bepaald woord of teken in de onderwerpregel van het bericht. U kunt het betreffende woord of teken in het geactiveerde tekstveld typen.

- ***Vragen voor rapportage van foutieve detectie*** - als u tijdens de installatieprocedure hebt aangegeven dat u wilt meewerken aan het project voor privacyvoorkeuren, zullen gedetecteerde bedreigingen aan AVG worden gerapporteerd. Het rapport wordt automatisch gemaakt. Als u dit selectievakje inschakelt, wordt u altijd om bevestiging gevraagd voordat gedetecteerde spam aan AVG wordt gerapporteerd, zodat u kunt bepalen of het bericht echt als spam moet worden geclassificeerd.

Het dialoogvenster ***Instellingen voor engine-prestaties*** (*dat u kunt weergeven via het item* ***Prestaties*** *in het linkernavigatievenster*) bevat de prestatie-instellingen voor het onderdeel ***Anti-Spam***:



Verplaats de schuifbalk naar links of rechts om de scanprestaties te wijzigen binnen een bereik van ***Low-end desktop*** tot ***High-end desktop***.

- ***Low-end desktop*** - tijdens het scanproces worden er voor het identificeren van spam geen regels gebruikt, maar alleen trainingsgegevens. Het is niet raadzaam deze modus voor normaal gebruik te selecteren, tenzij de computerhardware van lage kwaliteit is.

- ***High-end desktop*** - in deze modus wordt een grote hoeveelheid geheugen gebruikt. Tijdens het scanproces voor het detecteren van spam worden de volgende functies gebruikt: regels en spamdatabase, basisregels, geavanceerde regels, IP-adressen en spammerdatabases.

De optie ***Online controle inschakelen*** is standaard ingeschakeld. Dit resulteert in een meer precieze spamdetectie dankzij communicatie met de Mailshell-servers, dat wil zeggen dat de gescande gegevens online worden vergeleken met Mailshell-databases.

Over het algemeen is het raadzaam de standaardinstellingen aan te houden en die alleen te wijzigen als u daar een goede reden voor hebt. Alleen ervaren gebruikers mogen wijzigingen aanbrengen in deze configuratie.

De optie ***Witte lijst*** opent een dialoogvenster met de naam ***Lijst met goedgekeurde verzenders van e-mail*** met een algemene lijst met e-mailadressen van goedgekeurde afzenders en domeinnamen waarvan berichten nooit als spam worden gemarkeerd.

U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders waarvan u zeker weet dat deze u geen ongewenste e-mail (spam) zullen sturen. U kunt ook een lijst samenstellen met domeinnamen (*zoals avg.com*), waarvan u weet dat deze geen spam genereren. Als u eenmaal een dergelijke lijst met afzenders/domeinnamen hebt samengesteld, kunt u deze op twee manieren invoeren: door elk e-mailadres afzonderlijk in te voeren of in één keer door de lijst te importeren.

Knoppen

De volgende knoppen zijn beschikbaar:

- ***Bewerken*** - klik op deze knop om een dialoogvenster te openen waarin u handmatig een lijst met adressen kunt invoeren (*u kunt ook kopiëren en plakken*). Voeg één item (*afzender, domeinnaam*) per regel in.
- ***Exporteren*** - Als u de gegevens wilt exporteren, klikt u op deze knop. Alle gegevens worden dan naar

een tekstbestand opgeslagen.

- ***Importeren*** - Als u al een tekstbestand met e-mailadressen/domeinnamen hebt gemaakt, kunt u die gewoon importeren door op deze knop te klikken. In het bestand mag op iedere regel slechts één item (*adres, domeinnaam*) staan.

Het item ***Zwarte lijst*** biedt toegang tot een dialoogvenster met een algemene lijst met geblokkeerde e-mailadressen en domeinnamen. De berichten van deze afzenders worden altijd als spam gemarkeerd.

U kunt in het tekstverwerkingsgedeelte een lijst samenstellen met afzenders van wie u ongewenste e-mail verwacht (*spam*). U kunt ook een lijst met volledige domeinnamen samenstellen (*zoals spammingbedrijf.nl*), waarvan u spamberichten verwacht of ontvangt. Alle e-mailberichten die worden ontvangen van de weergegeven adressen/domeinen, worden gemarkeerd als spam. Als u eenmaal een dergelijke lijst met afzenders/domeinnamen hebt samengesteld, kunt u deze op twee manieren invoeren: door elk e-mailadres afzonderlijk in te voeren of in één keer door de lijst te importeren.

Knoppen

De volgende knoppen zijn beschikbaar:

- ***Bewerken*** - klik op deze knop om een dialoogvenster te openen waarin u handmatig een lijst met adressen kunt invoeren (*u kunt ook kopiëren en plakken*). Voeg één item (*afzender, domeinnaam*) per regel in.

- ***Exporteren*** - Als u de gegevens wilt exporteren, klikt u op deze knop. Alle gegevens worden dan naar een tekstbestand opgeslagen.

- ***Importeren*** - Als u al een tekstbestand met e-mailadressen/domeinnamen hebt gemaakt, kunt u die gewoon importeren door op deze knop te klikken.

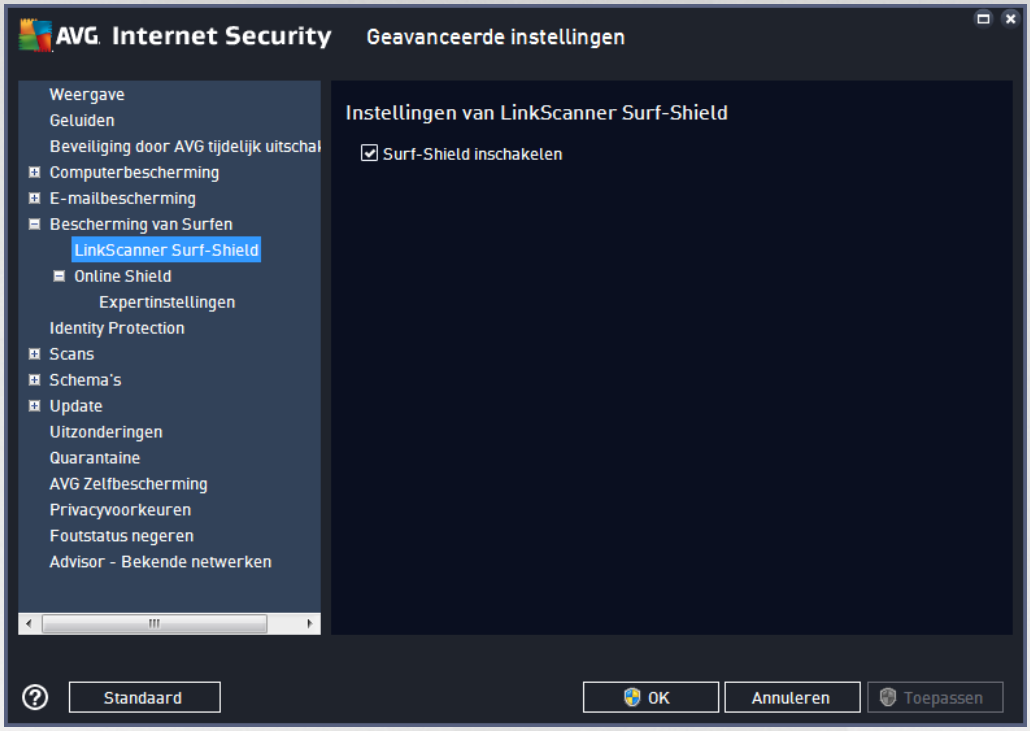
De vertakking Expertinstellingen bevat uitgebreide instelopties voor het onderdeel Anti-Spam. Deze instellingen zijn uitsluitend bedoeld voor ervaren gebruikers, gewoonlijk netwerkbeheerders, die de antispambeveiliging gedetailleerd willen kunnen configureren, zodat een optimale beveiliging van e-mailservers wordt geboden. Om die reden is er geen extra Help beschikbaar voor de afzonderlijke dialoogvensters. In de gebruikersinterface zelf is echter wel een korte beschrijving van elke optie beschikbaar. We raden u echter nadrukkelijk aan om geen instellingen te wijzigen, tenzij u volledig vertrouwd bent met de geavanceerde instellingen van Spamcatcher (MailShell Inc.). Onjuiste wijzigingen in het bestand kunnen leiden tot slechte prestaties of een onjuiste functionaliteit van het onderdeel.

Als u nog steeds van mening bent dat u de configuratie van Anti-Spam op het geavanceerde niveau wilt wijzigen, volgt u de instructies die in de gebruikersinterface worden weergegeven. Doorgaans vindt u in elk dialoogvenster één specifiek onderdeel dat u kunt bewerken. De beschrijving van dit onderdeel is altijd opgenomen in het dialoogvenster zelf. U kunt de volgende parameters bewerken:

- ***Filteren*** - Taallijst, Landenlijst, Goedgekeurde IP's, Geblokkeerde IP's, Geblokkeerde landen, Geblokkeerde tekensets, Spoof-verzenders
- ***RBL*** - RBL-servers, Multihit, Drempel, Time-out, Max IP's
- ***Internetverbinding*** - Time-out, Proxyserver, Proxyserververificatie

7.6. Bescherming van Surfen

In het dialoogvenster ***LinkScanner instellingen*** kunt u de volgende functies in-/uitschakelen:



- ***Surf-Shield inschakelen*** - (*standaard ingeschakeld*): actieve (*realtime*) bescherming tegen websites met exploits op het moment dat ze worden geopend. Bekende kwaadaardige sites en hun inhoud met exploits worden geblokkeerd op het moment dat de gebruiker ze opent in de browser (*of met een andere toepassing die HTTP gebruikt*).

7.6.1. Online Shield

Het dialoogvenster ***Online Shield*** biedt de volgende opties:

- ***Inschakelen Online Shield*** *(standaard ingeschakeld)* - Hiermee kunt u de ***Online Shield***-service inschakelen en uitschakelen. De geavanceerde instellingen van ***Online Shield*** worden weergegeven in het volgende dialoogvenster, het dialoogvenster Webbescherming.

- ***AVG accelerator inschakelen*** *(standaard ingeschakeld)* - schakel de service AVG accelerator in of uit. Met AVG accelerator worden online video's vloeiender afgespeeld en worden extra downloads eenvoudiger. Wanneer de videoacceleratie wordt uitgevoerd, wordt u daarvan in kennis gesteld via een pop-upvenster bij het systeemvak:

Modus melding bedreigingen

In het onderste deel van het dialoogvenster selecteert u hoe gedetecteerde mogelijke bedreigingen moeten worden gemeld: met een standaard pop-upvenster, met een systeemvakballontekstmelding of via systeemvaksignalering.

In het dialoogvenster ***Webbescherming*** kunt u de configuratie van het onderdeel aanpassen met betrekking tot het scannen van de inhoud van websites. U kunt de volgende basisopties aanpassen:

- ***Archiefbestanden controleren*** (*standaard uitgeschakeld*) - scan de inhoud van archieven die zijn ingesloten op de webpagina's die u wilt weergeven.
- ***Rapporteer bedreigingen door mogelijk ongewenste toepassingen en spyware*** (*standaard ingeschakeld*) - schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.
- ***Verbeterde set potentieel ongewenste toepassingen rapporteren*** (*standaard uitgeschakeld*) – schakel dit selectievakje in als u pakketten die met spyware zijn uitgebreid, wilt detecteren. Dit zijn programma's die in orde en onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.
- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - de inhoud scannen van een weer te geven pagina met behulp van de methode voor *heuristische analyse (dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving*).
- ***Grondig scannen inschakelen*** *(standaard uitgeschakeld*) - onder bepaalde omstandigheden (*bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd*) kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid

zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Gecodeerd (TLS en SSL) netwerkverkeer scannen*** (*standaard ingeschakeld*) - laat deze optie ingeschakeld om AVG ook gecodeerde netwerkcommunicatie (verbindingen via beveiligingsprotocollen zoals SSL en de nieuwere versie TLS) te laten scannen. Dit geldt voor websites die HTTPS gebruiken en verbindingen van e-mailclients op basis van TLS/SSL. Het beveiligde verkeer wordt gedecodeerd, gecontroleerd op malware en weer gecodeerd om veilig te worden afgeleverd op uw computer. Bij deze optie kunt u ***Inclusief verkeer van servers met EV-certificaten (Extended Validation) kiezen*** om ook gecodeerde netwerkcommunicatie van servers met een EV-certificaat te scannen. Een EV-certificaat wordt uitsluitend verleend na uitgebreide validatie door de certificeringsinstantie en websites met het certificaat zijn dan ook veel betrouwbaarder *(minder kans dat ze malware verspreiden)*. Daarom kunt u ervoor kiezen verkeer van servers met een EV-certificaat niet te scannen om de gecodeerde communicatie sneller te laten verlopen.

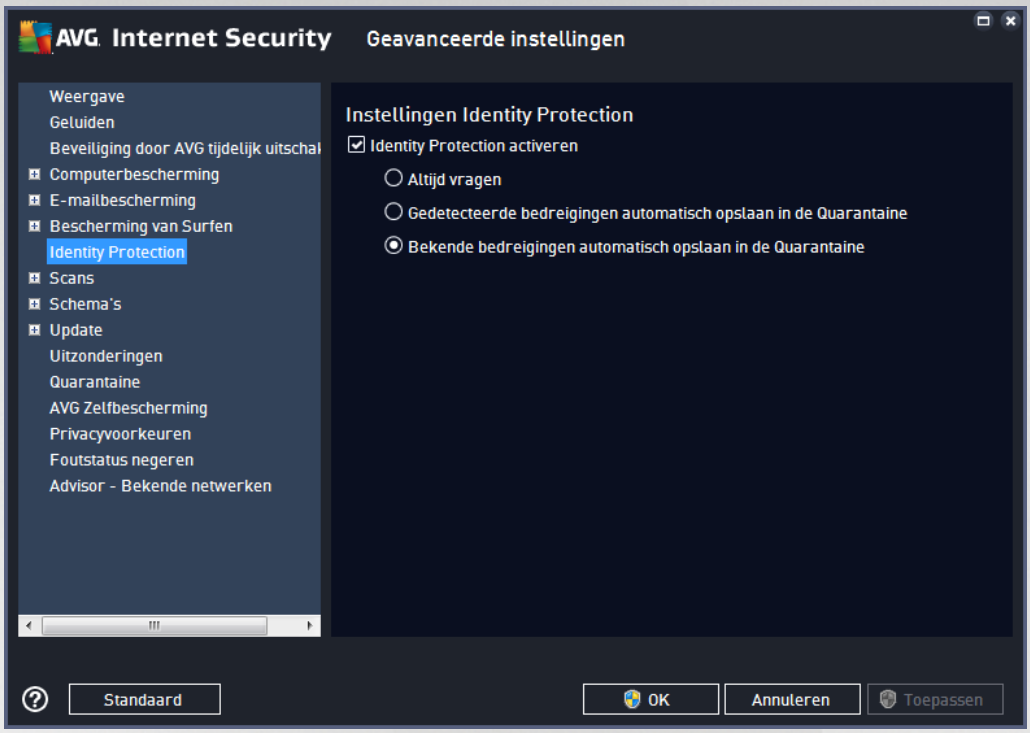
- ***Gedownloade uitvoerbare bestanden met Resident Shield scannen*** (*standaard ingeschakeld*) - uitvoerbare bestanden scannen *(gewoonlijk bestanden met de extensies exe, bat, com)* nadat deze zijn gedownload. Bestanden worden door Resident Shield gescand voordat ze worden gedownload om te voorkomen dat schadelijke bestanden op uw computer terechtkomen. Deze scans worden echter beperkt door de instelling ***Maximale deelgrootte van te scannen bestand*** - zie het volgende item in dit dialoogvenster. Daarom worden grote bestanden in delen gescand. Dit geldt tevens voor de meeste uitvoerbare bestanden. Door uitvoerbare bestanden kunnen verschillende taken op uw computer worden uitgevoerd en het is belangrijk dat deze 100% veilig zijn. U kunt hier zeker van zijn door het bestand in delen te scannen voordat het wordt gedownload en direct nadat het bestand is gedownload. We raden u aan deze optie ingeschakeld te laten. Als u deze optie uitschakelt, kunt u er nog steeds zeker van zijn dat alle mogelijk gevaarlijke code wordt gevonden. Het zal doorgaans echter niet mogelijk zijn om een uitvoerbaar bestand te evalueren als een complex bestand. Hierdoor kunnen enkele valse meldingen worden weergegeven.

Met de schuifregelaar onder in het dialoogvenster kunt u de gewenste waarde voor ***Maximale deelgrootte van te scannen bestand*** instellen. Als er bestanden zijn inbegrepen op een weer te geven pagina, kunt u de inhoud daarvan ook scannen voordat ze naar uw computer worden gedownload. Het scannen van grote bestanden neemt echter veel tijd in beslag, wat het downloaden van de webpagina aanzienlijk kan vertragen. Met de schuifregelaar kunt u de maximale grootte opgeven van bestanden die moeten worden gescand met ***Online Shield***. Zelfs als het gedownloade bestand groter is dan u hebt opgegeven, en dus niet wordt gescand met Online Shield, wordt u nog steeds beschermd: als het bestand is geïnfecteerd, wordt dat onmiddellijk gedetecteerd door ***Resident Shield***.

7.7. Identity Protection

Identity Protection is een onderdeel dat uw systeem beveiligt tegen allerlei vormen van malware (*spyware, bots, identiteitsdiefstal, enzovoort*) via gedragsherkenningstechnologieën. Dit onderdeel biedt u zonder vertraging bescherming tegen nieuwe virussen *(zie het hoofdstuk Identity Protection voor een gedetailleerde beschrijving van de functionaliteit van het onderdeel*).

In het dialoogvenster ***Instellingen Identity Protection*** kunt u de elementaire functies van het onderdeel Identity Protection in- en uitschakelen:



Identity Protection activeren (*standaard ingeschakeld*) - schakel dit selectievakje uit om het onderdeel Identity Protection uit te schakelen. ***We raden u sterk aan dit alleen te doen als het beslist moet.*** Als Identity Protection is ingeschakeld, kunt u opgeven wat er moet gebeuren als er een bedreiging wordt gedetecteerd:

- ***Altijd vragen*** - bij detectie van een bedreiging wordt u gevraagd of deze naar Quarantaine moet worden verplaatst. Zo wordt voorkomen dat er toepassingen naar Quarantaine worden verplaatst die u wilt uitvoeren.
- ***Gedetecteerde bedreigingen automatisch opslaan in de Quarantaine*** - schakel dit selectievakje in als u wilt dat alle gedetecteerde mogelijke bedreigingen meteen worden verplaatst naar de veilige omgeving van Quarantaine. Bij de standaardinstelling wordt u bij detectie van een bedreiging gevraagd of deze naar Quarantaine moet worden verplaatst. Op deze manier kunt u er zeker van zijn dat er naar Quarantaine geen toepassingen worden verplaatst die u wilt uitvoeren.
- ***Bekende bedreigingen automatisch opslaan in de Quarantaine*** (*standaard ingeschakeld*) - dit selectievakje moet ingeschakeld blijven als u wilt dat alle toepassingen die worden gedetecteerd als mogelijke malware automatisch en meteen naar Quarantaine worden verplaatst.

7.8. Scans

De geavanceerde scaninstellingen zijn onderverdeeld in vier categorieën die verwijzen naar specifieke typen scans die door de leverancier van de software zijn gedefinieerd:

- De hele computer scannen - vooraf gedefinieerde standaardscan waarbij de hele computer wordt gescand
- Mappen of bestanden scannen - vooraf gedefinieerde standaardscan van geselecteerde gedeelten van uw computer

- Scan van Shell-extensie - scan van een geselecteerd object rechtstreeks vanuit Windows Verkenner
- Scan van verwisselbaar apparaat - scan van verwisselbare apparaten die op de computer worden aangesloten

7.8.1. De hele computer scannen

De optie ***De hele computer scannen*** biedt toegang tot een dialoogvenster waarin u de parameters kunt aanpassen van een van de vooraf door de leverancier gedefinieerde scans, namelijk De hele computer scannen:

Scaninstellingen

In de sectie ***Scaninstellingen*** staat een lijst met scanparameters die u kunt in- en uitschakelen:

- ***Virusinfecties herstellen/verwijderen zonder te vragen***(*(standaard ingeschakeld*) - als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als deze beschikbaar is. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de map Quarantaine verplaatst.
- ***Rapporteer bedreigingen door mogelijk ongewenste programma's en spyware*** (*standaard ingeschakeld*) - schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.
- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*) - schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt,

maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Tracking cookies scannen*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of cookies bij het scannen moeten worden gedetecteerd (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*).

- ***Scannen in archieven*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, zoals ZIP en RAR.

- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - hiermee wordt een heuristische analyse (*dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving*) gebruikt als een van de methoden voor virusdetectie.

- ***Scansysteemomgeving*** (*standaard ingeschakeld*) - als deze parameter is ingeschakeld, worden ook de systeemgebieden van de computer gescand.

- ***Grondig scannen inschakelen*** ((*standaard uitgeschakeld*) - onder bepaalde omstandigheden (*bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd*) kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Scannen naar rootkits*** (*standaard ingeschakeld*) - Anti-Rootkitscan zoekt op uw pc naar rootkits. Dit zijn programma's en technologieën die malware-activiteiten in de computer kunnen verhullen. Als een rootkit wordt gedetecteerd, wil dat nog niet zeggen dat uw computer is geïnfecteerd. In sommige gevallen worden bepaalde stuurprogramma's of delen van reguliere programma's abusievelijk herkend als rootkit.

U moet ook bepalen wat voor type scan u wilt uitvoeren:

- ***Alle bestandstypen*** - u kunt een lijst opgeven met door komma's gescheiden bestandsextensies die moeten worden genegeerd bij het scannen (*als deze lijst is opgeslagen, veranderen de komma's in puntkomma's*).

- ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden - als u deze optie niet inschakelt, beperkt u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu op basis van extensies opgeven welke bestanden altijd moeten worden gescand.

- U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn verdacht en moeten altijd worden gescand.

Scansnelheid aanpassen

In de sectie ***Scansnelheid aanpassen*** kunt u nader opgeven hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op de systeembronnen van uw computer. Standaard is deze functie ingesteld op het niveau *gebruikerafhankelijk* voor gebruik van systeembronnen. Als u sneller wilt scannen, duurt het scannen minder lang, maar worden aanzienlijk meer systeembronnen gebruikt, zodat andere activiteiten op de computer trager worden uitgevoerd (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt het beroep op systeembronnen echter ook beperken door te kiezen voor een langere scanduur.

Aanvullende scanrapporten instellen...

Klik op de koppeling ***Aanvullende scanrapporten instellen...*** om een afzonderlijk dialoogvenster te openen dat ***Scanrapporten*** heet, waarin u selectievakjes kunt inschakelen voor resultaten die moeten worden weergegeven:

7.8.2. Bepaalde mappen of bestanden scannen

De bewerkingsinterface voor ***Mappen of bestanden scannen*** is bijna gelijk aan het bewerkingsvenster van De hele computer scannen, maar de standaardinstellingen voor De hele computer scannen zijn strenger:

Alle parameters die u instelt in dit configuratievenster hebben alleen betrekking op het scannen met de optie Mappen of bestanden scannen.

Opmerking: *zie het hoofdstuk Geavanceerde instellingen AVG / Scans / De hele computer scannen voor een beschrijving van specifieke parameters.*

7.8.3. Shell-extensiescan

Evenals bij het item De hele computer scannen kunt u ook bij het item ***Scan van Shell-extensie*** verschillende opties instellen om de vooraf door de leverancier gedefinieerde scan aan te passen. Deze keer heeft de configuratie betrekking op het scannen van specifieke objecten direct vanuit Windows Verkenner (*Shell-extensie*). Zie het hoofdstuk Scannen in Windows Verkenner:

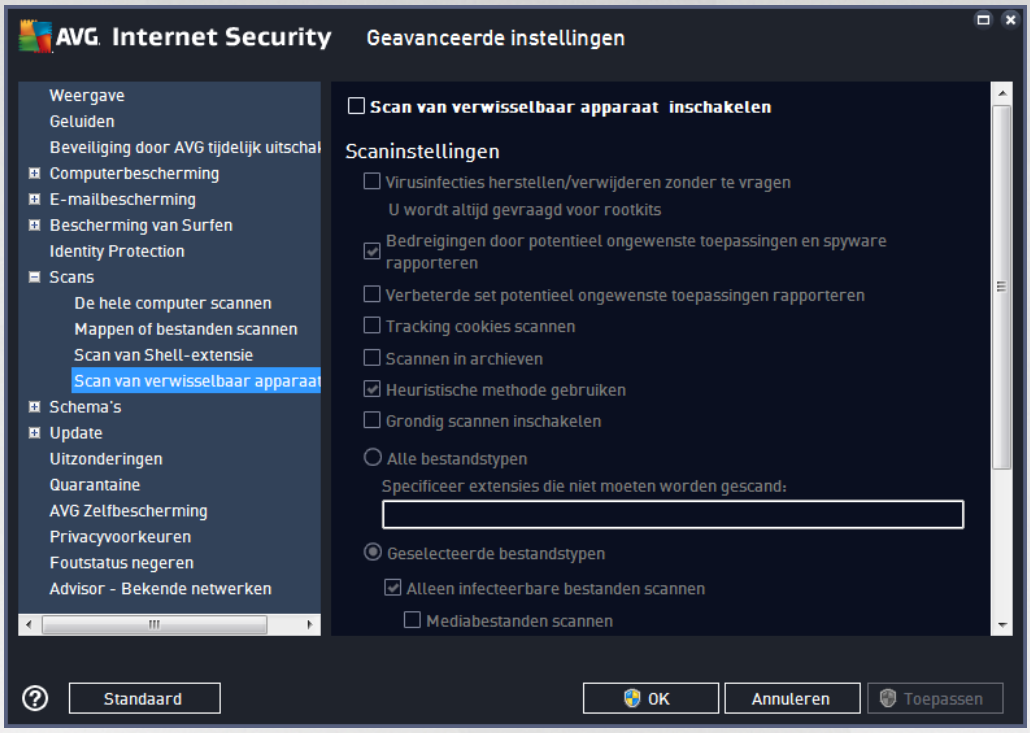
De bewerkingsopties zijn bijna gelijk aan de opties voor De hele computer scannen, maar de standaardinstellingen zijn anders (*bij De hele computer scannen worden bijvoorbeeld niet standaard de archieven gecontroleerd, maar wordt de systeemomgeving gescand, en dat is andersom bij Shell-extensie scannen*).

Opmerking: *zie het hoofdstuk Geavanceerde instellingen AVG / Scans / De hele computer scannen voor een beschrijving van specifieke parameters.*

Vergeleken met het dialoogvenster De hele computer scannen heeft het dialoogvenster ***Shell-extensie scannen*** een extra sectie met de naam ***Weergave van scanvoortgang en -resultaten*** waar u kunt opgeven of de scanvoortgang en de scanresultaten ook toegankelijk moeten zijn vanuit de gebruikersinterface van AVG. Daarnaast kunt u opgeven dat het scanresultaat alleen moet worden weergegeven als er tijdens het scannen een infectie is gedetecteerd.

7.8.4. Scan van verwisselbaar apparaat

Het dialoogvenster voor het bewerken van de instellingen voor ***Scan van verwisselbaar apparaat*** is ook vrijwel identiek aan het dialoogvenster voor het bewerken van instellingen voor De hele computer scannen:



De ***Scan van verwisselbaar apparaat*** wordt automatisch uitgevoerd wanneer u een verwisselbaar apparaat op de computer aansluit. Standaard is deze scanfunctie uitgeschakeld. Het is echter van essentieel belang om verwisselbare apparaten te scannen op potentiële bedreigingen omdat ze een belangrijke bron van infecties zijn. Om ervoor te zorgen dat deze scan direct automatisch kan worden uitgevoerd wanneer dit noodzakelijk is, schakelt u het selectievakje ***Scan van verwisselbaar apparaat inschakelen*** in.

Opmerking: *zie het hoofdstuk Geavanceerde instellingen AVG / Scans / De hele computer scannen voor een beschrijving van specifieke parameters.*

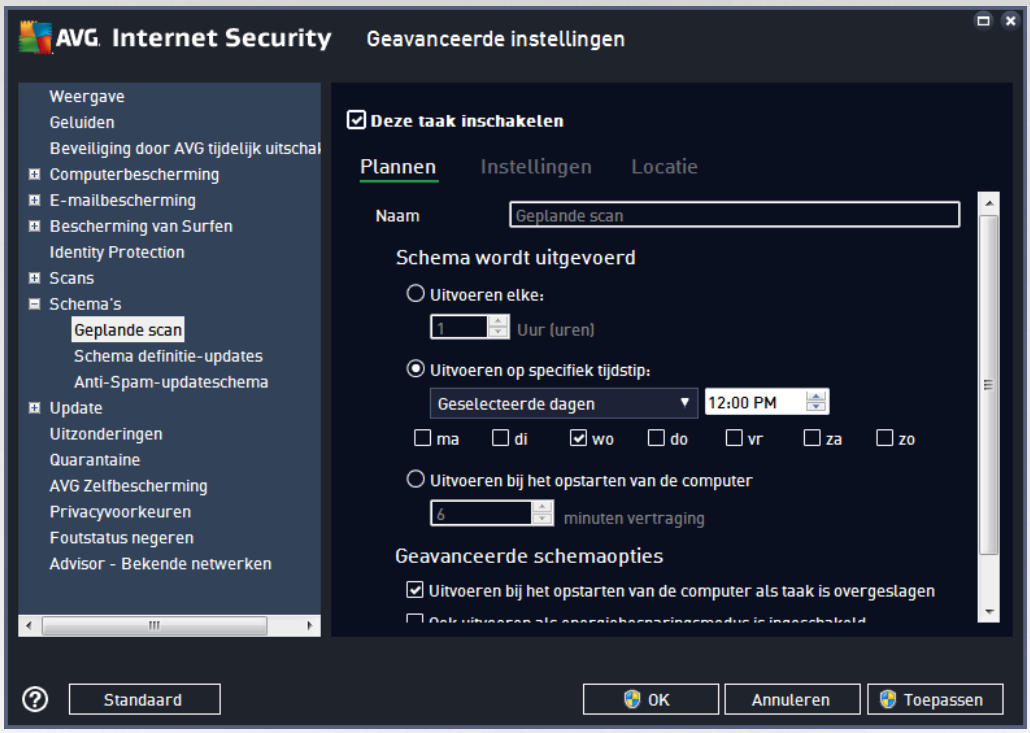
7.9. Schema's

In het gedeelte ***Schema's*** kunt u de standaardinstellingen bewerken van:

- Geplande scan
- Schema voor definitie-updates
- Updateschema programma
- Antispam-updateschema

7.9.1. Geplande scan

U kunt op drie tabbladen parameters instellen voor het schema van de geplande scan (*of een nieuw schema opstellen*): Op elk tabblad kunt u eerst het selectievakje ***Deze taak inschakelen*** uitschakelen als u de geplande scan tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient:



Het tekstveld ***Naam*** (*uitgeschakeld voor alle standaardschema's*) bevat de naam die door de leverancier van het programma is toegewezen aan de planning. Voor nieuwe schema's kunt u zelf een naam opgeven (*klik met de rechtermuisknop op het item* ***Geplande scan*** *in de navigatiestructuur links om een nieuw schema toe te voegen*). Deze naam kunt u vervolgens bewerken in het tekstveld. Probeer altijd korte, maar veelzeggende namen te gebruiken voor scans zodat u ze later gemakkelijker kunt onderscheiden van andere scans.

Het is bijvoorbeeld niet handig om een scan als naam Nieuwe scan of Mijn scan te geven, omdat die namen niet verwijzen naar wat de scan doet. Een naam als Scan systeemgebieden is daarentegen een voorbeeld van een veelzeggende naam voor een scan. Bovendien is het niet nodig om in de naam van de scan aan te geven of de hele computer wordt gescand of alleen een selectie van mappen en bestanden. Uw eigen scans zijn altijd aangepaste versies van het type Mappen of bestanden scannen.

In dit dialoogvenster kunt u daarnaast nog de volgende parameters instellen:

Schema wordt uitgevoerd

Hier kunt u tijdsintervallen opgeven waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt dit interval op verschillende manieren definiëren: als herhaalde scan die na verloop van een bepaalde tijd (***Uitvoeren elke...***) moet worden uitgevoerd, als een scan die op een bepaalde datum op een bepaald tijdstip (***Uitvoeren op specifiek tijdstip***) moet worden uitgevoerd of als een gedefinieerde gebeurtenis waaraan het uitvoeren van de scan is gekoppeld (***Uitvoeren bij het opstarten van de computer***).

Geavanceerde schemaopties

- ***Uitvoeren bij het opstarten van de computer als taak is overgeslagen*** - als u de scan voor een bepaalde tijd plant, kunt u deze optie inschakelen om er zeker van te zijn dat de scan achteraf alsnog wordt uitgevoerd als de computer op de geplande tijd is uitgeschakeld.

- ***Ook uitvoeren als energiebesparingsmodus is ingeschakeld*** - de taak moet ook worden uitgevoerd als de computer op de geplande tijd wordt gevoed door een accu.

Het tabblad ***Instellingen*** bevat een lijst met scanparameters die kunnen worden in- en uitgeschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de betreffende functie gebruikt bij het scannen. ***We raden u aan deze vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om deze instellingen te wijzigen***:

- ***Virusinfecties herstellen/verwijderen zonder te vragen*** *(standaard ingeschakeld):* als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de map Quarantaine verplaatst.

- ***Potentieel ongewenste programma's en spywarebedreigingen rapporteren*** *(standaard ingeschakeld):* schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*): schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn

programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Tracking cookies scannen*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of cookies bij het scannen moeten worden gedetecteerd (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*).

- ***Scannen in archieven*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die zijn gecomprimeerd, zoals ZIP en RAR.

- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - hiermee wordt een heuristische analyse (*dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving*) gebruikt als een van de methoden voor virusdetectie.

- ***Scansysteemomgeving*** (*standaard ingeschakeld*) - als deze parameter is ingeschakeld, worden ook de systeemgebieden van de computer gescand.

- ***Grondig scannen inschakelen*** (*standaard uitgeschakeld)* - in bepaalde omstandigheden (*bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd*) kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Scannen naar rootkits*** *(standaard ingeschakeld):* Anti-Rootkitscan zoekt op uw computer naar rootkits (programma's en technologieën die malware-activiteiten in de computer kunnen verhullen). Als een rootkit wordt gedetecteerd, wil dat nog niet zeggen dat uw computer is geïnfecteerd. In sommige gevallen worden bepaalde stuurprogramma's of delen van reguliere programma's abusievelijk herkend als rootkit.

U moet ook bepalen wat voor type scan u wilt uitvoeren:

- ***Alle bestandstypen*** - u kunt een lijst opgeven met door komma's gescheiden bestandsextensies die moeten worden genegeerd bij het scannen (*als deze lijst is opgeslagen, veranderen de komma's in puntkomma's*).

- ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden - als u deze optie niet inschakelt, beperkt u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu op basis van extensies opgeven welke bestanden altijd moeten worden gescand.

- U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn verdacht en moeten altijd worden gescand.

Scansnelheid aanpassen

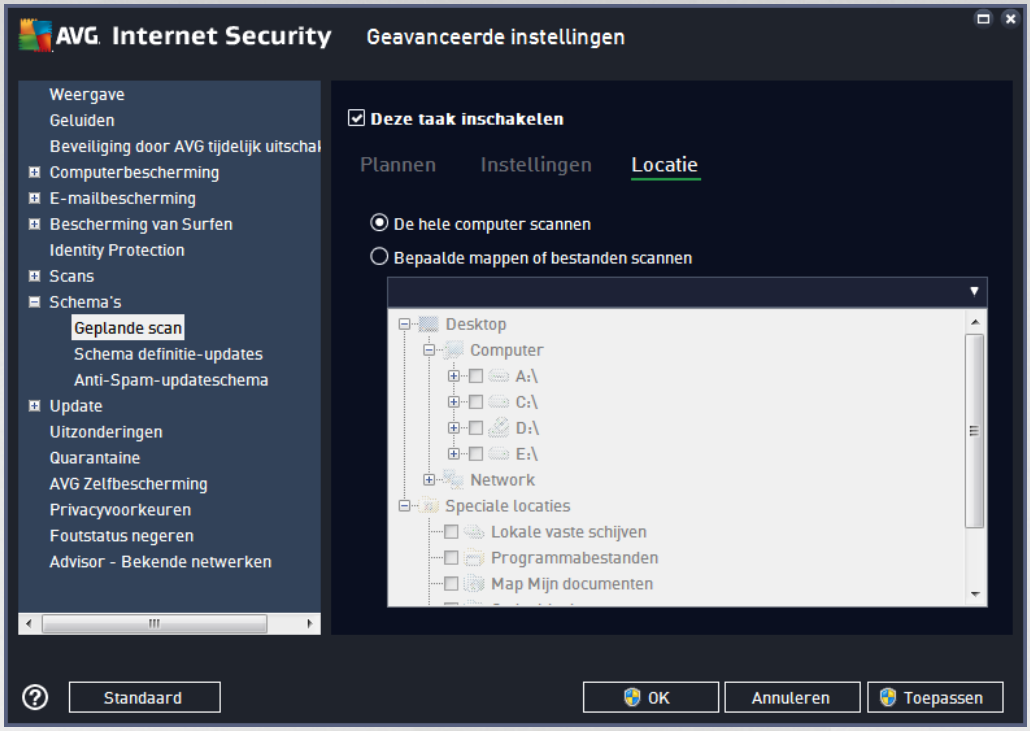
In deze sectie kunt u nader opgeven hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op de systeembronnen van uw computer. Standaard is deze optie ingesteld op het *gebruikerafhankelijke* niveau van automatisch brongebruik. Als u sneller wilt scannen, duurt het scannen minder lang, maar worden aanzienlijk meer systeembronnen gebruikt, zodat andere activiteiten op de computer trager worden uitgevoerd (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt het beroep op systeembronnen echter ook beperken door te kiezen voor een langere scanduur.

Aanvullende scanrapporten instellen

Klik op de koppeling ***Aanvullende scanrapporten instellen...*** om een afzonderlijk dialoogvenster te openen dat ***Scanrapporten*** heet, waarin u selectievakjes kunt inschakelen voor resultaten die moeten worden weergegeven:

Opties voor uitschakelen computer

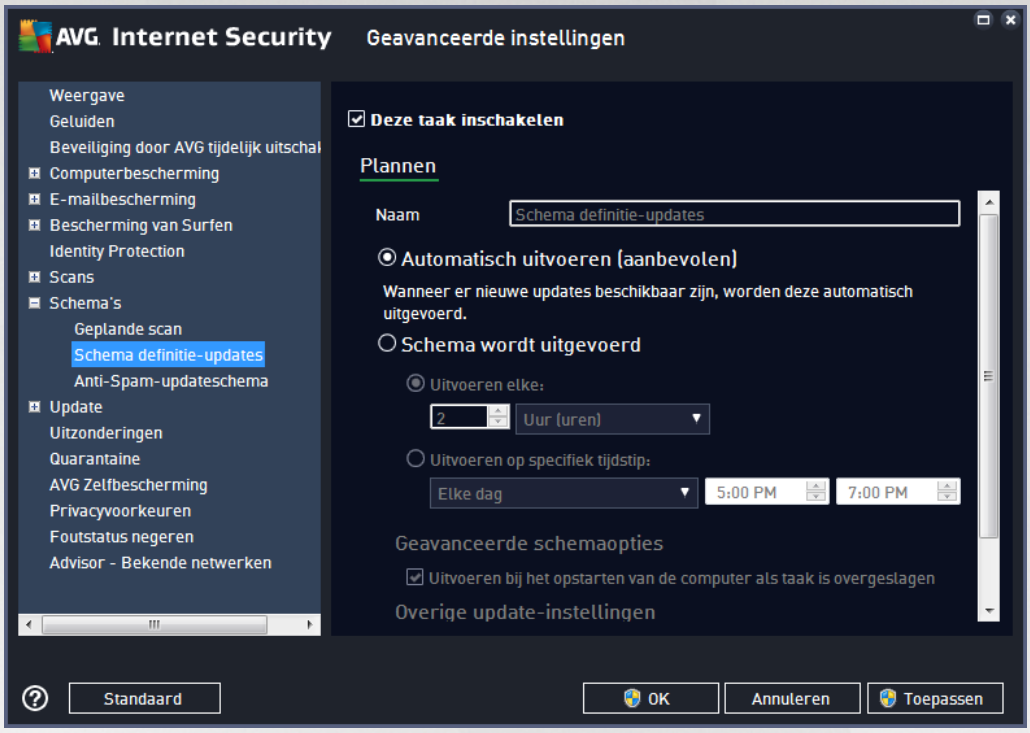
In de sectie ***Opties voor uitschakelen computer*** kunt u opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (***Computer uitschakelen na voltooien van scan***), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (***Geforceerd afsluiten als de computer blijft hangen***).



Op het tabblad ***Locatie*** kunt u opgeven welke scan moet worden uitgevoerd: een scan van de hele computer of een scan van bepaalde bestanden of mappen. Als u kiest voor het scannen van specifieke bestanden of mappen, wordt de in het onderste deel van het dialoogvenster weergegeven mapstructuur actief, zodat u mappen kunt opgeven die moeten worden gescand.

7.9.2. Schema voor definitie-updates

Als ***het echt nodig is***, kunt u de optie ***Deze taak inschakelen*** uitschakelen om een geplande update tijdelijk uit te schakelen. U kunt deze later weer inschakelen:



In dat dialoogvenster kunt u gedetailleerde instellingen opgeven voor het schema voor definitie-updates. Het tekstveld ***Naam*** (*uitgeschakeld voor alle standaardschema's*) bevat de naam die door de leverancier van het programma is toegewezen aan de planning.

Schema wordt uitgevoerd

Standaard wordt de taak automatisch gestart (***Automatisch uitvoeren***) zodra er een nieuwe virusdefinitie-update beschikbaar is. We raden u aan deze configuratie niet te wijzigen, tenzij u een goede reden hebt om dat wel te doen! Vervolgens kunt u het starten van de taak handmatig instellen en de intervallen opgeven voor de start van de geplande definitie-update. U kunt dat interval op verschillende manieren definiëren: als steeds terugkerende update die na verloop van een bepaalde tijd (***Uitvoeren elke...***) moet worden uitgevoerd of als update die op een bepaalde datum en een bepaald tijdstip (***Uitvoeren op specifiek tijdstip***) moet worden uitgevoerd.

Geavanceerde schemaopties

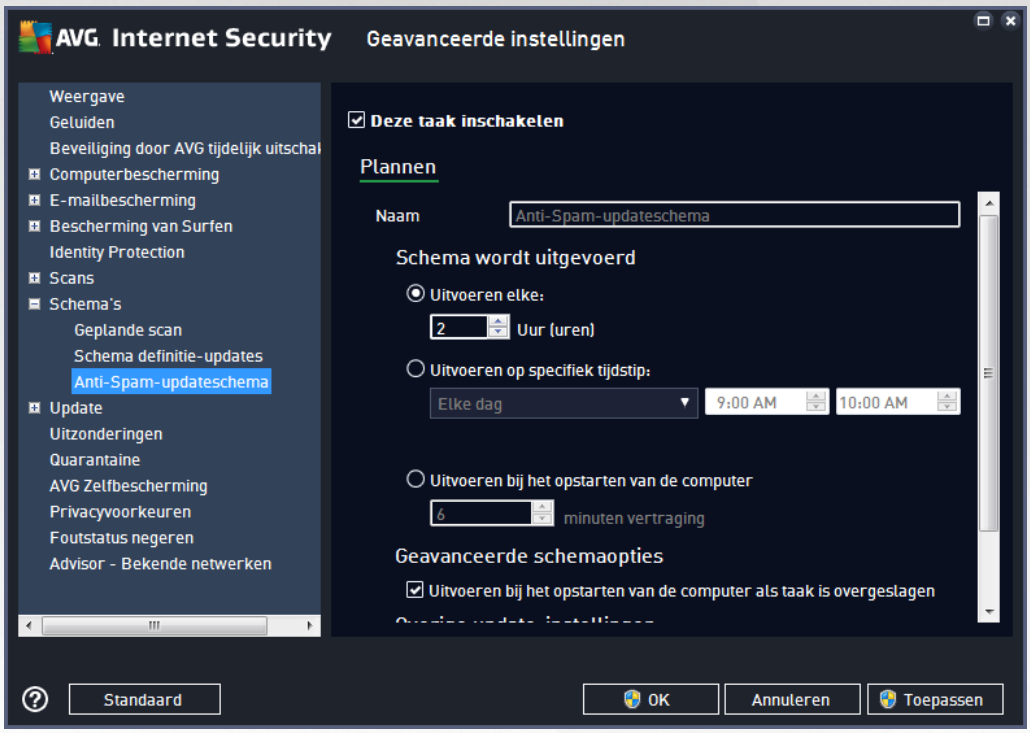
In deze sectie kunt u instellen onder welke omstandigheden de definitie-update wel of niet moet worden uitgevoerd als de computer zich in een energiebesparingsmodus bevindt of is uitgeschakeld.

Overige update-instellingen

Schakel tot slot het selectievakje ***Voer de update opnieuw uit als u een verbinding met internet hebt*** in om ervoor te zorgen dat de update direct opnieuw wordt uitgevoerd zodra de internetverbinding wordt hersteld als de update is mislukt omdat de internetverbinding werd verbroken. Zodra de geplande update wordt gestart op het tijdstip dat u hebt opgegeven, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend bij het AVG-pictogram in het systeemvak (*als u de standaardconfiguratie van het dialoogvenster Geavanceerde instellingen/Weergave niet hebt gewijzigd).*

7.9.3. Updateschema programma

Als het ***echt nodig*** is, kunt u de optie ***Deze taak inschakelen*** uitschakelen om een geplande update van Anti-Spam tijdelijk uit te schakelen, en later weer in te schakelen.



Het tekstveld ***Naam*** (*uitgeschakeld voor alle standaardschema's*) bevat de naam die door de leverancier van het programma is toegewezen aan de planning.

Schema wordt uitgevoerd

Geef een tijdsinterval op waarmee de nieuwe programma-update moet worden uitgevoerd. U kunt dit interval op verschillende manieren definiëren: als steeds terugkerende update die na verloop van een bepaalde tijd (***Uitvoeren elke***) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip (***Uitvoeren op specifiek tijdstip***) moet worden uitgevoerd of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet worden gekoppeld aan (***Actie bij het opstarten van de computer***).

Geavanceerde schemaopties

In deze sectie kunt u bepalen onder welke omstandigheden de programma-update wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.

Overige update-instellingen

Schakel het selectievakje ***Voer de update opnieuw uit als u een verbinding met internet hebt*** in om ervoor te zorgen dat de update direct opnieuw wordt uitgevoerd zodra de internetverbinding wordt hersteld als de update is mislukt omdat de internetverbinding werd verbroken. Zodra de geplande update wordt gestart op het tijdstip dat u hebt opgegeven, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend bij het AVG-pictogram in het systeemvak (*als u de standaardconfiguratie van het dialoogvenster Geavanceerde instellingen/Weergave niet hebt gewijzigd).*

Opmerking: *bij tijdconflicten tussen een geplande programma-update en een geplande scan krijgt het updateproces een hogere prioriteit en zal het scannen worden onderbroken. In dat geval wordt u geïnformeerd over de botsing.*

7.9.4. Antispam-updateschema

Als het echt nodig is, kunt u de optie ***Deze taak inschakelen*** uitschakelen om een geplande update van Anti-Spam tijdelijk uit te schakelen. U kunt de taak later weer inschakelen.

In dit dialoogvenster kunt u gedetailleerde instellingen opgeven voor het updateschema. Het tekstveld ***Naam*** (*uitgeschakeld voor alle standaardschema's*) bevat de naam die door de leverancier van het programma is toegewezen aan het schema.

Schema wordt uitgevoerd

Geef een tijdsinterval op voor het starten van de nieuwe geplande Anti-Spam-update. U kunt dit interval op verschillende manieren definiëren: als steeds terugkerende Anti-Spam-update die na verloop van een bepaalde tijd (***Uitvoeren elke***) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip

(***Uitvoeren op specifiek tijdstip***) moet worden uitgevoerd of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet worden gekoppeld aan (***Actie bij het opstarten van de computer***).

Geavanceerde schemaopties

Hier kunt u instellen onder welke omstandigheden de Anti-Spam-update wel of niet moet worden uitgevoerd als de computer zich in een energiebesparingsmodus bevindt of is uitgeschakeld.

Overige update-instellingen

Schakel het selectievakje ***Voer de update opnieuw uit als u een verbinding met internet hebt*** in om ervoor te zorgen dat de update direct opnieuw wordt uitgevoerd zodra de internetverbinding is hersteld als de Anti-Spam-update is mislukt omdat de internetverbinding werd verbroken. Zodra de geplande scan wordt gestart op het tijdstip dat u hebt opgegeven, ontvangt u hierover een bericht via een pop-upvenster dat wordt geopend bij het AVG-pictogram in het systeemvak (*als u de standaardconfiguratie van het dialoogvenster Geavanceerde instellingen/Weergave niet hebt gewijzigd).*

7.10. Bijwerken

Met de optie ***Update*** in de navigatiestructuur links opent u een nieuw dialoogvenster waarin u parameters kunt instellen voor AVG Update:

Wanneer bestanden moeten worden bijgewerkt

In deze sectie kunt u een keuze maken uit drie alternatieven als het updateproces een herstart van de

computer vereist Het voltooien van de update kan worden gepland voor de eerstvolgende start van de computer, maar u kunt de herstart ook meteen uitvoeren:

- ***Bevestiging vragen van de gebruiker*** *(standaardinstelling)* - u wordt gevraagd of u de computer opnieuw wilt opstarten voor het voltooien van de updateprocedure
- ***Onmiddellijk opnieuw opstarten*** - de computer wordt automatisch opnieuw gestart nadat de updateprocedure is voltooid. U hoeft wordt niet gevraagd of u de computer opnieuw wilt opstarten
- ***Voltooien na eerstvolgende herstart van de computer*** - het voltooien van het updateproces wordt uitgesteld tot de eerstvolgende keer dat u de computer opnieuw opstart. Deze optie wordt alleen aanbevolen als u de computer regelmatig opnieuw opstart, minstens één keer per dag.

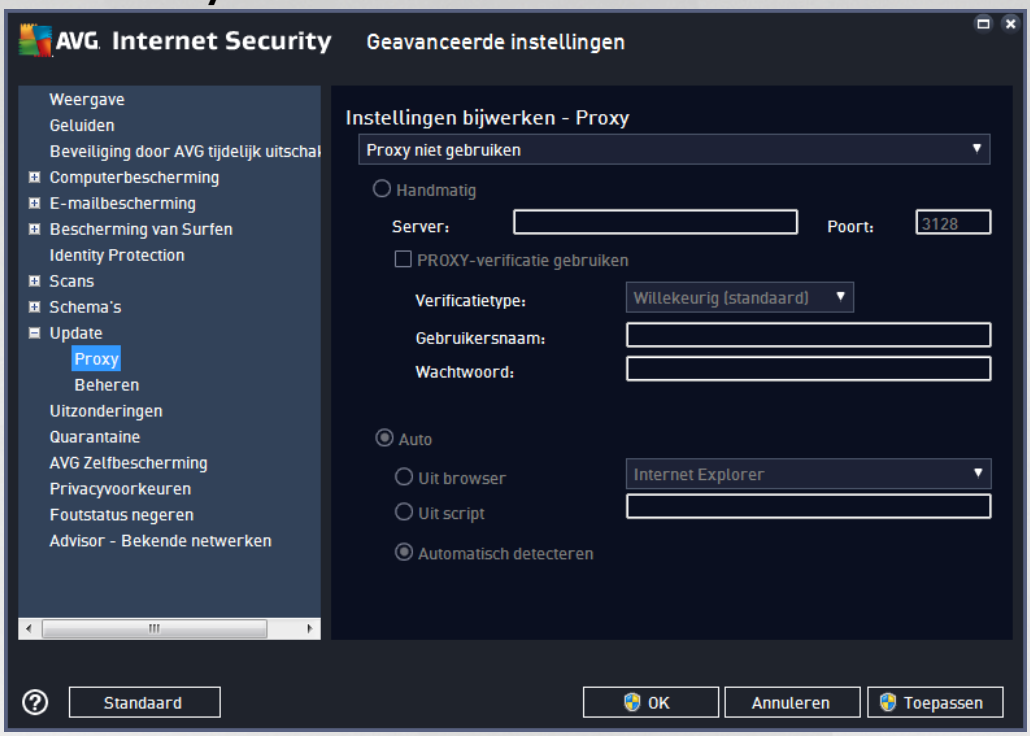
Geheugen- en processcan starten na een voltooide update

Schakel dit selectievakje in om aan te geven dat u na elke voltooide update een nieuwe geheugenscan wilt uitvoeren. Misschien bevat de laatst gedownloade update nieuwe virusdefinities die dan meteen kunnen worden gebruikt bij de scan.

Aanvullende opties voor updates

- ***Nieuw systeemherstelpunt maken tijdens iedere programma-update*** (*standaard ingeschakeld*) - er wordt een nieuw systeemherstelpunt gemaakt voorafgaand aan elke programma-update van AVG. Als het updateproces mislukt en uw besturingssysteem crasht, kunt u altijd de configuratie van uw besturingssysteem herstellen vanaf dit punt. Deze optie is toegankelijk via Start / Alle programma's / Bureau-accessoires / Systeemwerkset / Systeemherstel, maar het aanbrengen van wijzigingen wordt alleen aanbevolen voor ervaren gebruikers. Schakel dit selectievakje niet uit als u van deze functionaliteit wilt gebruikmaken.
- ***DNS-update gebruiken*** (*standaard ingeschakeld*) - als de update eenmaal is gestart, wordt door **AVG Internet Security** op de DNS-server gezocht naar informatie over de nieuwste versies van de virusdatabase en het programma. Vervolgens worden alleen de kleinste, onmisbare bestanden gedownload en geïmplementeerd. Dat reduceert het totaal aan gedownloade gegevens tot een minimum en maakt de update sneller.
- ***Bevestiging vragen voor het afsluiten van programma's die worden uitgevoerd*** (*standaard ingeschakeld*) - deze optie zorgt ervoor dat er geen actieve toepassingen worden afgesloten zonder uw expliciete toestemming, mocht dat nodig zijn voor het voltooien van de updateprocedure.
- ***Controleer de computertijd*** (*standaard ingeschakeld*) - schakel dit selectievakje in als er een melding moet worden weergegeven wanneer de computertijd met meer dan een opgegeven aantal uren afwijkt van de juiste tijd.

7.10.1. Proxy



De proxyserver is een zelfstandige server of een service die op een pc wordt uitgevoerd, die de verbinding met internet veiliger maakt. U hebt, afhankelijk van de instellingen voor het netwerk, rechtstreeks toegang tot internet of via een proxyserver. Het kan ook zijn dat beide mogelijkheden zijn toegestaan. Bij de eerste optie in het dialoogvenster ***Instellingen bijwerken - Proxy*** kiest u in de keuzelijst uit:

- ***Proxy niet gebruiken*** - standaardinstellingen
- ***Proxy gebruiken***
- ***Proberen te verbinden via proxy, en als dat niet lukt direct verbinden***

Als u een optie selecteert waarbij een proxyserver betrokken is, moet u aanvullende gegevens opgeven. U kunt de instellingen voor de server handmatig maar ook automatisch configureren.

Handmatige configuratie

Als u kiest voor handmatige configuratie (schakel *het selectievakje* ***Handmatig*** *in om het desbetreffende deel van het dialoogvenster te activeren*), specificeert u de volgende gegevens:

- ***Server*** - geef het IP-adres van de server of de naam van de server op
- ***Poort*** - geef de poort op die internettoegang mogelijk maakt (*standaard poort 3128; u kunt echter een andere poort instellen - neem contact op met uw netwerkbeheerder voor meer informatie als u niet zeker weet welke poort u moet instellen*)

Het is mogelijk dat op de proxyserver voor de afzonderlijke gebruikers verschillende regels zijn ingesteld. Als

dat voor uw proxyserver het geval is, schakelt u het selectievakje ***PROXY-verificatie gebruiken*** in om te controleren of uw gebruikersnaam en wachtwoord geldig zijn voor een verbinding met internet via de proxyserver.

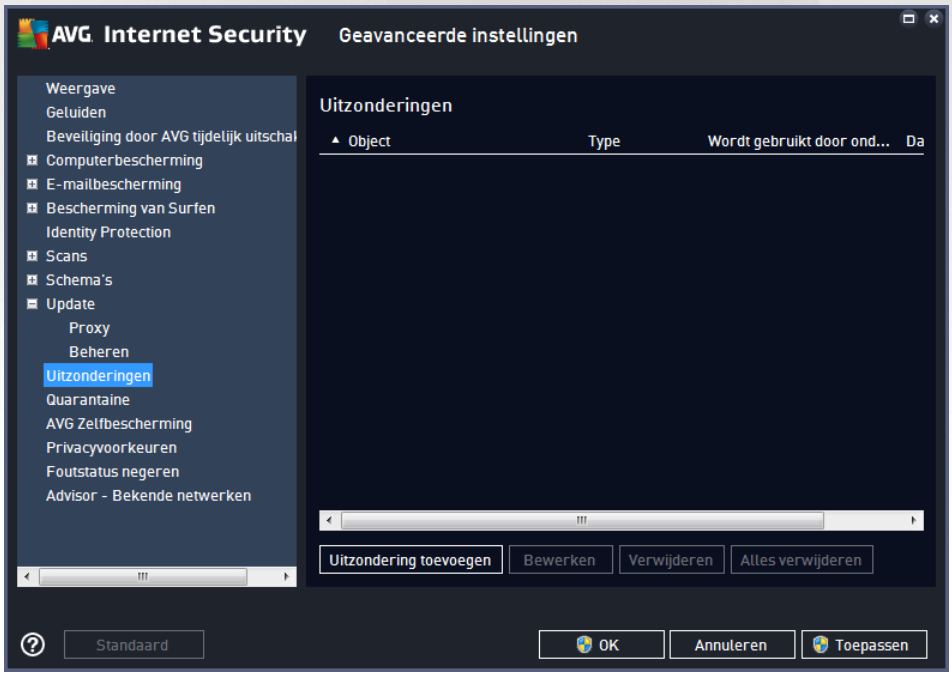
Automatische configuratie

Als u voor een automatische configuratie kiest (*schakel het selectievakje in bij **Auto** om het desbetreffende deel van het dialoogvenster te activeren*), geeft u op waar de configuratie van de proxy van overgenomen moet worden:

- ***Uit browser*** - de configuratie wordt overgenomen van de instellingen van uw standaardinternetbrowser
- ***Uit script*** - de configuratie wordt overgenomen uit een gedownload script, waarbij de functie het proxy-adres retourneert
- ***Automatisch detecteren*** - de configuratie wordt automatisch vastgesteld vanuit de proxyserver

7.10.2. Beheer

In het dialoogvenster ***Updatebeheer*** vindt u twee opties die toegankelijk zijn via twee knoppen:

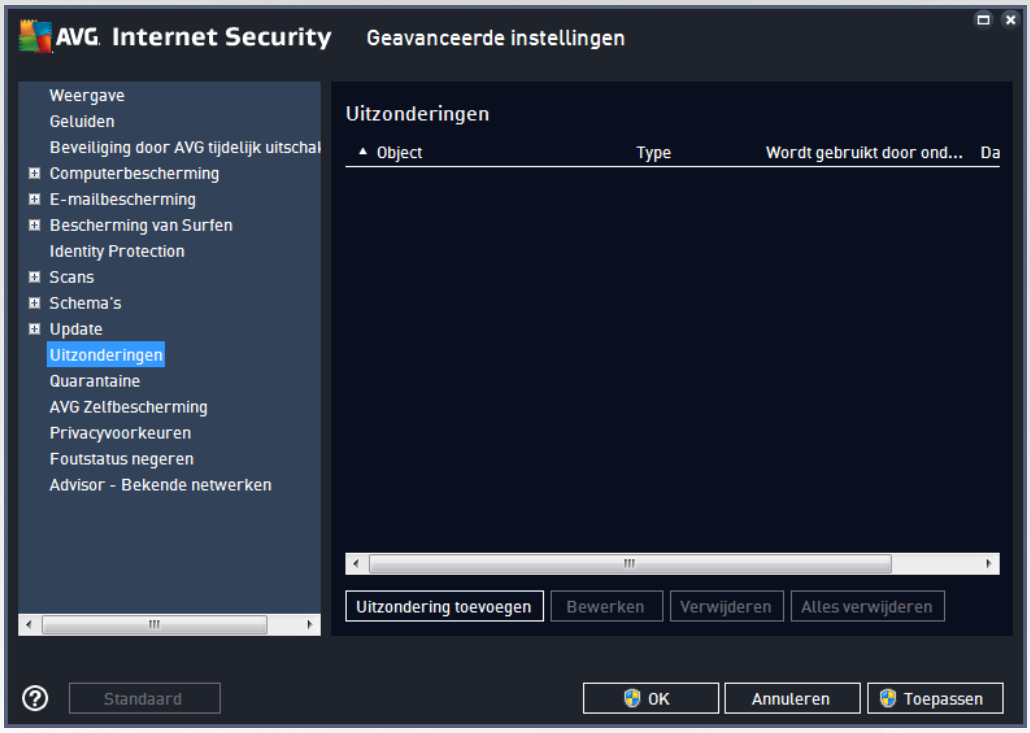


- ***Tijdelijke updatebestanden verwijderen*** - klik op deze knop als u alle redundante updatebestanden wilt verwijderen van uw vaste schijf (*standaard worden deze bestanden 30 dagen bewaard*)
- ***Vorige versie van de virusdatabase herstellen*** - klik op deze knop als u de nieuwste versie van de virusdatabase van uw vaste schijf wilt verwijderen en wilt vervangen door de vorige versie (*de nieuwe versie van de database wordt dan een onderdeel van de volgende update*)

7.11. Uitzonderingen

In het dialoogvenster ***Uitzonderingen*** kunt u uitzonderingen opgeven. Dit zijn items die moeten worden genegeerd door **AVG Internet Security**. Doorgaans moet u een uitzondering opgeven als AVG een programma of bestand als bedreiging blijft detecteren of een website als gevaarlijk blijft blokkeren. Als u dergelijke bestanden of websites toevoegt aan deze uitzonderingenlijst, worden deze door AVG niet meer gerapporteerd of geblokkeerd.

Voeg alleen bestanden, programma's of websites toe als u zeker weet dat deze veilig zijn.



In het dialoogvenster wordt een lijst met uitzonderingen weergegeven, als er al uitzonderingen zijn opgegeven. Voor elk item wordt een selectievakje weergegeven. Als het selectievakje is ingeschakeld, is de uitsluiting van kracht. Is het selectievakje niet ingeschakeld, dan is de uitzondering wel opgegeven, maar wordt deze momenteel niet gebruikt. Door op een kolomkop te klikken, kunt u de toegestane items sorteren op de betreffende criteria.

Knoppen

- ***Uitzondering toevoegen*** - klik hierop om een nieuw dialoogvenster te openen waarin u het item kunt opgeven dat moet worden uitgesloten van AVG-scans.

Eerst wordt u gevraagd het objecttype op te geven (een toepassing, bestand, map, URL of certificaat). Vervolgens geeft u het pad naar het betreffende object op of typt u de URL. Ten slotte kunt u opgeven welke AVG-functies *(Resident Shield, Identity Protection, Scannen)* het geselecteerde object moeten negeren.

- ***Bewerken*** - deze knop is alleen beschikbaar als er al uitzonderingen zijn opgegeven en worden weergegeven. Vervolgens kunt u de knop gebruiken om het bewerkingsvenster voor een geselecteerde uitzondering te openen en de parameters van de uitzondering te configureren.

- ***Verwijderen*** - gebruik deze knop om een eerder opgegeven uitzondering te annuleren. U kunt uitzonderingen een voor een verwijderen of een blok uitzonderingen in de lijst selecteren en de opgegeven uitzonderingen annuleren. Wanneer u een uitzondering hebt geannuleerd, wordt het bestand, de map of de URL waarvoor de uitzondering was opgegeven, weer gecontroleerd. Alleen de uitzondering wordt verwijderd, niet het bestand of de map zelf.

- ***Alles verwijderen*** - met deze knop verwijdert u alle gedefinieerde uitzonderingen in de lijst.

7.12. Quarantaine

In het dialoogvenster ***Onderhoud quarantaine*** kunt u verschillende parameters instellen voor het beheer van objecten die zijn opgeslagen in Quarantaine:

- ***Grootte Quarantaine beperken*** - geef met behulp van de schuifbalk een maximale grootte op voor de Quarantaine. U stelt de grootte in in verhouding tot de grootte van de lokale schijf.
- ***Bestand automatisch verwijderen*** - deze sectie bepaalt hoe lang objecten maximaal worden opgeslagen in Quarantaine (***Bestanden verwijderen ouder dan ... dagen***) en het aantal bestanden dat maximaal wordt opgeslagen in Quarantaine (***Maximum aantal bestanden voor opslaan***).

7.13. AVG Zelfbescherming

Met ***AVG Zelfbescherming*** kan **AVG Internet Security** voorkomen dat de eigen processen, bestanden, registersleutels en stuurprogramma's worden gewijzigd of gedeactiveerd. De belangrijkste reden voor dit type bescherming is dat met bepaalde geavanceerde bedreigingen wordt geprobeerd de antivirusbescherming uit te schakelen om vervolgens ongestoord schade te kunnen veroorzaken op uw computer.

We raden u aan deze functie ingeschakeld te laten.

7.14. Privacyvoorkeuren

In het dialoogvenster ***Privacyvoorkeuren*** wordt u uitgenodigd deel te nemen aan het AVG-programma voor productverbetering en ons te helpen het totale niveau van de internetbeveiliging te verbeteren. Op deze manier kunnen we actuele informatie over de nieuwste bedreigingen van alle deelnemers van over de hele wereld verzamelen en op onze beurt iedereen een betere beveiliging bieden. Deze rapporten worden automatisch samengesteld en dit kost u geen tijd. In de rapporten worden geen persoonlijke gegevens opgenomen. Het rapporteren van gedetecteerde bedreigingen is optioneel. Het wordt echter aanbevolen om deze optie ingeschakeld te laten. U helpt ons op deze wijze om de beveiliging voor u en andere AVG-gebruikers te verbeteren.

In dit dialoogvenster zijn de volgende instellingsopties beschikbaar:

- ***Ik wil AVG helpen haar producten te verbeteren en neem deel aan het AVG-programma voor productverbetering*** *(standaard ingeschakeld)* - schakel het selectievakje niet uit als u ons wilt helpen **AVG Internet Security** te verbeteren. In dat geval worden alle gedetecteerde bedreigingen gerapporteerd aan AVG, kunnen wij actuele informatie verzamelen over malware van iedereen die waar dan ook ter wereld deelneemt en kan de bescherming voor iedereen worden verbeterd. Omdat de rapporten automatisch worden samengesteld, hebt u hier geen last van. Er worden geen persoonlijke gegevens in de rapporten opgenomen.
    - ***Gegevens over foutief geïdentificeerde e-mail na bevestiging van gebruiker*** *(standaard ingeschakeld)* - verzend informatie over e-mail die ten onrechte is aangemerkt als spam en over spam die niet als zodanig is herkend door de service Anti-Spam. Voor het versturen van dergelijke gegevens wordt uw toestemming gevraagd.
    - ***Anonieme gegevens over geïdentificeerde of verdachte bedreigingen*** *(standaard ingeschakeld)* - informatie versturen over verdachte of gevaarlijke code of gedragspatronen *(dit kan gaan om een virus, spyware of schadelijke webpagina die u probeert te openen)* die op uw computer zijn waargenomen.
    - ***Anonieme gegevens over productgebruik*** *(standaard ingeschakeld)* - basisgegevens versturen over activiteit van AVG, zoals het aantal detecties, het aantal uitgevoerde scans, voltooide of mislukte updates, enzovoort.
- ***Detectieverificatie in de cloud toestaan*** *(standaard ingeschakeld)* - gedetecteerde bedreigingen worden gescand om na te gaan of ze werkelijk geïnfecteerd zijn, om zo valse meldingen te voorkomen.
- ***Ik wil dat AVG mijn ervaring persoonlijker maakt door AVG-personalisatieprogramma in te***

schakelen *(standaard uitgeschakeld)* - met deze functie wordt het gedrag geanalyseerd van programma's en toepassingen die op uw pc zijn geïnstalleerd. Op basis van deze analyse kan AVG u services aanbieden die aansluiten bij uw behoeften, voor een optimale beveiliging.

7.15. Foutstatus negeren

In het dialoogvenster ***Foutstatus negeren*** kunt u aangeven over welke onderdelen u geen informatie wilt weergeven:

Standaard is geen enkel onderdeel geselecteerd in deze lijst. Dit houdt in dat als een onderdeel een foutstatus krijgt, u hierover onmiddellijk wordt geïnformeerd via:

- Het systeemvakpictogram - zolang alle onderdelen van AVG correct werken, wordt het pictogram weergegeven in vier kleuren. Als er echter een fout optreedt, verschijnt er een geel uitroepteken in het pictogram,
- Een tekstbeschrijving van het huidige probleem in het gedeelte Info Beveiligingsstatus van het hoofdvenster van AVG.

Er kunnen zich situaties voordoen waarin u om welke reden dan ook een onderdeel tijdelijk moet uitschakelen. ***Dit wordt niet aanbevolen, aangezien u moet proberen alle onderdelen altijd ingeschakeld te houden (in de standaardconfiguratie)***, maar het kan voorkomen. In dat geval wordt in het systeemvakpictogram automatisch de foutstatus van het onderdeel weergegeven. In dit specifieke geval kan echter niet worden gesproken van een echte fout, omdat u deze opzettelijk hebt veroorzaakt en omdat u zich bewust bent van het potentiële risico. Tegelijkertijd kan het pictogram, zodra dit grijs wordt weergegeven, niet eventuele echte fouten rapporteren die zich zouden kunnen voordoen.

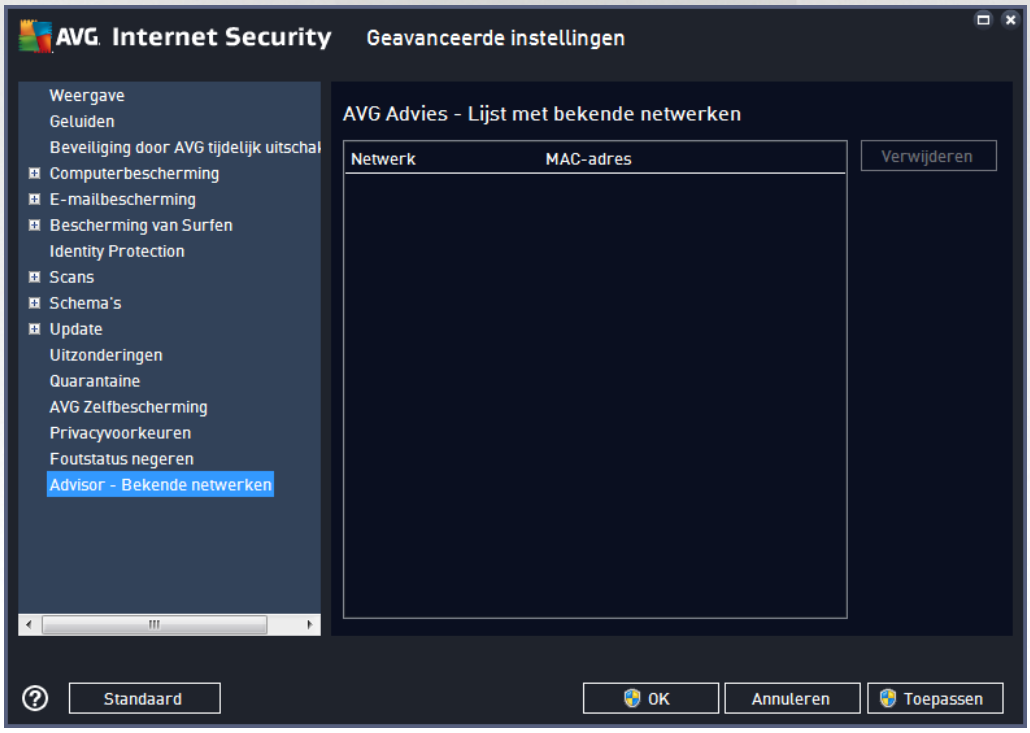
Daarom kunt u in het dialoogvenster ***Foutstatus negeren*** onderdelen selecteren die een foutstatus hebben (*of die uitgeschakeld zijn*) en waarover u niet wilt worden geïnformeerd. Klik op de knop ***OK*** om de wijzigingen te

bevestigen.

7.16. Advisor – Bekende netwerken

In AVG Advies is een functie opgenomen waarmee de netwerken worden gecontroleerd waarmee u verbinding maakt. *Als er een nieuw netwerk wordt gevonden (met een eerder gebruikte netwerknaam, wat tot verwarring kan leiden)*, wordt u hiervan op de hoogte gesteld en wordt u aangeraden de veiligheid van het netwerk te controleren. Als u besluit dat veilig verbinding kan worden gemaakt met het nieuwe netwerk, kunt u het netwerk ook opslaan in deze lijst *(via de koppeling in de systeemvakmelding van AVG Advies die boven het systeemvak wordt weergegeven wanneer een onbekend netwerk wordt gedetecteerd. Zie voor meer informatie het hoofdstuk over AVG Advies)*. AVG Advies onthoudt vervolgens de unieke kenmerken van het netwerk *(het MAC-adres)* en de melding wordt niet meer weergegeven. Elk netwerk waarmee u verbinding maakt, wordt automatisch beschouwd als het bekende netwerk en toegevoegd aan de lijst. U kunt afzonderlijke items verwijderen door te klikken op de knop ***Verwijderen***. Het betreffende netwerk wordt in dat geval weer als onbekend en mogelijk onveilig beschouwd.

In dit dialoogvenster kunt u controleren welke netwerken als bekend worden beschouwd:



Opmerking: *de functie voor bekende netwerken in AVG Advies wordt niet ondersteund in 64-bits versies van Windows XP.*

8. Firewallinstellingen

De configuratie van Firewall wordt geopend in een nieuw venster waarin u via verscheidene dialoogvensters geavanceerde parameters kunt instellen voor het onderdeel. De Firewall-configuratie wordt geopend in een nieuw venster waarin u via verscheidene dialoogvensters de geavanceerde parameters voor het onderdeel kunt bewerken. De configuratie kan worden weergegeven in de standaard- of expertmodus. Wanneer u het configuratievenster voor het eerst opent, is de standaardmodus ingeschakeld en kunt u de volgende parameters bewerken:

- Algemeen
- Toepassingen
- Bestanden en printers delen

Onder aan het dialoogvenster bevindt zich de knop ***Expertmodus***. Klik op de knop om de zeer geavanceerde opties voor de configuratie van Firewall weer te geven in het dialoogvenster:

- Geavanceerde instellingen
- Gedefinieerde netwerken
- Systeemservices
- Logboeken

8.1. Algemeen

Het dialoogvenster ***Algemene informatie*** bevat een overzicht van alle beschikbare Firewall-modi. U kunt de geselecteerde Firewall-modus eenvoudig wijzigen door een andere modus te selecteren in het menu.

De leverancier van de software heeft echter alle onderdelen van AVG Internet Security ingesteld met het oog op optimale prestaties. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen uitsluitend te worden aangebracht door ervaren gebruikers.

Met Firewall kunt u specifieke regels voor het beveiligingsniveau definiëren, afhankelijk van of de computer zich in een domein bevindt, een zelfstandige computer is of zelfs een notebook is. Voor deze opties zijn verschillende beveiligingsniveaus vereist. De niveaus worden bepaald door de betreffende profielen. Kortom, een Firewall-modus is een specifieke configuratie van het onderdeel Firewall. U kunt een aantal van dergelijke vooraf gedefinieerde configuraties gebruiken:

- ***Automatisch*** - in deze modus wordt al het netwerkverkeer automatisch afgehandeld. U wordt niet gevraagd beslissingen te nemen. Verbindingen worden toegestaan voor bekende toepassingen. Daarnaast wordt voor de toepassing een regel gemaakt waarin wordt aangegeven dat de toepassing in de toekomst altijd verbinding kan maken. Voor andere toepassingen wordt op basis van het gedrag van de toepassing beslist of de verbinding moet worden toegestaan. In dergelijke gevallen wordt er echter geen regel gemaakt. Dit betekent dat de toepassing altijd wordt gecontroleerd als deze probeert verbinding te maken. ***De automatische modus is een niet-inbreukmakende modus en wordt aanbevolen voor de meeste gebruikers.***

- ***Interactief*** - deze modus is handig als u volledige controle wilt over al het netwerkverkeer naar en van uw computer. Firewall controleert het verkeer voor u en er wordt een melding weergegeven zodra er wordt geprobeerd te communiceren of gegevens te verzenden. Op deze manier kunt u bepalen wat wel en niet is toegestaan. Alleen aanbevolen voor ervaren gebruikers.

- ***Toegang tot internet blokkeren*** - de internetverbinding wordt volledig geblokkeerd. U hebt geen toegang tot internet en niemand kan extern toegang verkrijgen tot uw computer. Gebruik deze modus alleen in speciale gevallen en voor een beperkte tijd.

- ***Firewallbescherming uitschakelen*** - wanneer u Firewall uitschakelt, is al het netwerkverkeer van en naar uw computer toegestaan. Uw computer is in dat geval kwetsbaar voor aanvallen van hackers. Ga altijd zorgvuldig om met deze optie.

Er is nog een specifieke automatische modus beschikbaar in Firewall. Deze modus wordt op de achtergrond geactiveerd als het onderdeel Computer of Identiteit wordt uitgeschakeld en uw computer als gevolg daarvan kwetsbaarder is. In dergelijke gevallen worden alleen bekende en absoluut veilige toepassingen automatisch

toegestaan. In alle andere gevallen wordt u gevraagd een beslissing te nemen. Dit wordt gedaan ter compensatie van de uitgeschakelde beveiligingsonderdelen en om uw computer veilig te houden.

8.2. Toepassingen

In het dialoogvenster ***Toepassingen*** worden alle toepassingen weergegeven die tot nu toe hebben geprobeerd te communiceren via het netwerk. Daarnaast worden pictogrammen weergegeven voor de toegewezen actie:

De toepassingen in de ***lijst met toepassingen*** zijn toepassingen die op uw computer zijn gedetecteerd (*en waaraan de desbetreffende acties zijn toegewezen*). De volgende typen acties kunnen worden gebruikt:

- - communicatie toestaan voor alle netwerken
- - communicatie blokkeren
- - geavanceerde instellingen gedefinieerd

Alleen al geïnstalleerde toepassingen kunnen worden gedetecteerd. Als de nieuwe toepassing voor het eerst probeert een verbinding tot stand te brengen via het netwerk, wordt automatisch in overeenstemming met de vertrouwde database een regel voor de toepassing gemaakt of wordt u gevraagd of u de communicatie wilt toestaan of blokkeren. In het laatste geval kunt u uw antwoord opslaan als permanente regel (die vervolgens zal worden opgenomen in de lijst van dit dialoogvenster).

Vanzelfsprekend kunt u ook direct regels voor de nieuwe toepassing maken - in dit dialoogvenster klikt u op ***Toevoegen*** en vult u de toepassingsgegevens in.

Behalve de toepassingen bevinden zich twee speciale items in de lijst. ***Prioriteitstoepassingen-regels*** (*boven aan de lijst*) zijn voorkeursregels en worden altijd toegepast vóór de regels voor afzonderlijke toepassingen. ***Overige toepassingen-regels*** (*onder aan de lijst*) zijn regels die in laatste instantie worden toegepast als er

geen specifieke toepassingsregels zijn, dus bij onbekende en niet-gedefinieerde toepassingen. Selecteer de actie die moet worden geactiveerd wanneer een dergelijke toepassing probeert te communiceren via het netwerk: Blokkeren *(communicatie wordt altijd geblokkeerd)*, Toestaan *(communicatie wordt voor elk netwerk toegestaan)*, Vragen *(u wordt gevraagd te bepalen of de communicatie moet worden toegestaan of geblokkeerd)*. ***Deze items hebben andere instellingsopties dan reguliere toepassingen en zijn alleen bedoeld voor ervaren gebruikers. Het wordt met klem aangeraden om deze instellingen niet te wijzigen.***

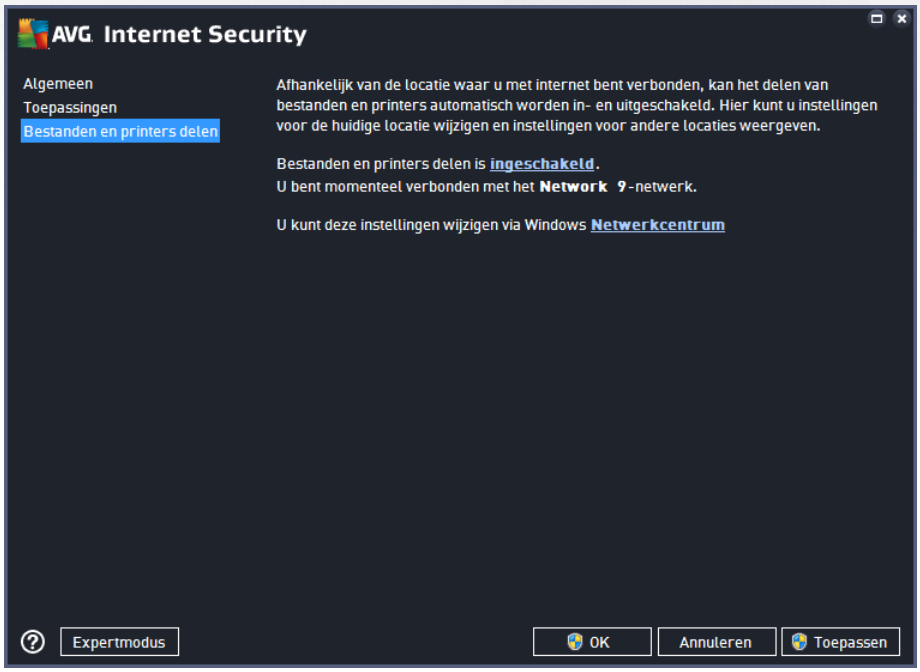
Knoppen

U kunt de lijst bewerken met behulp van de volgende knoppen:

- ***Toevoegen*** - hiermee opent u een leeg dialoogvenster waarin u nieuwe toepassingsregels kunt opgeven.
- ***Bewerken*** - hiermee opent u hetzelfde dialoogvenster, maar dan met gegevens, waarin u de bestaande regels van een toepassing kunt bewerken.
- ***Verwijderen*** - hiermee verwijdert u de geselecteerde toepassing uit de lijst.

8.3. Bestanden en printers delen

Bestanden en printers delen heeft betrekking op alle bestanden of mappen die u markeert als Gedeeld in Windows en alle gemeenschappelijke stations, printers, scanners en vergelijkbare apparaten. Het delen van dergelijke items is alleen gewenst in netwerken die kunnen worden beschouwd als veilig *(bijvoorbeeld thuis, op het werk of op school)*. Wanneer u echter bent verbonden met een openbaar netwerk *(zoals een Wi-Fi-hotspot op een luchthaven of in een internetcafé)*, kunt u beter niets delen. In AVG Firewall kunt u het delen eenvoudig blokkeren of toestaan en kunt u uw keuze voor bezochte netwerken opslaan.

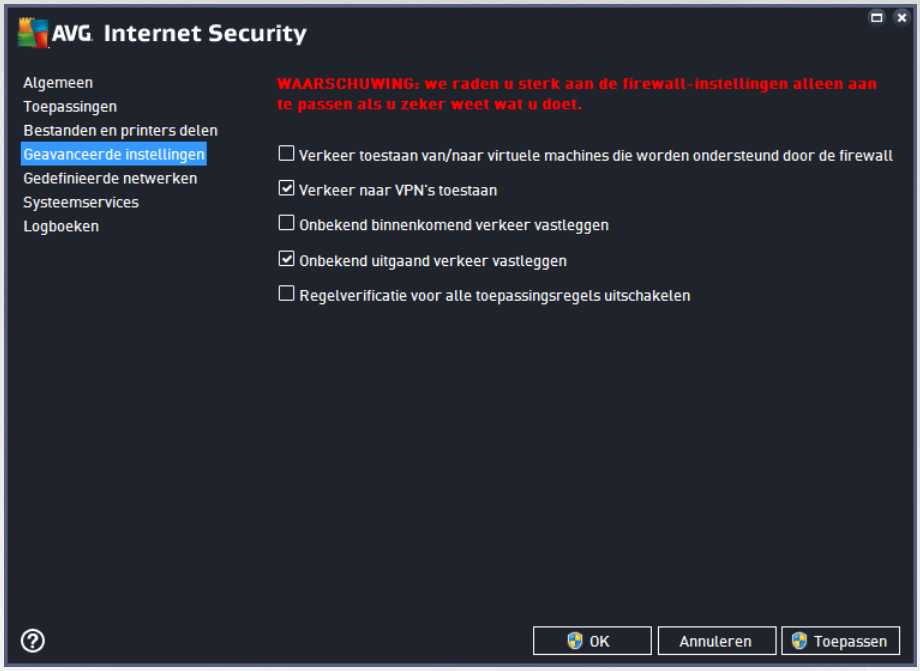


In het dialoogvenster ***Bestanden en printers delen*** kunt u de configuratie voor het delen van bestanden en

printers, en de momenteel verbonden netwerken bewerken. In Windows XP komt de naam van het netwerk overeen met de naam die u voor het specifieke netwerk opgeeft als u voor het eerst verbinding maakt. In Windows Vista en hoger wordt de netwerknaam automatisch opgehaald uit Netwerkcentrum.

8.4. Geavanceerde instellingen

Breng alleen wijzigingen in het dialoogvenster Geavanceerde instellingen aan als u een ERVAREN GEBRUIKER bent.



In het dialoogvenster ***Geavanceerde instellingen*** kunt u de volgende Firewall-parameters in- en uitschakelen:

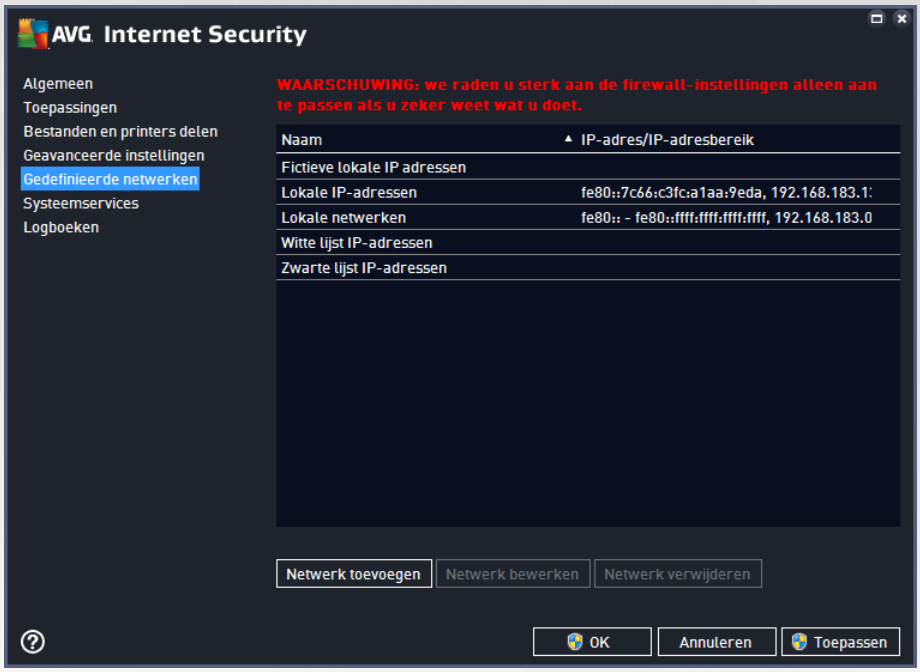
- ***Verkeer toestaan van/naar virtuele machines die worden ondersteund door de firewall*** - ondersteuning voor netwerkverbindingen in virtuele machines zoals VMWare.
- ***Verkeer naar VPN's toestaan*** - ondersteuning voor VPN-verbindingen *(wordt gebruikt voor verbindingen met externe computers)*.
- ***Onbekend binnenkomend/uitgaand verkeer vastleggen*** - alle communicatiepogingen *(binnenkomend/uitgaand)* door onbekende toepassingen worden vastgelegd in het Firewall-logboek.
- ***Regelverificatie uitschakelen voor alle toepassingsregels*** - alle bestanden waarop de toepassingsregels van toepassing zijn, worden voortdurend gecontroleerd door Firewall. Bij een wijziging van het binaire bestand wordt nogmaals geprobeerd de veiligheid van de toepassing te controleren op basis van standaardmethoden, bijvoorbeeld door het certificaat te verifiëren of de toepassing op te zoeken in de database van vertrouwde toepassingen. Als de toepassing niet als veilig kan worden beschouwd, wordt de toepassing behandeld op basis van de geselecteerde modus:
    - Als Firewall wordt uitgevoerd in de ***automatische modus***, wordt de toepassing standaard toegestaan.
    - Als Firewall wordt uitgevoerd in de ***interactieve modus***, wordt de toepassing geblokkeerd en

wordt er een dialoogvenster weergegeven waarin de gebruiker wordt gevraagd te bepalen hoe de toepassing moet worden behandeld.

Daarnaast kan voor elke specifieke toepassing een gewenste behandelingsprocedure worden opgegeven in het dialoogvenster Toepassingen.

8.5. Gedefinieerde netwerken

Breng alleen wijzigingen in het dialoogvenster Gedefinieerde netwerken aan als u een ERVAREN GEBRUIKER bent.

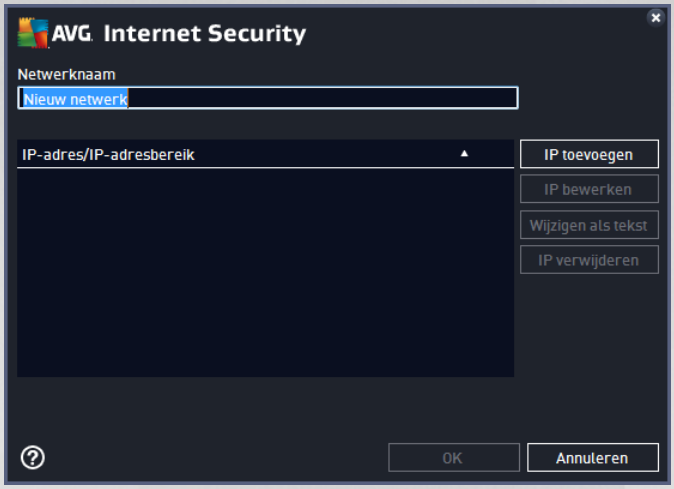


Het dialoogvenster ***Gedefinieerde netwerken*** bevat een lijst met alle netwerken waarop uw computer is aangesloten. De lijst bevat de volgende informatie over elk gedetecteerd netwerk:

- ***Netwerken*** - de lijst met namen van netwerken waarmee de computer is verbonden.
- ***IP-adresbereik*** - elk netwerk wordt automatisch gedetecteerd en weergegeven in de vorm van een IP-adresbereik.

Knoppen

- ***Netwerk toevoegen*** - hiermee opent u een nieuw dialoogvenster waarin u parameters voor het nieuwe netwerk kunt opgeven (de ***netwerknaam*** en het ***IP-adresbereik***):

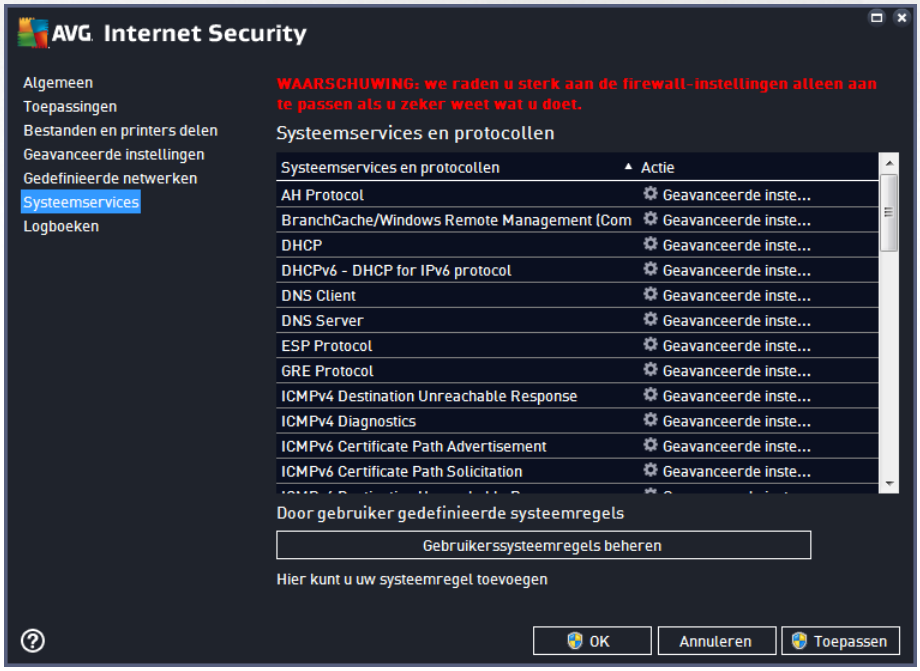


- ***Netwerk bewerken*** - hiermee opent u het dialoogvenster ***Netwerkeigenschappen*** (*zie hierboven*) waarin u de parameters van een gedefinieerd netwerk kunt opgeven (*het dialoogvenster is identiek aan het dialoogvenster voor het toevoegen van een nieuw netwerk, zie de beschrijving in de vorige paragraaf*).

- ***Netwerk verwijderen*** - hiermee verwijdert u de verwijzing naar een geselecteerd netwerk uit de lijst met netwerken.

8.6. Systeemservices

We raden u sterk aan ALLEEN instellingen te wijzigen in het dialoogvenster Systeemservices en protocollen als u een ervaren gebruiker bent.



Het dialoogvenster ***Systeemservices en protocollen*** bevat een overzicht van de standaardsysteemservices en protocollen van Windows die misschien moeten communiceren via het netwerk. Het overzicht bevat de

volgende kolommen:

- ***Systeemservices en protocollen*** - deze kolom bevat de naam van de betreffende systeemservice.
- ***Actie*** - in deze kolom wordt een pictogram voor de toegewezen actie weergegeven:
  - Communicatie voor alle netwerken toestaan
  - Communicatie blokkeren

Als u de instellingen voor een item in de lijst (*inclusief de toegewezen acties*) wilt bewerken, klikt u met de rechtermuisknop op het item en selecteert u ***Bewerken***. ***Alleen zeer ervaren gebruikers kunnen systeemregels bewerken. AVG raadt het bewerken van systeemregels ten sterkste af.***

Door gebruiker gedefinieerde systeemregels

Als u een nieuw dialoogvenster wilt openen voor het maken van uw eigen systeemserviceregel (*zie de afbeelding hieronder*), klikt u op de knop ***Gebruikerssysteemregels beheren***. Hetzelfde dialoogvenster wordt geopend als u de configuratie van een van de bestaande items in de lijst met systeemservices en protocollen bewerkt. Het bovenste deel van het dialoogvenster bevat een overzicht van alle details van de systeemregel die op dat moment wordt bewerkt. In het onderste deel wordt het geselecteerde detail weergegeven. Regeldetails kunnen worden bewerkt, toegevoegd of verwijderd met de betreffende knoppen:

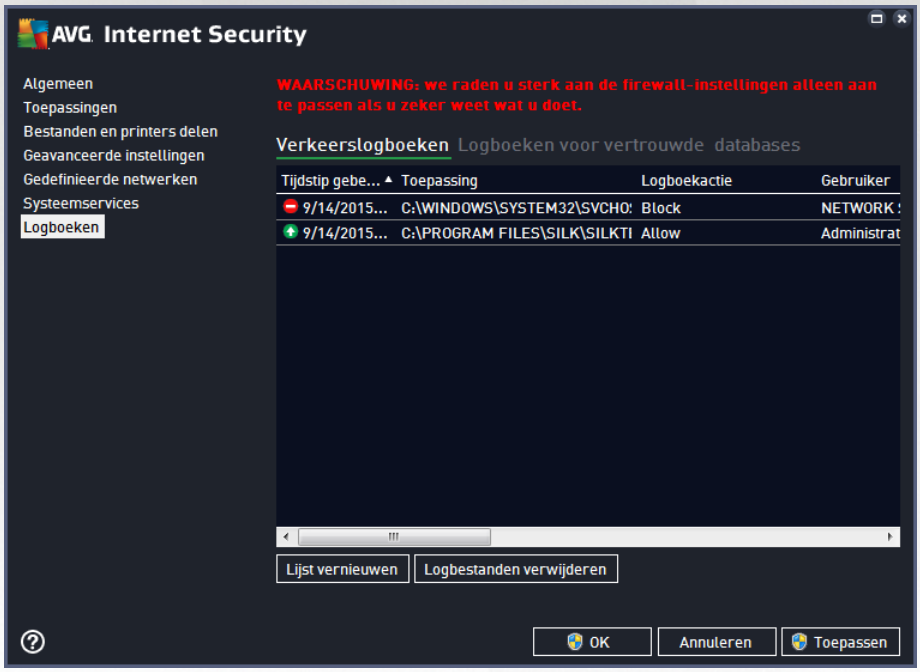
Houd er rekening mee dat detailregelinstellingen geavanceerde instellingen zijn die hoofdzakelijk zijn bedoeld voor netwerkbeheerders die de volle controle moeten hebben over de Firewall-configuratie. Als u niet bekend bent met typen communicatieprotocollen, nummers van netwerkpoorten, definities van IP-adressen, enzovoort, kunt u deze instellingen beter niet wijzigen! Als u de configuratie echt moet wijzigen, raadpleegt u de help bij de desbetreffende dialoogvensters voor specifieke details.

8.7. Logboeken

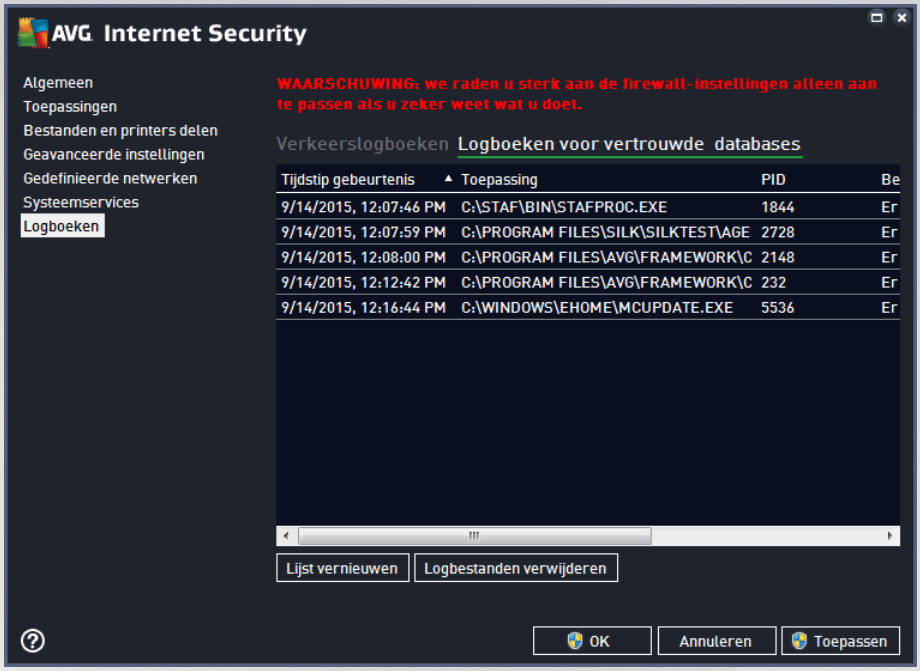
Breng alleen wijzigingen in het dialoogvenster Logboeken netwerken aan als u een ERVAREN GEBRUIKER bent.

Het dialoogvenster ***Logboeken*** bevat de lijst met alle vastgelegde Firewall-acties en -gebeurtenissen, met een uitgebreide beschrijving van de relevante parameters.

- ***Verkeerslogboeken*** - dit tabblad biedt informatie over alle toepassingen die hebben geprobeerd verbinding te maken met het netwerk. Voor elk item wordt er informatie weergegeven over het tijdstip van de gebeurtenis, de toepassingsnaam, de logboekactie, de gebruikersnaam, PID, verkeersrichting, het protocoltype, de nummers van de externe en lokale poorten, en informatie over het lokale en externe IP-adres.



- ***Logboeken voor vertrouwde databases*** - de *vertrouwde database* is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en vertrouwde toepassingen die altijd online mogen communiceren. De eerste keer dat een nieuwe toepassing probeert een verbinding tot stand te brengen met het netwerk (*wanneer er nog geen firewallregel voor de toepassing is gedefinieerd*), moet worden bepaald of de betreffende toepassing mag communiceren via het netwerk. Eerst zoekt AVG in de *vertrouwde database* en als de toepassing daarin wordt vermeld, wordt automatisch toegang tot het netwerk verleend. Pas daarna, als duidelijk is dat er geen informatie over de toepassing is opgeslagen in de vertrouwde database, wordt u in een afzonderlijk dialoogvenster gevraagd of de toepassing toegang mag krijgen tot het netwerk.



Knoppen

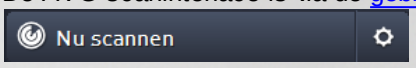
- ***Lijst vernieuwen*** - alle geregistreerde parameters kunnen worden gerangschikt op het geselecteerde attribuut: chronologisch (*datums*) of alfabetisch (*andere kolommen*) - klik op de kolomkop. Werk de op een bepaald moment weergegeven informatie bij met nieuwe gegevens door op de knop ***Lijst vernieuwen*** te klikken.

- ***Logbestanden verwijderen*** - klik op deze knop als u alle vermeldingen wilt verwijderen.

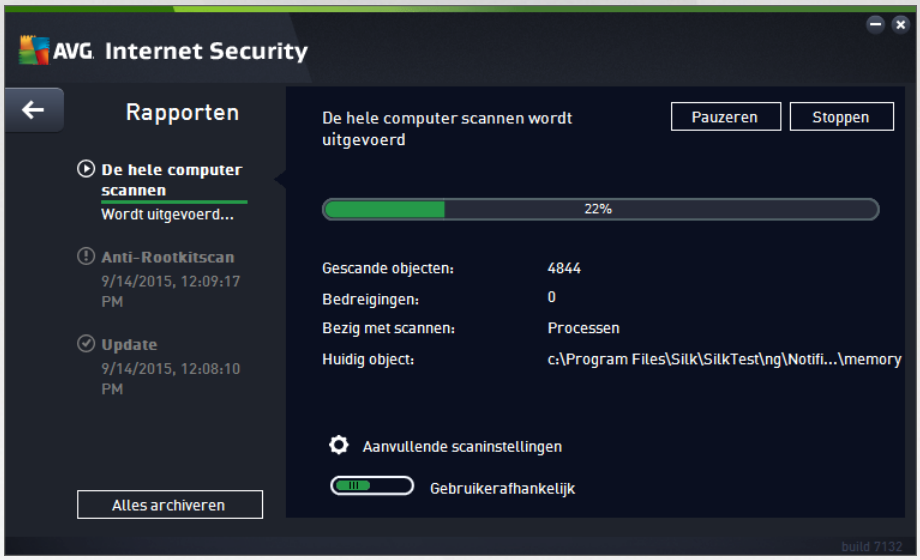
9. AVG scannen

Standaard worden door **AVG Internet Security** geen scans meer uitgevoerd na de eerste scan *(die u wordt gevraagd te starten*), omdat u dan volledig beschermd wordt door de residente onderdelen van **AVG Internet Security**. Deze onderdelen zijn altijd waakzaam en blokkeren elke toegang van schadelijke code tot de computer. Natuurlijk kunt u ook een scan plannen die op basis van een ingesteld interval wordt uitgevoerd en u kunt scans handmatig starten.

De AVG-scaninterface is via de gebruikersinterface toegankelijk via de knop die uit twee gedeelten bestaat:



- ***Nu scannen*** - klik op deze knop om de scan De hele computer scannen te starten. U kunt de voortgang bekijken in het automatisch geopende venster Rapporten:



- ***Opties*** - selecteer deze knop *(grafisch weergegeven als drie horizontale lijnen in een groen veld)* om het dialoogvenster ***Scanopties*** te openen waarin u geplande scans kunt beheren en de parameters van De hele computer scannen / Mappen of bestanden scannen kunt bewerken.

Het dialoogvenster ***Scanopties*** bestaat uit drie configuratieonderdelen:

- ***Geplande scans beheren*** - klik op deze optie om een nieuw dialoogvenster met een overzicht van alle scanschema's te openen. Voordat u uw eigen scans definieert, wordt er slechts één geplande scan weergegeven: de door de softwareleverancier gedefinieerde scan. De scan is standaard uitgeschakeld. Als u deze scan wilt inschakelen, klikt u hier met de rechtermuisknop op en selecteert u *Taak inschakelen* in het contextmenu. Wanneer de geplande scan is ingeschakeld, kunt u de configuratie bewerken via de knop *Bewerken*. U kunt ook op de knop *Toevoegen* klikken om zelf een schema te maken.

- ***De hele computer scannen/Instellingen*** - de knop bestaat uit twee gedeelten. Klik op de optie *De hele computer scannen* om direct de hele computer te scannen *(zie het hoofdstuk Vooraf ingestelde scans / De hele computer scannen voor meer informatie)*. Klik op het gedeelte *Instellingen* om het configuratievenster voor het scannen van de hele computer te openen.

- ***Mappen of bestanden scannen / Instellingen*** - ook deze knop bestaat uit twee gedeelten. Klik op de optie *Mappen of bestanden scannen* om direct te beginnen met het scannen van bepaalde gedeelten van uw computer *(zie het hoofdstuk Vooraf ingestelde scans/Mappen of bestanden scannen voor meer informatie)*. Klik op het gedeelte *Instellingen* om het configuratievenster voor het scannen van mappen of bestanden te openen.

- ***Computer controleren op rootkits / Instellingen*** - het linkergedeelte van de knop met de titel *Computer controleren op rootkits* start onmiddellijk de Anti-Rootkitscan *(zie hoofdstuk Vooraf ingestelde scans / Computer controleren op rootkits)*. Klik op het gedeelte *Instellingen* om het configuratievenster voor het controleren op rootkits te openen.

9.1. Vooraf ingestelde scans

Een van de belangrijkste voorzieningen van **AVG Internet Security** is de mogelijkheid om op verzoek scans uit te voeren. De scans op verzoek zijn ontworpen voor het scannen van verschillende onderdelen van uw computer in gevallen waarin u vermoedt dat er mogelijk sprake is van een virusinfectie. Het wordt met klem aangeraden om dergelijke scans regelmatig uitvoeren. Dat geldt ook als u vermoedt dat er geen virussen op uw computer zullen worden gevonden.

In **AVG Internet Security** zijn de volgende scantypen vooraf gedefinieerd door de softwareleverancier:

9.1.1. De hele computer scannen

De hele computer scannen - de hele computer wordt gescand op mogelijk infecties en/of potentieel ongewenste toepassingen. Alle vaste schijven van de computer worden gescand, alle virussen worden gedetecteerd en vervolgens hersteld of verplaatst naar Quarantaine. Er moet minstens één keer per week een scan van de hele computer worden uitgevoerd.

Scan starten

U kunt de scan ***De hele computer scannen*** rechtstreeks vanuit de hoofdgebruikersinterface starten door te klikken op de knop ***Nu scannen***. U hoeft verder geen instellingen te configureren voor dit type scan en de scan wordt direct gestart. In het dialoogvenster ***Scan wordt uitgevoerd*** (*zie schermopname*) kunt u de voortgang en resultaten bekijken. De scan kan desgewenst tijdelijk worden onderbroken (***Pauzeren***) of worden geannuleerd (***Stoppen***).

Scanconfiguratie bewerken

U kunt de configuratie voor ***De hele computer scannen*** bewerken in het dialoogvenster ***De hele computer scannen - Instellingen*** *(het dialoogvenster is toegankelijk via de koppeling Instellingen voor De hele computer scannen in het dialoogvenster Scanopties).* ***U wordt aangeraden de standaardinstellingen aan te houden, tenzij u een goede reden hebt om deze te wijzigen.***

In de lijst met scanparameters kunt u specifieke parameters in- en uitschakelen:

- ***Virusinfecties herstellen/verwijderen zonder te vragen*** *(standaard ingeschakeld)* - als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, indien beschikbaar. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de map Quarantaine verplaatst.

- ***Rapporteer bedreigingen door mogelijk ongewenste toepassingen en spyware*** *(standaard ingeschakeld)* - schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste toepassingen rapporteren*** *(standaard uitgeschakeld)* - schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Tracking cookies scannen*** *(standaard uitgeschakeld)* - deze parameter bepaalt of cookies bij het scannen moeten worden gedetecteerd *(HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes)*.

- ***Scannen in archieven*** *(standaard uitgeschakeld)* - met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, zoals ZIP en RAR.

- ***Heuristische methode gebruiken*** *(standaard ingeschakeld)* - heuristische analyse *(dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving)* wordt gebruikt als een van de methoden voor virusdetectie als deze parameter is ingeschakeld.

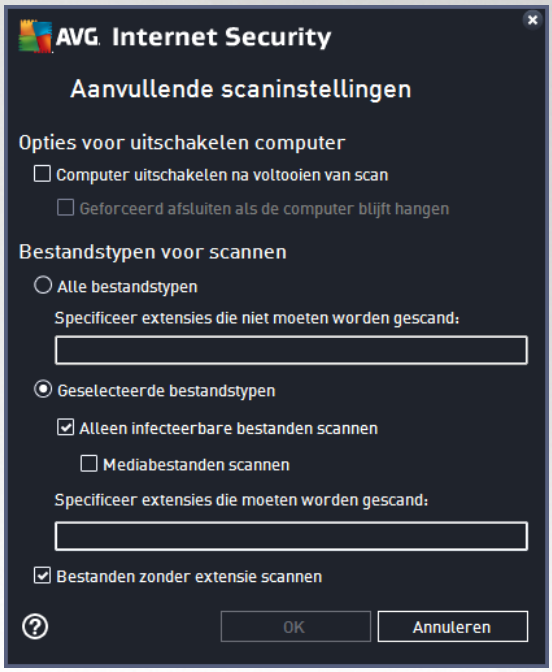
- ***Scansysteemomgeving*** *(standaard ingeschakeld)* - als deze parameter is ingeschakeld, worden ook

de systeemgebieden van de computer gescand.

- ***Grondig scannen inschakelen*** *(standaard uitgeschakeld)* - in bepaalde omstandigheden *(bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd)* kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Controleren op rootkits*** *(standaard ingeschakeld)* - als deze optie is ingeschakeld, wordt er bij een scan van de hele computer ook een controle op rootkits uitgevoerd. De anti-rootkitscan kan ook apart worden gestart.

- ***Aanvullende scaninstellingen*** - er wordt een nieuw dialoogvenster Aanvullende scaninstellingen geopend waarin u de volgende parameters kunt opgeven:



  - o ***Opties voor uitschakelen computer*** - opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (***Computer afsluiten na voltooien van scanproces***), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (***Geforceerd afsluiten als de computer vergrendeld is***).

  - o ***Bestandstypen voor scannen*** - u moet ook bepalen of u het volgende wilt scannen:

    - ➢ ***Alle bestandstypen*** - u kunt een door komma's gescheiden lijst opgeven met bestandsextensies die moeten worden genegeerd bij het scannen.

    - ➢ ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden - als u deze optie niet inschakelt, beperkt u de tijd die nodig is voor het scannen nog meer,*

omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties). U kunt ook nu op basis van extensies opgeven welke bestanden altijd moeten worden gescand.

- U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn verdacht en moeten altijd worden gescand.

- ***Aanpassen hoe snel de scan wordt uitgevoerd*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is deze optie ingesteld op het *gebruikerafhankelijke* niveau van automatisch brongebruik. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*dat is handig als u met de computer aan het werk bent en het u niet uitmaakt hoe lang het scanproces duurt*), of sneller, waarbij een groter beroep wordt gedaan op systeembronnen (*bijvoorbeeld op een moment dat u de computer niet gebruikt*).

- ***Aanvullende scanrapporten instellen*** - als u op deze koppeling klikt, wordt een nieuw dialoogvenster ***Scanrapporten*** geopend waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

Waarschuwing: *deze scaninstellingen zijn gelijk aan de parameters voor een nieuwe gedefinieerde scan, zoals beschreven in het hoofdstuk AVG scannen / Scans plannen / Scannen. Mocht u besluiten de standaardconfiguratie van* ***De hele computer scannen*** *te wijzigen, dan kunt u uw nieuwe instellingen opslaan als standaardconfiguratie die voor alle toekomstige scans van de computer moet worden gebruikt.*

9.1.2. Bepaalde mappen of bestanden scannen

Mappen of bestanden scannen - scant alleen die gebieden die u hebt geselecteerd voor het scannen (*geselecteerde mappen, vaste schijven, diskettes, cd's, enz.*). De voortgang van het scannen als een virus wordt gedetecteerd, en de manier waarop het virus wordt behandeld, is hetzelfde als bij een scan van de hele computer: een gedetecteerd virus wordt hersteld of in Quarantaine geplaatst. Met de functie voor het scannen van bepaalde mappen of bestanden kunt u eigen scans plannen die tegemoet komen aan uw eisen.

Scan starten

De scan ***Mappen of bestanden scannen*** kan direct vanuit het dialoogvenster Scanopties worden gestart door te klikken op de knop **Mappen of bestanden scannen**. Er wordt een nieuw dialoogvenster ***Mappen of bestanden scannen*** geopend. Selecteer de mappen die u wilt scannen in de bestandsstructuur van de computer. Het pad naar elke geselecteerde map wordt automatisch gegenereerd en weergegeven in het

tekstvak in het bovenste deel van het dialoogvenster. Desgewenst kunt u wel een map, maar niet de submappen van die map scannen. In dat geval typt u een minteken "**-**" voor het automatisch gegenereerde pad (*zie de schermafbeelding*). Als u de hele map wilt uitsluiten van het scannen, gebruikt u de parameter "**!**". U start de scan door te klikken op de knop ***Start scan***. Het scanproces zelf komt in principe overeen met dat van de scan De hele computer scannen.

Scanconfiguratie bewerken

U kunt de configuratie voor ***Mappen of bestanden scannen*** bewerken in het dialoogvenster ***Mappen of bestanden scannen - Instellingen*** *(dat u opent via de koppeling Instellingen voor Mappen of bestanden scannen in het dialoogvenster Scanopties).* ***U wordt aangeraden de standaardinstellingen aan te houden, tenzij u een goede reden hebt om deze te wijzigen.***

In de lijst met scanparameters kunt u specifieke parameters in- en uitschakelen:

- ***Virusinfecties herstellen/verwijderen zonder te vragen*** *(standaard ingeschakeld)*: als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de map Quarantaine verplaatst.

- ***Potentieel ongewenste programma's en spywarebedreigingen rapporteren*** *(standaard ingeschakeld)*: schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** *(standaard uitgeschakeld)*: schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Tracking cookies scannen*** *(standaard uitgeschakeld)*: deze parameter bepaalt of cookies bij het scannen moeten worden gedetecteerd *(HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes)*.

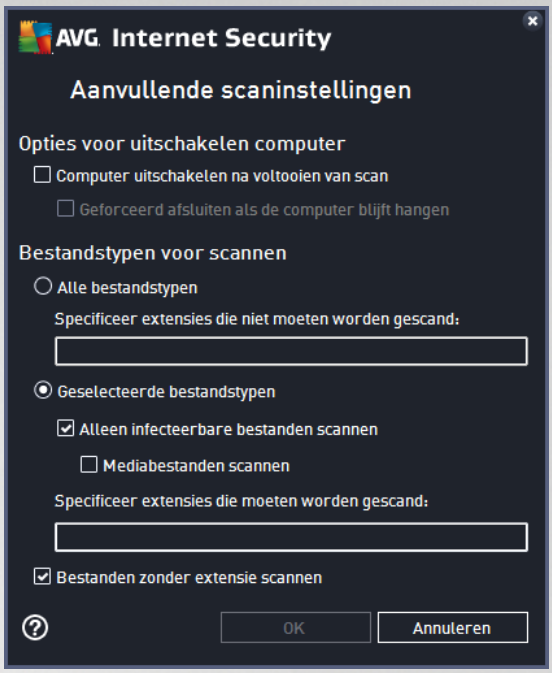
- ***Scannen in archieven*** *(standaard ingeschakeld)*: met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, zoals ZIP en RAR.

- ***Heuristische methode gebruiken*** *(standaard ingeschakeld)*: heuristische analyse *(dynamische emulatie van de instructies van gescande objecten in een virtuele computeromgeving)* wordt gebruikt als één van de methoden voor virusdetectie als de parameter is ingeschakeld.

- ***Scansysteemomgeving*** *(standaard uitgeschakeld)*: bij het scannen worden ook de systeemgebieden van de computer gecontroleerd.

- ***Grondig scannen inschakelen*** *(standaard uitgeschakeld)*: in bepaalde omstandigheden *(bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd)* kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Aanvullende scaninstellingen*** - er wordt een nieuw dialoogvenster ***Aanvullende scaninstellingen*** geopend waarin u de volgende parameters kunt opgeven:



- ***Opties voor uitschakelen computer*** - opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (***Computer uitschakelen na voltooien van scan***), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (***Geforceerd afsluiten als de computer blijft hangen***).

- ***Bestandstypen voor scannen*** - u moet ook bepalen of u het volgende wilt scannen:

  - ***Alle bestandstypen*** - u kunt een door komma's gescheiden lijst opgeven met bestandsextensies die moeten worden genegeerd bij het scannen.

  - ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die geïnfecteerd kunnen worden (*bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn*), inclusief mediabestanden (*videobestanden, audiobestanden - als u deze optie niet inschakelt, beperkt u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties*). U kunt ook nu op basis van extensies opgeven welke bestanden altijd moeten worden gescand.

  - U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn verdacht en moeten altijd worden gescand.

- ***Aanpassen hoe snel de scan wordt uitgevoerd*** - met de schuifbalk kunt u de prioriteit voor het scanproces wijzigen. Standaard is deze optie ingesteld op het *gebruikerafhankelijke* niveau van automatisch brongebruik. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*dat is handig als u met de computer aan het werk bent en het u niet uitmaakt hoe lang het scanproces duurt*), of sneller, waarbij een groter beroep wordt gedaan op systeembronnen (*bijvoorbeeld op een moment dat u de computer niet gebruikt*).

- ***Aanvullende scanrapporten instellen*** - als u op deze koppeling klikt, wordt een nieuw dialoogvenster ***Scanrapporten*** geopend waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

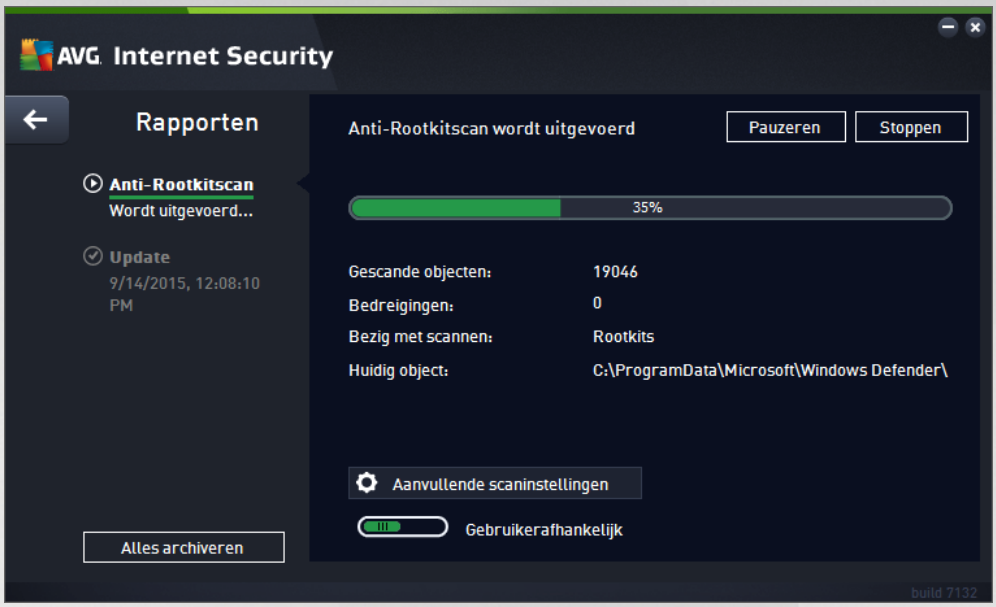
Waarschuwing: *deze scaninstellingen zijn gelijk aan de parameters voor een nieuwe gedefinieerde scan, zoals beschreven in het hoofdstuk AVG scannen / Scans plannen / Scannen. Mocht u besluiten de standaardconfiguratie van* ***Bepaalde mappen of bestanden scannen*** *te wijzigen, dan kunt u uw nieuwe instellingen opslaan als standaardconfiguratie die voor alle toekomstige scans van de computer moet worden gebruikt. De configuratie wordt bovendien gebruikt als sjabloon voor alle nieuwe geplande scans (alle aangepaste scans worden gebaseerd op de dan actuele configuratie van de Scan van bepaalde mappen of bestanden).*

9.1.3. Computer controleren op rootkits

Computer controleren op rootkits detecteert en verwijdert doeltreffend gevaarlijke rootkits, programma's en technologie die de aanwezigheid van schadelijke software op een computer kunnen camoufleren. Een rootkit is ontwikkeld om de controle over een computersysteem over te nemen zonder toestemming van de eigenaren en rechtmatige beheerders van het systeem. De scan kan rootkits herkennen aan de hand van een vooraf gedefinieerde set regels. Als er een rootkit wordt gevonden, betekent dit niet dat deze geïnfecteerd is. Soms worden rootkits gebruikt als stuurprogramma's of maken ze deel uit van een niet-verdacht programma.

Scan starten

U kunt ***Computer controleren op rootkits*** rechtstreeks starten vanuit het dialoogvenster Scanopties door te klikken op de knop ***Computer controleren op rootkits***. Een nieuw dialoogvenster ***Anti-Rootkitscan bezig*** wordt geopend met de voortgang van de gestarte scan:



Scanconfiguratie bewerken

U kunt de configuratie voor anti-rootkitscans bewerken in het dialoogvenster ***Anti-Rootkit instellingen*** *(u opent het dialoogvenster via de koppeling Instellingen voor Computer controleren op rootkits in het dialoogvenster Scanopties).* ***U wordt aangeraden de standaardinstellingen aan te houden, tenzij u een goede reden hebt om deze te wijzigen.***

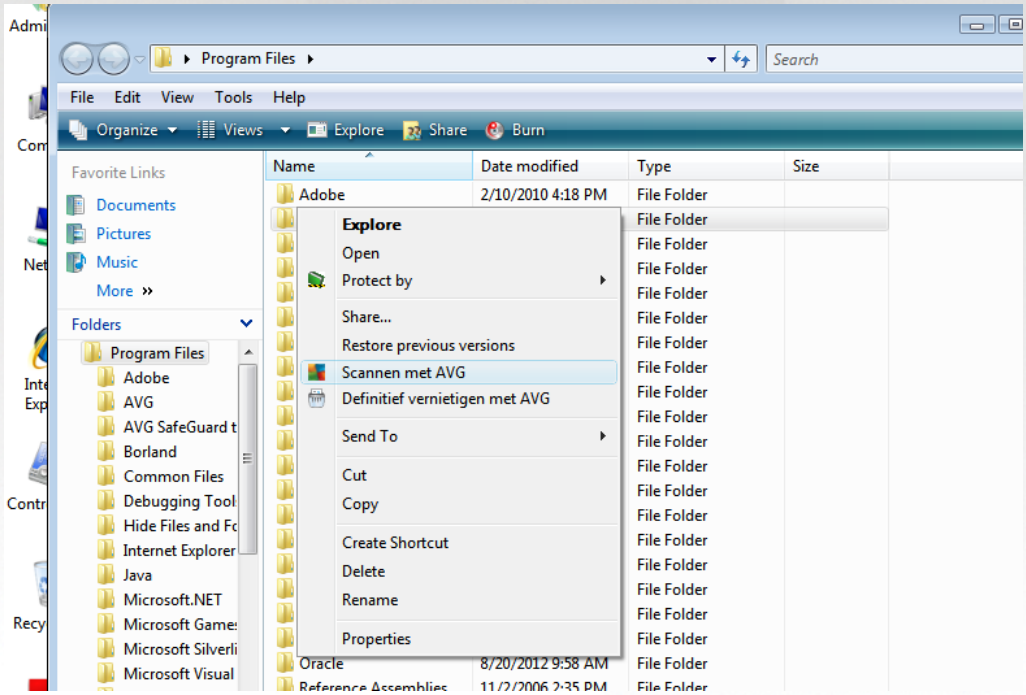
Via de opties ***Toepassingen scannen*** en ***Stuurprogramma's scannen*** kunt u gedetailleerd opgeven wat moet worden opgenomen in de rootkitscan. Deze instellingen zijn bedoeld voor geavanceerde gebruikers en we

raden u aan geen opties uit te schakelen. U kunt ook de scanmodus kiezen:

- ***Snelle rootkitscan*** - scannen van alle lopende processen, geladen stuurprogramma's en de systeemmap (*gewoonlijk C:\Windows*)
- ***Volledige rootkitscan*** - scannen van alle lopende processen, geladen stuurprogramma's en de systeemmap (*gewoonlijk C:\Windows*) plus alle lokale schijven (*inclusief flashstations, maar exclusief diskette-/cd-stations*)

9.2. Scannen in Windows Verkenner

Naast de mogelijkheden om met vooraf gedefinieerde scans de hele computer te scannen of een bepaald gedeelte, kunt u met **AVG Internet Security** ook snel een specifiek object scannen in Windows Verkenner. Als u een onbekend bestand wilt openen en niet zeker weet of de inhoud veilig is, kunt u het op verzoek scannen. Ga als volgt te werk:



- Selecteer in Windows Verkenner het bestand *(of de map)* dat u wilt controleren
- Klik met de rechtermuisknop op het object om het snelmenu te openen
- Kies de optie ***Scannen met AVG*** om het bestand te scannen met **AVG Internet Security**

9.3. Scannen vanaf de opdrachtregel

In **AVG Internet Security** hebt u de mogelijkheid om een scan uit te voeren vanaf de opdrachtregel. U kunt deze optie bijvoorbeeld op servers gebruiken of voor het maken van een batch-script dat onmiddellijk na het opstarten van de computer moet worden uitgevoerd. U kunt vanaf de opdrachtregel scans starten met vrijwel alle parameters die beschikbaar zijn in de grafische gebruikersinterface van AVG.

Voer, als u de AVG-scan vanaf de opdrachtregel wilt starten, de volgende opdracht uit in de map waarin AVG

is geïnstalleerd:

- ***avgscanx*** voor 32-bits besturingssystemen
- ***avgscana*** voor 64-bits besturingssystemen

Syntaxis van de opdracht

De opdracht volgt de onderstaande syntaxis:

- ***avgscanx /parameter*** ... bijv. ***avgscanx /comp*** voor het scannen van de hele computer
- ***avgscanx /parameter /parameter*** .. bij gebruik van meerdere parameters moeten deze achter elkaar worden geplaatst en worden gescheiden door een spatie en een slash
- als een parameter bepaalde waarden vereist (bijvoorbeeld de parameter ***/scan*** die informatie nodig heeft over welke gebieden van de computer u wilt scannen, terwijl u een exact pad moet opgeven voor het geselecteerde gedeelte), worden die waarden gescheiden door puntkomma's, bijvoorbeeld: ***avgscanx /scan=C:\;D:***

Scanparameters

Als u een volledig overzicht wilt weergeven van beschikbare parameters, typt u de desbetreffende opdracht gevolgd door de parameter /? of /HELP (bijv. ***avgscanx /?***). De enige verplichte parameter is /SCAN om te specificeren welke gedeelten van de computer moeten worden gescand. Voor een gedetailleerdere uitleg van de opties, raadpleegt u het overzicht van de opdrachtregelparameters.

Druk op ***Enter*** om de scan uit te voeren. Tijdens het scannen kunt u het proces stoppen door op ***CTRL+C*** of ***CTRL+Pause*** te drukken.

CMD-scannen gestart vanuit grafische interface

Wanneer u uw computer gebruikt in de veilige modus van Windows, kunt u de opdrachtregelscan ook starten vanuit de grafische gebruikersinterface. De scan zelf wordt gestart vanaf de opdrachtregel. In het dialoogvenster ***Opdrachtregelcomposer*** kunt u slechts de meeste scanparameters opgeven in de handige grafische interface.

Omdat dit dialoogvenster alleen toegankelijk is in de veilige modus van Windows, raadpleegt u het Help-bestand, dat direct beschikbaar is in het dialoogvenster, voor een gedetailleerde beschrijving van dit dialoogvenster.

9.3.1. CMD-scanparameters

Hier volgt een overzicht van de parameters die beschikbaar zijn voor scannen via de opdrachtregel:

- /SCAN Mappen of bestanden scannen /SCAN=pad;pad *(bijvoorbeeld /SCAN=C:\;D:\)*
- /COMP De hele computer scannen

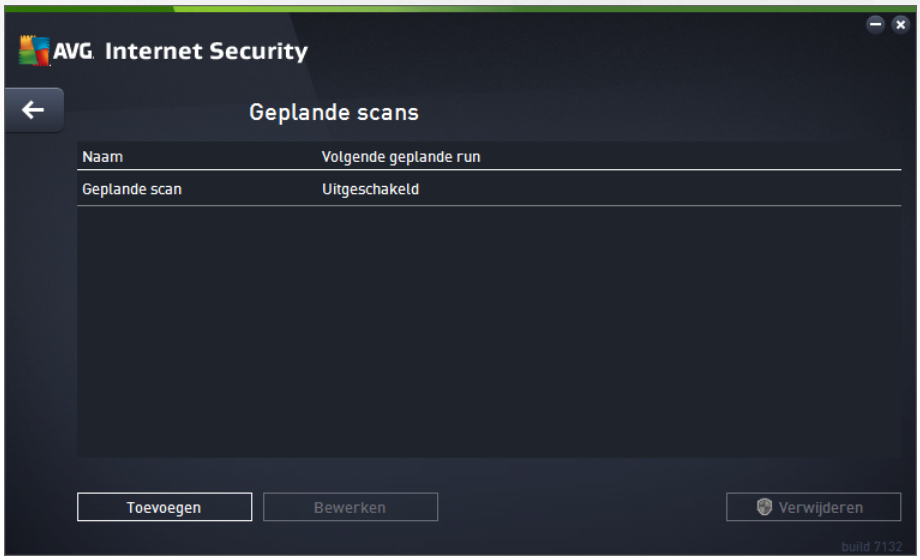
- /HEUR Heuristische methode gebruiken
- /EXCLUDE Pad of bestanden uitsluiten van scan
- /@ Opdrachtbestand /bestandsnaam/
- /EXT Deze extensies scannen /bijvoorbeeld EXT=EXE,DLL/
- /NOEXT Deze extensies niet scannen /bijvoorbeeld NOEXT=JPG/
- /ARC Archieven scannen
- /CLEAN Automatisch opschonen
- /TRASH Geïnfecteerde bestanden verplaatsen naar de quarantaine
- /QT Snelle test
- /LOG Een bestand met scanresultaten genereren
- /MACROW Macro's in rapport opnemen
- /PWDW Bestanden met wachtwoordbeveiliging in rapport opnemen
- /ARCBOMBSW Archiefbommen rapporteren *(meermaals gecomprimeerde archieven)*
- /IGNLOCKED Vergrendelde bestanden negeren
- /REPORT Rapporteren naar bestand /bestandsnaam/
- /REPAPPEND Toevoegen aan het rapportbestand
- /REPOK Niet geïnfecteerde bestanden als OK in rapport opnemen
- /NOBREAK CTRL-BREAK niet toestaan voor afbreken
- /BOOT MBR/BOOT-controle inschakelen
- /PROC Actieve processen scannen
- /PUP Potentieel ongewenste toepassingen rapporteren
- /PUPEXT Verbeterde set potentieel ongewenste toepassingen rapporteren
- /REG Register scannen
- /COO Cookies scannen
- /? Help over dit onderwerp weergeven
- /HELP Help over dit onderwerp weergeven
- /PRIORITY Scanprioriteit instellen /Laag, Auto, Hoog/ *(zie Geavanceerde instellingen / Scans)*

- /SHUTDOWN Computer uitschakelen na voltooien van scan
- /FORCESHUTDOWN Computer geforceerd uitschakelen na voltooien van scan
- /ADS Alternatieve gegevensstromen scannen *(alleen NTFS)*
- /HIDDEN Bestanden met verborgen extensie rapporteren
- /INFECTABLEONLY Alleen bestanden met infecteerbare extensie scannen
- /THOROUGHSCAN Grondig scannen inschakelen
- /CLOUDCHECK Controleren op valse meldingen
- /ARCBOMBSW Meervoudig gecomprimeerde bestanden opnemen in rapport

9.4. Scans plannen

Met **AVG Internet Security** kunt u scans op verzoek uitvoeren (bijvoorbeeld als u vermoedt dat uw computer geïnfecteerd is geraakt) of volgens schema. U wordt sterk aangeraden de scans volgens schema uit te voeren: op die manier weet u zeker dat uw computer wordt beschermd tegen alle mogelijke infecties en hoeft u zich geen zorgen te maken over de vraag of en wanneer u een scan moet uitvoeren. Voer de scan De hele computer scannen minstens één maal per week uit. Indien mogelijk is het verstandig om de hele computer dagelijks te scannen, zoals ook is ingesteld in de standaardconfiguratie voor scanschema's. Als de computer altijd 'aan staat', kunt u de scans buiten kantooruren plannen. Als de computer zo nu en dan wordt uitgeschakeld, kunt u plannen dat scans worden uitgevoerd bij het opstarten van de computer, als er een scan is overgeslagen.

Het scanschema kan worden gemaakt/bewerkt in het dialoogvenster ***Geplande scan*** dat u opent via de knop ***Geplande scans beheren*** in het dialoogvenster Scanopties. In het nieuwe dialoogvenster ***Geplande scan*** wordt een volledig overzicht weergegeven van alle geplande scans:

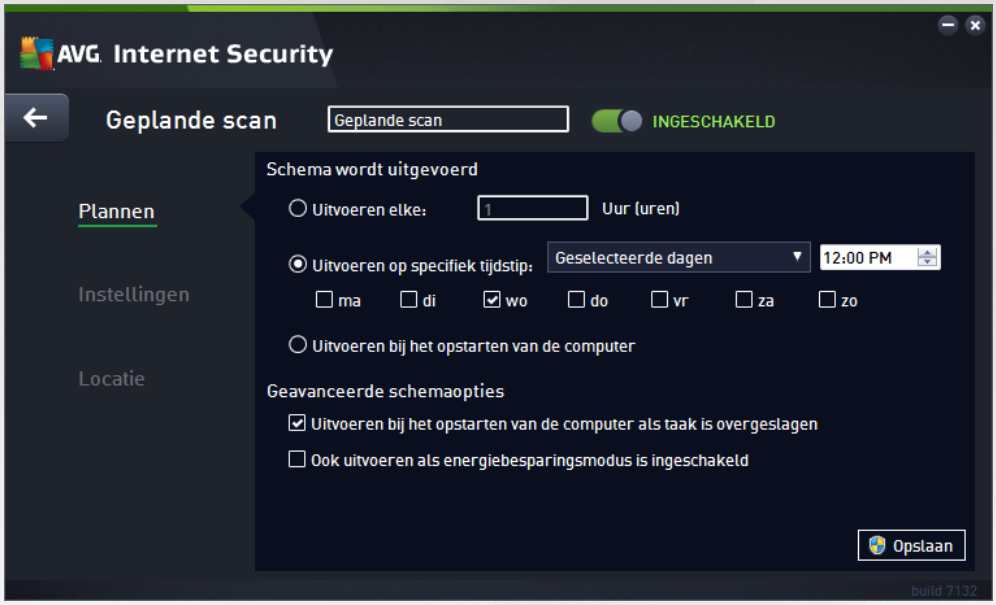


In het dialoogvenster kunt u uw eigen scans opgeven. Gebruik de knop ***Toevoegen*** om zelf een nieuw scanschema te maken. U kunt op drie tabbladen parameters instellen voor het schema van de geplande scan (*of een nieuw schema opstellen*):

- Plannen
- Instellingen
- Locatie

Op elk tabblad kunt u de verkeerslichtknop eenvoudig in- en uitschakelen om de geplande scan tijdelijk uit te schakelen en weer in te schakelen als dit nodig is.

9.4.1. Plannen



In het bovenste gedeelte van het tabblad ***Plannen*** vindt u het tekstveld waarin u de naam kunt opgeven van het scanschema dat momenteel wordt opgegeven. Probeer altijd korte, maar veelzeggende namen te gebruiken voor scans zodat u ze later gemakkelijker kunt onderscheiden van andere scans. Het is bijvoorbeeld niet handig om een scan als naam Nieuwe scan of Mijn scan te geven, omdat die namen niet verwijzen naar wat de scan doet. Een naam als Scan systeemgebieden is daarentegen een voorbeeld van een veelzeggende naam voor een scan.

In dit dialoogvenster kunt u daarnaast nog de volgende parameters instellen:

- ***Schema wordt uitgevoerd*** - hier kunt u tijdsintervallen opgeven waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt dit interval op verschillende manieren definiëren: als herhaalde scan die na verloop van een bepaalde tijd *(Uitvoeren elke...)* moet worden uitgevoerd, als een scan die op een bepaalde datum op een bepaald tijdstip *(Uitvoeren op specifiek tijdstip)* moet worden uitgevoerd of als een gedefinieerde gebeurtenis waaraan het uitvoeren van de scan is gekoppeld *(Uitvoeren bij het opstarten van de computer)*.

- ***Geavanceerde schemaopties*** - hier kunt u opgeven onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de energiebesparingsmodus is ingeschakeld of als de computer helemaal is uitgeschakeld. Zodra de geplande scan is gestart op het tijdstip dat u hebt opgegeven, wordt u hierover geïnformeerd via een pop-upvenster dat wordt geopend boven het systeemvakpictogram van AVG. Vervolgens verschijnt een nieuw systeemvakpictogram van AVG (in kleur met een flitslicht) waarmee u wordt geïnformeerd dat een scan wordt uitgevoerd. Klik met de rechtermuisknop op het

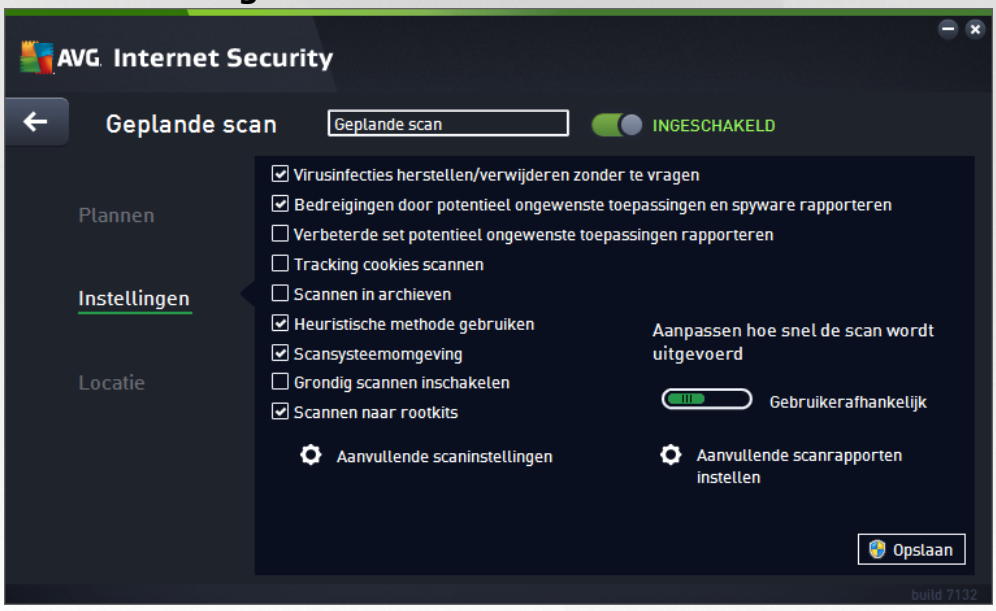
AVG-pictogram van de scan die wordt uitgevoerd om een snelmenu te openen waarin u opties kunt kiezen om de scan te onderbreken of af te breken, of de prioriteit te wijzigen van de scan die wordt uitgevoerd.

Opties in het dialoogvenster

- ***Opslaan*** - u slaat alle wijzigingen op de tabbladen van dit dialoogvenster op en keert terug naar het overzicht Geplande scans. Klik daarom pas op de knop nadat u alle gewenste wijzigingen op alle tabbladen hebt doorgevoerd.

- ← - Gebruik de pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar het overzicht Geplande scans.

9.4.2. Instellingen



In het bovenste gedeelte van het tabblad ***Instellingen*** vindt u het tekstveld waarin u de naam kunt opgeven van het scanschema dat momenteel wordt opgegeven. Probeer altijd korte, maar veelzeggende namen te gebruiken voor scans zodat u ze later gemakkelijker kunt onderscheiden van andere scans. Het is bijvoorbeeld niet handig om een scan als naam "Nieuwe scan" of "Mijn scan" te geven, omdat die namen niet verwijzen naar wat de scan doet. Een naam als "Scan systeemgebieden" is daarentegen een voorbeeld van een veelzeggende naam voor een scan.

Het tabblad ***Scaninstellingen*** bevat een lijst met scanparameters die kunnen worden in- en uitgeschakeld. ***We raden u aan deze vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om deze instellingen te wijzigen***:

- ***Virusinfecties herstellen/verwijderen zonder te vragen*** *(standaard ingeschakeld):* als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch kan worden hersteld, wordt het naar de map Quarantaine verplaatst.

- ***Potentieel ongewenste programma's en spywarebedreigingen rapporteren*** *(standaard*

ingeschakeld): schakel dit selectievakje in als u niet alleen op virussen, maar ook op spyware wilt scannen. Spyware behoort tot een twijfelachtige categorie malware: ook al vormt het gewoonlijk een veiligheidsrisico, sommige van deze programma's worden bewust geïnstalleerd. Het is raadzaam deze functie niet uit te schakelen omdat deze de bescherming van uw computer vergroot.

- ***Verbeterde set potentieel ongewenste programma's rapporteren*** (*standaard uitgeschakeld*): schakel dit selectievakje in als u pakketten wilt detecteren die met spyware zijn uitgebreid. Dit zijn programma's die volkomen onschadelijk zijn wanneer u deze rechtstreeks van de fabrikant verkrijgt, maar die op een later tijdstip kunnen worden misbruikt voor schadelijke doeleinden. Dit is een aanvullende maatregel om de veiligheid van uw computer te vergroten, maar de kans bestaat dat legale programma's er ook door worden geblokkeerd. Om die reden is de functie standaard uitgeschakeld.

- ***Tracking cookies scannen*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of cookies bij het scannen moeten worden gedetecteerd (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*).

- ***Scannen in archieven*** (*standaard uitgeschakeld*) - met deze parameter bepaalt u of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die zijn gecomprimeerd, zoals ZIP en RAR.

- ***Heuristische methode gebruiken*** (*standaard ingeschakeld*) - hiermee wordt een heuristische analyse (*dynamische emulatie van de instructies van het gescande object in een virtuele computeromgeving*) gebruikt als een van de methoden voor virusdetectie.

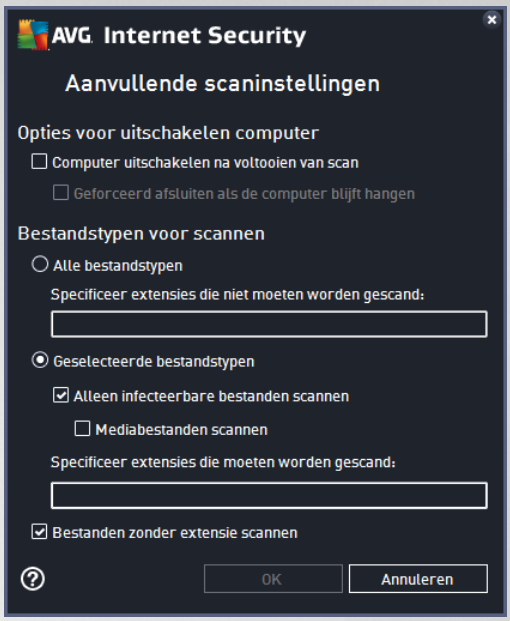
- ***Scansysteemomgeving*** (*standaard ingeschakeld*) - als deze parameter is ingeschakeld, worden ook de systeemgebieden van de computer gescand.

- ***Grondig scannen inschakelen*** (*standaard uitgeschakeld)* - in bepaalde omstandigheden (*bijvoorbeeld wanneer wordt vermoed dat de computer is geïnfecteerd*) kunt u deze optie inschakelen om de meest rigoureuze scanalgoritmes te activeren waardoor voor alle zekerheid zelfs gedeelten van de computer worden gescand waar de kans op infectie vrijwel verwaarloosbaar is. Deze manier van scannen kost echter erg veel tijd.

- ***Scannen naar rootkits*** *(standaard ingeschakeld):* Anti-Rootkitscan zoekt op uw computer naar rootkits (programma's en technologieën die malware-activiteiten in de computer kunnen verhullen). Als een rootkit wordt gedetecteerd, wil dat nog niet zeggen dat uw computer is geïnfecteerd. In sommige gevallen worden bepaalde stuurprogramma's of delen van reguliere programma's abusievelijk herkend als rootkit.

Aanvullende scaninstellingen

Via de koppeling opent u een nieuw dialoogvenster ***Aanvullende scaninstellingen*** waarin u de volgende parameters kunt opgeven:



- ***Opties voor uitschakelen computer*** - opgeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt *(Computer uitschakelen na voltooien van scan)*, wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld *(Geforceerd afsluiten als de computer blijft hangen)*.

- ***Bestandstypen voor scannen*** - u moet ook bepalen of u het volgende wilt scannen:

    - ***Alle bestandstypen*** - u kunt een door komma's gescheiden lijst opgeven met bestandsextensies die moeten worden genegeerd bij het scannen.

    - ***Geselecteerde bestandstypen*** - u kunt opgeven dat u alleen bestanden wilt scannen die geïnfecteerd kunnen worden *(bestanden die niet geïnfecteerd kunnen worden, worden niet gescand, bijvoorbeeld bepaalde niet-opgemaakte tekstbestanden, of andere bestanden die niet uitvoerbaar zijn)*, inclusief mediabestanden *(videobestanden, audiobestanden - als u deze optie niet inschakelt, beperkt u de tijd die nodig is voor het scannen nog meer, omdat dit vaak grote bestanden zijn met een kleine kans op virusinfecties)*. U kunt ook nu op basis van extensies opgeven welke bestanden altijd moeten worden gescand.

    - U kunt bovendien aangeven of u ***bestanden zonder extensie wilt scannen*** - deze optie is standaard ingeschakeld en we raden u aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen. Bestanden zonder extensie zijn verdacht en moeten altijd worden gescand.

Scansnelheid aanpassen

In deze sectie kunt u nader opgeven hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op de systeembronnen van uw computer. Standaard is deze optie ingesteld op het *gebruikerafhankelijke* niveau van automatisch brongebruik. Als u sneller wilt scannen, duurt het scannen minder lang, maar worden aanzienlijk meer systeembronnen gebruikt, zodat andere activiteiten op de computer trager worden uitgevoerd (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt het beroep op systeembronnen echter ook beperken door te kiezen voor een langere scanduur.

Aanvullende scanrapporten instellen

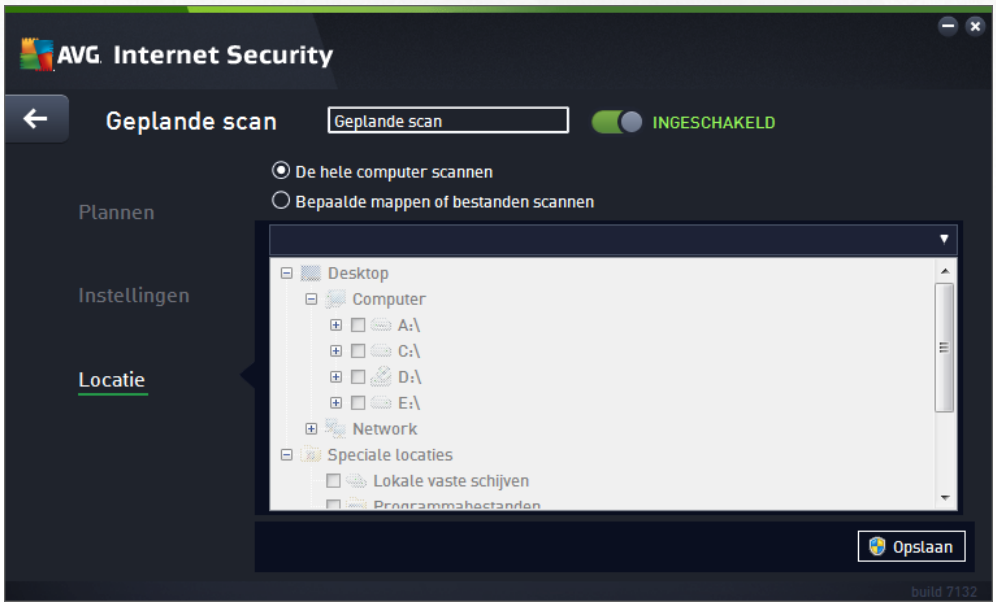
Klik op de koppeling ***Aanvullende scanrapporten instellen...*** om een afzonderlijk dialoogvenster te openen dat ***Scanrapporten*** heet, waarin u selectievakjes kunt inschakelen voor resultaten die moeten worden weergegeven:

Opties in het dialoogvenster

- ***Opslaan*** - u slaat alle wijzigingen op de tabbladen van dit dialoogvenster op en keert terug naar het overzicht Geplande scans. Klik daarom pas op de knop nadat u alle gewenste wijzigingen op alle tabbladen hebt doorgevoerd.

- ← - Gebruik de pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar het overzicht Geplande scans.

9.4.3. Locatie



Op het tabblad ***Locatie*** kunt u opgeven welke scan moet worden uitgevoerd: een scan van de hele computer of een scan van bepaalde bestanden of mappen. Als u kiest voor het scannen van bepaalde bestanden of mappen, wordt de in het onderste deel van het dialoogvenster weergegeven mapstructuur actief, zodat u mappen kunt opgeven die moeten worden gescand (*klik op het plusteken om de structuur uit te vouwen, totdat u de map vindt die u wilt scannen*). U kunt meerdere mappen selecteren door de betreffende selectievakjes in te schakelen. De geselecteerde mappen worden weergegeven in het tekstveld boven het dialoogvenster en in de vervolgkeuzelijst wordt de geschiedenis van uw geselecteerde scans bewaard voor later gebruik. U kunt het volledige pad naar de gewenste map ook handmatig invoeren (*als u meerdere paden invoert, moet u deze met een puntkomma zonder extra spatie scheiden*).

De mapstructuur bevat ook een vertakking ***Speciale locaties***. Hieronder vindt u een lijst met locaties die alleen worden gescand als u het betreffende selectievakje hebt ingeschakeld.

- ***Lokale vaste schijven*** - alle vaste schijven van uw computer
- ***Programmabestanden***
  - C:\Program Files\
  - *in de 64-bits versie* C:\Program Files (x86)
- ***Map Mijn documenten***
  - *voor Win XP:* C:\Documents and Instellingen\Default User\My Documents\
  - *voor Windows Vista/7*: C:\Users\user\Documents\
- ***Gedeelde documenten***
  - *voor Win XP*: C:\Documents and Settings\All Users\Documents\
  - *voor Windows Vista/7*: C:\Users\Public\Documents\
- ***Map Windows*** - C:\Windows\
- ***Overig***
  - *Systeemstation* - de vaste schijf waarop het besturingssysteem is geïnstalleerd (meestal C:)
  - *Systeemmap* - Windows/System32\
  - *Map tijdelijke bestanden* - C:\Documents and Settings\User\Local\ (*Windows XP*) of C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Tijdelijke internetbestanden* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*) of C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Opties in het dialoogvenster

- ***Opslaan*** - u slaat alle wijzigingen op de tabbladen van dit dialoogvenster op en keert terug naar het

overzicht Geplande scans. Klik daarom pas op de knop nadat u alle gewenste wijzigingen op alle tabbladen hebt doorgevoerd.

- - Gebruik de pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar het overzicht Geplande scans.

9.5. Scanresultaten

Het dialoogvenster ***Overzicht scanresultaten*** bevat een overzicht van alle tot nu toe uitgevoerde scans. Voor elk scanresultaat wordt het volgende weergegeven:

- ***Pictogram*** - in de eerste kolom wordt een informatiepictogram met een beschrijving van de status van de scan weergegeven:
  - Geen infecties gevonden, scan voltooid
  - Geen infecties gevonden, scan afgebroken voor voltooiing
  - Infecties gevonden, niet hersteld, scan voltooid
  - Infecties gevonden, niet hersteld, scan afgebroken voor voltooiing
  - Infecties gevonden en hersteld of verwijderd, scan voltooid
  - Infecties gevonden en hersteld of verwijderd, scan afgebroken voor voltooiing
- ***Naam*** - deze kolom bevat de naam van de betreffende scan. Dit kan een van de twee vooraf ingestelde scans of uw eigen geplande scan zijn.
- ***Begintijd*** - exacte datum en tijd waarop de scan is gestart.
- ***Eindtijd*** - exacte datum en tijd waarop de scan is voltooid, gepauzeerd of onderbroken.

- ***Geteste objecten*** - het totale aantal objecten dat is gescand.
- ***Infecties*** - het aantal gevonden verwijderde/totale infecties.
- ***Hoog / Gemiddeld / Laag*** - in deze kolommen wordt aangegeven hoeveel infecties van elk niveau zijn gevonden.
- ***Rootkits*** - hier wordt aangegeven hoeveel rootkits zijn gevonden tijdens het scannen.

Dialoogvensteropties

Details weergeven - klik op deze knop om gedetailleerde informatie te bekijken over een geselecteerde scan *(gemarkeerd in het bovenstaande diagram)*.

Resultaat verwijderen - klik op deze knop om geselecteerde scanresultaatgegevens te verwijderen uit het diagram.

 - Gebruik de groene pijl in de linkerbovenhoek van het dialoogvenster om terug te keren naar de hoofdgebruikersinterface met het overzicht van de onderdelen.

9.6. Details scanresultaten

Als u een overzicht met gedetailleerde informatie over een geselecteerd scanresultaat wilt weergeven, klikt u op de knop ***Details weergeven*** in het dialoogvenster Overzicht scanresultaten. Vervolgens wordt het dialoogvenster met gedetailleerde informatie over het betreffende scanresultaat weergegeven. De gegevens zijn verdeeld over drie tabbladen:

- ***Samenvatting*** - dit tabblad biedt algemene informatie over de scan: of deze is voltooid, of er bedreigingen zijn gevonden en wat hiermee is gebeurd.
- ***Details*** - op dit tabblad wordt alle informatie over de scan weergegeven, inclusief informatie over gedetecteerde bedreigingen. Met Overzicht exporteren naar bestand kunt u deze informatie opslaan als een CSV-bestand.
- ***Detecties*** - dit tabblad wordt alleen weergegeven als tijdens de scan andere bedreigingen zijn gedetecteerd en biedt gedetailleerde informatie over de bedreigingen:

   ***Informatie***: informatie of waarschuwingen, niet echte bedreigingen. Dit zijn doorgaans documenten met macro's, documenten of archieven die worden beschermd door een wachtwoord, vergrendelde bestanden, enzovoort.

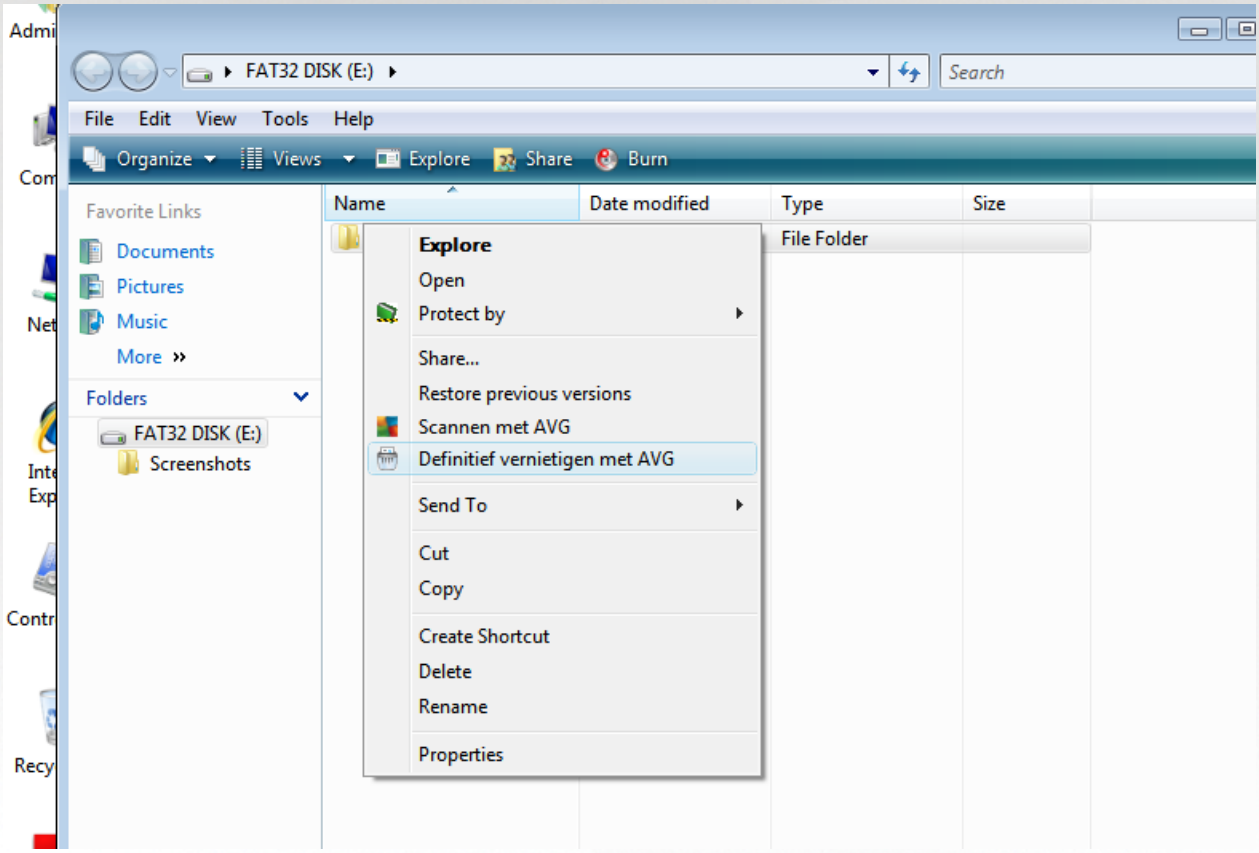
   ***Gemiddeld***: dit zijn doorgaans potentieel ongewenste programma's *(bijvoorbeeld adware)* of tracking cookies.

   ***Hoog***: ernstige bedreigingen zoals virussen, Trojaanse paarden, exploits, enzovoort. Daarnaast zijn dit objecten die zijn gedetecteerd met de heuristische detectiemethode (bedreigingen die nog niet worden beschreven in de virusdatabase.

10. AVG File Shredder

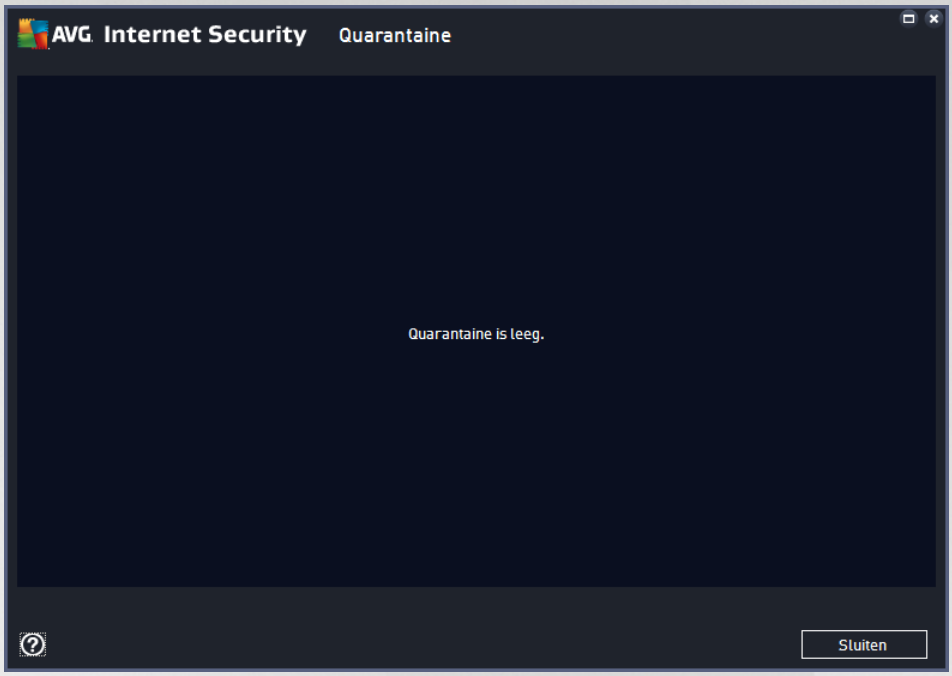
AVG File Shredder is ontworpen om bestanden veilig te verwijderen. Veilig betekent dat bestanden niet kunnen worden hersteld, zelfs niet met geavanceerde software die hiervoor bedoeld is.

Als u een bestand of map wilt vernietigen, klikt u met de rechtermuisknop in een programma voor bestandsbeheer *(Windows Verkenner, Total Commander, ...)* en selecteert u ***Definitief vernietigen met AVG*** in het contextmenu. U kunt ook bestanden in de Prullenbak vernietigen. Als een bepaald bestand op een specifieke locatie *(bijvoorbeeld een cd-rom)* niet betrouwbaar kan worden verwijderd, wordt u hiervan op de hoogte gesteld of is de optie niet beschikbaar in het contextmenu.



Houd er rekening mee dat u een vernietigd bestand niet meer kunt herstellen.

11. Quarantaine



Quarantaine voorziet in een veilige omgeving voor het beheren van verdachte of geïnfecteerde objecten die tijdens AVG-scans zijn gedetecteerd. Als er tijdens het scannen een geïnfecteerd object wordt gedetecteerd, wordt u gevraagd wat er met het verdachte object moet gebeuren als het desbetreffende object niet automatisch kan worden hersteld. Het wordt aanbevolen om het object in een dergelijk geval naar de ***Quarantaine*** te verplaatsen, zodat het daar kan worden afgehandeld. Het hoofddoel van de ***Quarantaine*** is elk verwijderde bestand gedurende een bepaalde periode te bewaren, zodat u zich ervan kunt vergewissen dat u het bestand niet langer nodig hebt op de oorspronkelijke locatie. Mocht het ontbreken van het bestand problemen veroorzaken, dan kunt u het betreffende bestand opsturen voor analyse of de oorspronkelijke locatie herstellen.

De interface van ***Quarantaine*** wordt in een eigen venster geopend en biedt een overzicht met informatie over in quarantaine geplaatste, geïnfecteerde objecten:

- ***Datum*** - datum en tijdstip van detectie van het verdachte bestand en verplaatsing naar Quarantaine.
- ***Bedreiging*** - als u besluit om het onderdeel Identiteit te installeren in uw **AVG Internet Security**, vindt u een grafische identificatie van de ernst in deze sectie: van onschadelijk *(drie groene punten)* tot zeer gevaarlijk *(drie rode punten)*. U vindt ook informatie over het infectietype en de oorspronkelijke locatie. Via de koppeling *Meer info* wordt u doorverwezen naar een pagina in de online virusencyclopedie met gedetailleerde informatie over de gedetecteerde bedreiging.
- ***Bron*** - hier wordt aangegeven welk onderdeel van **AVG Internet Security** de betreffende bedreiging heeft gedetecteerd.
- ***Meldingen*** - in zeldzame gevallen kan deze kolom enige aanvullende informatie over de gedetecteerde bedreiging bevatten.

Knoppen

De interface van de ***Quarantaine*** heeft de volgende knoppen:

- ***Herstellen*** - het geïnfecteerde bestand wordt weer naar de oorspronkelijke locatie verplaatst.
- ***Herstellen als*** - het geïnfecteerde bestand wordt verplaatst naar een geselecteerde map.
- ***Verzenden voor analyse*** - deze knop is alleen actief als u een object markeert in de lijst met detecties hierboven. In dat geval kunt u de geselecteerde detectie naar de viruslabs van AVG verzenden voor verdere, gedetailleerde analyse. Deze functie dient alleen voor het verzenden van valse meldingen. Dat zijn bestanden die door AVG zijn gedetecteerd als geïnfecteerd of verdacht, maar die volgens u geen kwaad kunnen.
- ***Details*** - voor gedetailleerde informatie over de specifieke bedreiging in ***Quarantaine*** markeert u het geselecteerde item in de lijst en klikt u op de knop ***Details*** om een nieuw dialoogvenster met een beschrijving van de gedetecteerde bedreiging te openen.
- ***Verwijderen*** - het geïnfecteerde bestand wordt volledig en onherroepelijk uit ***Quarantaine*** verwijderd.
- ***Quarantaine leegmaken*** - alle bestanden in de ***Quarantaine*** worden volledig verwijderd. Als u de bestanden uit de ***Quarantaine*** verwijdert, worden ze onherroepelijk verwijderd van de schijf (*ze worden niet eerst naar de Prullenbak verplaatst*).

12. Geschiedenis

De sectie ***Historie*** bevat informatie over alle eerdere gebeurtenissen *(zoals updates, scans, detecties, enzovoort)* en rapporten over deze gebeurtenissen. Deze sectie is toegankelijk vanuit de hoofdgebruikersinterface via het item ***Opties / Historie***. De historie van alle vastgelegde gebeurtenissen is als volgt onderverdeeld:

- Scanresultaten
- Resultaten Resident Shield
- Resultaten e-mailbescherming
- Resultaten Online Shield
- Gebeurtenishistorie
- Firewall-logboek

12.1. Scanresultaten

Het dialoogvenster ***Overzicht scanresultaten*** is toegankelijk via ***Opties / Historie / Scanresultaten*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security**. Het dialoogvenster bevat een overzicht van alle eerder uitgevoerde scans en informatie over de resultaten:

- ***Naam*** - de naam van de scan; dat kan de naam zijn van een vooraf gedefinieerde scan, maar ook de naam van een door u zelf gedefinieerde scan. Bij elke naam staat ook een pictogram waarmee het scanresultaat wordt aangeduid:

  - een groen pictogram duidt erop dat er tijdens de scan geen infectie is gedetecteerd

  - een blauw pictogram duidt erop dat er een infectie is gedetecteerd, maar dat het geïnfecteerde object automatisch is verwijderd

 - een rood pictogram duidt erop dat er een infectie is gedetecteerd die AVG niet heeft kunnen verwijderen!

De pictogrammen kunnen volledig of voor de helft worden weergegeven - volledig weergegeven pictogrammen duiden erop dat de scan op de juiste manier volledig is uitgevoerd; een half pictogram betekent dat de scan is afgebroken of onderbroken.

Let op: *Raadpleeg het dialoogvenster Scanresultaten dat u opent door op de knop Details weergeven (onder in dit dialoogvenster) te klikken, als u meer informatie wenst over een uitgevoerde scan*

- ***Begintijd*** - datum en tijdstip waarop de scan is gestart
- ***Eindtijd*** - datum en tijdstip waarop de scan is beëindigd
- ***Geteste objecten*** - het aantal objecten dat tijdens de scan is getest
- ***Infecties*** - het aantal virusinfecties dat is gedetecteerd/verwijderd
- ***Hoog / Gemiddeld*** - deze kolommen bevatten informatie over het verwijderde/totale aantal infecties van hoog en gemiddeld niveau
- ***Info*** - informatie over het scanverloop en -resultaat *(doorgaans bij voltooiing of onderbreken)*
- ***Waarschuwingen*** - aantal gedetecteerde rootkits

Knoppen

Het dialoogvenster ***Overzicht scanresultaten*** heeft de volgende knoppen:

- ***Details weergeven*** - druk op deze knop om het dialoogvenster Scanresultaten weer te geven waarin u gedetailleerde informatie over de geselecteerde scan kunt bekijken
- ***Resultaat verwijderen*** - druk op deze knop om het geselecteerde item uit de lijst met scanresultaten te verwijderen
-  - als u weer het AVG-hoofdvenster *(overzicht van onderdelen) wilt weergeven,* klikt u op de groene pijl in de linkerbovenhoek van dit dialoogvenster

12.2. Resultaten Resident Shield

De service ***Resident Shield*** maakt deel uit van het onderdeel ***Computer*** en scant bestanden terwijl ze worden gekopieerd, geopend of opgeslagen. Als een virus of een andere bedreiging wordt gedetecteerd, wordt u meteen gewaarschuwd door het volgende dialoogvenster:

Dit waarschuwingsvenster bevat informatie over het object dat is gedetecteerd en is aangemerkt als geïnfecteerd (*Bedreiging*) en enkele feiten over de herkende infectie (*Omschrijving*). Via de koppeling Meer info wordt u doorverwezen naar een pagina in de online virusencyclopedie met gedetailleerde informatie over de gedetecteerde bedreiging (indien aanwezig). In het dialoogvenster wordt een overzicht van beschikbare oplossingen weergegeven en wordt aangegeven hoe u moet omgaan met de gedetecteerde bedreiging. Een van de alternatieven wordt gelabeld als aanbevolen: ***Bescherm me (aanbevolen). Kies zo mogelijk altijd voor deze optie.***

Opmerking: *mogelijk is het gedetecteerde object te groot voor de beschikbare capaciteit van Quarantaine. Als dat gebeurt, wordt in een berichtvenster melding van het feit gemaakt op het moment dat u probeert het geïnfecteerde object naar Quarantaine te verplaatsen. U kunt de grootte van Quarantaine echter aanpassen. De grootte van de Quarantaine wordt ingesteld als percentage van de capaciteit van de vaste schijf. Selecteer om de Quarantaine groter te maken Quarantaine in het linkerdeelvenster van het dialoogvenster Geavanceerde instellingen AVG en kies met de schuifregelaar bij 'Grootte Quarantaine beperken' een hoger percentage.*

In het onderste gedeelte van het dialoogvenster vindt u de koppeling ***Details weergeven***. Klik hierop om een nieuw venster te openen met gedetailleerde informatie over het proces dat werd uitgevoerd toen de infectie werd gedetecteerd en over de identificatie van het proces.

In het dialoogvenster ***Resident Shield-detectie*** wordt een overzicht weergegeven van alle Resident Shield-detecties. Dit dialoogvenster is toegankelijk via ***Opties / Historie / Resident Shield-detectie*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security**. Dit dialoogvenster biedt een overzicht van objecten die door Resident Shield zijn gedetecteerd, beoordeeld en aangemerkt als gevaarlijk en vervolgens zijn hersteld of verplaatst naar Quarantaine.

Bij elk object wordt de volgende informatie weergegeven:

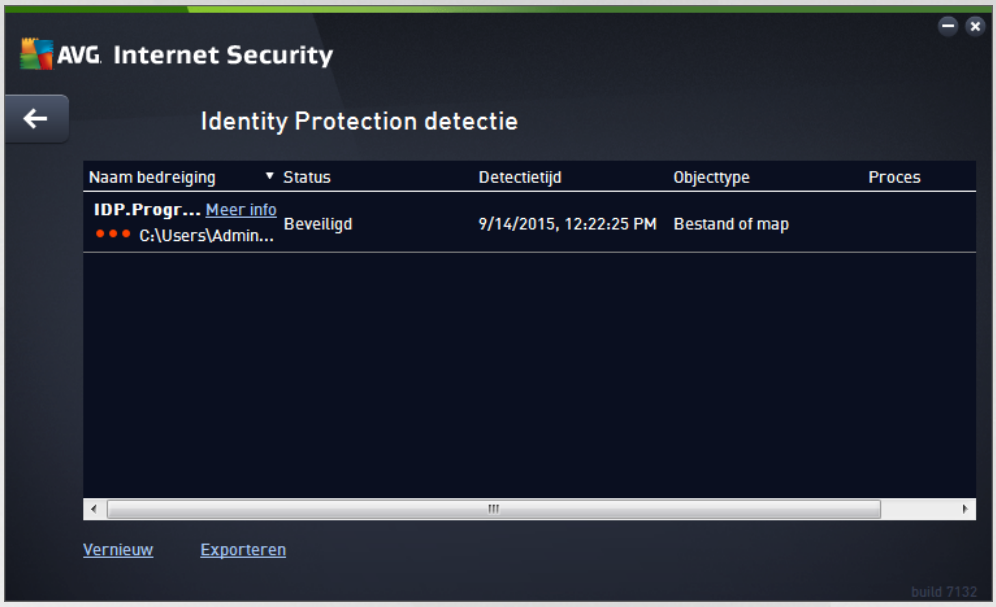
- ***Naam bedreiging*** - omschrijving (*mogelijk zelfs de naam*) van het gedetecteerde object en de locatie. Via de koppeling *Meer info* wordt u doorverwezen naar een pagina in de online virusencyclopedie met gedetailleerde informatie over de gedetecteerde bedreiging.
- ***Status*** - de bewerking die met het gedetecteerde object is uitgevoerd
- ***Detectietijd*** - datum en tijdstip waarop de bedreiging is gedetecteerd en geblokkeerd
- ***Objecttype*** - type van het gedetecteerde object
- ***Proces*** - het proces dat werd uitgevoerd en dat ertoe leidde dat het potentieel gevaarlijke object werd opgeroepen en gedetecteerd

Knoppen

- ***Vernieuwen*** - hiermee werkt u de lijst met gedetecteerde items door ***Online Shield***
- ***Exporteren*** - hiermee exporteert u de hele lijst met gedetecteerde objecten naar een bestand
- ***Selectie verwijderen*** - in de lijst kunt u meerdere records selecteren en vervolgens op deze knop klikken om alleen de geselecteerde items te verwijderen
- ***Alles verwijderen*** - gebruik deze knop om alle records in dit dialoogvenster te verwijderen
- ← - als u weer het AVG-hoofdvenster *(overzicht van onderdelen) wilt weergeven,* klikt u op de groene pijl in de linkerbovenhoek van dit dialoogvenster

12.3. Resultaten Identity Protection

Het dialoogvenster ***Resultaten Identity Protection*** is toegankelijk via ***Opties / Historie / Resultaten Identity Protection*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security**.



Het dialoogvenster bevat een overzicht van alle resultaten gedetecteerd door het onderdeel Identity Protection. Voor elk gedetecteerd object wordt de volgende informatie weergegeven:

- ***Naam bedreiging*** - omschrijving (*mogelijk zelfs de naam*) van het gedetecteerde object en de locatie. Via de koppeling *Meer info* wordt u doorverwezen naar een pagina in de online virusencyclopedie met gedetailleerde informatie over de gedetecteerde bedreiging.
- ***Status*** - de bewerking die met het gedetecteerde object is uitgevoerd
- ***Detectietijd*** - datum en tijdstip waarop de bedreiging is gedetecteerd en geblokkeerd
- ***Objecttype*** - type van het gedetecteerde object
- ***Proces*** - het proces dat werd uitgevoerd en dat ertoe leidde dat het potentieel gevaarlijke object werd opgeroepen en gedetecteerd

In het onderste gedeelte van het dialoogvenster, onder de lijst, vindt u informatie over het totale aantal gedetecteerde objecten dat erboven wordt weergegeven. Bovendien kunt u de hele lijst met gedetecteerde objecten exporteren naar een bestand (***Lijst exporteren naar een bestand***) en alle items over gedetecteerde objecten wissen (***Lijst leegmaken***).

Knoppen

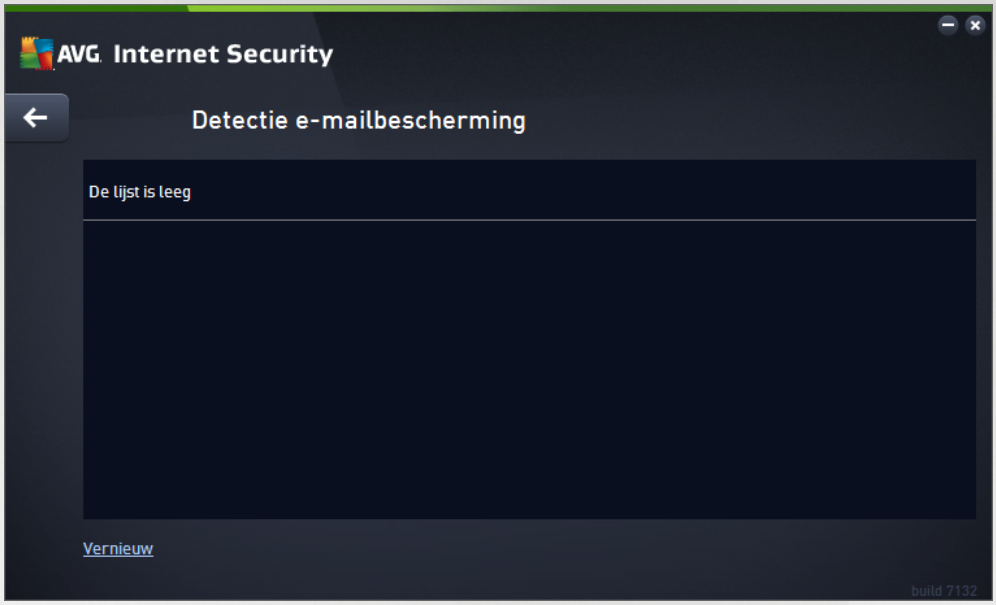
In de interface ***Resultaten Identity Protection*** zijn de volgende opties beschikbaar:

- ***Lijst vernieuwen*** - hiermee werkt u de lijst met gedetecteerde bedreigingen bij

- ← - als u weer het AVG-hoofdvenster *(overzicht van onderdelen) wilt weergeven,* klikt u op de groene pijl in de linkerbovenhoek van dit dialoogvenster

12.4. Resultaten e-mailbescherming

Het dialoogvenster ***Resultaten e-mailbescherming*** is toegankelijk via ***Opties / Historie / Resultaten e-mailbescherming*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security** .



Het dialoogvenster bevat een overzicht van alle resultaten gedetecteerd door het onderdeel E-mailscanner. Bij elk object wordt de volgende informatie weergegeven:

- ***Detectienaam*** - omschrijving *(mogelijk zelfs de naam)* van het gedetecteerde object en de bron
- ***Resultaat*** - de bewerking die met het gedetecteerde object is uitgevoerd
- ***Detectietijd*** - datum en tijdstip waarop het object is gedetecteerd
- ***Objecttype*** - type van het gedetecteerde object
- ***Proces*** - het proces dat werd uitgevoerd en dat ertoe leidde dat het potentieel gevaarlijke object werd opgeroepen en gedetecteerd

In het onderste gedeelte van het dialoogvenster, onder de lijst, vindt u informatie over het totale aantal gedetecteerde objecten dat erboven wordt weergegeven. Bovendien kunt u de hele lijst met gedetecteerde objecten exporteren naar een bestand (***Lijst exporteren naar een bestand***) en alle items over gedetecteerde objecten wissen (***Lijst leegmaken***).

Knoppen

De interface van ***E-mailscannerdetectie*** heeft de volgende knoppen:

- ***Lijst vernieuwen*** - de lijst met gedetecteerde bedreigingen bijwerken met nieuwe gegevens

- ← - als u weer het AVG-hoofdvenster *(overzicht van onderdelen) wilt weergeven,* klikt u op de groene pijl in de linkerbovenhoek van dit dialoogvenster

12.5. Resultaten Online Shield

Online Shield scant de inhoud van bezochte webpagina's en eventuele bestanden die daarvan deel uitmaken zelfs voordat deze worden weergegeven in uw webbrowser of worden gedownload naar uw computer. Als een bedreiging wordt gedetecteerd, wordt u meteen gewaarschuwd door het volgende dialoogvenster:

Dit waarschuwingsvenster bevat informatie over het object dat is gedetecteerd en is aangemerkt als geïnfecteerd (*Bedreiging*) en enkele feiten over de herkende infectie (*Objectnaam*). Via de koppeling *Meer info* wordt u doorverwezen naar de online virusencyclopedie waar u gedetailleerde informatie over de gedetecteerde infectie kunt vinden, indien beschikbaar. Dit dialoogvenster bevat de volgende knoppen:

- ***Details weergeven*** - klik op de koppeling om een nieuw pop-upvenster te openen met informatie over het proces dat werd uitgevoerd op het moment dat de infectie werd gedetecteerd en over de identificatie van het proces.
- ***Sluiten*** - klik op deze knop om het waarschuwingsvenster sluiten.

De verdachte webpagina wordt niet geopend en de detectie wordt vastgelegd in de lijst met ***Online Shield-resultaten***. Dit overzicht van gedetecteerde bedreigingen is toegankelijk via ***Opties / Historie / Online Shield-resultaten*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security**.

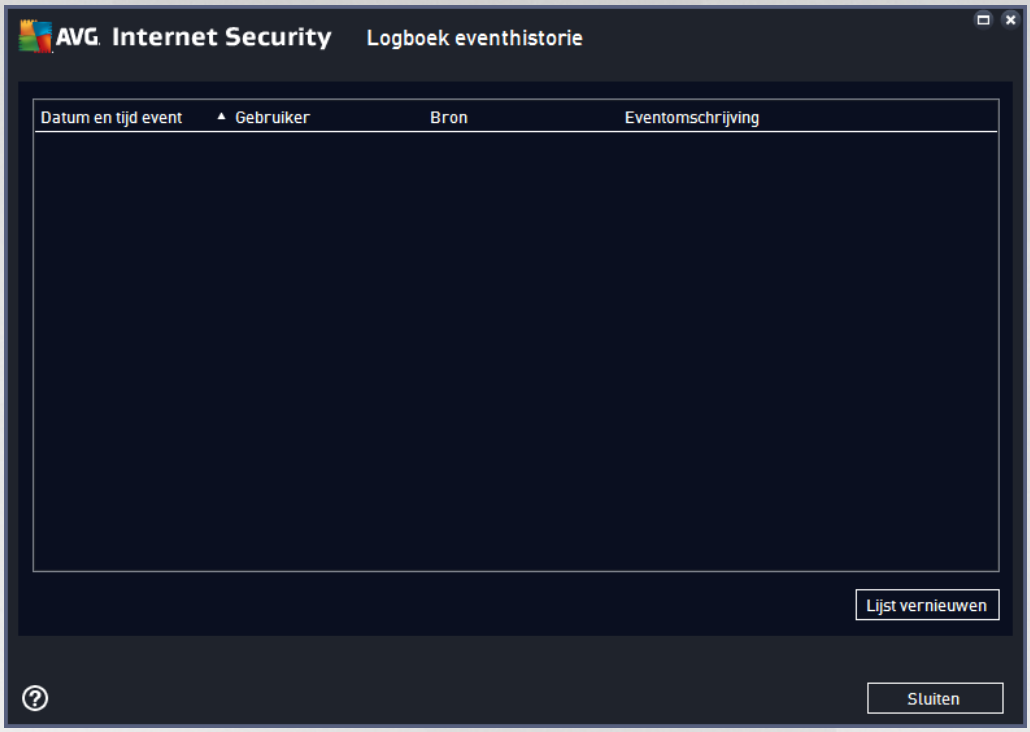
Bij elk object wordt de volgende informatie weergegeven:

- ***Naam bedreiging*** - omschrijving (*mogelijk zelfs de naam*) van het gedetecteerde object en de bron (*webpagina*); via de koppeling *Meer info* wordt u doorverwezen naar een pagina in de online virusencyclopedie met gedetailleerde informatie over de gedetecteerde bedreiging.
- ***Status*** - de bewerking die met het gedetecteerde object is uitgevoerd
- ***Detectietijd*** - datum en tijdstip waarop de bedreiging is gedetecteerd en geblokkeerd
- ***Objecttype*** - type van het gedetecteerde object

Knoppen

- ***Vernieuwen*** - hiermee werkt u de lijst met gedetecteerde items door ***Online Shield***
- ***Exporteren*** - hiermee exporteert u de hele lijst met gedetecteerde objecten naar een bestand
- ← - als u weer het AVG-hoofdvenster *(overzicht van onderdelen) wilt weergeven,* klikt u op de groene pijl in de linkerbovenhoek van dit dialoogvenster

12.6. Eventhistorie



Het dialoogvenster ***Logboek eventhistorie*** is toegankelijk via ***Opties / Historie / Logboek eventhistorie*** in de navigatiebalk in het hoofdvenster van **AVG Internet Security**. In het dialoogvenster wordt een overzicht weergegeven van belangrijke gebeurtenissen die tijdens het uitvoeren van **AVG Internet Security** zijn opgetreden. Het dialoogvenster bevat records van de volgende typen gebeurtenissen: informatie over updates van de AVG-toepassing, informatie over de start, het einde of de beëindiging van de scan (*inclusief automatisch uitgevoerde tests*), informatie over gebeurtenissen met betrekking tot de detectie van virussen (*door het residente schild of door scannen*), inclusief de locatie, en andere belangrijke gebeurtenissen.

Voor elke gebeurtenis worden de volgende gegevens vastgelegd:

- ***Datum en tijd event*** - het exacte moment waarop de gebeurtenis plaatsvond.
- ***Gebruiker*** - de naam van de gebruiker die was aangemeld op het moment dat de gebeurtenis plaatsvond.
- ***Bron*** - het onderdeel of het deel van het systeem dat de aanleiding vormde voor de gebeurtenis.
- ***Eventomschrijving*** - een korte samenvatting van wat er feitelijk is gebeurd.

Knoppen

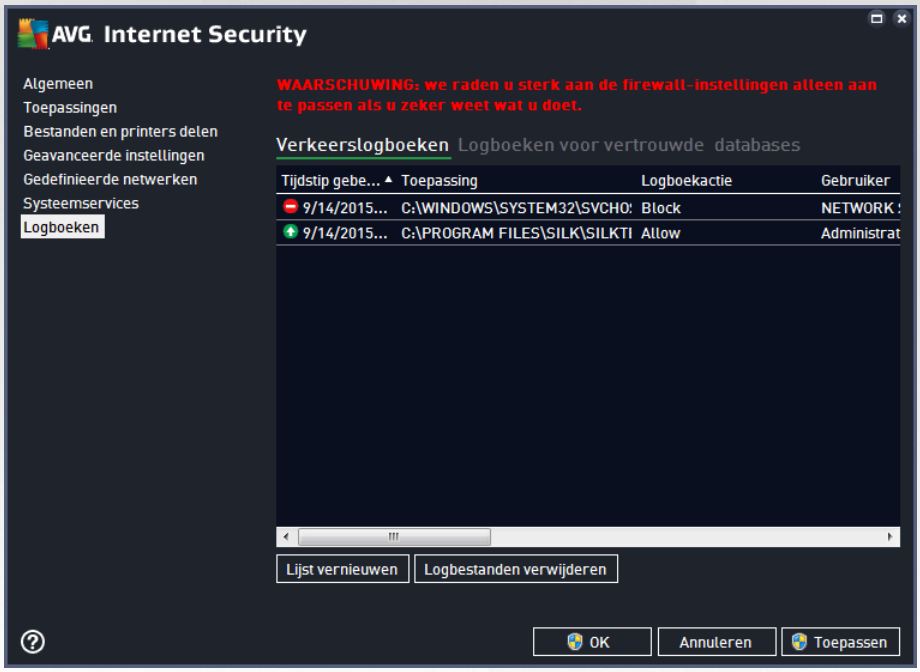
- ***Lijst vernieuwen*** - klik op deze knop als u alle vermeldingen in de lijst wilt vernieuwen
- ***Sluiten*** - klik op deze knop om terug te keren naar het **AVG Internet Security**-hoofdvenster

12.7. Firewall logboek

Dit dialoogvenster is bedoeld voor een configuratie door een expert en we raden u aan de instellingen alleen te wijzigen als u hier zeker van bent.

Het dialoogvenster ***Logboeken*** bevat de lijst met alle vastgelegde Firewall-acties en -gebeurtenissen, met een uitgebreide beschrijving van de relevante parameters.

- ***Verkeerslogboeken*** - dit tabblad biedt informatie over alle toepassingen die hebben geprobeerd verbinding te maken met het netwerk. Voor elk item wordt er informatie weergegeven over het tijdstip van de gebeurtenis, de toepassingsnaam, de logboekactie, de gebruikersnaam, PID, verkeersrichting, het protocoltype, de nummers van de externe en lokale poorten, en informatie over het lokale en externe IP-adres.



- ***Logboeken voor vertrouwde databases*** - de *vertrouwde database* is de interne database van AVG waarin informatie wordt verzameld over gecertificeerde en vertrouwde toepassingen die altijd online mogen communiceren. De eerste keer dat een nieuwe toepassing probeert een verbinding tot stand te brengen met het netwerk (*wanneer er nog geen firewallregel voor de toepassing is gedefinieerd*), moet worden bepaald of de betreffende toepassing mag communiceren via het netwerk. Eerst zoekt AVG in de *vertrouwde database* en als de toepassing daarin wordt vermeld, wordt automatisch toegang tot het netwerk verleend. Pas daarna, als duidelijk is dat er geen informatie over de toepassing is opgeslagen in de vertrouwde database, wordt u in een afzonderlijk dialoogvenster gevraagd of de toepassing toegang mag krijgen tot het netwerk.

Knoppen

- ***Lijst vernieuwen*** - alle geregistreerde parameters kunnen worden gerangschikt op het geselecteerde attribuut: chronologisch (*datums*) of alfabetisch (*andere kolommen*) - klik op de kolomkop. Werk de op een bepaald moment weergegeven informatie bij met nieuwe gegevens door op de knop ***Lijst vernieuwen*** te klikken.

- ***Logbestanden verwijderen*** - klik op deze knop als u alle vermeldingen wilt verwijderen.

13. AVG Updates

Geen enkel beveiligingsprogramma kan een daadwerkelijke beveiliging garanderen tegen allerlei bedreigingen als dit niet regelmatig wordt bijgewerkt. De makers van virussen zoeken steeds naar nieuwe tekortkomingen in software en besturingssystemen die ze kunnen uitbuiten. Elke dag verschijnen er nieuwe virussen, nieuwe malware en nieuwe hacker-aanvallen. Om die reden laten de leveranciers van software steeds nieuwe updates en beveiligingspatches verschijnen, om de gaten te dichten die in de beveiliging zijn ontdekt.

Gezien het aantal nieuwe computerbedreigingen en de snelheid waarmee deze zich verspreiden, is het van essentieel belang dat u **AVG Internet Security** regelmatig bijwerkt. Dit kunt u het beste doen door de standaardinstellingen van het programma, waarbij er automatische updates worden uitgevoerd, te behouden. Houd er rekening mee dat de meest recente bedreigingen niet door het programma kunnen worden gedetecteerd als de virusdatabase van **AVG Internet Security** niet is bijgewerkt.

Het is van essentieel belang dat u regelmatig updates van AVG uitvoert. Essentiële updates van virusdefinities dienen, indien mogelijk, dagelijks te worden uitgevoerd. Minder urgente updates kunnen ook wekelijks worden uitgevoerd.

13.1. Update starten

AVG Internet Security controleert standaard om de vier uur of er nieuwe virusdatabase-updates beschikbaar zijn zodat een maximale beveiliging kan worden geboden. Aangezien AVG-updates niet volgens een vast schema worden uitgebracht, maar eerder in reactie op de hoeveelheid bedreigingen en de ernst daarvan, is deze controle van groot belang om ervoor te zorgen dat de AVG-virusdatabase altijd is bijgewerkt.

Als u onmiddellijk wilt controleren of er nieuwe updates beschikbaar zijn, kunt u de koppeling Nu bijwerken in de hoofdgebruikersinterface gebruiken. Deze koppeling is altijd toegankelijk vanuit alle dialoogvensters van de gebruikersinterface. Als u de updateprocedure start, wordt eerst gecontroleerd of er nieuwe updates beschikbaar zijn. Als dit het geval is, worden deze gedownload door **AVG Internet Security** en wordt het updateproces gestart. U wordt over de updateresultaten geïnformeerd in het dialoogvenster dat wordt weergegeven boven het AVG-pictogram in het systeemvak.

Als u minder vaak wilt controleren op updates, kunt u uw eigen parameters instellen. Het wordt echter ***met klem aangeraden om ten minste één keer per dag een update te starten.*** Deze configuratie kan worden bewerkt in de volgende dialoogvensters, die u opent via Geavanceerde instellingen/Schema's:

- Schema definitie-updates
- Updateschema programma
- Updateschema Anti-Spam

13.2. Updateniveaus

U kunt in **AVG Internet Security** kiezen uit twee updateniveaus:

- ***Update van definities*** bevat wijzigingen die noodzakelijk zijn voor een betrouwbare beveiliging tegen virussen, spam en malware. In een dergelijke update zijn normaal gesproken geen wijzigingen in de code opgenomen. Alleen de virusdatabase wordt bijgewerkt. Deze update moet worden toegepast zodra deze beschikbaar is.
- ***Update van programma*** bevat diverse programmawijzigingen, reparaties en verbeteringen.

U kunt tijdens het plannen van een update specifieke parameters instellen voor beide updateniveaus:

- Schema definitie-updates
- Updateschema programma

Opmerking: *als een geplande programma-update tegelijkertijd wordt uitgevoerd met een geplande scan, krijgt het updaten een hogere prioriteit en de scan wordt onderbroken. In dat geval wordt u geïnformeerd over de botsing.*

14. Veelgestelde vragen en technische ondersteuning

Als u op problemen met betrekking tot de verkoop of op technische problemen met uw **AVG Internet Security**-toepassing stuit, kunt u op verscheidene manieren naar hulp zoeken. U kunt kiezen uit de volgende mogelijkheden:

- ***Ondersteuning***: vanuit de AVG-toepassing kunt u rechtstreeks naar een speciale ondersteuningspagina op de website van AVG gaan (*http://www.avg.com/*). Selecteer de optie ***Help / Ondersteuning*** in het hoofdmenu om te worden doorverwezen naar de AVG-website met beschikbare ondersteuningsmogelijkheden. Volg vervolgens de instructies op de webpagina.

- ***Ondersteuning*** *(koppeling in het hoofdmenu)*: het AVG-toepassingsmenu dat (*boven aan de hoofdgebruikersinterface wordt weergegeven*) bevat de koppeling ***Ondersteuning***. U kunt met deze koppeling een nieuw dialoogvenster openen dat alle informatie bevat die u nodig hebt wanneer u hulp nodig hebt. Het dialoogvenster omvat basisgegevens over het geïnstalleerde AVG-programma (*programma-/databaseversie*), gedetailleerde licentie-informatie en een lijst met snelkoppelingen voor ondersteuning:

- ***Problemen oplossen in Help-bestand***: een nieuwe sectie ***Problemen oplossen*** is rechtstreeks vanuit het Help-bestand in **AVG Internet Security** *beschikbaar (druk op F1 vanuit een willekeurig dialoogvenster in de toepassing om het Help-bestand te openen)*. Deze sectie biedt een lijst met de meest voorkomende situaties waarin een gebruiker behoefte heeft aan professionele hulp met betrekking tot een technisch probleem. Selecteer de situatie die uw probleem het beste beschrijft en klik op de koppeling om gedetailleerde instructies weer te geven voor het oplossen van het probleem.

- ***Ondersteuningscentrum op de AVG-website***: het is ook mogelijk om naar een oplossing voor uw probleem te zoeken op de website van AVG (*http://www.avg.com/*). In de sectie ***Ondersteuning***vindt u een overzicht van thematische groepen over verkoopproblemen en technische problemen, een gestructureerde sectie met veelgestelde vragen en alle beschikbare contactgegevens.

- ***AVG ThreatLabs***: een speciale AVG-website (*http://www.avg.com/about-viruses*) over virussen met overzichtelijke informatie over online bedreigingen. Daarnaast vindt u hier instructies voor het verwijderen van virussen en spyware en advies met betrekking tot hoe u beveiligd kunt blijven.

- ***Discussieforum***: u kunt ook gebruikmaken van het AVG-discussieforum op http://community.avg.com/.